МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
Харьковский национальный университет радиоэлектроники

На правах рукописи

КОТУХ ЕВГЕНИЙ ВЛАДИМИРОВИЧ

УДК 681.3.06

МЕТОДЫ И СРЕДСТВА УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ ПО АЛГЕБРАИЧЕСКИМ КРИВЫМ СУДЗУКИ

05.13.21 – системы защиты информации

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
Халимов Геннадий Зайдулович,
доктор технических наук, профессор

Цей примірник дисертаційної роботи
ідентичний за змістом з іншими,
поданими до спеціалізованої вченої ради.

Учений секретар спецради К.64.052.05 Т.В. Носова

Харьков – 2016

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АГК	алгеброгеометрические коды
ИС	информационная система
ИТС	информационная техническая система
ИОК	инфраструктура открытых ключей
HC	коды по кривым Эрмита
RS	коды Рида – Соломона
SC	коды по кривым Судзуки
HCh_q	хеш-функция по кривой Эрмита
PSh_q	хеш-функция по проективной прямой
SCh_q	хеш-функция по кривой Судзуки
Ch_q	каскадное хеширование
$\Diamond$	конец доказательства
MAC	Message Authentication Codes
$ВКУ$	Вейля – Карлитца – Ушиямы

ВВЕДЕНИЕ

Необходимость защиты информации в информационно-телекоммуникационных системах закреплена в Законах Украины «О защите персональных данных» [1], «Об электронных документах и электронном документообороте» [2], «Об электронной цифровой подписи» [3], «О защите информации в информационно-телекоммуникационных системах» [4], в Постановлении Кабинета Министров Украины [1–5]. Анализ нормативных документов показывает, что ко всем участникам информационного обмена предъявляются высокие требования обеспечения целостности и подлинности данных, передаваемых между узлами распределенных информационно-телекоммуникационных систем (ИТС) через незащищенные каналы связи. В соответствии с требованиями стандартов в области криптографии ДСТУ ISO/IEC 9798, ISO/IEC 10181, ISO/IEC 9797 базовая услуга аутентификации может быть обеспечена за счет использования кодов аутентификации (MAC-кодов) [16]. Построение MAC-кодов определяется тремя общими подходами: применением блочных шифров, на основе бесключевой хеш-функции, с использованием семейства универсальных хеш-функций.

Значительное повышение производительности и доступности GPGPU-процессоров и GRID-систем в совокупности с новыми методологиями распределительных вычислений позволило реализовать известные и новые угрозы безопасности на криптоалгоритмы. Ряд значительных недостатков конструкции, математически обоснованные атаки на коллизионную стойкость и недостаточная вычислительная сложность дали возможность реализовать для хеш-функций SHA-1 и MD-5 атаки полного перебора за допустимое время, что стало причиной отказа мировых лидеров в области разработки программного обеспечения от их использования. Снижение фактических временных затрат на преодоление практической стойкости подсистемы аутентификации до неприемлемого уровня, в свою очередь, повышает

требования к безопасности, скорости и подходам в реализации алгоритмов аутентификации.

Достижение высоких требований аутентификации при передаче сообщений определяется в рамках теории доказуемо стойкой аутентификации и состоятельных протоколов обмена информацией между объектами аутентификации. В практическом аспекте следует отметить международные стандарты ISO/IEC 9797-1,2, ISO/IEC 9798-1÷5, ISO/IEC 10118-1÷4, гармонизированные в Украине, определяющие обмен информацией между объектами аутентификации, применение протоколов аутентификации и механизмов вычисления хеш-функций и MAC-кодов [6–16]. Разработана и введена в действие 1 апреля 2015 г. криптографическая хэш-функция «Купина», использованная при создании проекта спецификации нового национального стандарта Украины ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція ґешування" для алгоритма хеширования, что обеспечивает высокий и сверхвысокий уровень устойчивости, с уровнем производительности, превосходящим российские и белорусские аналоги на 32-битных и 64-битных платформах [19]. Государственные стандарты Украины отвечают высоким требованиям по быстродействию и криптографической стойкости, предъявляемым для криптографических примитивов с использованием эллиптических кривых и алгоритмов симметричных блочных преобразований [17–19].

Преимуществом универсальных хеш-функций является то, что они имеют обоснованные комбинаторные свойства и обеспечивают доказуемую вероятность коллизии, которая прямо пропорциональна вероятности навязывания ложной информации. Практические алгоритмы формирования кодов аутентификации сообщений должны включать классы хеш-функций с большим коэффициентом сжатия для данных большого объема, при этом сохраняя свои коллизионные свойства. Поэтому интерес представляют схемы универсального хеширования на основе длинных алгеброгеометрических

кодов. Эффективное снижение вероятности коллизии возможно за счет применения композиционных схем с использованием универсального хеширования на основе длинных алгеброгеометрических кодов. Вместе с тем применение каскадных схем хеширования, как наиболее эффективных в отношении сложность вычисления/вероятность коллизии, возможно в поле ограниченной размерности.

Ряд фундаментальных результатов по аутентификации и идентификации получены И.Д. Горбенко, В. К. Задиракой, А.Г. Корченко, А.А. Кузнецовым, Ю.И. Горбенко и др. [20–24]. Использование алгеброгеометрических кодов конструкций рассмотрено в трудах В. Столлингса, Т. Йохансона, Б. Смиитса [25–27]. В работах Г. Кабатиански, Г. Симмонса, Д. Стинсона рассмотрены и предложены практические конструкции [28–34]. Эти работы во многом определили направления исследований диссертационной работы.

Таким образом, актуальность диссертационной работы обусловливается необходимостью построения доказуемо стойкой аутентификации сообщений, удовлетворяющей требованиям сложности и скорости вычисления, характеристикам и реализациям алгоритма для построения национального стандарта.

Связь с научными программами, планами, темами. Основу работы составляют результаты теоретических и практических исследований, выполненных автором в научно-исследовательских работах по госбюджетным темам ХНУРЭ: «Обоснование требований, разработка и внедрение инфраструктуры электронной цифровой подписи в МОН» (№ ДР 0103U001981), «Методы, системы и средства криптографической защиты информации с гарантированным уровнем устойчивости и повышенным быстродействием» (№ ДР 0115U002431) по хоздоговорам «Организация и разработка проекта национального стандарта Украины и методических рекомендаций по применению международных стандартов» (шифр «Гармония» – 2007).

Цель исследования. Целью работы является разработка метода универсального хеширования по рациональным функциям кривых Судзуки для построения доказуемо стойкой аутентификации с обеспечением гарантированной вероятности коллизии с уменьшенной сложностью вычисления.

Для достижения цели необходимо решить следующие научные задачи:

1. Провести анализ свойств существующих методов построения MAC-кодов, методов универсального и строго универсального хеширования, построенных на основе использования ортогональных массивов, слабо смещенных массивов, линейного алгебраического кодирования, и определить оценки секретности, ограничения на параметры доказуемо стойкой и безусловной аутентификации;

2. Разработать метод универсального хеширования по рациональным функциям алгебраической кривой Судзуки;

3. Разработать метод каскадного универсального хеширования по произведению функциональных полей алгебраических кривых;

4. Провести оценку свойств и характеристик разработанных методов, а также сравнительный анализ разработанных методов по критериям устойчивости и сложности;

5. Разработать математические и программные модели, реализующие предложенные методы выработки кодов аутентификации сообщений.

Объектом исследования являются процессы аутентификации сообщений в компьютерных системах и сетях на основе семейства универсального класса хеш-функций с высокими требованиями к доказуемой стойкости и минимизации затрат на аутентификацию.

Предметом исследований являются методы аутентификации данных на основе универсального хеширования, удовлетворяющие требованиям доказуемой коллизионной устойчивости, сложности нахождения прообраза и

второго прообраза, высокого быстродействия, простоты реализации с минимизацией затрат на ключевое пространство.

Методы исследований. При выполнении диссертационной работы использовались: теория алгебраических кривых; теория линейного пространства над функциональным полем проективных разнообразий для построения метода универсального хеширования по рациональным функциям алгебраических кривых; теорема Римана – Роха для вычисления размерности линейного базисного пространства и оценки параметров универсального хеширования; теория композиционного хеширования Стинсона для разработки методов каскадного универсального хеширования; теория вероятности для оценки коллизионных свойств каскадного хеширования;

Научная новизна полученных результатов. В работе получены следующие новые научные результаты:

1. Впервые предложен метод универсального хеширования на основе упорядочивания полюсов рациональных функций по кривой Судзуки, что приводит к существенному снижению сложности вычислений и уменьшению числа хешируемых данных; получены коллизионные оценки и оценки сложности хеширования;

2. Впервые предложен метод вычисления хеш-функций на основе четырехпараметрической схемы Горнера, в которой учитывается размерность рациональных функций кривых, что позволило обеспечить наименьшую сложность вычисления на уровне, пропорциональном размеру конечного поля;

3. Получил дальнейшее развитие метод универсального хеширования на основе скалярного произведения по рациональным функциям линейного базисного пространства, с использованием вычисления хеш-функций по подмножеству рациональных функций функционального поля с упорядоченными порядками полюсов.

Практическое значение полученных результатов заключается в следующем:

1. Построено функциональное поле кривой, ассоциированной с подгруппой группы Судзуки над конечным полем произвольной степени расширения. Получены оценки алгеброгеометрических параметров кривых Судзуки над конечными полями.

2. Построен алгоритм хеширования по кривой Судзуки по методу вычисления хэш-кода на основе четырехпараметрической схемы Горнера, что позволило получить наименьшую сложность вычислений (акт внедрения НТК ГП «Импульс» от 17.10.2015).

3. Разработаны лекция «Методы построения доказуемо стойкой аутентификации на основе универсального хеширования», практические рекомендации по использованию универсального хеширования по кривой Судзуки в схемах многократного, многокаскадного, композиционного хеширования доказуемо стойкой и безусловной аутентификации сообщений, что позволило минимизировать вероятность коллизии, сложность вычислений и оптимизировать затраты на ключевое пространство (акт внедрения ХНУРЭ от 17.02.2016).

4. Получены оценки универсального хеширования, сложности вычисления хэш-кода для двухкаскадного хеширования и многокаскадного хеширования по кривой Судзуки в схеме, когда во внутреннем каскаде используется хеширование по проективной прямой.

5. Разработаны программные средства (библиотека) для построения кривых, вычислений их точек и свойств (кратности), моделирования линейного базисного пространства с рациональными функциями кривых и статистического оценивания вероятности коллизии хеширования путем вычисления кратности пересечения гиперповерхностей линейного пространства с точками кривой (акт внедрения ХНУРЭ от 17.02.2016).

Результаты диссертационной работы внедрены в исследовательских и конструкторских работах в НТК ГП «Импульс» (акт внедрения от 17.10.2015), а также в учебном процессе кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники при изучении дисциплины «Системы и средства аутентификации», в курсовом и дипломном проектировании (акт внедрения ХНУРЭ от 17.02.2016).

Личный вклад соискателя. Все положения диссертации, выносимые на защиту, основные результаты теоретических и экспериментальных исследований получены автором самостоятельно. В научных статьях, опубликованных в соавторстве, соискателю принадлежат: оценки сложности и секретности алгоритма Whirpool [35]; оценки безопасности MAC-алгоритмов стандарта ISO/IEC 9797-2 [36]; оценки безопасности MAC-алгоритмов стандарта ISO/IEC 9797-1 [37]; метод универсального хеширования по рациональным функциям кривой Судзуки, доказательство утверждения о порядках полюсов рациональных функций кривой Судзуки [38]; метод вычисления хеш-функций на основе четырехпараметрической схемы Горнера [39], практический алгоритм универсального хеширования по рациональным функциям кривой Судзуки на основе схемы Горнера с вычислением по подгруппе Вейерштрасса размерности четыре, оценки для вероятности коллизии и сложности хеширования [39]; метод каскадного универсального хеширования по кривой Судзуки на основе произведения функциональных полей [40]; метод универсального хеширования на основе скалярного произведения по рациональным функциям линейного базисного пространства с ограничением функционального поля алгебраических кривых [41]; требования к криптографическим примитивам нового поколения [42]; оценки универсального хеширования на основе многопотоковых вычислений [43]; алгеброгеометрические параметры Судзуки над конечными полями и оценки параметров универсального хеширования по кривым Судзуки [44].

Апробация результатов диссертации. Основные научные результаты и положения диссертационной работы докладывались и обсуждались на следующих международных и национальных научно-технических конференциях: международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах», Киев, 20 – 23 мая 2008 г.; вторая Международная научно-техническая конференция «Компьютерные науки и технологии КНиТ-2011», Белгород, 2011 г.; XV Международная научно-практическая конференция «Безопасность в информационно-телекоммуникационных системах», Киев, 22 – 25 мая 2012 г.; международная научно-практическая конференция «Применение информационных технологий в подготовке и деятельности сил охраны правопорядка», Академия внутренних войск МВД Украины, 17 – 18 марта 2011 г.; всеукраинская научно-практическая конференция «Информационная безопасность государства, общества и личности», Кировоград, КНТУ, 16 апреля 2015 г.; студенческая научная конференция физико-технического факультета ДонНУ, 2015.

Публикации. По результатам диссертационной работы опубликовано 10 статей в 5 специализированных изданиях, входящих в перечень, утвержденный ВАК Украины, 6 материалов и тезисов научных конференций.

Структура и объем диссертации. Диссертация состоит из введения, пяти разделов и заключения, имеет общий объем 209 страниц, из которых 169 страниц основного текста, содержит 16 рисунков, 25 таблиц, список использованных источников из 164 наименований на 17 страницах.

Автор выражает благодарность научному руководителю, доктору технических наук Халимову Геннадию Зайдуловичу за постановку задачи, постоянное внимание к работе, поддержку в работе над диссертацией, за критические замечания при обсуждении теоретических и практических результатов, полученных в научных исследованиях.

РАЗДЕЛ 1
АНАЛИЗ СОВРЕМЕННЫХ ТРЕБОВАНИЙ К КРИПТОГРАФИЧЕСКИМ ПРИМИТИВАМ

В первом квартале 2015 г. компания Google официально прекратила поддержку SHA-1 (*Secure Hash Algorithm*) [51]. Практически это означает, что с выходом браузера Chrome версии 41 все сайты, подписанные сертификатом с указанным алгоритмом, будут признаваться небезопасными. В свою очередь, компания Microsoft анонсировала вначале отказ от 160-битных хешей с 1 января 2017 г., но затем выпустила анонс отказа от использования SHA-1 уже со второго квартала 2016 [52,53]. Это стало возможным благодаря значительному повышению производительности в совокупности с новыми методологиями распределительных вычислений, что позволило реализовать известные и новые угрозы безопасности, характеризуемые снижением фактических временных затрат на преодоление практической стойкости подсистемы аутентификации до неприемлемого уровня. Два последних десятилетия активно разрабатывались математические методы, представляющие практический интерес для криптоанализа. Вычислительная сложность решения определенного класса математических задач лежит в основе безопасности ряда систем защиты коммерческих информационно-коммуникационных технологий.

В данной связи одной из актуальных научных задач является разработка перспективных криптопримитивов с доказуемой стойкостью. Задачей раздела является анализ безопасности и производительности современных крипто-примитивов-финалистов конкурса NIST (*National Institute of Standard and Technology)*, анализ причин выбора криптопримитива Keccak в качестве финалиста, современных требований к безопасности, вычислительной сложности и скорости, методов повышения скорости без увеличения сложности реализации.

Результаты международных проектов NESSIE (2000 – 2003 гг.) и NISTSHA-3 Competition (2007 – 2012 гг.) определяют требования к построению коллизионно стойких функций хеширования и ключевых функций хеширования для вычисления кодов аутентификации сообщений, аутентификации и установления ключей в криптографических протоколах, прежде всего в протоколах электронной цифровой подписи [55,56]. Критериями оценивания кандидатов на стандарт SHA-3 являются стойкость к атакам на хеш-функцию, сложность и скорость вычисления, характеристики и реализация алгоритма. Кандидаты финального раунда NISTSHA-3 Competition рассмотрены в подразделе 1.5.

1.1 Определения и классификация MAC-кодов

Код аутентификации сообщения (MAC-код) определяется как вычисленная для блока данных ключевая криптографическая контрольная сумма (аутентификатор), с помощью которой можно проверить аутентичность сообщения. Имеем следующее определение.

Определение 1.1 [58]. MAC-код является функцией отображения $h: K \times D \to R$, где пространство ключей $K = \{0,1\}^k$, пространство сообщений $D = \{0,1\}^*$ и пространство MAC значений $R = \{0,1\}^n$ для $k, n \geq 1$. Для заданных значений ключа $k \in K$ и сообщения $X \in D$ функция производит MAC-вычисление $Y \in R$.

Замечание 1.1.

– функция вычисления MAC-кода должна обладать следующими свойствами:

1) должно быть вычислительно трудно, зная M и $CK(M)$, найти сообщение M', такое, что $CK(M) = CK(M')$;

2) значения $CK(M)$ должны быть равномерно распределенными, для любых сообщений M и M' вероятность того, что $CK(M)=CK(M')$ должна быть равна 2^{-n}, где n – длина значения MAC;

– пусть длина ключа, используемого при вычислении MAC, равна k. При условии сильной MAC-функции криптоаналитику потребуется выполнить 2^k попыток для перебора всех ключей. Если длина значения, создаваемого MAC, равна n, то всего существует 2^n различных значений MAC-кодов;

– предположим, криптоаналитик имеет доступ к открытому сообщению и соответствующему ему значению MAC. Определим усилия, необходимые криптоаналитику для нахождения ключа MAC.

Пусть длина ключа $k>n$ больше длины MAC. По известным M_1 и $MAC_1=CK(M_1)$ криптоаналитик может вычислить $MAC_1=CK_i(M_1)$ для всех возможных ключей K_i. По крайней мере, для одного из ключей будет получено совпадение $MAC_i=MAC_1$. Криптоаналитик вычислит 2^k значений MAC. При длине MAC n бит существует всего 2^n значений MAC. Правильное значение MAC будет получено для нескольких значений ключей. В среднем совпадение будет иметь место для $2^k/2^n=2^{(k-n)}$ ключей. Для вычисления единственного ключа оппоненту потребуется знать несколько пар сообщений и соответствующих им MAC-кодов. Таким образом, простой перебор всех ключей требует больше усилий, чем поиск ключа симметричного шифрования той же длины.

Международные стандарты построения алгоритмов аутентификации данных представлены в таблице 1.1.

Таблица 1.1 – Стандарты построения *MAC*-кодов

Стандарт	Механизм выработки *MAC*-кода
FIPSPUB 113 Computer Data Authentication (2002)	Алгоритм на основе DES
FIPS PUB 198-1 The Keyed-Hash Message Authentication Code	Алгоритм HMAC
ISO/IEC 9797-1	Алгоритмы на основе блочного шифра
ISO/IEC 9797-2 Mechanisms using a dedicated hash-function	Алгоритмы на основе хеш-функций

Основные алгоритмы вычисления *MAC*-кодов представлены в таблице 1.2.

Таблица 1.2 – Алгоритмы вычисления *MAC*-кодов

Алгоритм	Рекомендация		Схема реализации
	текущая	в будущем	
EMAC	да	да	любой БСШ как *PRP*
CMAC	да	да	любой БСШ как *PRP*
HMAC	да	да	любой БСШ как *PRP*
UMAC	да	да	любая хеш-функция как *PRP*
GMAC	да	нет	операции в конечном поле
AMAC	да	нет	любой БСШ

Замечание 1.2. Можно выделить следующие подходы к построению кодов аутентификации сообщений [11,30]:

– коды аутентификации сообщений, построенные с применением блочных шифров;

– коды аутентификации сообщений, построенные на основе бесключевых хеш-функций;

– коды аутентификации сообщений, построенные с использованием семейства универсальных хеш-функций;

– коды аутентификации сообщений, построенные на основе специализированных алгоритмов;

– *MAC*-коды на основе блочного шифра.

Коды аутентификации сообщений, построенные с применением блочных шифров, определяются стандартом *ISO*/*IEC* 9797-1 и используют шифрование в режиме *CBC* сцепления шифр текстов [15].

Определение 1.2. *MAC*-код, основанный на применении блочного шифра в *CBC* режиме, определяется выражением $H_1 = E_K(X_1)$, $H_i = E_K(X_i \otimes H_{i-1})$, $2 \le i \le t$. Безопасность *CBC MAC*-конструкций основывается на криптографической стойкости блочного шифра, оценки стойкости получены для статистической модели блочного шифра как псевдослучайной функции [15].

Длина блока данных должна быть равна длине данных блочного шифра. Длина *MAC*-кода устанавливается равной длине блока блочного шифра. На каждом шаге итерации ключ *MAC*-кода используется как ключ шифра, а блок сообщения, после побитового сложения с результатом вычисления шифра текста, полученный на предыдущем шаге, подается на вход блока шифрования.

Основная *CBC*-конструкция уязвима к атаке типа *exor* подделки и, следовательно, может использоваться только в приложениях, где сообщения имеют фиксированную длину. Также существуют несколько более защищенных разновидностей этого алгоритма: *EMAC* и *RMAC* схемы. *EMAC* код использует дополнительное шифрование исходного результата преобразований, ключ для этой операции шифрования может быть получен с ключа *MAC*. *RMAC* алгоритм заменяет последнее шифрование на шифрование с двумя ключами. Безопасность этих конструкций может быть доказана при условии, что основной блочный шифр является псевдослучайным [15]. Все эти схемы содержатся в ISO/IEC 9797-1, что

является международным стандартом для кодов аутентификации сообщений, использующих блочные шифры [15].

Коды аутентификации сообщений на основе бесключевых хеш-функций (*HMAC*) используют значение секретного ключа при исчислении хеш-результата. Эти коды аутентификации сообщений имеют большую скорость по сравнению с кодами аутентификации сообщений, используют блочные шифры. *HMAC* является вложенной конструкцией, вычисляет *MAC*-код на основе хеш-функции, сообщения и секретного ключа [16].

Определение 1.3. *HMAC* код определяется выражением

$$HMAC(K, X) = h\left((K \otimes opad) \| h(K \otimes ipad \| X)\right).$$

Ключ K дополняется нулевыми битами до полного блока, *opad* та *ipad* – постоянные значения. Безопасность этой конструкции была доказана в [56], основываясь на таких предположениях: основная хеш-функция является коллизионно стойкой при условии, что начальное значение – секретное; ключевая функция сжатия с помощью начального значения является защищенным *MAC*-алгоритмом (для сообщений размером в один блок); функция сжатия – слабая псевдослучайная функция.

Альтернативой *HMAC* кодам являются *MDX-MAC* конструкции [16], основанные на *MD*5, *SHA* та *RIPEMD* хеш-функциях. Здесь основная хеш-функция изменена в *MAC*-код за счет внесения небольших модификаций: включения секретного ключа на начало, на конец и к каждому шагу итерационного вычисления хеш-функции. Защищенность *MDX-MAC* может быть доказана при условии, что основная функция сжатия является псевдослучайной.

Практическими алгоритмами хеширования в *HMAC* (ISO/IEC 9797-2) алгоритме являются: ГОСТ 34.311-95, HAVAL, SHA-1, RIPEMD-160, MD-5, ГОСТ 28147-89 режим 4 [17], Whirpool [35], SHA-2 [13].

Три алгоритма серии *MD* (*MD*-2, *MD*-4, *MD*-5) разработаны Роном Райвестом в 1989, 1990 и 1991-м годах соответственно. Они оперируют с

блоками данных, совпадающими с длиной результирующего значения свертки, причем $n=128$ для алгоритма *MD*-4, и $n=160$ – для *MD*-5 и *SHA*. Указанные алгоритмы спроектированы специально с учетом эффективной реализации на 32-разрядных процессорах.

Исходное сообщение M разбивается на блоки длиной 512 бит. Последний блок формируется путем дописывания к концу сообщения комбинации 10…0 до получения блока размера 448 бит, к которому затем добавляется комбинация из 64 бит, представляющая битовую длину сообщения. Затем вычисляется значение свертки согласно процедуре с использованием одношаговой сжимающей функции, заданной формулой $f(\chi, H)=E\chi(H)\oplus H$, где χ – блок сообщения длины 512 бит, H – блок из η бит, а $E\chi$ – некоторое преобразование множества блоков. Значение начального вектора определяется в описании преобразования $E\chi$.

Алгоритм *MD*-2 (*RFC* 1319) предполагает:

– дополнение текста до длины, кратной 128 бит;

– вычисление 16-битной контрольной суммы (старшие разряды отбрасываются);

– добавление контрольной суммы к тексту;

– повторное вычисление контрольной суммы.

Алгоритм *MD*-4 предусматривает:

– дополнение текста до длины, равной 448 бит по модулю 512;

– добавляется длина текста в 64-битном представлении;

– 512-битные блоки подвергаются процедуре Damgard – Merkle, причем каждый блок участвует в трех разных циклах.

В алгоритме *MD*-4 довольно быстро были найдены критические уязвимости, поэтому он был заменен алгоритмом *MD*5, в котором каждый блок участвует не в трех, а в четырех различных циклах.

Алгоритм *MD*-5 предназначен для создания «отпечатков» или «дайджестов» сообщений произвольной длины, является улучшенной в плане безопасности версией *MD*-4. Зная *MD*-5, невозможно восстановить входное

сообщение, так как одному *MD*-5 могут соответствовать разные сообщения. Используется для проверки подлинности опубликованных сообщений путем сравнения дайджеста сообщения с опубликованным. Эту операцию называют «проверка хеша» (hashcheck). На вход алгоритма поступает входной поток данных, хеш которого необходимо найти. Длина сообщения может быть любой (в том числе нулевой). Запишем длину сообщения в L. Это число целое и неотрицательное. Кратность каким-либо числам необязательна. После поступления данных идет процесс подготовки потока к вычислениям.

Алгоритм *SHA* разработан *NIST* и повторяет идеи серии *MD*. В *SHA* используются тексты более 264 бит, которые закрываются сигнатурой длиной 160 бит. Данный алгоритм предполагается использовать в программе Capstone. *RIPEMD* семейство функций хеширования использует две параллельные схемы вычисления, которые являются модифицированными версиями *MD*-4. В таблице 1.3 представлены сравнительные данные *MD* подобных алгоритмов [16].

Функция хеширования *SHA*-1 входит в стандарт *FIPS* 180-1 и рекомендованный *NIST* для цифровых подписей вместе с *DSA* стандартом. *NIST* обновил этот стандарт, представив *FIPS* 180-2 [59], который включает, кроме *SHA*-1, три новые хеш-функции *SHA*-2/256, *SHA*-2/384 и *SHA*-2/512 с функциями хеширования большей длины, чтобы отвечать уровню защиты нового стандарта блокового шифра AES. ANSI принял банковские стандарты криптографии с открытыми ключами: стандарт *X*9.30 [60], который определяет алгоритм *SHA*-1 вместе с *DSA*, и стандарт *X*9.31 [61], который определяет алгоритм *MDC*-2 с цифровой подписью на базе *RSA*.

Алгоритм Whirlpool был признан лучшим в проекте NESSIE в категории «Устойчивая к коллизиям хеш-функция». Алгоритм Whirlpool вычисляет 512-битный хеш-код с использованием в качестве функции сжатия блочного шифра, который является модификацией алгоритма Rijndael. В работе [35] исследовалось существование квадратичной зависимости во входных и выходных значениях блока подстановки алгоритма Whirlpool.

Таблица 1.3 – Параметры *MD* подобных функций хеширования

Алгоритм	Размер хеш-кода (бит)	Размер блока (бит)	Размер слова (бит)	Число циклов на число шагов в цикле
MD-4	128	512	32	3/16
MD-5	128	512	32	4/16
RIPEMD-128	128	512	32	4/16/2
RIPEMD-160	160	512	32	5/16/2
SHA-1	160	512	32	4/20
SHA-2/256	256	512	32	1/64
SHA-2/384	384	1024	64	1/80
SHA-2/512	512	1024	64	1/80

Было показано, что для блоков подстановки Rijndael и Serpent существуют квадратичные уравнения для входных и выходных бит с вероятностью 1. Такие уравнения всегда существуют для n бит n-битного блока подстановки, если $n \le 6$, но для $n > 6$ – не всегда. Были проведены исследования по выявлению квадратичных зависимостей в блоке перестановки Whirlpool. Блок перестановки – это 8-битная перестановка. Существует максимум 137 возможных степеней свободы в многомерном выражении для 8 входных и8 выходных бит. Простейший метод проверки наличия таких зависимостей – это вычисление 256 раз определителя 137-мерных двоичных матриц. Для полной таблицы подстановки Whirlpool не было найдено квадратичных зависимостей. Тем не менее, так как блок подстановки состоит из нескольких четырех битовых подстановок, задача построения маленькой системы многомерных квадратичных уравнений существенно упрощается. Алгоритм Whirlpool имеет очень высокую стойкость, сравнимую с *SHA*-2 (512), но невысокое быстродействие и, соответственно, его можно рекомендовать к применению в системах, где необходимо обеспечить стойкость в течение длительного периода времени, где критерий стойкости является определяющим и намного важнее скорости. Математическая простота алгоритма, достигнутая в процессе разработки, позволяет упростить и процесс анализа стойкости. Длина *MAC*-кода в 512 бит

обеспечивает эффективную защиту от атак, основанных на парадоксе «день рождения», а также улучшает показатели устойчивости к коллизиям. Оптимальная длина ключевых данных, отвечающая современным требованиям, позволила данному алгоритму стать победителем в категории «Алгоритм, устойчивый к коллизиям» в рамках проекта NESSIE.

ISO/IEC развил стандарт 10118 для разных классов функций хеширования [11–14]. В части 10118-2 [12] определены функции хеширования, основанные на блоковых шифрах в конструкции Matyas – Meyer – Oseas, когда независимый блоковый шифр в алгоритме*MDC*-2 с двумя и более функциями делает значения хеша двойной и тройной длины соответственно. Часть 10118-3 [13] определяет три алгоритма: *RIPEMD*-128, *RIPEMD*-160 и *SHA*-1. Эта часть стандарта в настоящее время пересматривается с учетом оценки новых криптографических примитивов, которые будут приняты как стандарты ISO. Кроме указанных трех алгоритмов изучаются функции хеширования: *SHA*-2/256, *SHA*-2/384, *SHA*-2/512 и Whirlpool. Часть 10118-4 [14] описывает *MASH*-1 и *MASH*-2 функции хеширования, которые используют модулярную арифметику. Оценки стойкости функций хеширования представлены в таблице 1.4 [62].

Коды аутентификации сообщений, которые основаны на универсальном хешировании, используют комбинаторные свойства семейства хеш-функций.

Определение 1.4. *MAC*-код на основе универсального хеширования является отражением $h = H_k : D \to R$ (где для каждого $k \in K$, H_k – функция из семейства хеш-функций $H = \{h : D \to R\}$, D – общая область определения, R – конечный диапазон значений), таким, что для каких-либо разных $x, x' \in D$ вероятность того, что $h(x) = h(x')$ будет не больше $\varepsilon \le 1$, при случайном выборе $h \in H$ [32].

Комбинаторные свойства универсального хеш-семейства позволяют получить точные границы секретности MAC-кодов.

Таблица 1.4 – Верхние границы стойкости функций хеширования

Функция хеширования	n	m	Стойкость прообразу	Стойкость к коллизии
Матис – Мейер – Озиса[a]	n	n	2^n	$2^{n/2}$
MDC-2 (*DES*)[b]	64	128	$2 \cdot 2^{82}$	$2 \cdot 2^{54}$
MDC-4 (*DES*)	64	128	2^{109}	$4 \cdot 2^{54}$
Меркли(*DES*)	106	128	2^{112}	2^{56}
MD-4	512	128	2^{128}	2^{20}
MD-5	512	128	2^{128}	2^{64}
RIPEMD-128	512	128	2^{128}	2^{64}
SHA-1, *RIPEMD*-160	512	160	2^{160}	2^{80}

a – эта же стойкость предполагается для функций хеширования Дэвиса – Мейера и Миягучи – Принеля;

b – стойкость может быть увеличена путем применения шифра с длиной ключа, равной длине блока шифра.

Коды аутентификации сообщения, построенные на основе специализированных алгоритмов, представляют собой модификацию известных хеш-функций и имеют, как правило, наивысший уровень защиты для *MAC*-примитивов.

Примером таких алгоритмов является Two-Track-MAC (K.U. Leuven, Бельгия и debisAG, Германия). TTMAC (Two-Track-MAC) алгоритм основан на хеш-функции *RIPEMD*-160 с небольшими модификациями [63]. Алгоритм работает на блоках 512 бит, разделенных на слова по 32 бит, использует секретный ключ 160 бит и производит выход до 160 бит. Большой размер внутреннего состояния (320 бит) в Two-Track-MAC дает алгоритму высокий уровень защиты от атак, основанных на внутренних коллизиях [63]. Сложность основных атак на этот примитив следующая:

– приблизительно 2^{159} вычислений *MAC*-кода и $160/m$ известных пар текст – *MAC* необходимы для исчерпывающего поиска ключа, где m – длина *MAC*-результата (значение для *m* поддерживается алгоритмом между 32 и 160 битами);

– угадывание значения *MAC*-кода имеет вероятность успеха 2^{-m};

– атаки, основанные на внутренних коллизиях, требуют приблизительно 2^{160} известных пар текст – *MAC*-код и приблизительно 2^{320-m} выбранных текстов.

Алгоритм TTMAC имеет самый высокий уровень защиты для *MAC*-примитивов, определенные преимущества в быстродействии, особенно в случае коротких сообщений, и оптимальную длину ключевых данных. Вместе с тем, TTMAC имеет низкую скорость, что делает проблематичным применение для приложений, где требуется хешировать данные больших объемов. В таблице 1.5 представлены основные результаты по параметрам и оценке быстродействия основных алгоритмов аутентификации. Скорость вычислений определяется количеством циклов процессора, затрачиваемых на один байт обрабатываемого сообщения.

Таблица 1.5 – Быстродействие *MAC*-алгоритмов

Алгоритм	Длина *MAC* кода (бит)	Длина ключа (бит)	Тип ПЭВМ, количество циклов				
			Pentium 2	*P*III/*Linux*	*Pentium* 4	*Xeon*	*AMD*
TTMAC	160	160	21	21	40	37	21
UMAC-16	64	128	6.1	6.0	6.2	6.1	6.2
UMAC-32	64	128	2.5	2.9	6.7	6.6	1.9
HMAC-Whirlpool	512	512	86	72	98	103	100
HMAC-MD-4	128	512	4.7	4.7	6.4	6.4	4.7
HMAC-MD-5	128	512	7.2	7.3	9.4	9.4	7.4
HMAC-RIPE-MD	160	512	23	18	27	26	21
HMAC-SHA-0	160	512	16	15	23	23	13
HMAC-SHA-1	160	512	16	15	25	24	12
HMAC-SHA-2	256 384 512	512	40 84 84	39 84 84	40 124 124	39 132 132	33 72 72
HMAC-Tiger	192	512	24	21	28	26	20
CBCMAC-Rijndael	128	128	24	26	26	27	31
CBCMAC-DES	64	56	62	61	72	69	54
CBCMAC-Shacal	512	160	31	31	67	74	29

1.2 Влияние вычислительной мощности на требования к хеш-функциям

В качестве основных составляющих прироста мощности вычислительных систем можно выделить: рост производительности выделенных вычислительных устройств; организацию массовых вычислений в совокупности устройств, в том числе и мобильных; использование эффективных моделей вычислений на существующих классах архитектур. Одним из наиболее перспективных направлений в решении задач вычислений общего назначения является использование технологии GPGPU (General-purpose graphics processing units) [43]. Графический процессор (GPU) обладает меньшим набором исполняемых команд (RISC-подобные архитектуры), чем CPU, но большей производительностью. Технология GPGPU позволяет на одном вычислителе достигать достаточно высокого уровня параллелизма без временных затрат на передачу данных между узлами и синхронизацию результатов вычислений. Относительная низкая стоимость, простота добавления вычислительных модулей и удельное энергопотребление в сочетании с высокой удельной производительностью GPU позволяют реализовать на практике массовые распределенные параллельные вычисления, которые доступны более широкому кругу потенциальных нарушителей. Сравнительный анализ возможностей CPU и GPU архитектур в практической реализации алгоритмов *SHA*-1 и *MD*-5 представлен на рис. 1.1 [43].

Слабая вычислительная сложность, ряд значительных недостатков конструкции и математически обоснованные атаки на коллизионную стойкость позволили реализовать для хеш-функций *SHA*1 и *MD*5 атаки полного перебора за допустимое время. В практической реализации [43] представлены результаты скорости подбора *MD*5-паролей на nVidiaTitanX (около 135,2 миллиардов комбинаций в секунду), что позволяет найти пароль длиной восемь символов менее чем за пять минут.

В таблице 1.6 представлены результаты производительности реализации атаки «полного перебора» для семейства хеш-функций на тестовом стенде (Ubuntu 14.04, 64 bit, ForceWare 346.29, 8xNVidiaTitanX, stockcoreclock, oclHashcatv 1.3).

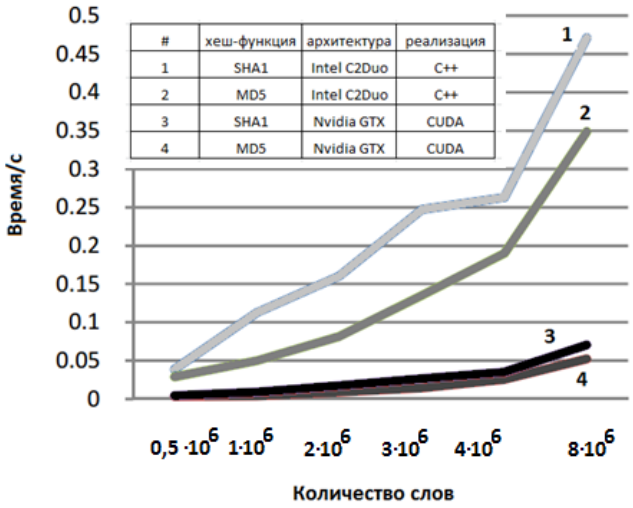


Рис. 1.1. Сравнительный анализ скорости реализации хеш-функций на CPU/GPU архитектурах

Таблица 1.6 – Производительность атак полного перебора для различных хеш-функций

Алгоритм	Производительность (комбинаций/с)
MD-5	$135232*10^6$
SHA-1	$42408*10^6$
SHA-256	$16904*10^6$
SHA-512	$5240*10^6$
RipeMD-160	$28368*10^6$
Whirpool	$1122402*10^6$

Успешные атаки и рост вычислительной емкости предъявляют высокие требования к стойкости хеш-функций. Недостатки, выявленные у криптографических стандартов 90-х, и обоснованные теоретические атаки обусловливают развитие новых методов реализации криптопримитивов. Конкурс SHA-3, организованный NIST, показал развитие требований к безопасности, архитектуре и производительности при реализации криптографических примитивов. В финале конкурса SHA-3, организованного

NIST, двое из пяти финалистов (Keccak и Skein) оказались универсальными криптопримитивами, которые могут использоваться не только для хеширования, но и для выполнения множества других криптографических операций, обеспечивая упрощение проектируемых криптографических протоколов. Три этапа конкурса фактически формализовали дальнейший подход к процедуре выбора криптопримитивов. Рассмотрим требования к безопасности, архитектуре и производительности, предъявляемые к современным криптопримитивам.

1.3 Требования к безопасности современных хеш-функций

Основные определения безопасности хеш-функций представлены в [15,16,24,25,35].

Определение 1.5. (Стойкость к вычислению прообраза). Хеш-функция $h: \{0,1\}^* \to R$ является стойкой к вычислению прообраза силой (t, ε), если не существует вероятностного алгоритма Ih, с входными значениями $Y \in_R R$ и значениями на выходе $X \in \{0,1\}^*$, временем выполнения не более чем t, где $h(X) = Y$, и вероятностью не менее ε, оцененной при случайном выборе Y и Ih.

Стойкость хеш-функций к вычислению прообраза имеет большое значение для систем аутентификации, использующих хеш-значения паролей и секретных ключей.

Определение 1.6. (Стойкость к вычислению второго прообраза). Пусть S – конечное подмножество $\{0,1\}^*$. Хеш-функция $h: \{0,1\}^* \to R$ является стойкой к вычислению второго прообраза силой (t, ε, S), если не существует вероятностного алгоритма Sh, с $X \in_R S$ и $X' \in \{0,1\}^*$, временем выполнения не более чем t, где $X' \neq X$ и $h(X') = h(X)$, и вероятностью не менее ε, оцененной при случайном выборе X и Sh.

Стойкость хеш-функций к вычислению второго прообраза определяет безопасность систем аутентификации с цифровой подписью.

Определение 1.7. (Стойкость к коллизиям). Хеш-функция $h:\{0,1\}^* \to R$ является стойкой к коллизиям силой (t,ε), если не существует вероятностного алгоритма Ch с известными выходными значениями $X, X' \in \{0,1\}^*$, временем выполнения не более чем t, где $X' \neq X$ и $h(X) = h(X')$, и вероятностью не менее ε, оцененной при случайном выборе Ch.

Основные требования к безопасности хеш-функций, используемые NIST, представлены в работе [64]. Более 40 кандидатов не удовлетворили этим определениям и были исключены в первом раунде конкурса [56].

Сравнительный анализ финалистов конкурса NIST, удовлетворяющих основным требованиям к безопасности, приведен в таблице 1.7 [57].

Таблица 1.7 – Безопасность финалистов конкурса NIST

Кандидат	Стойкость к коллизиям	Количество раундов сжатия	Сложность вычисления		
			про-образа	второго прообраза	Псевдо pre
Blake-256	Inner-collision	2.5	2^{224}	2^{256}	-
Blake-512	Inner-collision	4	2^{448}	2^{256}	-
Groestl-256	2^{64}	5	2^{256}	$2^{256\text{-}512}$	$2^{244.85}$
Groestl-512	2^{128}	8	2^{512}	$2^{512\text{-}1024}$	2^{248}
JH-256	$2^{96,12}$	16	-	2^{-388}	-
JH-512	$2^{95,63}$	22	-	2^{-900}	-
Keccak-224	близко к 2^{256}	4-5	2^{112}	2^{288}	
Keccak-256	близко к 2^{256}	5-10	2^{1370}	2^{512}	
Keccak-512	2^{512}	24	2^{1590}	$2^{511.5}$	2^{1576}
Skein-256	$>2^{-265}$	32-36	2^{105}	2^{200}-2^{824}	$2^{511.7}$
Skein-512	$>2^{-265}$	32-36	2^{105}	2^{200}-2^{824}	$2^{511.7}$
Skein-1024	$>2^{-265}$	32-36	2^{105}	2^{200}-2^{824}	2^{1045}-2^{125}

1.4 Требования к архитектуре и реализации MAC-алгоритмов

Обобщим требования к архитектуре и особенности реализации, являющиеся частью интегральной оценки алгоритма. Функция сжатия как основной элемент архитектуры хеш-функции была заявлена в большинстве кандидатов. С точки зрения требований к архитектуре важными атрибутами являются: особенности реализации структуры *SPN* и блоков подстановок (*S-box*) или блоков перестановок (*P-box*), схемы Фейстеля для преобразований функций $F(L_i, K_i)$, математическая сложность функции ключевого расширения (функции разворачивания подключей раунда из основного ключа), структуры Merkle-Damgard, WidePipe, размерность *MDS*-матрицы. В работе [39] рассмотрено влияние булевых операций, *OUT*-трансформации, *FSR, ARX*-сдвигов на конечную реализацию хеш-функций.

С точки зрения оптимизации вычислений, наиболее важным параметром является размер кэша 1-го уровня для инструкций. Кэш 1-го уровня для данных важен для функций, которые используют табличную реализацию (такие, как хеш-функция ECHO). Несоответствие количества выполняемых для цикла инструкций предполагает серьезное снижение производительности (примером являются некоторые реализации Skein), где впоследствии предполагается использовать метод «разворачивания» [37,41]. Этот метод заключается в повторении кода для одного раунда нескольких последовательных раундов и позволяет «обнулить» затраты на маршрутизацию данных в памяти. Так, например, в алгоритме *SHA*-256 в каждом раунде «вращаются» восемь слов, что для восьми последовательных раундов «разворачивания» позволяет использовать те же переменные и сократить затраты на копирование данных между ними. Кроме того, если «разматывать» 64 последовательных раунда *SHA*-256, то можно отказаться от получения констант из таблицы и сэкономить на косвенной адресации в памяти. Такой подход является общим инструментом уменьшения затрат на

маршрутизацию данных во время выполнения. Если реализация в процессе полного «разворачивания» помещается в кэш 1-го уровня, то она оптимизирована, в обратном случае возникают дополнительные затраты на копирование и косвенную адресацию. Важной особенностью реализации является возможность использования 64-разрядных целых чисел для систем с собственными 64-разрядными регистрами [41]. На 32-битных системах без таких регистров использование 64-битных целых неэффективно и требует два регистра. Это увеличивает затраты на коды операций (перенос между нижними и верхними словами) для 32-битных архитектур. Наиболее очевидно это проявляется на диаграммах с полученным на 64-битных архитектурах 512-битным хеш-кодом. В архитектуре *x*.86 отсутствие 64-разрядного целого типа часто компенсируется в реализациях хеш-функций с использованием специальных блоков с 64-разрядными регистрами (MMX, SSE). Недостаток реализаций в подобных случаях состоит в необходимости использовать особенные, встроенные в компилятор инструкции (C/C++) [41]. Это ограничивает возможности реализации на других платформах, в частности в JavaVM. Порядок байт для современных алгоритмов хеш-функций уже не имеет существенного значения для достижения высокой производительности.

Для большинства функций текущий набор инструкций также не важен. В больших системах коды операций динамически транслируются во внутренние элементарные инструкции, для которых CPU применяет оптимизации (параллельное выполнение, изменение порядка, спекулятивное выполнение инструкций и т. д.).

Большинство из кандидатов NIST второго раунда соревнований показали композитную схему реализации. Некоторые из них были представлены парой функций для разной длины выходов (224, 256, 384, 512 бит). Fugue и Lufa состояли из трех функций, а Keccak – из четырех, хотя и с разделяемым ядром. В свою очередь, такой подход в архитектуре имеет ряд негативных последствий для производительности: реализация семейства

функций требует больше ресурсов для разработки, чем для оптимизации; увеличивается размер кода; проблемы производительности и безопасности более не являются взаимозависимыми. Архитектура CubeHash, JH и Shabal позволила избежать подобного эффекта и показала стабильную производительность для всех размеров выходных данных.

Минимальный размер ключа, необходимый для защиты информации от атак злоумышленника, будет расти по мере повышения быстродействия компьютеров. Но, тем не менее, приведенные вычисления показывают, что можно выбрать такую длину ключа, при которой атаку методом полного перебора провести будет в принципе невозможно, вне зависимости от повышения вычислительной мощности компьютеров или успехов в области классической теории алгоритмов.

Таблица 1.8 – Сравнительный анализ скорости хеш-функций

Хеш-функция	Производительность 32-бит		Производительность 64-бит	
	cpb	класс скорости	*cpb*	класс скорости
SHA-256	29.3	*C*	20.1	*C*
SHA-512	55.2	*C*	13.1	*C*
Blake-256	28.3	*B*	16.7	*B*
Blake-512	61.7	*C*	12.3	*B*
Groestl-256	22.9	*B*	22.4	*D*
Groestl-512	37.5	*A*	30.1	*E*
JH-256	21.3	*B*	16.8	*B*
JH-512	21.3	*AA*	16.8	*D*
Keccak-256	35.4	*C*	10.1	*A*
Keccak-512	68.9	*C*	20.3	*D*
Skein-256	21.6	*A*	7.6	*AA*
Skein-512	20.1	*AA*	6.1	*AA*

В работе [64] проанализирован подход к классификации современных хеш-функций на основе сравнения с эталонной реализацией алгоритма *SHA*-256/512 в NIST (IntelCore 2 Duo). По результатам конкурса класс скорости в работе был определен следующим образом:

$AA = x < 1/2\,SHA\text{-}2$;

$A = 1/2\,SHA\text{-}2 \le x < 3/4\,SHA\text{-}2$;

$B = 3/4\,SHA\text{-}2 \le x < SHA\text{-}2$;

$C = SHA\text{-}2 \le x < 5/4\,SHA\text{-}2$;

$D = 5/4\,SHA\text{-}2 \le x < 2SHA\text{-}2$;

$E = x > 2SHA\text{-}2$.

Проанализируем особенности архитектуры и реализации финалистов NIST, их влияние на вычислительную сложность, скорость и безопасность.

1.5 Анализ схем реализации финалистов NIST

1.5.1 Алгоритм BLAKE.

Представлен в качестве альтернативы существующим *SHA*-2/*MD*-5 применениям, значительно превосходя их по надежности, практически не уступая в производительности [65] (рис. 1.2).

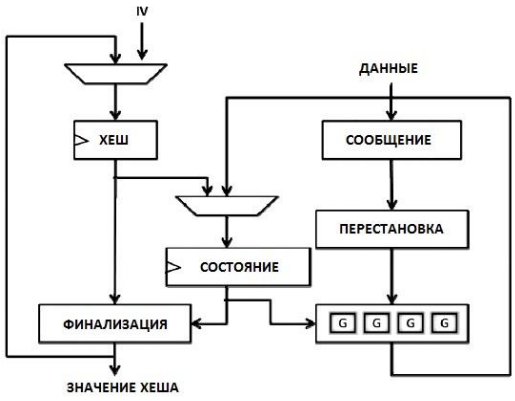


Рис. 1.2. Высокоуровневая архитектура BLAKE

Хеш-функция BLAKE не чувствительна к размеру хешируемых данных и защищена от всех свойственных *SHA*-1 и *MD*5 видов атак, связанных с возникновением коллизий в процессе хеширования [66]. Реализации для различных архитектур с поддержкой распараллеливания позволяют существенно увеличить производительность.

1.5.2 Алгоритм Groestl.

Функция хеширования Groestl способна возвращать хеш-значение произвольной длины от 1 до 64 байт, т.е. от 8 до 512 бит, при этом хеш-значение должно быть кратно байту (см. рис. 1.3). Функция сжатия базируется на двух t - битовых перестановках P и Q (1) [67]:

$$F(h,m)=P(h\oplus m)\oplus Q(m)\oplus h. \tag{1.1}$$

Выходное хеширование Ω можно описать с помощью формулы

$$\Omega(h)=\text{truncn}(P(x)\oplus x). \tag{1.2}$$

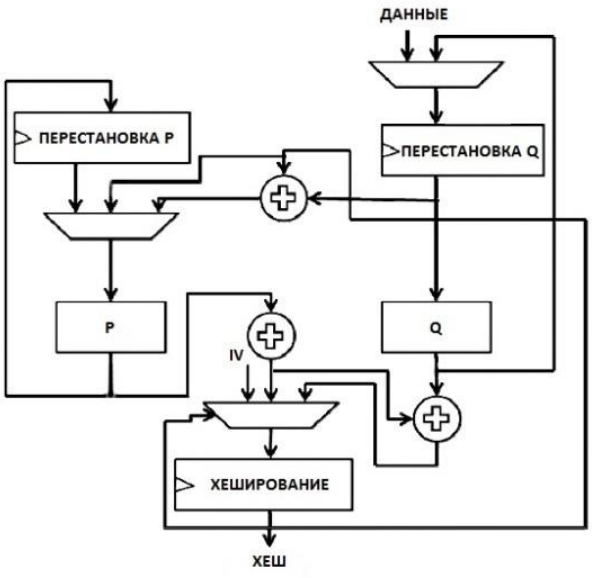


Рис. 1.3. Высокоуровневая архитектура Groestl

1.5.3 Алгоритм JH.

Алгоритм JH использует функцию сжатия. Сообщение разбивается на блоки по 512 бит (хеш-значение может иметь размер 224, 256, 384 и 512 бит). Функция сжатия формирует 1024-битное значение, которое урезается до требуемого размера хеш-значения. На вход функции сжатия поступают 512-битные блоки сообщения, а на этапе финализации – 1024-битное выходное значение после обработки предыдущего блока H_{i-1} [68]. Для обработки первого блока используется значение вектора инициализации IV (рис. 1.4).

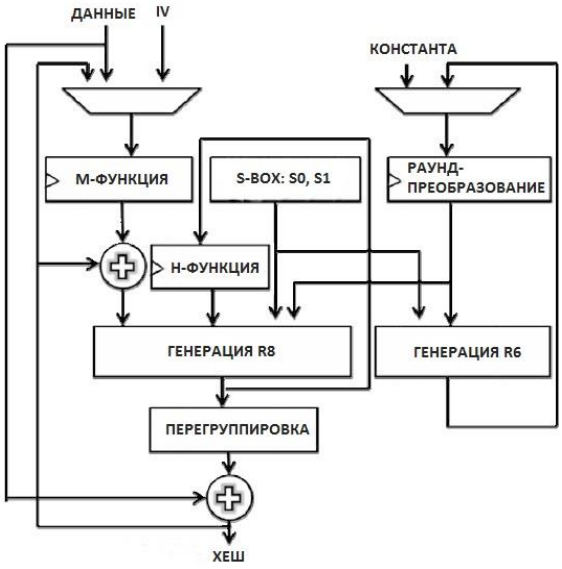


Рис.1.4. Высокоуровневая архитектура *JH*

Функция сжатия выполняет следующие действия. Обрабатываемый блок сообщения M_i складывается по модулю два с левой 512-битной половиной значения H_{i-1}. Результат предыдущей операции обрабатывается функцией преобразования E. Сообщение M_i складывается по модулю два с правой половиной 1024-битного выходного значения функции E. В результате получается значение H_i. Выходное 1024-битное значение функции E представляется в виде восьмимерного массива, каждое измерение которого содержит два слова по четыре бита. В основе E функции лежит блочный шифр, который представляет собой *SPN* преобразование на основе подстановок и перестановок и состоит из 35 раундов. В каждом раунде используются: замена с помощью двух S-блоков $S0$ или $S1$; линейное преобразование, поочередно обрабатывающее по два слова состояния с помощью операций *XOR* над определенными битами входных слов; перестановка слов состояния.

1.5.4 Алгоритм Skein.

Функция хеширования Skein благодаря использованию нового класса блочных шифров TBC (Tweakable Block Ciphers) в совокупности с уникальной блочной итерацией (UBI) и возможностью использовать выборочную систему параметров обладает широким набором свойств. Данный подход позволил реализовать множество режимов работы, таких как: простая хеш-функция, функция древовидного хеширования, *MAC*-код, в качестве составной части HMAC. Skein поддерживает рандомизированное хеширование, использование в цифровых подписях, в качестве функции вычисления производных ключей (KDF), ключа из пароля (PBKDF), в качестве генератора псевдослучайных чисел (PRNG), в качестве потокового шифра [69]. Использование настраиваемого блочного алгоритма шифрования с UBI режимом гарантирует, что каждый блок будет обработан с использованием уникальной функции сжатия. В отличие от псевдослучайных функций (Pseudo Random Function – PRF) в конструкции функций сжатия псевдослучайные перестановки (Pseudo Random Permutation – PRP), используемые в блочных шифрах, позволяют получить более быструю реализацию (достаточно использовать шифр с размером блока и размером ключа 512 бит и можно будет получить функцию сжатия $m \to n\,(m > n)$). Часто конструкция блочного шифра обусловливает использование облегченного или слабого ключевого расширения. Потенциально это позволяет реализовать атаки со связанными ключами, что ослабляет надежность функции сжатия на основе блочного шифра [70]. Идеальная функция «разворачивания ключа» для идеального блочного шифра должна обладать свойствами идеальной псевдослучайной функции.

Skein защищена от новых видов специфических атак на хеш-функции – подбор удлиненных сообщений, псевдоколлизии. Вместо выбора разных схем и стандартов, изучения особенностей их применения, работы и реализации разработчикам криптоприложений можно использовать Skein и Keccak с различными параметрами. Традиционное построение хеш-функций основано на

использовании функции сжатия. Эта функция отображает значение $m \to n\,(m > n)$ псевдослучайным образом. При этом значение n должно быть до 512 бит, а m – порядка $2n$. Повторяя эту функцию в течение нескольких раундов с различными константами, достигают нужного значения стойкости. Дополняя и сцепляя между собой блоки от разных фрагментов исходного текста, получают возможность вычислить хеш от сообщения произвольной длины. Такой метод является алгоритмически сложным. Многораундовые повторения сглаживают дефектность, но наличие быстрой возможности найти частичную коллизию в исходной функции сжатия не гарантирует стойкость всей конструкции (рис. 1.5).

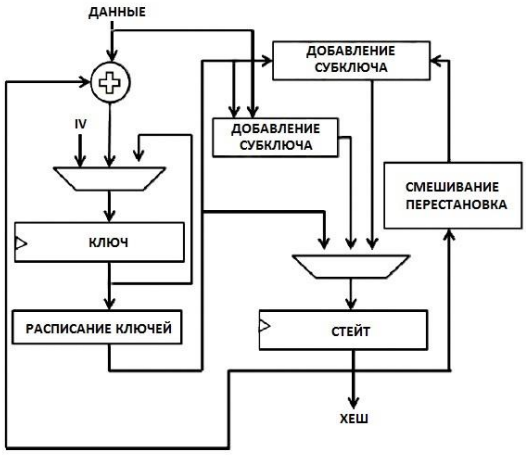


Рис. 1.5. Высокоуровневая архитектура Skein

1.5.5 Алгоритм Keccak.

Авторы алгоритма Keccak («Кеччак») утверждают, что сконструировать надежную функцию сжатия вида $m \to n\,(m > n)$ как одноraундовый блок криптопримитива не представляется возможным. В Keccak в качестве стойкого криптопреобразования вместо функции сжатия была реализована бесключевая PRF [71]. Архитектурой всего алгоритма является конструкция Sponge (англ. Spongeconstruction), относящаяся к классу алгоритмов с конечным внутренним состоянием, на вход которой поступает двоичная

строка произвольной длины и которая возвращает двоичную строку также произвольной длины $f:\{0,1\}\wedge n\to\{0,1\}^{\wedge *}$ [71]. Губка является обобщением хеш-функций, потоковых и блочных шифров, генераторов псевдослучайных чисел, имеющих произвольную длину входных данных. Простое добавление секретного ключа на вход хеш-функции Keccak превращает ее в код аутентификации сообщений. Это было невозможно в обычных хеш-функциях *SHA*-1 или *SHA*-2 и требовало громоздкой конструкции HMAC. Рассмотрим архитектуру алгоритма Keccak.

Инициализация. Массив из 5×5 строк, указывающих в направлении ось z. В официально представленной версии число двоичных элементов в строке z определено для вычислений на 64-разрядных процессорах как $w=64$ [71]. Таким образом, состояние содержит $b=5\times5\times64=1600$ бит. Строка S из $5\times5\times w$ бит сопоставлена с b битами состояния a следующим образом [71]:

$$s\left[w\left(5\times y+x\right)+z\right]=a\left[x\right]\left[y\right]\left[z\right]. \qquad (1.3)$$

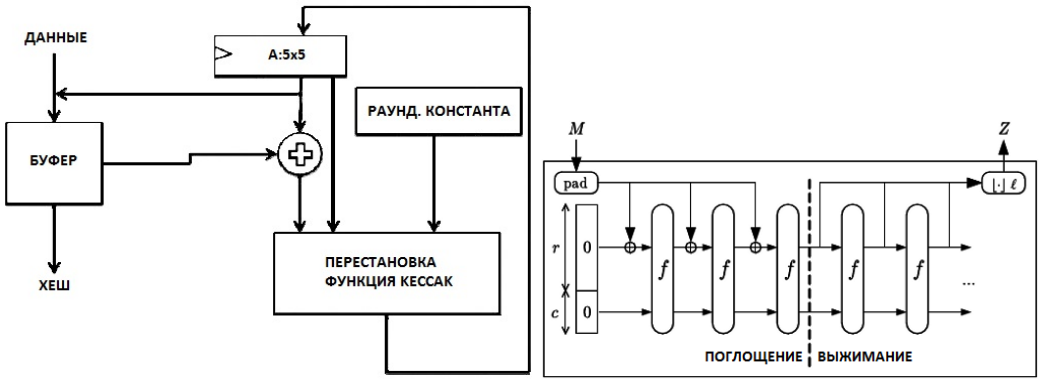
На фазе инициализации блок данных размера b заполняется нулями, а входные данные M разбиваются на блоки размера r. Исходное сообщение M дополняется до размера блока, равного части блока $b=r+c$.

Смежные b биты в состоянии могут быть разделены между «внешней частью» (первые r бит) и «внутренней частью» (переменное значение c бит). Значение c выбирается как $2N$, где N – размер выходных данных, сгенерированных алгоритмом.

Фаза «поглощения». В фазе «поглощения» выполняется операция *XOR* очередного блока исходного сообщения с первой частью состояния размерностью r бит, оставшаяся часть состояния, размерностью c бит, остается незатронутой. Результат операции и нетронутая часть передаются на вход функции *Keccak-f* – многораундовой бесключевой псевдослучайной перестановки и повторяется до исчерпания блоков исходного сообщения. Рассмотрим конструкцию многораундовой перестановки:

Хеш-функция Keccak-f. Функция f в алгоритме Keccak, представленная на рис. 6, *б*, удовлетворяет требованиям безопасности к хеш-функции. Количество раундов $R(p)$ увеличивается на размер w в соответствии с формулой $p = 12 + 2 * l$, где $l = \log 2(w)$. При $w = 64$ количество $R(p) = 24$. Каждый раунд состоит из пяти перестановок состояния:

$$R = \theta \circ \rho \circ \pi \circ \chi \circ \iota . \quad (1.4)$$



а *б*

Рис. 1.6. Высокоуровневая архитектура Keccak – *а*;
конструкция «губка» – *б*

Перестановка θ. Первая перестановка конструкции «губка» обеспечивает диффузию. Значение каждого бита в матрице состояния рассчитывается как *XOR* между суммами (над полем *GF* (2)) двух других рядов и собственного значения бита:

$$a[x][y][z] = a[x][y][z] + \sum_{y'=0}^{4} a[x-1][y'][z] + \sum_{y'=0}^{4} a[x][y'][z-1]. \quad (1.5)$$

Перестановка ρ. Перестановка выполняет вращение строк в состоянии с помощью предопределенной константы. Для каждого бита в состоянии в раунде *n* имеем:

$$a[x][y][z] = a[x][y][z + T(n)]. \quad (1.6)$$

Перестановка π. Перестановка при $x = y'$ и $y = 2x' + 3y'$ упорядочивает строки следующим образом:

$$a[x][y][z] = a[x'][y'][z]. \quad (1.7)$$

Перестановка χ. Перестановка является единственной нелинейной функцией. Без нее функция *Keccak-f* была бы линейным отображением над GF(2) [37]. Перестановка χ применяется к каждой строке состояния, что практически реализует известную конструкцию *S-boxes* для каждой строки состояния:

$$a[x][y][z] = a[x][y][z] + \left(a[x][y][z+1] \wedge a[x][y][z+2]\right). \quad (1.8)$$

Перестановка ι. Перестановка предназначена для внесения асимметрии в конструкцию за счет добавления раундовых констант, что нивелирует свойства инварианта и позволяет избежать трансляции, тем самым предупреждая слайд-атаки, использующие симметрию [71].

Фаза «выжимания». В этой фазе состояние S подается на функцию f, после чего часть $S1$ подается на выход. Эти действия повторяются, пока не будет получена последовательность нужной длины (длины хеша). Последние биты зависят от входных блоков лишь опосредованно и не выводятся в ходе фазы «выжимания».

Атаки на нахождение коллизий и вторых прообразов имеют важное практическое и теоретическое значение, но наряду с неинвертируемостью не обеспечивают полной оценки стойкости хеш-функции. Существует класс атак, связанных с практическими и теоретическими уязвимостями конструкций хеш-функций: атаки на удлинение сообщения, атаки на частичные коллизии с подобранным префиксом и др. Для доказуемой стойкости функции «губка» авторами Keccak был предложен критерий «случайного оракула» (Random Oracle) – идеализированной функции, описывающей работу идеального автомата с практически бесконечным объемом памяти, который на любой запрос выдает идеально случайное число и запоминает пару «запрос-ответ».

При повторе запроса ответ не генерируется, а выдается из ранее сгенерированного массива. Если функция *Keccak-f* с пятью многораундовыми перестановками идеальна, то хеш-функция доказуемо неразличима с RO. Неразличимость хеш-функции со случайным оракулом считается единственным и достаточным критерием стойкости. Данное утверждение позволило обосновать использование хеш-функции Keccak в качестве практически универсального криптопримитива.

Если перед блоками сообщения ввести блок с секретным ключом K, то получится код аутентификации сообщения. Практический интерес представляет возможность вычисления MAC-кода в параллельном режиме.

Ранее считалось, что такие параллельные режимы возможны только для блочных шифров (*OCB, GCM*) или при использовании громоздкого режима древовидного хеширования.

В работе [72] предложен способ параллельного вычисления MAC-кода на основе конструкции «губка» (рис. 1.7). Ключ объединяется с вектором инициализации (Nonce) и подается на вход множества параллельных конструкций, где предварительно объединяется еще и со значением счетчика каждой конструкции. Возможность использовать Keccak в параллельном режиме существенно упрощает создание протоколов, требующих шифрования с аутентификацией, и избавляет от множества потенциальных ошибок в их проектировании и реализации. Это является более стойкой альтернативой патентованным и легкоуязвимым при неправильном исполнении режимам аутентифицированного шифрования на блочных шифрах (OCB, GCM). Keccak (в отличие от Skein) не содержит в своей основе блочный шифр и поэтому не является универсальным, но может использоваться в протоколах, где нужно использовать блочный шифр в режиме счетчика. Фактически Keccak может работать в четырех режимах: MAC-код, потоковый шифр, потоковый шифр с произвольным доступом, генерация симметричных ключей из паролей.

Keccak так же универсален, как и Skein, но область его применения может быть шире. При необходимости этот алгоритм может быть внедрен как в миниатюрные устройства с ограниченными ресурсами, так и на высокопроизводительные серверы, работающие с большим объемом соединений.

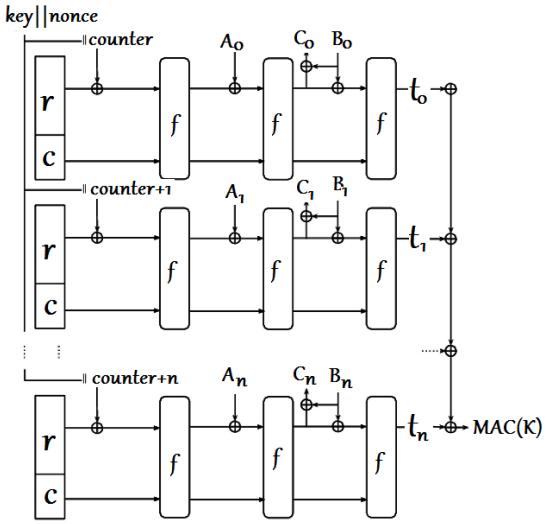


Рис. 1.7. Параллельное вычисление Keccak-*MAC*

Оба алгоритма имеют самую сильную доказательную базу среди всех финалистов, но по оценкам Keccak имеет более строгие доказательства в модели *RO*. В частности, он не подвержен атакам на функции конструкции NarrowPipe. Нерешенными вопросами остается оптимизация данных алгоритмов выявления оптимального количества раундов хеш-функции.

1.6 Коллизионные свойства MAC-кодов универсального хеширования

Идея универсального хеширования была предложена Картером и Вегманом для построения коллизионно стойких и высокоскоростных кодов аутентификации [28,29]. Универсальные семейства хеш-функций характеризуются прозрачными комбинаторными свойствами и имеют доказуемую стойкость. Основные определения универсальных классов и

свойства комбинаторных схем рассмотрены в работах [73,74] и обобщены в работах [75,76].

Определение 1.8. $(N; n, m)$ хеш-семейство есть множество из N функций H такое, что $h: A \to B$, где $h \in H$, $|A| = n$ и $|B| = m$, $n \geq m$.

Определение 1.9. $(N; n, m)$ хеш-семейство является ε-универсальным, если для любых двух различных элементов $x_1, x_2 \in A$ существует самое большее εN функций $h \in H$ таких, что $h(x_1) = h(x_2)$. Аббревиатура $\varepsilon - U$ используется для обозначения ε-универсальных хеш-функций.

Очевидно, если h выбирается случайно из заданного $\varepsilon - U(N; n, m)$ хеш-семейства, то вероятность коллизии хеш-значений для двух разных входных сообщений $x_1, x_2 \in A$ не превышает ε:

$$\Pr h \in H\left[h(x_1) = h(x_2)\right] \leq \varepsilon.$$

Первоначальное определение универсальных хеш-функций Картера и Вегмана было предложено для $\varepsilon = 1/m$. Следующее определение является обобщением предыдущего.

Определение 1.10. H является ε–почти универсальным семейством хеш-функций $(\varepsilon - AU(N; n, m))$, если $\Pr h \in H\left[h(x_1) = h(x_2)\right] \leq \varepsilon$, для $x_1, x_2 \in A$, $x_1 \neq x_2$, $1/m < \varepsilon \leq 1$.

Следующие определения определяют классы хеш-функций строгой универсальности.

Определение 1.11. H является ε – строго универсальным семейством хеш-функций $(\varepsilon - SU(N; n, m))$, если для всех $x_1, x_2 \in A$, $x_1 \neq x_2$ и всех $a, b \in B$, $\Pr h \in H\left[h(x_1) = a, h(x_2) = b\right] = \varepsilon$, $\varepsilon = 1/|B|$.

Определение 1.12. H является ε – почти строго универсальным семейством хеш-функций $(\varepsilon - ASU(N; n, m))$, если для всех $x_1, x_2 \in A$, $x_1 \neq x_2$ и всех $a, b \in B$, $\Pr h \in H\left[h(x_1) = a, h(x_2) = b\right] \leq \varepsilon$.

Одним из наиболее известных универсальных семейств хеш-функций является PolyCW хеширование (polynomial Carter-Wegmanhashing) [28]. Главное свойство PolyCW функции определено фундаментальной теоремой алгебры: многочлен отличный от нуля, степени не меньше k, имеет не меньше k корней. Вероятность коллизии для полиномиальной хеш-функции ограничивается отношением k/q, где q – простое число, определяющее поле Z_q для вычисления многочленов. Множество ключей определяется значением q. Чем больше размер ключевого пространства, тем большее количество слов можно хешировать до достижения допустимой вероятности коллизии. При увеличении q возрастают временные затраты на вычисление хеш-значений в Z_q. При движении q от 232 к 264 временные затраты увеличиваются в два раза. Ограничения, связанные с вычислениями в больших полях Z_q, частично снимаются в конструкции сползающего полиномиального хеширования RPHash (ramped polynomial hashing), использованного в UMAC алгоритме [77,78]. В соответствии со спецификацией UMAC размер поля вычисления хеша Z_q возрастает по мере увеличения длины сообщения. Недостаток RP хеширования заключается в том, что вероятность коллизии возрастает линейно с ростом длины сообщения и ее уменьшение возможно путем ограничения длины хешируемого сообщения или увеличения размера поля вычисления хеша Z_q.

Еще одним подходом, снижающим противоречие между вычислительными затратами в больших полях и необходимостью обеспечить на большой длине сообщения малое значение вероятности коллизии, является применение универсального хеширования по алгебраическим кодам [53]. Связь между универсальным семейством хеш-функций и кодовыми схемами впервые была отмечена Биербрауэром, Джохансоном, Кабатиански и Смитсом [31]. В схемах с алгебраическими кодами (n, k, d) вероятность коллизии

определяется значением $1-d/n$. Для известных к настоящему времени кодов вероятность коллизии ограничивается, в лучшем случае, значением, обратно пропорциональным квадрату размерности поля Z_q.

В работе [80] представлен универсальный класс с кодами Рида – Соломона (Rsh), эквивалентный полиномиальному хешированию. Отличие заключается в том, что вычисление хеш-кода может быть реализовано не только в конечном поле простого числа, но и в расширенном поле Галуа. В ряде случаев это может быть более предпочтительным, так как упрощается разбиение сообщения на слова, которые должны быть приведены к размеру поля вычисления хеша. Наиболее приемлемыми значениями q для хеширования данных, которые лежат в диапазоне разрядности современных процессоров, являются 2^{32} и 2^{64}. Вероятность коллизии возрастает линейно с возрастанием объемов данных. Для вероятности коллизии в диапазоне значений $10^{-3}\left(2^{-10}\right) \div 10^{-9}\left(2^{-30}\right)$ размер хешируемых данных должен лежать в диапазоне $2^3 \div 2^{22}$ 32-разрядных слов.

При RSh хешировании вычисление MAC-кодов в конечном поле Fq реализуется выражением

$$h_x(m) = \sum_{i=0}^{k} m_i \cdot x_i ,$$

где x – ключевое слово, $m = (m_1, m_2, \ldots, m_k)$ – сообщение, $x, m_i \in F_q$, k – объем сообщения, $k < q$ и определяет $\dfrac{k-1}{q}$ – $U(q; q_k, q)$ семейство хеш-функций $\left(RSh_q\right)$.

В случае, когда $q = p$, где p – простое число, вычисление хеш-кодов в простом поле определяется модулярной арифметикой.

Вычисление RSh_q хеш-функции можно осуществить по итерационной схеме Горнера с одной операцией умножения и сложения в конечном поле на

каждом шаге. Лучший результат достигается в арифметике $Z_p(w)$ при как можно большом простом числе $p(w) \le 2w$. Итерационная схема Горнера вычисления хеш-функции предполагает вычисление

$$y \leftarrow xy + m \cdot \bmod p(w). \tag{1.9}$$

Как следует из анализа зависимостей вероятности коллизии от значения поля вычислений, размер конечного поля F_q должен быть как можно большим. Применение *ASM* операции $\bmod p(32)$ потребует 12.4*cpb* (циклов процессора на байт).

Можно использовать более эффективный алгоритм для вычисления $y \leftarrow xy + m \cdot \bmod p(w)$ [77]. Простой модуль $p(w)$ можно представить в виде $p(w) = 2^w - c$. Используя представление $xy = a2^w + b$ и учитывая, что $a \cdot 2^{32} = ca$ в $Z_p(w)$, получим

$$y = xy + m \cdot \bmod p(w) = ca + b + m \cdot \bmod p(w). \tag{1.10}$$

Из анализа последнего выражения следует, что при вычислениях на одном шаге итерации значения *y* потребуется одно умножение и два сложения на w разрядных регистрах и несколько команд, которые позволяют контролировать выход результата вычислений за пределы диапазона представления чисел в $Z_p(w)$. Недостатком отмеченного высокоскоростного алгоритма вычислений является уменьшение ключевого пространства до величины $d = 2^w / c$ и увеличение вероятности коллизии до $k2^{-d}$.

Для максимального значения модуля $p(32) = 2^{32} - 5$ эффективный алгоритм использует восемь строк ассемблерной программы и достигает производительности 3.69*cpb* [77]. Уменьшение ключевого пространства приводит к величине $2^{32}/5 = 2^{29}$ и увеличению вероятности коллизии до $k2^{-29}$. Практическая схема эффективного алгоритма вычисления *Rshp* хеша должна включать еще одно дополнительное преобразование. Векторы чисел с

w битами, которые имеют элементы вне диапазона представления $Zp(w)$, необходимо преобразовать в вектор, который их не имеет, с помощью так называемого двойного представления, как это сделано в UMAC алгоритме. Это приведет к удвоению размера данных и к увеличению вероятности коллизии до $k2^{-(d-1)}$ соответственно, снизится скорость вычислений. Так, по оценкам разработчиков UMAC алгоритма, скорость вычислений для $p(32)$ снижается до значения $3.86cpb$ [77].

Дальнейшее повышение разрядности регистров вычисления *RShp* хеш $p(w)$ за значение $w-32$ приводит к значительному снижению скорости вычислений. Так, реализация *RShp* хеш-функции для $p(64)=2^{64}-59$ имеет вероятность коллизии $k2^{-49}$, использует 40 строк ассемблерной программы и имеет пиковую производительность $6.8cpb$ [79]. Снижение скорости вычислений всего в два раза определяется тем, что авторы использовали MMX технологию, которая основана на четырехвекторном представлении 16-разрядных данных и соответствующих командах скоростного умножения.

В работе [79] представлены результаты увеличения вероятности коллизии от используемых модулей. Анализ показывает, что уменьшение ключевого пространства достигает величины $\approx 2 \div 3$ бит и приводит соответственно к увеличению вероятности коллизии в $2^2 \div 2^8$ раз в зависимости от используемого модуля.

Линейное возрастание вероятности коллизии для *RShp* хеширования ограничивает размер хешируемого сообщения. Чем больше размер ключевого пространства, тем большее количество слов можно хешировать до достижения допустимой вероятности коллизии. Мощность множества ключей определяется значением простого числа $p(w)$, определяющего поле $Z_p(w)$. При увеличении $p(w)$ возрастают временные затраты на вычисление

многочленов в $Z_p(w)$. При движении $p(w)$ от 2^{32} к 2^{64} временные затраты увеличиваются в два раза.

Арифметика $GF(2w)$ менее удобна для современных микропроцессоров, хотя обеспечивает легкое разделение хешируемых битовых строк на w битовые подстроки. При этом отсутствуют потери по вероятности коллизии и по объему ключевых данных, которые возникают при хешировании в арифметике $Z_p(w)$.

Вычисление RSh хеш-кодов определяется выражением (1.9) в расширенном конечном поле F_q характеристики $p=2$, так же, как и в $Z_p(w)$, реализуется по схеме Горнера $y \leftarrow xy+m$. Ключевым моментом данной схемы есть вычисление произведения элементов поля $GF\left(2^w\right)$. Известно несколько эффективных алгоритмов быстрого умножения в $GF\left(2^w\right)$, ориентированных на табличное умножение элементов поля или являющихся модификациями схемы Монтгомери.

Практические схемы хеширования должны включать классы хеш-функций с большим коэффициентом сжатия для данных возможно очень большого объема. Для этих целей интерес представляют семейства хешей на основе длинных алгебраических кодов. Длинные алгебраические коды реализуются в классе кодов по алгебраическим кривым [80]. В основу кодирования положено отображение векторного пространства Римана – Роха над конечным полем рациональных функций по точкам алгебраической кривой. Применение скалярного произведения по рациональным функциям алгебраических кривых определяет метод универсального хеширования. Алгебраические кривые с большим числом точек и плотно упакованным по полюсам функциональным полем рациональных функций реализуют наилучшие результаты универсального хеширования. Универсальное хеширование по кодам Рида – Соломона в алгеброгеометрической

интерпретации определяется как хеширование по проективной прямой; в параметрической интерпретации является полиномиальным хешированием.

Параметрически более сложными кривыми являются максимальные кривые, кривые Судзуки и кривые Ри. Кривые имеют наименьшие отношения значения полюса рациональных функций к числу точек, что определяет наименьшее значение вероятности коллизии в схеме универсального хеширования, и являются наилучшими для применения.

1.7 Формулировка задач исследований

Анализ методов универсального и строго универсального хеширования показывает, что решение задачи построения коллизионно стойких функций хеширования и ключевых функций хеширования, удовлетворяющих международным требованиям гарантированной стойкости к атакам, сложности и скорости вычисления, характеристикам и реализациям алгоритма, возможно в теории доказуемо стойкой аутентификации. Основные положения теории аутентификации определены в [28,81]. Научная задача построения доказуемо стойкой аутентификации впервые сформулирована в [81]. Решение этой задачи было предложено в классе универсальных хеш-функций как аутентификации с максимальной теоретически достижимой секретностью. Идеи универсальной аутентификации получили развитие в теории безусловной аутентификации с использованием строго универсального хеширования [32,74,75].

Основное противоречие доказуемо стойкой аутентификации состоит в том, что для обеспечения гарантированной вероятности обмана на уровне нижней границы размер ключа должен быть не меньше размера сообщения, а фиксирование размера ключа на нижней границе определяемой мощностью пространства хешей приводит к пропорциональному росту вероятности коллизии от длины данных. На практике это означает, что для

аутентификации с секретностью на нижней границе $P_{\text{col}} = 1/|B|$ ($|B|$ – мощность пространства хеш-кодов) по закрытому каналу связи следует передавать ключевых данных больше, чем по открытому – информационных данных.

Анализ методов универсального хеширования показывает, что основными путями разрешения этого противоречия являются универсальное хеширование на основе алгебраического кодирования по линейному векторному пространству Римана – Роха, построенному по рациональным функциям функционального поля, ассоциированного с алгебраической кривой на проективном многообразии ее точек. Основной результат определяется тем, что вероятность коллизии следует из отношения значения полюса рациональных функций функционального поля к числу точек алгебраической кривой. Вероятность коллизии связывается с длиной сообщения, ключа и полем вычисления хешей, а также с функциональным полем алгебраической кривой. Ключевое пространство определяется числом точек алгебраической кривой. Выбор алгебраической кривой и ассоциированного с ней функционального поля позволяет оптимизировать затраты на аутентификацию.

Наилучший результат в отношении значения полюса рациональных функций к мощности точек кривой получен для кривых Судзуки. Цель работы –разработка метода универсального хеширования по кривой Судзуки для построения доказуемо стойкой аутентификации.

Функция цели (Z) состоит в обеспечении гарантированной вероятности коллизии P_{col} функции хеширования, минимизации затрат на ключевое пространство $|K|$, сложности вычислений $N_{\text{выч}}$ в условиях фиксированной длины сообщений $\log|M|$, поля вычисления F_q характеристики 2 нечетной степени расширения и проективного многообразия по кривой Судзуки $F_q(C)$:

$$Z = \min\{P_{\text{col}}, |K|, N_{\text{выч}}\} | \log|M| = fix, F_q(C) = \text{var}. \qquad (1.11)$$

Научная задача состоит в разработке метода универсального хеширования по рациональным функциям алгебраической кривой Судзуки для построения доказуемо стойкой аутентификации сообщений с обеспечением гарантированной вероятности коллизии и минимизацией затрат на ключевое пространство, размер хеш-кода и сложность вычислений.

Для достижения цели следует решить следующие частные задачи:

1) провести анализ методов построения *MAC*-кодов универсального и строго универсального хеширования;

2) разработать метод универсального хеширования по рациональным функциям алгебраической кривой Судзуки;

3) разработать метод скоростного универсального хеширования по кривой Судзуки на основе применения схемы вычисления Горнера;

4) разработать метод универсального хеширования с ограничением функционального поля алгебраических кривых с уменьшенной сложностью вычислений;

5) разработать метод каскадного универсального хеширования по кривой Судзуки на основе произведения функциональных полей;

6) разработать практические рекомендации по применению универсального хеширования по кривой Судзуки.

1.8 Выводы

Увеличение доступной вычислительной мощности, распределенные вычисления и удешевление стоимости обусловливает отказ от коммерческого использования криптографических стандартов 90-х (MD5, SHA-1). Практическая реализация классических конструкций на процессорах и архитектурах нового поколения ведет к увеличению уязвимостей. Особенности атрибутов конструкций хеш-функций оказывают все большее влияние на безопасность и производительность в конечной реализации. В

данной связи актуальной становится разработка криптопримитивов с учетом новых требований к коллизионной стойкости и безопасности, производительности и практической реализации хеш-функций с использованием новых конструкций в целях снижения уязвимости к атакам. Новое поколение криптопримитивов поддерживает различные комбинации исходных параметров без использования дополнительных средств. Перспективным направлением исследований является применение универсальных семейств хеш-функций, характеризующихся прозрачными комбинаторными свойствами и имеющих доказуемую стойкость. Одним из наиболее известных универсальных семейств хеш-функций является PolyCW хеширование, недостатком которого является существенное увеличение временных затрат на вычисление хеш-значений. Существующие практические реализации универсального хеширования (UMAC) частично снимают ограничения, связанные с вычислениями в больших полях. Одним из подходов, снижающим противоречие между вычислительными затратами в больших полях и необходимостью обеспечить на большой длине сообщения малое значение вероятности коллизии, является применение универсального хеширования по алгебраическим кодам.

РАЗДЕЛ 2

ДОКАЗУЕМО СТОЙКАЯ АУТЕНТИФИКАЦИЯ НА ОСНОВЕ МЕТОДОВ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ

Построение доказуемо стойкой аутентификации определяется классами универсальных хеш-функций с прозрачными комбинаторными свойствами. Универсальное хеширование связывается с распределениями хешей для сообщений по ключевому пространству, что определяет аутентификацию со счетчиком на массивах аутентификаторов. Аутентификация со счетчиком предполагает применение сеансового ключа для каждого MAC-вычисления. Коллизионные оценки почти строго универсального хеширования связываются с распределениями хешей для пар сообщений по ключевому пространству, что определяет безусловную аутентификацию на массивах аутентификаторов.

Разработка методов универсального хеширования лежит в плоскости оптимизации затрат ключевого пространства при хешировании данных фиксированной длины и вероятности коллизии. Таким образом, задачей является сравнение методов универсального хеширования для построения доказуемо секретной аутентификации. Классификация методов универсального хеширования представлена в подразделе 2.1 по результатам работ [28,32,74,75]. Безусловная аутентификация на основе строго универсального хеширования рассмотрена в подразделе 2.2. Определение универсального хеширования на основе алгебраического кодирования по рациональным функциям алгебраических кривых, свойства универсальных хеш-функций, асимптотические границы для вероятности коллизии представлены в подразделах 2.3, 2.4.

2.1 Классификация методов универсального хеширования

Коды аутентификации сообщений в представлении Картера – Вегмана определяются семейством хеш-функций [28]. Массив значений MAC-кодов состоит из N строк, n столбцов, элементы принимают одно из m значений. Каждая функция $f \in H$ определяется значением используемого ключа, связывается со строкой и определяет правило отображения элементов множества X (номеров столбцов массива) в элементы Y (собственные значения элементов массива).

Определение MAC-кода с учетом секретности имеет следующий вид.

Определение 2.1. [84]. MAC-код $f : A \to B$ является $(t; \varepsilon; q)$ секретным, если при случайно взятом ключе k противник не может подделывать новое сообщение за время t с вероятностью больше чем ε, если ему предоставлены значения q MAC-кодов других сообщений по его выбору.

Замечание 2.1.

1. Представление MAC-кодов в виде массива значений позволяет рассматривать статистические распределения аутентификаторов на пространстве $A \times B$, что в свою очередь связано с коллизионными характеристиками;

2. Для точного вычисления имитационной и коллизионной стойкости MAC-кодов необходимо использовать статистику совместных распределений MAC-кодов по ключам для исходных и навязываемых сообщений. Для практических MAC-кодов знание такой статистики выглядит проблематичным из-за чрезвычайно больших размеров массива аутентификаторов;

3. Нижние границы для вероятности подмены определяются мощностью пространства ключей и MAC-кодов, не учитывают статистические свойства массивов аутентификаторов. Требования к вероятности подмены определяют

минимальные требования к размеру ключевого пространства и пространства MAC-значений;

4. Верхние границы для вероятностей имитации и подмены связаны с комбинаторными свойствами MAC-массивов и определяют значения вероятности коллизий на пространстве $A \times B$ для наихудшего случая выбора ключей и сообщений.

Коллизионные оценки почти универсального хеширования связываются с распределениями хешей для сообщений по ключевому пространству, что определяет аутентификацию со счетчиком на массивах аутентификаторов. Аутентификация со счетчиком предполагает применение исключительного сеансового ключа для каждого MAC-вычисления.

Универсальное хеширование реализуется на основе следующих методов:

– скалярного произведения;

– полиномиального хеширования;

– хеширования на основе алгебраических кодов;

– скалярного произведения по рациональным функциям алгебраических кривых.

2.1.1 Универсальное хеширование на основе скалярного произведения.

Хеш-вычисление y над конечным полем F_q определяется функцией вида

$$y = \sum_{i=1}^{k} x_i m_i , \qquad (2.1)$$

где $y, x_i, m_i \in F_q, m_i$ – слова сообщения;

x_i – слова ключа;

k – число слов сообщения.

Замечание 2.2.

1. Хеш-функция на основе скалярного произведения определяет хеш-класс $\varepsilon - U\left(q^k, q^k, q\right)$ с вероятностью коллизии $\varepsilon = 2/q$;

2. Реализуется доказуемо секретная аутентификация с максимальной теоретически достижимой секретностью;

3. Недостатком универсального хеширования (2.1) является требование – размер ключевого пространства должен быть не меньше пространства сообщения.

Ограничение на размер ключевого пространства снимается в методе полиномиального хеширования.

2.1.2 Полиномиальное универсальное хеширование.

Полиномиальное универсальное хеширование (polynomial Carter–Wegman hashing) предложено для снятия ограничения на пространство ключей.

Полиномиальное хеширование y над конечным полем F_q определяется функцией вида

$$y = \sum_{i=1}^{k} m_i x^i \qquad (2.2)$$

где $y, x_i, m_i \in F_q, m_i$ – слова сообщения,

x – ключевое слово,

k – число слов сообщения $k < q$.

Замечание 2.3.

1. Хеш-функция на основе полиномиального вычисления определяет хеш-класс $\varepsilon - U\left(q, q^k, q\right)$ с вероятностью коллизии $\varepsilon = k/q$. Вероятность коллизии для полиномиальной хеш-функции ограничивается отношением k/q, где q – простое число, определяющее поле F_q. Значение ε определяется

фундаментальной теоремой алгебры: многочлен отличный от нуля, степени не меньше k, имеет не меньше k корней;

2. Множество ключей определяется значением q. Чем больше размер ключевого пространства, тем большее количество слов можно хешировать до достижения допустимой вероятности коллизии;

3. Вычисление хеш-кодов в простом поле определяется модулярной арифметикой. Хеш-функцию (2.2) можно вычислить по итерационной схеме Горнера с одной операцией умножения и сложения в конечном поле на каждом шаге. Лучший результат достигается в арифметике Z_q при как можно большом простом числе $q < 2^w$.

Как следует из анализа зависимостей вероятности коллизии от значения поля вычислений, размер конечного поля F_q должен быть как можно большим;

4. Практическая схема эффективного алгоритма хеш-вычисления должна включать еще одно дополнительное преобразование. Векторы чисел с w битами, которые имеют элементы вне диапазона представления Z_q, необходимо преобразовать в вектор, который их не имеет, с помощью так называемого двойного представления, как это сделано в *UMAC* алгоритме. Это приводит к удвоению размера данных и к увеличению вероятности коллизии, и соответственно снижается скорость вычислений;

5. Арифметика над расширенным полем F_q характеристики 2 является менее удобной для современных микропроцессоров, хотя обеспечивает легкое разделение хешируемых битовых строк на w битовые подстроки. При этом отсутствуют потери по вероятности коллизии и по объему ключевых данных, которые возникают при хешировании в арифметике Z_q. Известно несколько эффективных алгоритмов быстрого умножения в F_{2^w}, ориентированных на

табличное умножение элементов поля или являющихся модификациями схемы Монтгомери.

Недостатком полиномиального хеширования является требование – размер пространства сообщений ограничивается условием для вероятности коллизии $\varepsilon = k/q$ и размером поля вычислений. Ограничение на размер пространства сообщений снимается в методе на основе алгебраического кодирования.

2.1.3 Универсальное хеширование на основе алгебраических кодов.

Хеш-значение для сообщения $m = (m_0, m_1, \ldots, m_{k-1})$, $m_i \in F_q$ определяется выражением

$$h_x(m) = \sum_{i=0}^{k-1} f_{i,x} \cdot m_i \qquad (2.3)$$

где $h_x(m) \in F_q$ и $f_{i,x}$ – значения элементов столбца x порождающей матрицы G линейного кода $(n, k, d)_q$.

Замечание 2.4.

1. Универсальное хеширование, образованное $(n, k, d)_q$ линейным кодом, определяет $1 - \frac{d}{n} - U(n, q^k, q)$ почти универсальное семейство хеш-функций;

2. Верхняя граница вероятности навязывания для универсального семейства хеш-функций на основе алгебраического кода $(n, k, d)_q$ без единицы определяется относительным кодовым расстоянием, нижняя граница – значностью кода;

3. Криптоанализ прямой атаки на универсальное семейство хеш-функций с алгебраическим кодированием при условии многократных попыток угадывания *MAC*-значений и ключей рассмотрен в [86]. Вероятность навязывания путем подмены и угадывания сообщений обратно

пропорционально зависит от значности кодовых слов и относительного кодового расстояния $(n, k, d)_q$ кода;

4. Для практической аутентификации следует использовать $(n, k, d)_q$ коды большой размерности и с большим относительным кодовым расстоянием. Наилучшим алгебраическим кодом для построения универсальных хеш-функций является код Рида – Соломона.

2.1.4 Универсальное хеширование по рациональным функциям алгебраических кривых.

Хеш-функция $h_{P_j}(m) \in F_q$ для сообщения $m = (m_1, \ldots, m_k)$, $m_i \in F_q$ в точке P_j определяется выражением

$$h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i \qquad (2.4)$$

где $f_i(P_j)$ – значение рациональной функции в точке P_j кривой χ;

$f_i \in F_q(\chi) \setminus \{0\}$ – рациональные функции функционального поля кривой χ с упорядоченными порядками полюсов $0 < \rho_1 < \rho_2 < \ldots < \rho_k$.

Хеш-функция $h_{P_j}(m)$ определяет универсальный хеш-класс $\varepsilon - U(N, q^k, q)$, где N – число точек алгебраической кривой; q^k – объем пространства сообщений; q – объем пространства хеш-кодов; $\varepsilon = \rho_k / N$ – вероятность коллизии; ρ_k – значение полюса рациональной функций f_k.

Универсальное хеширование по рациональным функциям алгебраических кривых определяется свойствами линейного базисного пространства, ассоциированного с функциональным полем кривой.

Универсальное хеширование по рациональным функциям алгебраических кривых имеет лучшие асимптотические результаты. Верхняя граница вероятности коллизии для алгеброгеометрического универсального

хеширования $\varepsilon = \rho_k / N$ определяется отношением значения полюса рациональной функции f_k к числу точек алгебраической кривой.

Проблематика построения схем универсального хеширования по рациональным функциям алгебраических кривых заключается в выборе алгебраических кривых с требуемыми параметрами.

2.2 Методы строго универсального хеширования

Строго (почти строго) универсальное хеширование определяет безусловную аутентификацию, что было представлено Стинсоном [74,75]. Коллизионные оценки почти строго универсального хеширования связываются с распределениями хешей для пар сообщений по ключевому пространству, что определяет безусловную аутентификацию на массивах аутентификаторов. В общем случае можно говорить о распределениях t сообщений, что определяет t связанную аутентификацию.

Для построения строго универсального хеширования используют методы на основе ортогональных массивов.

Ортогональным массивом $OA_{\lambda}(t, k, \upsilon)$ называется массив элементов $y_i \in Y$ со столбцами, соответствующими элементам множества X, и строками, определяемыми элементами множества m, в котором для любой выборки из t элементов $y_1, y_2, \ldots, y_t$ из Y существует только λ функций $f \in m$, для которых справедливо $f(x_i) = y_i$, $i = 1, 2, \ldots, t$, где X, Y являются множествами из k и υ элементов соответственно, и H есть множество функций, осуществляющих отображение $f : X \to Y$ [87].

Строго универсальный класс хеш-функций, построенный на ортогональном массиве силы $t = 2$, имеет параметры $\frac{k}{q^b} - SU\left(q^{a+b}, q^{ka}, q^b\right)$.

Семейство хеш-функций определяется отображением $\phi : F_{q^a} \to F_{q^b}$.

X является множеством полиномов $p(X)$, определенным над F_{q^a} степени $\le k$, без постоянного члена.

Элементы матрицы отображения $X \to Y$ на пересечении (u, υ) строки, $u \in F_{q^a}$, $\upsilon \in F_{q^b}$, и $p(X)$ столбца можно определить как $\phi(p(u)) + \upsilon = y$.

Замечание 2.5.

1. Если $k = 1$, имеем строго универсальный класс хеш-функций $\frac{1}{q^b} - SU(q^{a+b}, q^a, q^b)$. Размер ключевых данных N определяется произведением пространства аутентификаторов и пространства сообщений.

2. Для почти строго универсального хеширования снижаются требования к размеру ключевых данных, которые ограничиваются размерами поля вычислений F_{q^a} и F_{q^b}.

3. Линейное отображение $\phi: F_q^n \to F_q^m$ определяет умножение элементов в F_{q^n}, проектирование m координат $F_{q^n} \to F_{q^m}$ и сложение в F_{q^m}

2.2.1 Строго универсальное хеширование на основе почти независимых массивов.

Почти независимые массивы (almost independent arrays) были рассмотрены Куросавой, Стинсоном [88,89]. Теория почти независимых массивов снимает ограничение на равновероятное распределение наборов хешей по столбцам массива. Почти независимые массивы являются обобщением ортогональных массивов.

Пусть $(n, k)_p$ – массив, содержащий n строк, k столбцов и записи из набора p элементов. Для $\forall a \in F_p$ частота $v_a(u)$ появления значения a в столбцах массива $u = (u_1, u_2, \ldots, u_n) \in F_p^n$ удовлетворяет условию $|v_a(u)/n - 1/p| \le \varepsilon_1$, и для любых пар столбцов u, u' частота $v_{(a,a')}(u, u')$

появления в столбцах значений a и a' удовлетворяет условию $\left|v_{(a,a')}(u,u')/n-1/p^2\right|\le\varepsilon_2$. Тогда $(n,k)_p$ – массив есть семейство $\varepsilon-ASU(n,k,p)$ хеш-функций и $\varepsilon=\left(p^{-2}+\varepsilon_2\right)/\left(p^{-1}-\varepsilon_1\right)$.

Замечание 2.6.

1. Параметр ε определяется условной вероятностью появления любых записей a,a' для различных столбцов u, u' при равновероятном выборе i строки $\varepsilon=\Pr(u_i'=a'/u_i=a)$ и характеризует отклонение от равномерного распределения совместных вероятностей появления кодовых комбинаций в t произвольных столбцах случайно выбранной строки $(n,k)_p$ массива.

2. Значение параметра зависимости ε определяет вероятность коллизии МАС-кодов и в общем случае, как показано в [85], коллизионные свойства t кратных кодов аутентификации.

Практическое построение почти независимых массивов проблематично, так как нужны методы, которые позволяют формировать массивы хешей с заданными распределениями по столбцам. В этом отношении для построения строго универсальных хеш-функций более продуктивным является применение слабо смещенных массивов.

2.2.2 Строго универсальное хеширование на основе слабосмещенных массивов.

Слабосмещенные массивы рассмотрены в работах [90,91] для массивов дискретных значений большой размерности с распределением, незначительно отличающимся от равномерного. Слабосмещенные массивы определяют свойства распределений хешей в столбцах массива.

Пусть $(n,k)_p$ – массив, содержащий n строк, k столбцов и записи из набора p элементов и $0\le\varepsilon\le1$. Массив $(n,k)_p$ является ε-смещенным (ε-

biased), если любая нетривиальная линейная комбинация столбцов имеет смещение $bias \le \varepsilon$. Смещение вектора u определяется как

$$bias(u) = \frac{1}{n}\left|\sum_{i \in F_p} \delta_i(u)\xi^i\right| = \frac{1}{n}\left|\sum_{i \in F_p} v_i(u)\xi^i\right| \qquad (2.5)$$

где $v_i(u)$ – частота появления элемента i в последовательности u, $v_i(u) = \frac{n}{p} + \delta_i(u)$, где $\delta_i(u)$ – отклонение частоты $v_i(u)$ от среднего значения и $\sum_{i \in F_p} \delta_i(u) = 0$; ξ – комплексный корень p-степени из единицы.

Замечание 2.7.

1. Смещение массива является свойством F_p-линейного кода, построенного с помощью столбцов порождающей матрицы.

2. Для двоичных массивов параметр ε смещения прямо связывается с вероятностями появления 0 и 1 в столбцах массива.

3. Для строго универсального класса массив хеш-значений определяется $(n, k)_p$ массивом со смещением равным нулю [92].

Практическим методом построения слабосмещенных массивов является метод сумм экспонент Вейля – Карлитца – Ушиямы (ВКУ).

Метод сумм экспонент ВКУ определяет массив $\left(p^f,\ f*(n - n/p)\right)_p$ со смещением $bias \le (n-1)p^{-f/2}$, с записями вида $Tr\left(a_j \alpha^i\right)$, где a_j – базис поля $F_{p^f} \left| F_p \right.$, $i \le n$ и i не кратно p, $Tr : F_{p^f} \to F_p$ – след элемента $a_j \alpha^i$.

Массив аутентификаторов $(n, k)_p$ является ε почти строго универсальным ASU_2, если каждый столбец имеет смещение 0 и для двух записей e, e' одной строки в любых столбцах c, c' условная вероятность $\Pr(c_i = e \mid c_i' = e') \le \varepsilon$ и равномерное распределение номера строка i [93]. Строка

массива $(n,k)_p$ определяется значением ключа, столбец – сообщением источника и значение записи является аутентификационным тегом.

Замечание 2.8.

1. Универсальное хеширование определяется через слабосмещенные массивы, является обобщением конструкций линейных кодов, ВКУ массивов.

2. Построение ASU_2 аутентификации определяется тем, что используется специальное индексирование строк массива аутентификаторов и записей, что увеличивает пространство ключей и записей и приводит к лучшим оценкам параметров аутентификации.

2.3 Универсальное хеширование на основе алгебраического кодирования

Универсальное хеширование по рациональным функциям алгебраических кривых определяется выражением (2.3) и ассоциируется с кодовыми схемами, в основу которых положено отображение векторного пространства над конечным полем рациональных функций по точкам алгебраической кривой. Построение кодов по алгебраическим кривым впервые предложено В.Д. Гоппой [81].

Алгеброгеометрический подход имеет следующее определение [92].

Определение 2.2. Пусть

χ – алгебраическая кривая над полем F_q;

$F_q(\chi)$ – поле F_q рациональных функций на χ;

$\mathrm{Div}_q(\chi)$ – дивизор кривой χ;

$\mathrm{div}(f)$ – дивизор, ассоциированный с $f \in F_q(\chi)\setminus\{0\}$;

$L(G)$ – векторное пространство Римана – Роха, ассоциированное с $G \in \mathrm{Div}_q(\chi)$ так, что $L(G) = \{ f \in F_q(\chi) \setminus \{0\} : G + \mathrm{div}(f) \succ 0 \} \cup \{0\}$; $\ell(G) := \dim(L(G))$;

$D := P_1 + \ldots + P_n$, где $P_1, \ldots, P_n$ – рациональные точки кривой χ.

Алгеброгеометрический код $C_{D,G} := e(L(G))$, ассоциированный с D и G, определяется как F_q – линейное отображение вида $e = e_{P_1,\ldots,P_n} : L(G) \to F_q^n$:

$$f \to (f(P_1), \ldots, f(P_n)). \tag{2.6}$$

Лемма 2.1 [92]. Пусть $k := \dim(C_{D,G})$ и d – минимальное расстояние кода $C_{D,G}$. Тогда 1) $k = \ell(G) - \ell(G - D)$, 2) $d \geq n - \deg(G)$.

Следствие 2.1 [92]. Пусть $C_{D,G}$ – алгеброгеометрический код с параметрами k и d. Пусть g – род алгебраической кривой.

1. Если $n > \deg(G)$, тогда $k = \ell(G)$. В случае $k \geq \deg(G) + 1 - g$ имеет место $d + k \geq n + 1 - g$. Порождающая матрица $C_{D,G}$ имеет вид

$$M = \begin{vmatrix} f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\ f_2(P_1) & f_2(P)_2 & \ldots & f_2(P_n) \\ \vdots & \vdots & \ldots & \vdots \\ f_k(P_1) & f_k(P_2) & \ldots & f_k(P_n) \end{vmatrix},$$

где $f_1, \ldots, f_k$ образуют базис $L(G)$.

2. Если $n > \deg(G) > 2g - 2$, тогда $k = \deg(G) + 1 - g$.

3. Алгеброгеометрический код имеет параметры

$$[n, \deg(G) - g + 1, d], \; d \geq n - \deg(G) \tag{2.7}$$

и определяется как

$$C = \{ f(P_1), \ldots, f(P_n) \mid f \in L(G) \}. \tag{2.8}$$

Для хеширования на основе алгеброгеометрического кодирования получим универсальное семейство хеш-функций с параметрами $1-\frac{d}{n}-U\left(n, q^k, q\right)$ (см. замечание 2.4).

Универсальное хеширование по PC кодам $\left(Rsh\right)$ в алгеброгеометрической интерпретации имеет следующее представление [94]. Пусть F – алгебраическое покрытие F_q. Точки χ определяются гомогенными координатами $\left(x, y\right)$, имеют значения $P_i=\left(\alpha_i,1\right)$, $0\le i\le q-1$ и $Q=\left(1,0\right)$ – особая точка (точка неопределенности). Пусть $f\in F_q\left(\chi\right)$ – рациональные функции, которые определены в каждой P_i с коэффициентами в F_q и которые имеют полюс порядка меньше, чем m в точке Q, и нет других полюсов. Рациональная функция f имеет вид $\frac{\alpha\left(x, y\right)}{\beta\left(x, y\right)}$, где $\alpha\left(x, y\right)$ и $\beta\left(x, y\right)$ – гомогенные полиномы степени $<k$. Алгеброгеометрический код определим как

$$C=\left\{\left(f\left(P_0\right), f\left(P_1\right),\ldots, f\left(P_{q-1}\right)\right)\middle| f\in L\left(mQ\right)\right\}.$$

Код $\tilde{N}$ имеет размерность пространства $L\left(mQ\right)$, $g=0$, $k=\dim C=m-g+1=m+1$ и минимальное расстояние $d\ge n-m$.

Таким образом, получим PC код $\left(q, k, q-k+1\right)_q$ в алгеброгеометрической интерпретации и универсальный класс хеш-функций $\frac{k-1}{q}-U\left(q, q^k, q\right)$.

Следующий пример – алгеброгеометрическое хеширование по кодам Эрмита $\left(Hch\right)$. Кривая Эрмита определяется уравнением $y^{\sqrt{q}}+y=x^{\sqrt{q}+1}$ над квадратичным полем $F_{q=p^2}$. Число точек кривой $N=q\sqrt{q+1}$, род $g=\sqrt{q}\left(\sqrt{q}-1\right)/2$. Пусть $P_\infty=(0:1:0)$ и $G=mP_\infty$. Базис пространства $L\left(mQ\right)$

задается функциями вида $\left\{x^i \cdot y^j : i\sqrt{q} + j(\sqrt{q}+1) \le m\right\}$. При алгеброгеометрическом кодировании код Эрмита имеет параметры $\left[q\sqrt{q}, k, d \ge q\sqrt{q} - k + 1 - g\right]$, что приводит к параметрам универсального хеширования: $\frac{1}{\sqrt{q}}\left(\frac{k-1}{q}+1-\frac{1}{\sqrt{q}}\right) - U\left(q\sqrt{q}, q^k, q\right)$ [95].

Зависимости вероятности коллизий для универсального хеширования на PC кодах и кодах Эрмита от длины хешируемого сообщения представлены на рис. 2.1. Для асимптотической границы построены графики зависимости вероятности коллизии для HCh_q от длины данных и размера поля вычислений, которые представлены на рис. 2.1, 2.2, где:

– вероятность коллизии для HCh_q

$$\varepsilon = \frac{1}{\sqrt{q}}\left(\frac{k-1}{q}+1-\frac{1}{\sqrt{q}}\right) \text{ при } 1 \le k \le q\sqrt{q};$$

– вероятность коллизии для RSh_q

$$\varepsilon = \frac{k-1}{q} \text{ при } 1 \le k \le q.$$

Для малых длин данных, когда $k < \sqrt{q} + 1$, схема RSh_q по асимптотической оценке имеет большее преимущество, так как реализует наименьшую вероятность коллизии. Анализ графиков показывает, что HCh_q обеспечивает увеличение объема хешируемых данных в $\sqrt{q}$ раз. Для $q = 2^{32}$ объем хешируемых данных может достигать 2^{39} 32-разрядных слов, что перекрывает весь диапазон практических применений. При этом вероятность коллизии ограничивается значением $10^{-3}\left(2^{-10}\right)$. Уменьшение вероятности коллизии возможно увеличением q. Так, при $q = 2^{64}$ вероятность коллизии уменьшается к асимптотической границе не меньше чем на пять порядков до 10^{-8}.

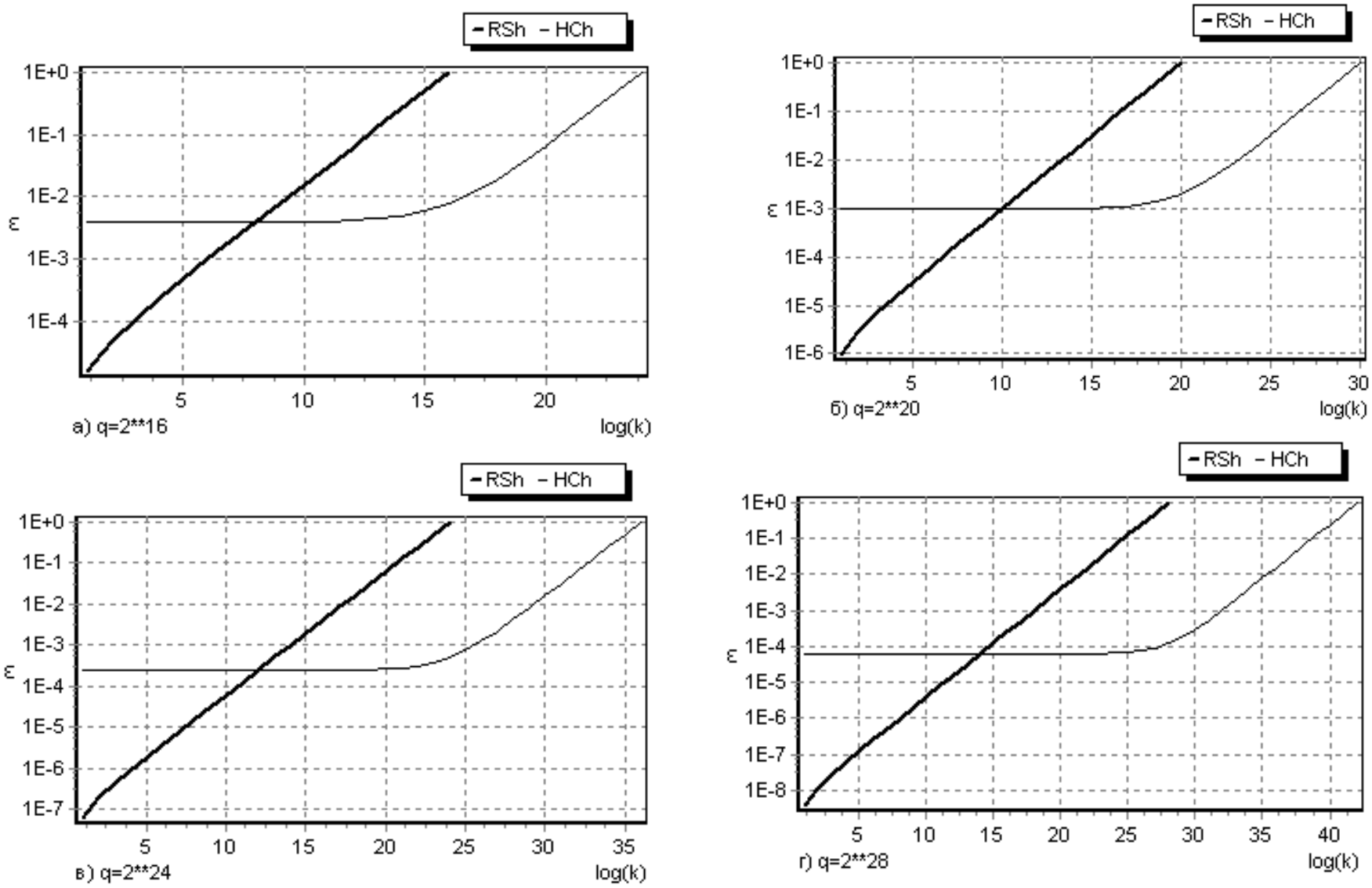


Рис. 2.1. Графики зависимости асимптотической границы вероятности коллизии для схемы хеширования с НС от длины данных при разных значениях размера конечного поля вычисления

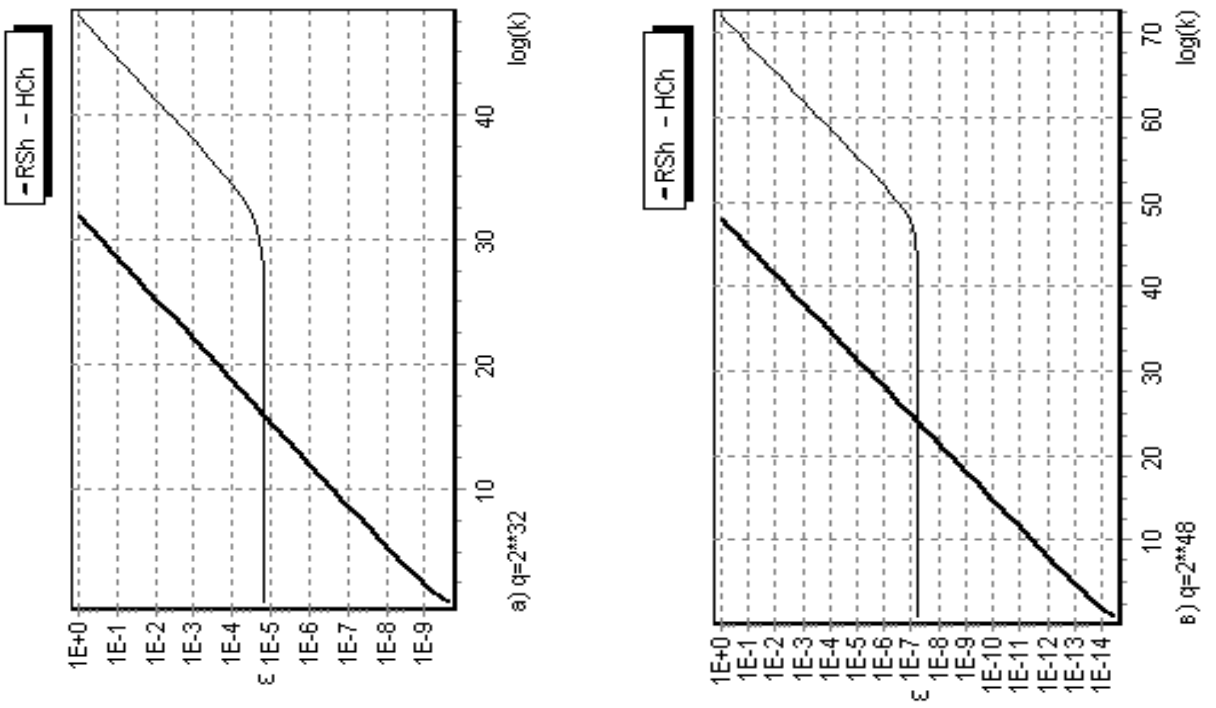


Рис. 2.2. Графики зависимости асимптотической границы вероятности коллизии для схемы хеширования с НС от длины данных при разных значениях размера конечного поля вычисления

HC кодирование является конструктивным, реализуется относительно просто в той же арифметике, что и RS кодирование. HCh_q хеширование обеспечивает меньшую вероятность коллизии по сравнению с RSh_q.

Для асимптотической оценки вероятности коллизии можно ввести пороговое значение длины k^*. Для универсального хеширования HCh_q k^*_{HC} определяется значением $k^*_{HC} = \sqrt{q} + 1$ и вероятность коллизии при $k = k^*_{HC}$ – $\varepsilon(k^*_{HC}) = 1/\sqrt{q}$ [95]. Пороговое значение k^* показывает, при какой длине данных вероятность коллизии HCh_q хеширования меньше в сравнении с RSh_q хешированием.

Среди длинных кодов по алгебраическим кривым практическое значение имеют коды Судзуки SC. Коды Судзуки определены над полем GF_q, $q = p^{2f+1}$ и имеют параметры $\left[q^2, k, q^2 - k + 1 - g\right]$, где $g = q\sqrt{q}/\sqrt{2}$ следует из рода кривой [100]. Применение кодов приводит к универсальному

хешированию SCh_q с параметрами $\frac{1}{q}\left[\frac{(k-1)}{q}+\sqrt{\frac{q}{2}}\right]-U(q^2,q^k,q)$ [71]. Графики зависимости вероятности коллизии для SCh_q по асимптотической границе от длины данных и размера поля вычислений представлены на рис. 2.3, 2.4, где:

вероятность коллизии для SCh_q

$$\varepsilon=\frac{1}{\sqrt{q}}\left(\frac{k-1}{q}+1-\frac{1}{\sqrt{q}}\right) \text{ при } 1\le k\le q^2;$$

вероятность коллизии для RSh_q

$$\varepsilon=\frac{k-1}{q} \text{ при } 1\le k\le q.$$

Анализ графиков показывает, что SCh_q обеспечивает увеличение объема хешируемых данных в q раз по сравнению с RSh_q. Для $q=2^{32}$ объем хешируемых данных может достигать 2^{54} 32-разрядных слов, что перекрывает весь диапазон практических применений. При этом вероятность коллизии ограничивается значением $10^{-3}\left(2^{-10}\right)$. Уменьшение вероятности коллизии возможно путем увеличения q. Так, при $q=2^{64}$ вероятность коллизии уменьшается к асимптотической границе не меньше чем на семь порядков до 10^{-10}. Это существенно лучше, чем при RSh_q и HCh_q.

Пороговое значение k_{SC}^* при хешировании сообщений в схеме SCh_q определяется значением $k_{SC}^*=\frac{\sqrt{q}}{2}+\frac{\sqrt{q}}{2(q-1)}+1$. Вероятность коллизии при $k=k_{SC}^*-\quad \varepsilon\left(k_{SC}^*\right)=\frac{1}{2\sqrt{q}}+\frac{1}{2\sqrt{q}(q-1)}$. Пороговое значение k_{SC}^* для SCh_q практически совпадает с пороговым значением k_{HC}^* для HCh_q. Универсальное хеширование SCh_q по асимптотической границе вероятности коллизии также проигрывает на малых длинах хешированию RSh_q.

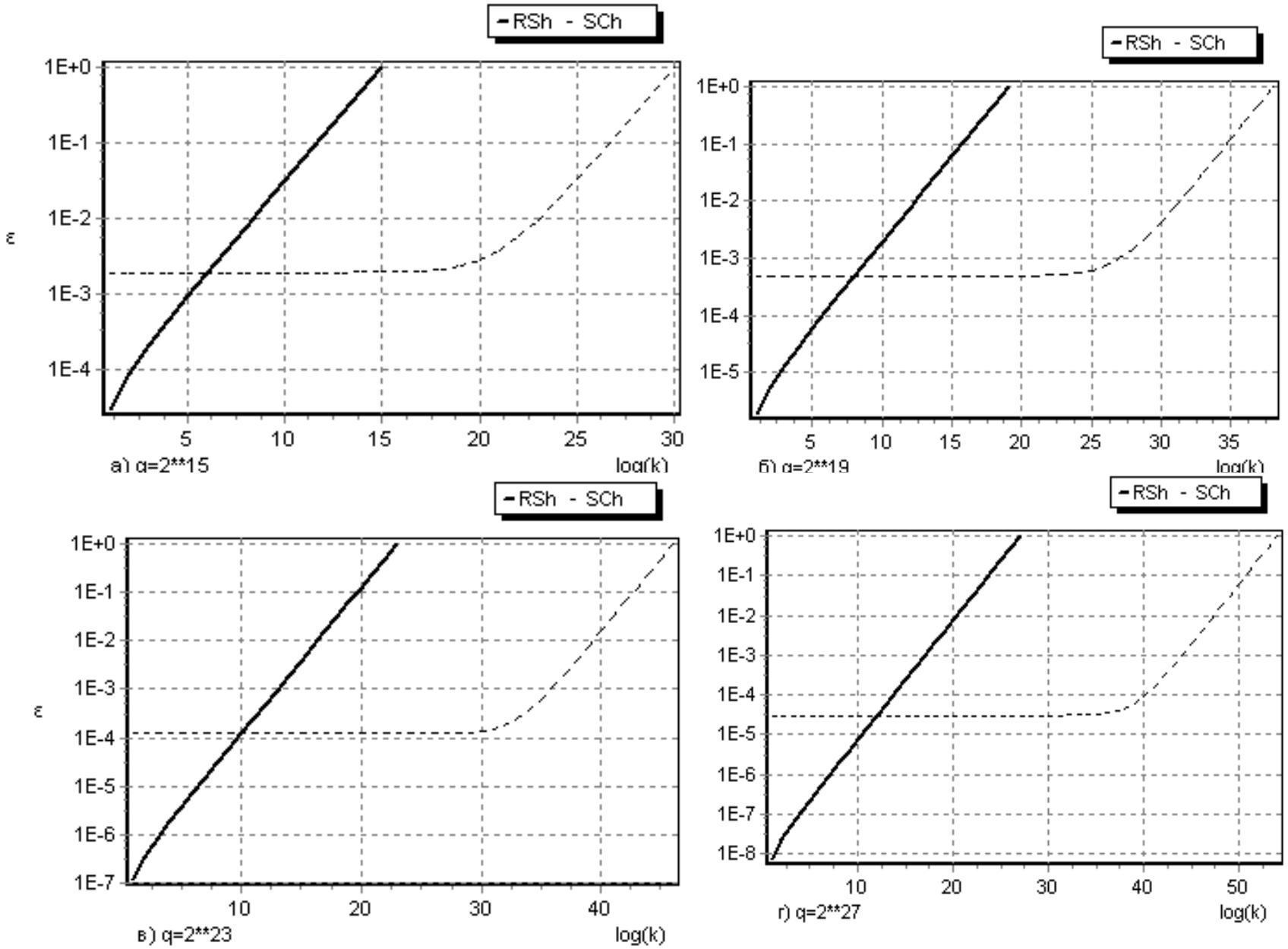


Рис. 2.3. Графики зависимости асимптотической границы вероятности коллизии для хеширования *SChq* от длины данных при разных значениях размера конечного поля вычисления

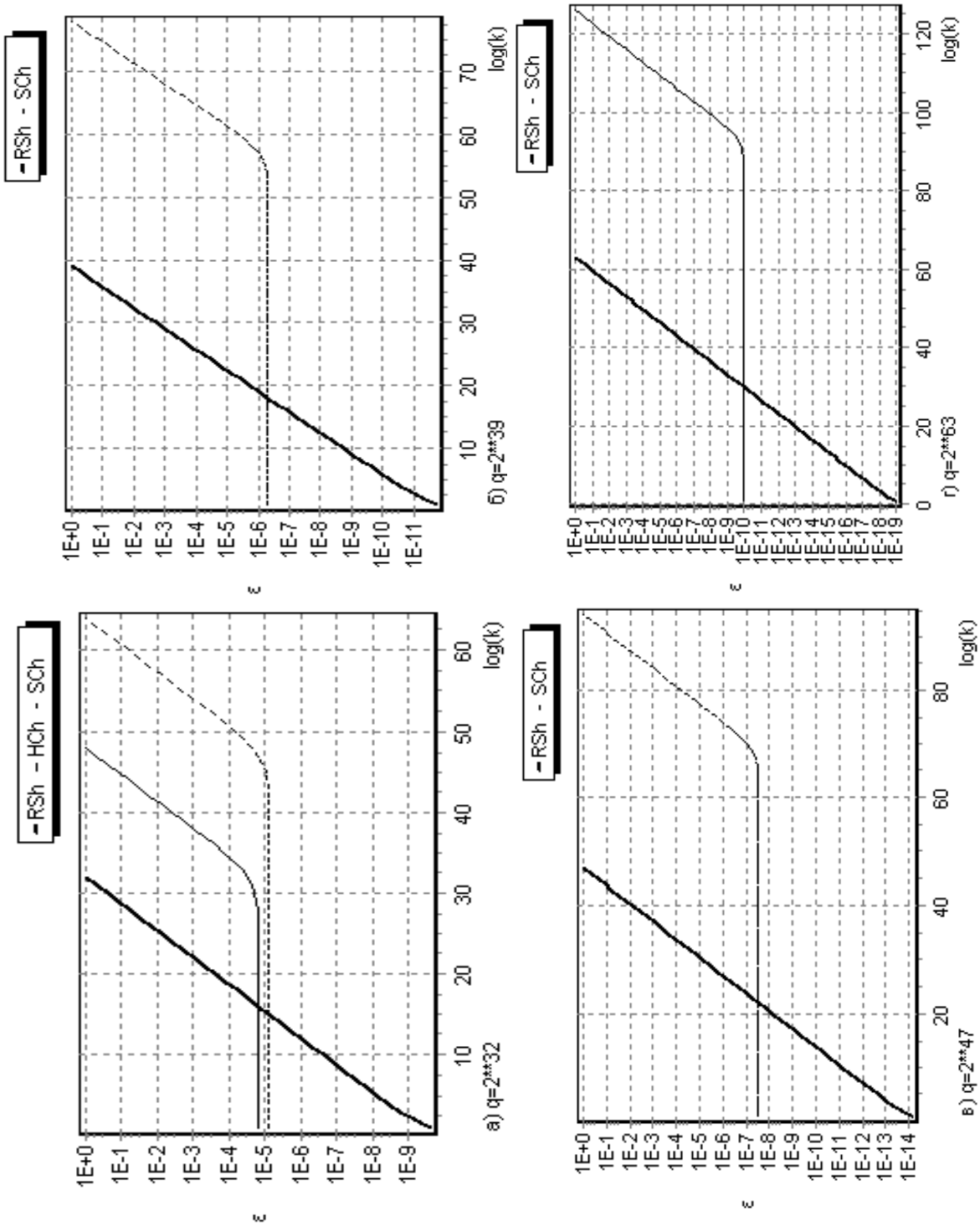


Рис. 2.4. Графики зависимости асимптотической границы вероятности коллизии для хеширования *SChq* от длины данных при разных значениях размера конечного поля вычисления

Основные результаты по схемам хеширования по кодовым конструкциям представлены в таблице 2.1.

Таблица 2.1 – Основные параметры схем хеширования по алгебраическим кодам

№	Схема хеширования	Асимптотические оценки для вероятности коллизии ε	Поле вычислений	Длина хешируемых данных
1	RSh_q	$\frac{k-1}{q}$	$GF_q,\ q=p^m$	$1 \le k \le q$
2	HCh_q	$\frac{1}{\sqrt{q}}\left(\frac{k-1}{q}+1-\frac{1}{\sqrt{q}}\right)$	$GF_q,\ q=p^2$	$1 \le k \le q\sqrt{q}$
3	SCh_q	$\frac{1}{q}\left[\frac{k-1}{q}+\sqrt{\frac{q}{2}}\right]$	$GF_q,$ $q=p^{2f+1}$	$1 \le k \le q^2$

Анализ показывает, что наиболее приемлемыми значениями q для хеширования данных, которые лежат в диапазоне разрядности современных процессоров, являются 2^{32} и 2^{64}. Вероятность коллизии возрастает линейно с возрастанием объема данных. Для вероятности коллизии в диапазоне значений 10^{-3} (2^{-10}) ÷ 10^{-9} (2^{-30}) размер хешируемых данных должен лежать в диапазоне $2^3 \div 2^{22}$ 32-разрядных слов.

Зависимости вероятности коллизий для универсального хеширования на РС кодах, кодах Эрмита и Судзуки от длины хешируемого сообщения представлены на рис. 2.5 [94-95].

На рис. 2.5 представлены абсолютно лучшие результаты для универсального хеширования по алгеброгеометрическим кодам. Алгеброгеометрические коды Эрмита и Судзуки обеспечивают меньшую вероятность коллизии универсального хеширования по сравнению с алгебраическим *PC* кодом.

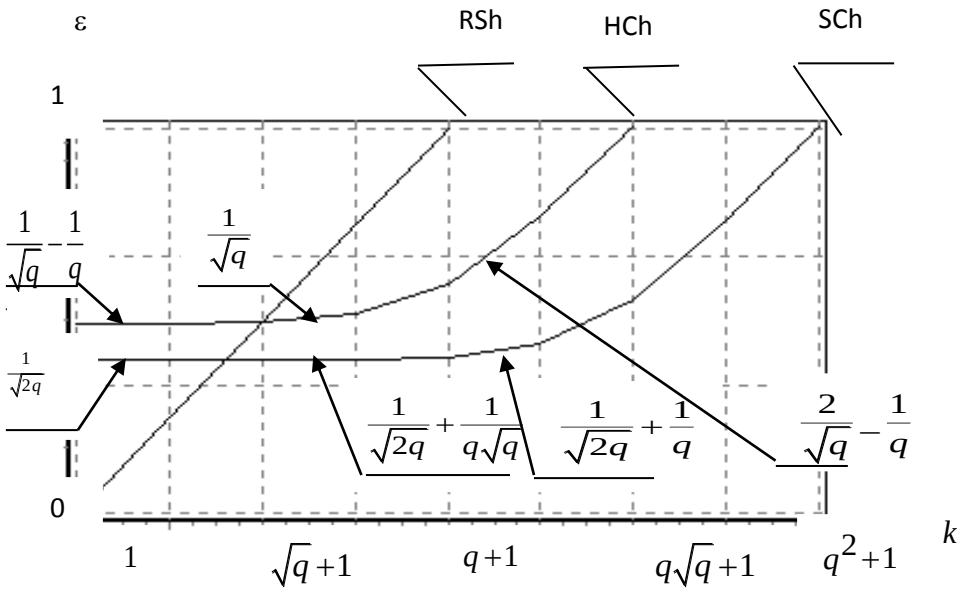


Рис. 2.5. Зависимости вероятности коллизий универсального хеширования с PC кодами, кодами Эрмита и Судзуки от длины сообщения

Для больших значений k это следует прямо из графиков. Для малых k проигрыш по вероятности коллизии PC коду (RSh) определяется неточной оценкой кодового расстояния кода Эрмита (HCh) и Судзуки (SCh).

Оценки вероятности коллизии для низкоскоростного кодирования не являются точными, так как параметры алгеброгеометрических кодов точно определяются при размерности $k > g - 1$.

Универсальное хеширование по рациональным функциям алгебраических кривых снимает ограничение на точность оценок параметров хеширования по параметрам алгеброгеометрических кодов.

2.4 Универсальное хеширование по рациональным функциям алгебраических кривых

2.4.1 Определение универсального хеширования по алгебраическим кривым.

Универсальное хеширование по рациональным функциям алгебраических кривых определяется свойствами линейного базисного пространства, ассоциированного с функциональным полем кривой. Свойства линейного векторного пространства по базису рациональных функций следуют из теоремы Римана – Роха.

Пусть $D \coloneqq P_1 + \ldots + P_n$ и $G \coloneqq \rho_k P_\infty$, где $P_1, \ldots, P_n$ – рациональные точки кривой χ и P_∞ – точка на бесконечности. Пусть порядки полюсов ρ_i рациональных функций $f_i \in F_q(\chi)$ упорядочены и меньше ρ_k; дивизоры $G + \mathrm{div}_\infty(f_i) \succ 0$ являются эффективными (имеют положительные коэффициенты по области определения) и по теореме Римана – Роха рациональные функции f_i образуют векторное пространство, ассоциированное с G. По следствию 2.1 значения рациональных функций $f_i(P_j)$ в точках кривой определяют строки порождающей матрицы кода $C_{D,\rho_k P_\infty}$ размерности, равной числу рациональных функций k, и кодовым расстоянием $d \geq N - \rho_k$ по лемме 2.1. По свойству универсального хеширования на основе алгебраического кодирования (2.3) получим, что хеш-функция $h_{P_j}(m)$ определяет универсальный хеш-класс $\varepsilon - U(N, q^k, q)$ с вероятностью коллизии $P_{\mathrm{col}} \leq \varepsilon = \rho_k / N$, где N – число точек алгебраической кривой, q^k – объем пространства сообщений, q – объем пространства хеш-кодов.

Метод универсального хеширования по алгебраическим кривым определяется как скалярное произведение по рациональным функциям алгебраических кривых:

$$h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i ,$$

что следует из конструкции алгеброгеометрического кода и определяется следующей последовательностью действий:

– определить проективное многообразие – алгебраическую кривую и ее точки;

– построить линейное векторное пространство для функционального поля алгебраической кривой;

– задать хеш-функцию как скалярное произведение слов данных и значений рациональных функций в точке кривой.

Параметры универсального хеш-класса $\varepsilon - U(N, q^k, q)$ на основе хеширования по рациональным функциям определяются свойствами алгебраической кривой либо ассоциированным с этой кривой проективным многообразием.

Замечание 2.9.

1. Параметры универсального хеш-класса $\varepsilon - U(N, q^k, q)$ на основе хеширования по рациональным функциям определяются свойствами алгебраической кривой. Подгруппа Вейерштрасса $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < \ldots\}$ определяется полюсами рациональных функций в особой точке кривой; рациональные функции, упорядоченные по значениям полюсов, образуют векторное линейное пространство размерности

$$\dim(L(G)) = v_\ell := \#\{(i, j) \in N^2 : \rho_i + \rho_j = \rho_{\ell+1}\}.$$

2. Ключевой параметр хеш-функции $h_{P_j}(m)$ определяется вычислением в точке алгебраической кривой.

3. Для построения алгоритма вычислений необходимо определить проективное многообразие алгебраической кривой (ее точки), построить линейное векторное пространство для функционального поля алгебраической кривой, задать хеш-функцию как скалярное произведение слов данных и значений рациональных функций в точке кривой, выбранной по ключу.

Проблематика построения схем универсального хеширования по рациональным функциям алгебраических кривых заключается в выборе алгебраических кривых с требуемыми параметрами.

2.4.2 Наилучшие алгебраические кривые для универсального хеширования.

Под кривой будем рассматривать проективную, геометрически неразложимую и несингулярную алгебраическую кривую, определенную над конечным полем F_q с q элементами.

Точка P кривой C называется несингулярной, если существует касательная линия к кривой в точке P. Например, если $P=(a,b)\in F_q\times F_q$ является точкой плоской кривой, ассоциированной с полиномом $f(X,Y)\in F_q[X,Y]$, тогда точка P называется несингулярной, если

$$f_X(a,b)\neq 0 \text{ или } f_Y(a,b)\neq 0,$$

где f_X и f_Y – частные производные.

Кривая C называется несингулярной, если каждая точка $P\in C$ является несингулярной.

Кривая $\tilde{C}$ является проективной моделью аффинной кривой C, ассоциированной с полиномом $f(X,Y)$ степени $d:=\deg f(X,Y)$, имеет представление

$$F(X,Y,Z)=Z^d f(X/Z,Y/Z) \text{ и } \tilde{C}:=\left\{(a:b:c)\in P^2(F_q)\middle| F(a,b,c)=0\right\}.$$

Если проективная плоская кривая является несингулярной, тогда для рода кривой справедлива оценка [103]:

$$g\left(\tilde{C}\right) \le (d-1)(d-2)/2 .$$

Точка $(a:b:c)$ кривой $\tilde{C}$ является рациональной точкой, если $a, b, c \in F_q$. Точка $(a:b:c)$ кривой $\tilde{C}$ является точкой бесконечности P_∞, если $c = 0$.

Пусть $N_q(g)$ обозначает максимальное число F_q рациональных точек, которое кривая рода g может иметь. Кривая C рода g является оптимальной (максимальной) над F_q, если ее число F_q рациональных точек $\#C\left(F_q\right)$ равно $N_q(g)$. Главный результат для теории определяется теоремой Хассе – Вейля.

Теорема 2.1 [100]. Пусть C – проективная и несингулярная, абсолютно неразложимая кривая, определенная над конечным полем F_q с q элементами. Тогда число F_q рациональных точек кривой определяется неравенством

$$N_q(g) \le 1 + q + 2\sqrt{q}g(C) \qquad (2.9)$$

Максимальные кривые над F_q – это кривые, число F_q рациональных точек которых удовлетворяет границе Хассе – Вейля (2.9).

Для максимальных кривых над конечным полем достигается максимальное отношение числа точек кривой к роду, что прямо связывается с вероятностью коллизии в схеме с универсальным хешированием, так как $P_{\text{êîë}} \le \varepsilon = \rho_k / N$.

Существуют три замечательные семейства таких кривых, которые связываются с Дэлигнэ – Лустига (Deligne – Lusztig) многообразием размерности $\dim = 1$. Кривая Дэлигнэ – Лустига ассоциируется с проективной специальной линейной группой (кривые Эрмита), с группой Судзуки (Suzuki) $Sz(q)$ (кривые Судзуки) и Ри (Ree) группой $R(q)$ [104].

Не существует максимальных кривых над полем F_q рода больше, чем $g > \sqrt{q}\left(\sqrt{q} - 1\right)/2$. Классификация максимальных плоских кривых

представлена в [105]. Основной результат по максимальным кривым представлен теоремой 2.2.

Теорема 2.2 [112]**.** Род g максимальной кривой над F_{l^2} соответствует значениям $g \le g_3 = \left\lfloor \left(l^2 - l + 4\right)/6 \right\rfloor$ или $g = g_2 = \left(l-1\right)^2/4$, или $g = g_1 = l\left(l-1\right)/2$.

Случай, когда $g = g_1$, выполняется только для кривой Эрмита $y^l + y = x^{l+1}$.

По классификации максимальных плоских кривых кривая Эрмита является кривой максимального рода $g = g_1 < q$.

Замечание 2.10.

1. В работе [113] показано, что $N_{l^2}\left(g\right) < 1 + l^2 + 2gl$ для $g_2 < g < g_1$, то есть не существует максимальных кривых, род которых принимает значения $g_2 < g < g_1$.

2. Известен результат, который определяет, что если кривая покрывается максимальной кривой, то она также является максимальной, что позволяет построить семейство максимальных кривых [106].

Максимальные кривые C_2 рода g_2, которые относятся к классу кривых, покрываемых кривой Эрмита, рассмотрены в [109,114–118] и имеют вид:

а) $C_{2a} \Rightarrow y^l + y = x^{(l+1)/2}$;

в) $C_{2b} \Rightarrow \sum_{i=1}^{t} y^{l/2^i} = x^{l+1}$;

с) $C_{2c} \Rightarrow \sum_{i=0}^{t-1} y^{2^i} = x^{l+1}$, $l = 2^t > 2$;

Максимальные кривые C_3 рода $g = g_3$, которые относятся к классу кривых покрываемых кривой Эрмита, рассмотрены в [114–118] и имеют вид:

а) $C_{3a} \Rightarrow x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0$, если $l \equiv 2\left(\mathrm{mod}\,3\right)$;

в) $C_{3b} \Rightarrow \omega x^{(l-1)/3} - yx^{2(l-1)/3} + y^l = 0$, если $l \equiv 1 (\mathrm{mod}\, 3)$, где $\omega \in F_{l^2}$, $\omega^{l-1} = -1$,

с) $C_{3c} \Rightarrow y^l + y = \left(\sum_i^t x^{l/3^i} \right)^2$, если $l = 3^t$;

d) $C_{3d} \Rightarrow x^{2(l+1)/3} y^{(l+1)/3} + y^{2(l+1)/3} + x^{(l+1)/3} = 0$, если $l \equiv 2 (\mathrm{mod}\, 3)$.

Максимальные кривые C_4 рода $g < g_3$, рассмотрены в [114–119]:

а) $C_{4a} \Rightarrow y^l + y = x^{(l+1)/3}$, $g = \left(l^2 - 3l + 2\right)/6 < g_3$;

в) $C_{4b} \Rightarrow \sum_{i=0}^{t-1} y^{3^i} = \omega x^{l+1}$, $l = 3^t$, $\omega \in F_{l^2}$, $\omega^{l-1} = -1$, $g = l(l-3)/6 < g_3$;

с) $C_{4c} \Rightarrow y^l + y = x^m$, где m – делитель $l+1$, $g = (m-1)(l-1)/2$;

d) $C_{4d} \Rightarrow \sum_{i=1}^{t} y^{l/p^i} + \omega x^{l+1} = 0$, $\omega \in F_{l^2}$, $\omega^{l-1} = -1$, $g = l(l-p)/2p$.

Замечание 2.11.

1. Кривая C_{3a} является частным случаем кривой $x^{(l+1)/d} + x^{2(l+1)/d} + y^{l+1} = 0$ рода $g = (l+1)(l-2)/2d + 1$ [114–116].

2. Кривая $C_{3b} \dfrac{\delta y}{\delta x}$ – частный случай кривой $\omega x^{(l-1)/d} - yx^{2(l-1)/d} + y^l = 0$ рода $g = l(l-1)/2d$ [114–116].

3. Кривая C_{3c} является частным случаем кривой $y^l + y = \left(\sum_i^t x^{l/p^i} \right)^2$, $l = p^t$ рода $g = l(l-1)/2p$ [114–116].

Оценки полюсов рациональных функций, размерность функциональных полей по максимальным кривым в квадратичном поле рода g_1, g_2 и g_3 представлены в таблице 2.2.

Таблица 2.2 – Максимальные кривые над F_q, $q=l^2$

Уравнение кривой $C\left(F_{l^2}\right)$	Значение рода кривой	Полюса рациональных функций	Значение подгруппы Вейерштрасса
$y^l+y=x^{l+1}$	$g_1=\frac{l(l-1)}{2}$	$(x)_\infty=l$, $(y)_\infty=l+1$	$\langle l, l+1\rangle$
$y^l+y=x^{(l+1)/2}$, l нечетное	$g_2=\frac{(l-1)^2}{4}$	$(x)_\infty=l$, $(y)_\infty=(l+1)/2$	$\langle (l+1)/2, l\rangle$
$\sum_{i=1}^{t} y^{l/2^i}=x^{l+1}$, $l=2^t$	$g_2'=\frac{l(l-2)}{4}$	$(x)_\infty=l/2$, $(y)_\infty=l+1$	$\langle l/2, l+1\rangle$
$y^l+y=x^{(l+1)/3}$, $l\equiv 2(\mathrm{mod}3)$	$g_3'=\frac{(l^2-3l+2)}{6}$	$(x)_\infty=(l+1)/3$, $(y)_\infty=l$	$\langle (l+1)/3, l\rangle$
$\sum_{i=0}^{t-1} y^{3^i}=\omega x^{l+1}$, $l=3^t$, $\omega\in F_{l^2}$, $\omega^{l-1}=-1$	$g_3''=\frac{l(l-3)}{6}$	$(x)_\infty=l/3$, $(y)_\infty=l+1$	$\langle l/3, l+1\rangle$
$x^{(l+1)/3}+x^{2(l+1)/3}+$, $+y^{l+1}=0$, $l\equiv 2(\mathrm{mod}3)$	$g_3=\frac{(l^2-l+4)}{6}$	$(x)_\infty=l+1$, $(y)_\infty=(l+1)/3$, $(v)_\infty=l$	$\langle 2(l+1)/3, l, l+1\rangle$
$\omega x^{(l-1)/3}-yx^{2(l-1)/3}+y^l=0$, $\omega\in F_{l^2}$, $\omega^{l-1}=-1$, $l\equiv 1(\mathrm{mod}3)$	$g_3'''=\frac{l(l-1)}{6}$	$(x)_\infty=l$, $(y)_\infty=(l-1)/3$, $(v)_\infty=l+1$	$\langle (2l-1)/3, l, l+1\rangle$
$y^l+y=\left(\sum_i^t x^{l/3^i}\right)^2$, $l=3^t$	$g_3'''=\frac{l(l-1)}{6}$,	$(x)_\infty=l$, $(y)_\infty=2l/3$, $(v)_\infty=l+1$	$\langle 2l/3, l, l+1\rangle$
$x^{2(l+1)/3}y^{(l+1)/3}+$ $+y^{2(l+1)/3}+x^{(l+1)/3}=0$	$g_3=\frac{(l^2-l+4)}{6}$		$\langle (2l+1)/3, l, l+1\rangle$

Замечание 2.12.

1. Алгебраические кривые $y^l+y=x^{l+1}$, $y^l+y=x^{(l+1)/2}$ и $\sum_{i=1}^{t} y^{l/2^t}=x^{l+1}, l=2^t$ являются максимальными кривыми первого и второго рода,

имеют подгруппу Вейерштрасса $H(P_\infty)=\langle \rho_1, \rho_2 \rangle$ размерности $\dim = 2$, функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

2. Алгебраические кривые $y^l + y = x^{(l+1)/3}, l \equiv 2 (\mathrm{mod} 3)$ и $\sum_{i=0}^{t-1} y^{3^t} = \omega x^{l+1}, l = 3^t, \omega \in F_{l^2}, \omega^{l-1} = -1$ – максимальные кривые третьего рода, имеют подгруппу Вейерштрасса $H(P_\infty)=\langle \rho_1, \rho_2 \rangle$ размерности $\dim = 2$, функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

3. Максимальные кривые вида:

– $x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0, l \equiv 2 (\mathrm{mod} 3)$,

– $\omega x^{(l-1)/3} - yx^{2(l-1)/3} + y^l = 0, \omega \in F_{l^2}, \omega^{l-1} = -1, l \equiv 2 (\mathrm{mod} 3)$,

– $y^l + y = \left(\sum_i^t x^{l/3^i} \right)^2, l = 3^t$

имеют подгруппу Вейерштрасса $H(P_\infty)$ размерности $\dim = 3$, функциональное поле определяется рациональными функциями вида $\{x^i \cdot y^j \cdot v^t\}$.

2.4.3 Коллизионные свойства универсального хеширования по алгебраическим кривым.

Определение хеш-функции следует из базиса пространства $L(\rho_k P_\infty)$ рациональных функций алгебраических кривых. Оценки для вероятности коллизии связаны со значением ρ_k полюса подгруппы Вейерштрасса $H(P_\infty)$, что, в свою очередь, определяется показателями степеней рациональных функций функционального поля и зависит от числа k слов данных.

Максимальные алгебраические кривые первого и второго рода имеют подгруппу Вейерштрасса $H(P_\infty)=\langle \rho_1, \rho_2 \rangle$ размерности $\dim = 2$, и функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

Хеш-функция $h_{x,y}(m) \in F_{q^2}$ для сообщения m по рациональным функциям в точке x, y максимальных кривых замечания 2, п. 1, 2, определяется выражением

$$h_{x,y}(m) = \sum_{i \geq 0,\ 0 \leq j \leq \rho_1,\ i \cdot \rho_1 + j \cdot \rho_2 \leq \rho_k} m_{i,j} \cdot x^i \cdot y^j , \qquad (2.10)$$

где ρ_k – полюс подгруппы Вейерштрасса $H(P_\infty)$;

$m_{i,j} \in F_{q^2}$ – слова сообщения m.

Хеш-функция $h_{P_j}(m)$ определяет универсальный хеш-класс $\varepsilon - U(N, q^k, q)$, где $\varepsilon = \rho_k / N$ – вероятность коллизии. Число F_{q^2} рациональных точек максимальной кривой лежит на границе Хассе – Вейля и определяется равенством

$$N_{q^2}(g) = 1 + q^2 + 2qg . \qquad (2.11)$$

Значение рода определяет число точек $N_{q^2}(g)$ и прямо следует из показателей координатных переменных уравнения кривой. Значения степеней переменных определяют порядки полюсов $\mathrm{div}_\infty(x) = \rho_1$, $\mathrm{div}_\infty(y) = \rho_2$, а аддитивная группа полюсов – подгруппу Вейерштрасса $H(P_\infty)$. Таким образом, наилучший результат хеширования – наименьшая верхняя граница вероятности коллизии, достигается на максимальных кривых наибольшего рода. Оценки вероятности коллизии для кривых первого, второго и третьего рода представлены в таблице 2.3.

Таблица 2.3 – Коллизионные оценки универсального хеширования по максимальным кривым над F_{q^2}

Уравнение кривой	Параметры универсального хеширования $\varepsilon - U\left(N, q^{2k}, q^2\right)$	Оценка вероятности коллизии ε, $k < g$	Асимптотическая оценка $\varepsilon_{q\to\infty}(k)$
$y^q + y = x^{q+1}$ F_{q^2}	$U\left(q^3, q^{2k}, q^2\right)$	$k/q^3 + s/q^2 -$ $-s(s-1)/\left(2q^3\right)$ $s = \left\lvert\left(2k+1/4\right)^{1/2} - 1/2\right\rvert$	$\sqrt{2}k^{1/2}/q^2$
$y^q + y = x^d$ F_{q^2} $d \mid q+1$	$U\left(q^2 + (d-1)\times\right.$ $\left.\times(q-1)q, q^{2k}, q^2\right)$	$\dfrac{(iq+jd)}{\left(q^2+(d-1)(q-1)q\right)}$ $s = \left\lvert\left(\dfrac{2k}{m}+\dfrac{1}{4}\right)^{1/2} - \dfrac{1}{2}\right\rvert$ $t = \left[k - m(s-1)s/2/s\right]$ $m = (q+1)/d$ $ind = 0, -1$	$\sqrt{2(q+1)/d}$ $k^{1/2}/q^2$
$\sum_{i=1}^{t} y^{q/p^i} + \omega x^{q+1} = 0$ F_{q^2}, $q = p^t$ $\omega^{q-1} = -1$	$U\left(q^3/p, q^{2k}, q^2\right)$	$\left(i(q+1)p + jq\right)/q^3$ $s = \left\lvert\left(\dfrac{2k}{m}+\dfrac{1}{4}\right)^{1/2} - \dfrac{1}{2}\right\rvert$ $t = \left\lfloor\dfrac{k - p(s-1)s/2}{2}\right\rfloor$ $ind = 0, -1$	$\sqrt{2p}k^{1/2}/q^2$
$x^{\frac{q+1}{d}} + x^{\frac{2(q+1)}{d}} + y^{q+1} = 0$ F_{q^2}, $q = 2 \pmod 3$ $x^{\frac{q+1}{3}} + x^{\frac{2(q+1)}{3}} + y^{q+1} = 0$	$U\left(\dfrac{q^3+2q^2+4q+3}{3}, q^{2k}, q^2\right)$	$\dfrac{3iq + 3j(q+1) + t\cdot 2(q+1)}{q^3+2q^2+4q+3}$ $s = \left\lvert\left(\dfrac{2k}{3}+\dfrac{1}{4}\right)^{1/2} - \dfrac{1}{2}\right\rvert$	$\sqrt{6}k^{1/2}/q^2$
$\omega x^{\frac{q-1}{d}} - yx^{\frac{2(q-1)}{d}} + y^q = 0$ F_{q^2} , $\omega^{q-1} = -1$ $q = 1 \pmod 3$ $\alpha^{(q+1)/2}x^{(q-1)/3} +$ $+\alpha^{\left(q^2-1\right)/2}x^{2(q-1)/3}y + y^q = 0$	$U\left(\dfrac{q^3+2q^2-q-2}{3}, q^{2k}, q^2\right)$	$\dfrac{3iq + 3j(q+1) + t(2q+1)}{q^3+2q^2-q-2}$ $s = \left\lvert\left(\dfrac{2k}{3}+\dfrac{1}{4}\right)^{1/2} - \dfrac{1}{2}\right\rvert$	$\sqrt{6}k^{1/2}/q^2$

Замечание 2.13.

1. Наилучшая асимптотическая оценка вероятности коллизии $\varepsilon_{q\to\infty}(k)$ определяется хешированием по кривой Эрмита – максимальной кривой наибольшего рода по классификации.

2. Проигрыш по вероятности коллизии универсальных схем хеширования по плоским максимальным кривым второго и третьего рода несущественный. Асимптотическая оценка чуть хуже в $\sqrt{2}\div\sqrt{6}$ раз по сравнению с кривой Эрмита.

Точные значения вероятности коллизии универсального хеширования по кривым Эрмита HCh_q над F_q от длины данных представлены на рис. 2.6, 2.7. Для сравнения здесь приведены зависимости хеширования по проективной прямой RSh_q и зависимости вероятности коллизии для хеширования на основе кодов Эрмита, которая не учитывает распределение полюсов рациональных функций при малых значениях k длин данных $HCh_{\text{àñ}}$.

Графики вероятности коллизии для HCh_q, $HCh_{\text{àñ}}$ и RSh_q хеширования вычислены по следующим соотношениям:

– асимптотические границы вероятности коллизии для $HCh_{\text{àñ}}$

$$\varepsilon = \frac{1}{\sqrt{q}}\left(\frac{k-1}{q}+1-\frac{1}{\sqrt{q}}\right) \text{ при } 1\le k\le q\sqrt{q};$$

– вероятность коллизии для RSh_q

$$\varepsilon = \frac{k-1}{q} \text{ при } 1\le k\le q.$$

Уточненная граница вероятности коллизии для $HCh_{\text{ôî÷}}$ взята из таблицы 2.3 для кривой $y^q + y = x^{q+1}$.

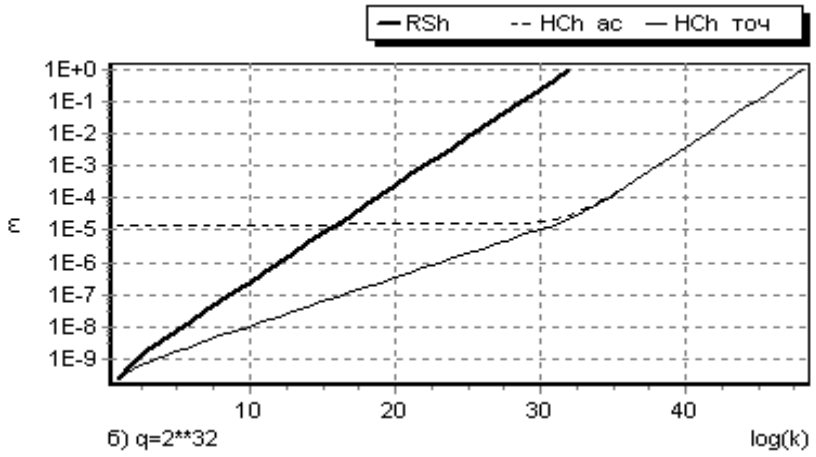


Рис. 2.6. Зависимости вероятности коллизии для *Hchq* хеширования в конечном поле F_q, $q = 2^{32}$ от длины данных

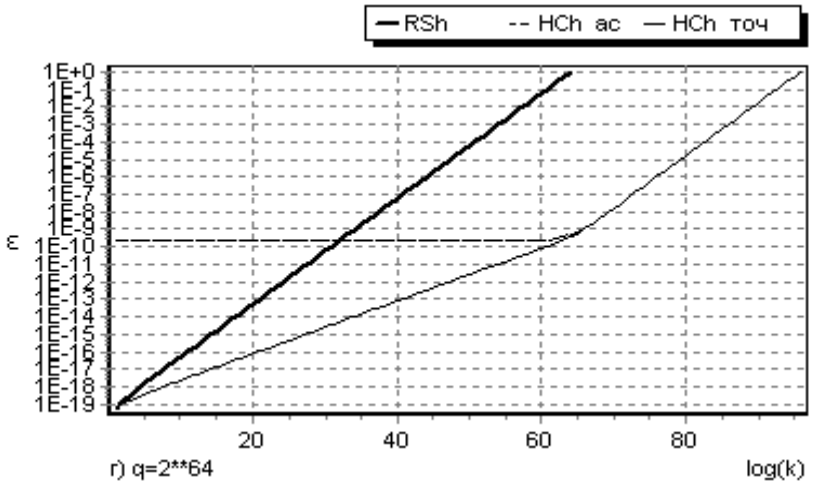


Рис. 2.7. Зависимости вероятности коллизии для *Hchq* хеширования в конечном поле F_q, $q = 2^{64}$ от длины данных

Анализ границы для вероятности коллизии показывает, что хеширование HCh_q имеет преимущество по сравнению с RSh_q при всех значениях длины данных в отличие от асимптотической границы для хеширования на основе кодового представления. При вычислении хеш-кодов в поле одинаковой размерности при фиксированной вероятности коллизии объем данных в схеме хеширования по кривой Эрмита HCh_q превышает допустимый объем данных по сравнению с RSh_q хешированием в степень 2 раз.

2.5 Выводы

1. Применение универсального хеширования для построения доказуемо стойкой аутентификации требует, чтобы ключевое пространство было не меньше пространства сообщений. Это ограничение снимается в конструкциях, где применяются алгебраические кодовые конструкции.

2. Основной результат универсального хеширования по алгебраическим кодам состоит в том, что вероятность коллизии определяется отношением кодо-вого расстояния к длине кода. Коды над большим алфавитом являются более предпочтительными, так как обеспечивают в универсальных схемах хеширования при фиксированной длине сообщения и значности кода потенциально меньшее значение вероятности коллизии.

3. Теория построения массивов строго универсальных аутентификаторов определяется ортогональными массивами. Основной результат строго универсального хеширования состоит в том, что оно реализуется при условии, когда размер ключа не меньше произведения размерностей пространства сообщений и хеш-кодов. Применение слабосмещенных массивов для построения почти строго универсальных хеш-функций снимает ограничение на размер ключей, но при этом увеличивается вероятность коллизии.

4. Проблематика практической реализации универсального хеширования на основе скалярного произведения по рациональным функциям алгебраических кривых определяется сложностью построения точек алгебраических кривых по ключевым данным. Вычислительные затраты на хеширование зависят от размерности функционального поля рациональных функций. Основное противоречие универсального хеширования по алгебраическим кривым состоит в том, что для обеспечения гарантированной вероятности обмана на нижнем уровне необходимо построить вычисления по рациональным функциям алгебраических кривых с как можно меньшим

отношением значения максимального полюса рациональных функций к числу точек кривой для фиксированной длины данных. Применение максимальных кривых большого рода приводит к увеличению размерности функционального поля, ассоциированного с кривой, и росту сложности вычислений.

5. Задача построения универсального хеширования по рациональным функциям алгебраических кривых заключается в выборе алгебраических кривых, вычислении их алгеброгеометрических параметров, разработке методов, алгоритмов и оценок универсального хеширования. Верхние оценки вероятности коллизии универсального хеширования по рациональным функциям алгебраических кривых показывают, что наилучшие результаты достигаются по кривым с большим числом точек.

Кривые, ассоциированные с группой Судзуки $Sz(q)$ (кривые Судзуки), являются неплоскими и имеют существенно большее число точек.

Актуальной задачей является оценка свойств группы Судзуки, алгебраической кривой, ассоциированной с группой Судзуки, построение ее функционального поля и универсального хеш-класса по кривой.

РАЗДЕЛ 3
УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО КРИВОЙ СУДЗУКИ

Проблематика практической реализации универсального хеширования на основе скалярного произведения по рациональным функциям алгебраических кривых определяется сложностью построения точек алгебраических кривых по ключевым данным. Вычислительные затраты на хеширование зависят от размерности функционального поля рациональных функций. Одна из задач универсального хеширования по алгебраическим кривым заключается в том, что необходимо построить вычисления по рациональным функциям алгебраических кривых с как можно меньшим отношением значения максимального полюса рациональных функций к числу точек кривой для фиксированной длины данных для обеспечения гарантированной вероятности обмана на нижнем уровне. Применение максимальных кривых большого рода приводит к увеличению размерности функционального поля, ассоциированного с кривой, и росту сложности вычислений.

Задачей раздела является оценка свойств группы Судзуки, алгебраической кривой, ассоциированной с группой Судзуки, построение функционального поля кривой Судзуки, универсального хеширования по рациональным функциям и оценка параметров.

3.1 Определение и свойства группы Судзуки

Семейство исключительных групп, известных как группы Судзуки, впервые представлены в [146,147]. Определения и свойства группы Судзуки $Sz(q)$ изложены в [148]. Группу $Sz(q)$ не следует путать с Судзуки 2-группой или спорадической группой Судзуки.

Замечание 3.1.

1. Существуют различные концептуальные определения группы Судзуки. Явное представление группы на основе матриц 4×4 над полями характеристики $p=2$ дано в оригинальной работе Судзуки [146]. Параметризация группы выполнена в работах [148,151].

2. Основные положения отображения автоморфизма и отображение Фробениуса имеют следующие представления.

Определение 3.1 [152]. Свойство гомоморфизма. Отображение $\varphi: G\to G^*$ группы G в группу G^* называется гомоморфизмом группы G в группу G^*, если для всех $a,b\in G$ имеет место равенство $(ab)^{\varphi}=a^{\varphi}b^{\varphi}$.

Если φ отображение на G^*, то оно называется эпиморфизмом. Гомоморфизм группы $G\to G$ называется эндоморфизмом. Если φ взаимно однозначный гомоморфизм группы G на группу G^*, то он называется изоморфизмом. Изоморфизм группы $G\to G$ называется автоморфизмом. Если φ, ψ – автоморфизмы группы G, то для любых $a,b\in G$ справедливо $(\varphi\circ\psi)(ab)=\varphi(\psi(ab))=\varphi(\psi(a)\psi(b))=(\varphi\circ\psi)(a)(\varphi\circ\psi)(b)$.

Определение 3.2. [152]. Полевой автоморфизм. Изоморфное отображение φ поля P на себя $\varphi: P\to P$ является автоморфным, для которого сохраняется равенство $a^{\varphi}\neq b^{\varphi}$, $a\neq b$, $a,b\in P$, $(ab)^{\varphi}=a^{\varphi}b^{\varphi}$ и $(a+b)^{\varphi}=a^{\varphi}+b^{\varphi}$.

Пусть $q=2^{2n+1}$ и F_q – конечное поле. Пусть $\theta=2^{n+1}$. Тогда, для любого $x\in F_q$ получим $\left(x^{\theta}\right)^{\theta}=x^2$. Говорят, что отображение $x\to x^{\theta}$ действует как «квадратный корень» из отображения Фробениуса $x\to x^2$.

Предложение 3.1. Отображение $x\to x^{\theta}$ является автоморфизмом поля F_q, $q=2^{2n+1}$.

Поле F_q содержит мультипликативную группу элементов $F_q^{\times}$ порядка $q-1$. Пусть образующий элемент группы α. Так как θ не делит $q-1$, тогда отображение $\varphi: x \to x^{\theta}$, $x \in F_q^{\times}$ приводит к мультипликативной группе с образующим элементом $\beta = \alpha^{\theta}$ порядка $q-1$.

Конечные или мультипликативные группы одинакового порядка являются изоморфными. Пусть $a = \alpha^i$ и $b = \alpha^j$, $i \neq j$, получим $a^{\varphi} = \alpha^{i \cdot \theta} = \beta^i$, $b^{\varphi} = \alpha^{j \cdot \theta} = \beta^j$ и $\beta^i \neq \beta^j$. Свойство $(ab)^{\varphi} = a^{\varphi} b^{\varphi}$ относительно операции умножения для отображения $\varphi: x \to x^{\theta}$ следует из вычислений показателей степеней $a = \alpha^i$, $b = \alpha^j$. Свойство $(a+b)^{\varphi} = a^{\varphi} + b^{\varphi}$ относительно операции сложения следует из вычислений степени суммы $(a+b)^{\theta} = a^{\theta} + b^{\theta}$ в поле F_q характеристики 2.

Замечание 3.2.

1. Множество элементов из F_q, остающихся неподвижными для отображения $\varphi: x \to x^{\theta}$, совпадает с простым подполем $\left\{\alpha \in F_q \middle| \alpha^{\theta} = \alpha\right\} = F_2$. Простое подполе F_2 является единственным неподвижным подполем поля F_q автоморфизма $\varphi: x \to x^{\theta}$. Так как $n+1$ не имеет общих делителей, отличных от единицы с $2n+1$, для отображения $\varphi: x \to x^{\theta}$ не существует других неподвижных подполей.

2. Результат предложения 3.1 является известным. Общий результат представлен в предложении 3.2.

Предложение 3.2. Для конечного поля F_{p^d} существует неподвижное поле автоморфизма $\varphi: \left\{\alpha \in F_{p^d} \middle| \alpha^{p^e} = \alpha\right\} = F_{p^c}$, где $c = \gcd(d, e)$.

Доказательство. Поле F_q, $q = p^d$ содержит мультипликативную группу элементов $F_q^{\times}$ порядка $q-1$. Пусть образующий элемент группы α. Так как $\theta = p^e$ не делит $q-1$, тогда отображение $\varphi: x \to x^{p^e}$, $x \in F_q^{\times}$ приводит к мультипликативной группе с образующим элементом $\beta = \alpha^{\theta}$ порядка $q-1$. Мультипликативные группы одинакового порядка являются изоморфными. По определению автоморфизма поля $a^{\varphi} \neq b^{\varphi}$, $a \neq b$, $a, b \in F_q$. Пусть $a = \alpha^i$ и $b = \alpha^j$, $i \neq j$, получим $a^{\varphi} = \alpha^{i\cdot\theta} = \beta^i$, $b^{\varphi} = \alpha^{j\theta} = \beta^j$ и $\beta^i \neq \beta^j$. Свойство $(ab)^{\varphi} = a^{\varphi} b^{\varphi}$ относительно операции умножения для отображения $\varphi: x \to x^{p^e}$ следует из вычислений показателей степеней $a = \alpha^i$, $b = \alpha^j$. Свойство $(a+b)^{\varphi} = a^{\varphi} + b^{\varphi}$ относительно операции сложения следует из вычислений степени суммы $(a+b)^{p^e} = a^{p^e} + b^{p^e}$ в поле F_{p^d} характеристики p.

Так как c делит d, F_{p^d} содержит подполе F_{p^c} с точками $\alpha^{i\cdot\left(p^d-1\right)/\left(p^c-1\right)}$, $i = \overline{0,\, p^c - 1}$. Следует показать, что множество элементов из F_{p^d}, остающихся неподвижными при отображении $\varphi: x \to x^{p^e}$, совпадает с подполем F_{p^c}, $c = \gcd(d, e)$. Пусть $e = c \cdot m$, тогда по свойству 1 получим

$$\varphi: x \to x^{p^e} = x^{p^{c\cdot m}} = \left(x^{p^c}\right)^{p^{c(m-1)}} = \left(\left(\left(x^{p^c}\right)^{p^c}\right)^{\cdots}\right)^{p^c} = \varphi^c\left(\varphi^c\left(\varphi^c \ldots \left(\varphi^c\left(x\right)\right)\right)\right),$$

где $\varphi^c(x): x \to x^{p^c}$. Автоморфизм $\varphi: x \to x^{p^e}$ является m кратным применением автоморфизма $\varphi^c(x): x \to x^{p^c}$. Применение $\varphi^c(x)$ к точкам F_{p^c} приводит к результату

$$\varphi^c(a) = \varphi^c\left(\alpha^{i\left(p^d-1\right)/\left(p^c-1\right)}\right) = \left(\alpha^{i\left(p^d-1\right)/\left(p^c-1\right)}\right)^{p^c} = \alpha^{i\left(p^d-1\right)p^c/\left(p^c-1\right)\bmod\left(p^d-1\right)} =$$

$$\alpha^{i\left(p^d-1\right)+i\left(p^d-1\right)/\left(p^c-1\right)\bmod\left(p^d-1\right)} = \alpha^{i\left(p^d-1\right)/\left(p^c-1\right)}.$$

Автоморфизм $\varphi: x \to x^{p^e}$ определяется m кратным вычислением автоморфизма $\varphi^c(x)$ и не смещает точки подполя F_{p^c}, так как на каждой итерации вычисляется один и тот же автоморфизм $\varphi^c(x)$, который оставляет неподвижными точки подполя F_{p^c}.

Замечание 3.3.

1. Результат предложения 3.2 достаточно очевиден и повторяет аналогичный результат в теории групп [153].

2. Неподвижное поле автоморфизма $\varphi: \left\{\alpha \in F_{p^d} \middle| \alpha^{p^e} = \alpha\right\} = F_{p^c}$ является наибольшим, так как $c = \gcd(d, e)$.

3. Особенно большое значение в теории конечных групп имеют элементы порядка 2, которые обычно называются инволюциями. Инволюции – элементы, обладающие свойством $a * a = e$.

Определение 3.3. (Группа Судзуки). Пусть $a, b, \alpha, \beta \in F_q$, $q = 2^{2n+1}$ и $c, \gamma \in F_q^{\times}$, где $F_q^{\times}$ – мультипликативная группа. Определим 4×4 матрицы над F_q

$$u(a, b, \alpha, \beta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \alpha a + \beta & a & 1 & 0 \\ \alpha^2 a + \alpha\beta + b & \beta & \alpha & 1 \end{pmatrix},$$

$$d(c, \gamma) = \begin{pmatrix} c\gamma & 0 & 0 & 0 \\ 0 & \gamma & 0 & 0 \\ 0 & 0 & \gamma^{-1} & 0 \\ 0 & 0 & 0 & \gamma^{-1}c^{-1} \end{pmatrix}, T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Пусть $U(\alpha, \beta) = u(\alpha^\theta, \beta^\theta, \alpha, \beta)$ и $D(\gamma) = d(\gamma^\theta, \gamma)$, $\theta = 2^{n+1}$. Группа Судзуки имеет представление

$$Sz(q)=\{U(\alpha,\beta)D(\gamma)TU(\alpha',\beta'):\alpha,\alpha',\beta,\beta'\in F_q,\gamma\in F_q^{\times}\}\cup \\ \cup\{U(\alpha,\beta)D(\gamma):\alpha,\beta\in F_q,\gamma\in F_q^{\times}\}. \quad (3.1)$$

Замечание 3.4.

1. Параметризация группы Судзуки по определению 3.3 впервые представлена в [151] и взята из работы [154]. Группа Судзуки следует из выражения (3.1) и определяется множествами матриц 4×4 над конечным полем F_q, $q=2^{2n+1}$ характеристики 2.

2. Свойства группы Судзуки достаточно полно исследованы в [148] с несколько отличным представлением матричных групп. Следуя работе [148], рассмотрим следующие определения.

Определение 3.4. Пусть $\pi(x)=x^t$, $t=2^{m+1}$ для $\forall x\in F_q$, $q=2^{2m+1}$, π – исключительный автоморфизм в F_q, такой что $\pi(\pi(x))=x^2$. Для $a,b\in F_q$ и $c\in F_q^{\times}$ определим матрицы:

$$S(a,b)=\begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & \pi(a) & 1 & 0 \\ a^2\pi(a)+ab+\pi(b) & a\pi(a)+b & a & 1 \end{pmatrix},$$

$$M(c)=\begin{pmatrix} c^{1+2^m} & 0 & 0 & 0 \\ 0 & c^{2^m} & 0 & 0 \\ 0 & 0 & c^{-2^m} & 0 \\ 0 & 0 & 0 & c^{-1-2^m} \end{pmatrix},\ T=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Замечание 3.5.

1. Матрицы $S(a,b)$ и $M(c)$ следуют из переопределений матриц $U(\alpha,\beta)$ и $D(\gamma)$ с заменой переменных $\alpha\to a$, $\alpha a+\beta\to b$, $\gamma\to c^{2^m}$.

Определение 3.5. Группа Судзуки в соответствии с выражением (3.1) определяется произведением матриц:

$$Sz(q)=\left\langle S(a,b),M(c),T\,\middle|\,a,b\in F_q,c\in F_q^{\times}\right\rangle, \tag{3.2}$$

имеет порядок

$$\left|Sz(q)\right|=q^2\left(q^2+1\right)(q-1),$$

где три делителя попарно взаимно простые и

$$\left(q^2+1\right)=(q+t+1)(q-t+1).$$

Предложение 3.3. Для всех $a,b,a',b'\in F_q$ и $c\in F_q^{\times}$ справедливо

$$S(a,b)S(a',b')=S\left(a+a',b+b'+\pi(a)a'\right), \tag{3.3}$$

$$S(a,b)^{M(c)}=S(ca,c\pi(c)b). \tag{3.4}$$

$$M(c)M(c')=M(cc'). \tag{3.5}$$

Соотношения (3.3)–(3.5) проверяются прямыми вычислениями. Результаты (3.3),(3.4) следуют из свойств автоморфизма $\pi\left(\pi(a)\right)=a^2$, $\pi(ab)=\pi(a)\pi(b)$ и $\pi(a+b)=\pi(a)+\pi(b)$, $a,b\in F_q$ в поле характеристики 2:

$$S(a,b)S(a',b')=\begin{pmatrix}1 & 0 & 0 & 0\\ a & 1 & 0 & 0\\ b & \pi(a) & 1 & 0\\ a^2\pi(a)+ab+\pi(b) & a\pi(a)+b & a & 1\end{pmatrix}\times$$

$$\times\begin{pmatrix}1 & 0 & 0 & 0\\ a' & 1 & 0 & 0\\ b' & \pi(a') & 1 & 0\\ a'^2\pi(a')+a'b'+\pi(b') & a'\pi(a')+b' & a' & 1\end{pmatrix}=$$

$$=\begin{pmatrix}1 & 0 & 0 & 0\\ a+a' & 1 & 0 & 0\\ b+b'+a'\pi((a)) & \pi(a)+\pi(a') & 1 & 0\\ \begin{array}{l}a^2\pi(a)+ab+\pi(b)+\\ +a'a\pi(a)+a'b+ab'+\\ +a'^2\pi(a')+a'b'+\pi(b')\end{array} & \begin{array}{c}a\pi(a)+b+a\pi(a')+\\ +b'+a'\pi(a')\end{array} & a+a' & 1\end{pmatrix}=$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ a+a' & 1 & 0 & 0 \\ b+b'+a'\pi(a) & \pi(a+a') & 1 & 0 \\ (a+a')^2\pi(a+a')+ & (a+a')\pi(a+a')+ & & \\ +(a+a')(b+b'+a'\pi(a))+ & +b+b'+a'\pi(a) & a+a' & 1 \\ +\pi(b+b'+a'\pi(a)) & & & \end{pmatrix} =$$

$$= S(a+a', b+b'+\pi(a)a').$$

Аналогично имеем

$$S(a,b)^{M(c)} = M(c)^{-1} S(a,b) M(c) = \begin{pmatrix} c^{-1-2^m} & 0 & 0 & 0 \\ 0 & c^{-2^m} & 0 & 0 \\ 0 & 0 & c^{2^m} & 0 \\ 0 & 0 & 0 & c^{1+2^m} \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & \pi(a) & 1 & 0 \\ a^2\pi(a)+ab+\pi(b) & a\pi(a)+b & a & 1 \end{pmatrix} M(c) =$$

$$= \begin{pmatrix} c^{-1-2^m} & 0 & 0 & 0 \\ ac^{-2^m} & c^{-2^m} & 0 & 0 \\ bc^{2^m} & \pi(a)c^{2^m} & c^{2^m} & 0 \\ (a^2\pi(a)+ab+\pi(b))c^{1+2^m} & (a\pi(a)+b)c^{1+2^m} & ac^{1+2^m} & c^{1+2^m} \end{pmatrix} \times$$

$$\times \begin{pmatrix} c^{1+2^m} & 0 & 0 & 0 \\ 0 & c^{2^m} & 0 & 0 \\ 0 & 0 & c^{-2^m} & 0 \\ 0 & 0 & 0 & c^{-1-2^m} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ ac & 1 & 0 & 0 \\ bc^{1+2^{m+1}} & \pi(a)c^{2^{m+1}} & 1 & 0 \\ \left(a^2\pi(a)+ab+\pi(b)\right)c^{2+2^{m+1}} & \left(a\pi(a)+b\right)c^{1+2^{m+1}} & ac & 1 \end{pmatrix} =$$

$$= S\left(ca, c\pi(c)b\right).$$

Умножение диагональных матриц $M(c), M(c')$ в поле F_q приводит к (3.5).

Следствие 1. Для всех $a, b, a', b' \in F_q$ и $c \in F_q^{\times}$, $q = 2^{2m+1}$ справедливо

$$S(a,b)^{-1} = S\left(a, b+\pi(a)a\right), \tag{3.6}$$

$$S(a,b)^{S(a',b')} = S\left(a, b+\pi(a)a'+\pi(a')a\right). \tag{3.7}$$

Доказательство. Выражения (3.6) и (3.7) проверяются прямыми вычислениями:

$$S(a,b)S(a,b)^{-1} = S(a,b)S\left(a, b+\pi(a)a\right) =$$
$$= S\left(a+a, b+b+\pi(a)a+\pi(a)a\right) = S(0,0).$$

$$S(a,b)^{S(a',b')} = S(a',b')^{-1}S(a,b)S(a',b') =$$
$$= S(a',b')^{-1}S\left(a+a', b+b'+\pi(a)a'\right) =$$
$$= S(a',b'+\pi(a')a')S(a+a',b+b'+\pi(a)a') =$$
$$= S\left(a'+a+a', b'+\pi(a')a'+b+b'+\pi(a)a'+\pi(a')\left(a+a'\right)\right) =$$
$$= S\left(a, b+\pi(a)a'+\pi(a')a\right).$$

Предложение 3.4. Пусть,

$$\Im = \left\{S(a,b)\middle| a,b \in F_q\right\},$$

$$H = \left\{M(c)\middle| c \in F_q^{\times}\right\},$$

тогда $\Im \le Sz(q)$ является второй группой с экспонентой 4, мощности $|\Im| = q^2$ и Н изоморфна циклической группе $F_q^{\times}$ порядка $q-1$.

Доказательство. Порядки элементов $g \in \Im$ принимают значения 2 и 4. Действительно, для $a, b \in F_q$ и $a \neq 0$ по правилу умножения (3.3) получим $S(a,b)S(a,b) = S(0, a\pi(a))$ и $S(0, a\pi(a))S(0, a\pi(a)) = S(0,0)$, где $S(0,0)$ является единицей группы. Порядок элементов $g = S(a,b)$, $a \neq 0$ равен 4.

В случае $a = 0$, $b \neq 0$ имеем $S(0,b)S(0,b) = S(0,0)$ с порядком 2. Значениями показателей степеней $m = 2$ и 4 таких, что $g^m = 1$ исчерпываются порядки элементов группы $g \neq 1$. По определению экспоненты, наименьшее значение порядков элементов группы $m \geq 1$ такое, что $g^m = 1$ для всех $g \in \Im$ получим $m = 4$.

Мощность группы $\Im$ равна q^2, так как определяется числом элементов $S(a,b)$, $a, b \in F_q$.

Группа $H = \left\{ M(c) \middle| c \in F_q^{\times} \right\}$ определяется диагональными матрицами $M(c)$ с операцией умножения (3.5) в поле F_q. Для любых $a \neq b$, $a, b \in F_q^{\times}$, $M(a) \neq M(b)$, так как степени диагональных элементов 2^{m+1} и 2^m не делят $q-1$. $M(c)$ является единичной матрицей для $c = 1$. Группа H имеет порядок $q-1$. Конечные мультипликативные группы H и $F_q^{\times}$ одинакового порядка являются изоморфными.

Определение 3.6 [148]. Группа Фробениуса является конечной группой G с нетривиальной нормальной подгруппой N (ядро Фробениуса) и нетривиальной подгруппой H (дополнение Фробениуса), порядки которых взаимно простые, и для каждого элемента $x \in G \setminus N$ существует единственный элемент $y \in N$ такой, что $x \in yHy^{-1}$.

Определение 3.7. Пусть G – некоторая группа. Подгруппа $N \subset G$ называется нормальной в G, если $gNg^{-1} = N$ для любого $g \in G$, где $gNg^{-1} = \left\{ gyg^{-1} : y \in N \right\}$.

Тот факт, что N – нормальная подгруппа группы G, традиционно обозначают символом $N \lhd G$.

Свойства:

1. Группа Фробениуса имеет представление $G = NH$ и $N \bigcap H = \{1\}$.

2. Для любого $g \in G \setminus H$ справедливо $H \bigcap gHg^{-1} = 1$.

3. Ядро Фробениуса является нильпотентом [148]

Замечание 3.6.

1. Просто показать, что для каждого элемента $x \in G \setminus N$ из определения группы Фробениуса существует единственный элемент $y \in N$ такой что $x \in yHy^{-1}$.

Действительно, пусть $y \in N$ и $h \in H$, тогда получим

$$yhy^{-1} = yhy^{-1}h^{-1}h = yy_1h = y_2h.$$

Здесь $y_1 = hy^{-1}h^{-1}$, $y_1 \in N$ в силу нормальности подгруппы N и $yy_1 = y_2$, $y_2 \in N$, так как $y, y_1 \in N$. Если y не является единицей группы, тогда и y_2 – не единица и $y_2h \in G \setminus N$.

2. Дополнение Фробениуса H является нормализатором для элементов $y \in G \setminus N$.

По определению нормализатора имеем

$$\mathrm{Norm}(H) = \left\{ g \in G \setminus N : gHg^{-1} = H \right\}.$$

Пусть $g = y_1h_1$, $y_1 \in H$, $h_1 \in H$ и не являются единицами. Для $h \in H$ вычислим

$$ghg^{-1} = y_1h_1hy_1^{-1}h_1^{-1} = y_1h_2y_1^{-1}h_1^{-1} = y_2h_1^{-1},$$

где $h_2 = h_1h$, $y_2 = y_1h_2y_1^{-1}$.

Для фиксированного $g = y_1h_1$ условие сопряжения $ghg^{-1} \in H$ выполняется для единственного элемента $h = h_1^{-1}$, $h \in H$. Отсюда следует справедливость $gHg^{-1} = H$ только для $g \in H$.

3. Свойство 2 определяет перестановочное групповое представление группы Фробениуса как конечную перестановочную группу G, в которой нет неединичного элемента, фиксирующего больше чем одну точку на некотором множестве Ω, на котором G действует транзитивно. Такое действие на множестве Ω представляет выбор H как точку стабилизатора.

4. Свойство 1 переводит задачу построения группы Фробениуса в задачу нахождения конечной группы N, которая допускает группу автоморфизмов H таких, что не существует неединичный элемент подгруппы H, который фиксирует какой-либо неединичный элемент подгруппы N.

5. Каноническим примером группы Фробениуса считается случай, когда N является аддитивной группой элементов конечного поля F_q, и H мультипликативной группой этого поля, которые действуют умножением (в поле) на N.

Предложение 3.5. [148]. Группа $H = \left\{ M\left(c\right) \middle| c \in F_q^{\times} \right\}$ действием $S\left(a,b\right)^{M(c)}$ порождает группу неподвижной точки свободных автоморфизмов на $\mathfrak{I} = \left\{ S\left(a,b\right) \middle| a,b \in F_q \right\}$, и $\mathfrak{I}H$ является группой Фробениуса с ядром Фробениуса $\mathfrak{I}$.

Доказательство. Выражение (3.4) предложения 3.3 определяет, что группа H транзитивно переставляет множество неединичных элементов группы $\mathfrak{I}$. В случае $c \neq 1$ соответственно $c\pi\left(c\right) \neq 1$ каждый неединичный элемент группы H трансформирует свободно неподвижную (фиксированную) точку $\mathfrak{I}$.

Группа Фробениуса $G = \mathfrak{I}H$ определяется нормальной подгруппой $\mathfrak{I}$ и дополнением H. Из предложения 3.4 следует, что порядки групп являются взаимно простыми. Выражения (3.4) и (3.7) определяют группу $\mathfrak{I}$ как нормальную группу в силу определения 3.5. Группа G является группой

Фробениуса, если существует собственная нетривиальная подгруппа H (дополнение Фробениуса), такая, что нормализатор H в $G\,\mathrm{Norm}_G(H)=H$.

Пусть $y=S(a,b)$ и $h=M(c)$, $h\in H$. Выполним следующие вычисления:

$$yhy^{-1}=S(a,b)M(c)S(a,b)^{-1}=$$
$$=M(c)M(c)^{-1}S(a,b)M(c)S(a,b)^{-1}=$$
$$=M(c)S(ca,c\pi(c)b)S(a,b+\pi(a)a)=$$
$$=M(c)S(ca+a,c\pi(c)b+b+\pi(a)a+\pi(ca)a)=$$
$$=M(c^{-1})^{-1}S(ca+a,c\pi(c)b+b+\pi(a)a+\pi(ca)a)M(c^{-1})M(c)=$$
$$=S(a+c^{-1}a,c^{-1}\pi(c^{-1})(c\pi(c)b+b+\pi(a)a+\pi(ca)a))M(c)=$$
$$=S(a+c^{-1}a,b+c^{-1}\pi(c^{-1})b+c^{-1}\pi(c^{-1})\pi(a)a+c^{-1}\pi(c^{-1})\pi(ca)a)M(c)=$$
$$=S(a+c^{-1}a,b+c^{-1}\pi(c^{-1})b+c^{-1}a\pi(c^{-1}a)+c^{-1}a\pi(a))M(c)=$$
$$=S(a(1+c^{-1}),b(1+c^{-1}\pi(c^{-1}))+a\pi(a)c^{-1}\pi(1+c^{-1}))M(c).$$

В случае $c\neq 1$, $a\neq 0$ и/или $b\neq 0$

$$S(a(1+c^{-1}),b(1+c^{-1}\pi(c^{-1}))+a\pi(a)c^{-1}\pi(1+c^{-1}))M(c)\notin H.$$

Пусть $y=S(a,b)M(c')$ и $h=M(c)$, получим

$$yhy^{-1}=S(a,b)M(c')M(c)S(a,b)^{-1}M(c')^{-1}=$$
$$=S(a,b)M(cc')S(a,b)^{-1}M(c')^{-1}=$$
$$=S(a(1+(cc')^{-1}),b(1+(cc')^{-1}\pi((cc')^{-1}))+$$
$$+a\pi(a)(cc')^{-1}\pi(1+(cc')^{-1}))M(cc')M(c')^{-1}=$$
$$=S(a(1+(cc')^{-1}),b(1+(cc')^{-1}\pi((cc')^{-1}))+$$
$$+a\pi(a)(cc')^{-1}\pi(1+(cc')^{-1}))M(c).$$

Только в одном случае $yhy^{-1}\in H$, если $c'=c^{-1}$. Как результат получим $\mathrm{Norm}_G(H)=H$.

Замечание 3.7.

1. Доказательство предложения 3.5 впервые представлено в развернутом виде.

2. По свойству 1 определения 3.7 порядок группы $\Im H$ равен $q^2(q-1)$.

3. Группа Судзуки содержит подгруппы $S(a,b)$, $M(c)$ и подгруппы Холла и подгруппы по делителям их порядков.

3.2 Кривые Дэлигнэ – Лустига, ассоциированные с группой Судзуки

Кривая максимального рода над квадратичным полем F_q, $q=l^2$ является кривой Эрмита. По классификации кривых Дэлигнэ – Лустига кривая Эрмита ассоциируется с проективной специальной линейной группой, покрывает максимальные плоские кривые меньшего рода в квадратичном поле и имеет наилучшую асимптотическую оценку:

$$A(q)=\limsup_{g\to\infty} N_q(g)\Big/ g,$$

$$A(q)\approx 2\sqrt{q},$$

где $N_q(g)$ – число точек кривой рода g.

Вторая и третья группа кривых Дэлигнэ – Лустига ассоциируются с группой Судзуки $Sz(q)$ и группой Ри $R(q)$ [105]. Кривые Судзуки и Ри широко рассмотрены в [155–157]. Эти кривые являются оптимальными кривыми в том смысле, что имеют число F_q рациональных точек относительно рода достаточно близким к границе Хассе – Вейля.

Главный результат по кривым Дэлигнэ – Лустига второго типа, ассоциированным с $Sz(q)$, определяется следующей теоремой.

Теорема [110]**.** Для положительного целого s заданы $q=2q_0^2$ и $q_0=2^s$. Пусть X кривая над F_q рода g и удовлетворяются следующие условия:

1) $g = q_0(q-1)$;

2) $\#X(F_q) = q^2 + 1$.

Тогда X является F_q изоморфной кривой Дэлигнэ – Лустига, ассоциированной с группой Судзуки $Sz(q)$.

Кривую с точностью до F_q изоморфизма, ассоциированную с подгруппой $S(a,b)$ группы Судзуки $Sz(q)$, основанную на роде, числе точек и групповом F_q автоморфизме кривой, определили Хансен Дж. и Стичтенот Х. [155].

Кривая Судзуки S является F_q изоморфной плоской кривой

$$y^q - y = x^{q_0}\left(x^q - x\right), \tag{3.8}$$

где $q = 2q_0^2$ и $q_0 = 2^s$.

Род кривой $g = q_0(q-1)$ и число F_q рациональных точек равно q^2+1 [155].

Кривая, ассоциированная с подгруппой $S(a,b)$ порядка q^2 из группы Судзуки порядка $q^2\left(q^2+1\right)(q-1)$,

$$S(a,b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & \pi(a) & 1 & 0 \\ a^2\pi(a) + ab + \pi(b) & a\pi(a) + b & a & 1 \end{pmatrix}.$$

Кривая Судзуки, рассмотренная Хансеном Дж. и Стичтенотом Х., имеет относительно своего рода максимальное число точек. Максимальное число F_q рациональных точек кривой определяется замечательной формулой Вейля и для кривой Судзуки чуть меньше границы Хассе – Вейля. Действительно, прямая подстановка в оценку числа точек Хассе – Вейля рода кривой дает значение

$$N_q(g)=1+q+2g\sqrt{q}=\sqrt{2}q^2-\left(\sqrt{2}-1\right)q+1 \tag{3.9}$$

и имеем, что $q^2+1<\sqrt{2}q^2-\left(\sqrt{2}-1\right)q+1.$

Число F_{q^r} рациональных точек кривой $N_{q^r}(g)$ можно определить на основе вычисления специального L полинома – энумератора дзета-функции

$$\zeta(X,t)=\exp\left(\sum N_{q^r}t^r/r\right).$$

Известен результат Хассе – Вейля

$$\zeta(X,t)=L(X,t)/\{(1-t)(1-qt)\},$$

где

$$L(X,t)=\prod_{k=1}^{2g}(1-\alpha_k t),\ L(X,t)\in Z(t), \tag{3.10}$$

$$\alpha_j\alpha_{j+g}=q,\ j=1,\ldots,g, \tag{3.11}$$

$$|\alpha_j|=\sqrt{q},\ j=1,\ldots,g. \tag{3.12}$$

Следуя [40,161], если

$$L(X,t)=\prod_{k=1}^{2g}(1-\alpha_k t),$$

число точек кривой в расширенном поле F_{q^r} определяется выражением

$$N_{q^r}(g)=q^r+1-\sum_{k=1}^{2g}\alpha_k^r. \tag{3.13}$$

Для кривой Судзуки, как показано в [156], энумератор имеет вид

$$L(X,t)=\left(1+2q_0t+qt^2\right)^g. \tag{3.14}$$

Полином $L(X,t)$ имеет $2g$ корней, и решения для α_k из (3.10) разбиваются на две группы по g одинаковых значений

$$\alpha=q_0(-1+i)$$

и

$$\beta=\tilde{\alpha}=q_0(-1-i).$$

Для α и β легко проверяются условия (3.11) и (3.12). Для $N_{q^r}(g)$ получим результирующее выражение

$$N_{q^r}(g)=q^r+1-g\left(\alpha^r+\beta^r\right). \tag{3.15}$$

Рассмотрим основные случаи расширенного поля F_{q^r} и значения числа точек для кривой Судзуки. Подставляя в (3.15) степени расширения $r=1,\ldots,4$, получим

$$N_q(g)=q+1-g(\alpha+\beta)=q+1+2gq_0=q+1+2q_0q_0(q-1)=q^2+1;$$

$$N_{q^2}(g)=q^2+1-g(\alpha^2+\beta^2)=q^2+1-gq_0{}^2(-2i+2i)=q^2+1;$$

$$N_{q^3}(g)=q^3+1-g(\alpha^3+\beta^3)=q^3+1-4gq_0{}^3=q^3+1-4q_0{}^4(q-1)=q^2+1;$$

$$N_{q^4}(g)=q^4+1-g(\alpha^4+\beta^4)=q^4+1+8gq_0{}^4=q^4+1+2q_0(q-1)q^2.$$

Замечание 3.8.

1. Кривая Судзуки над полем F_q является оптимальной для кривой рода $g=q_0(q-1)$, по числу точек лежит близко к границе Хассе – Вейля.

2. Кривая Судзуки над квадратичным и кубическим полем является неоптимальной.

3. Кривая Судзуки над конечным полем степени расширения 4 является максимальной. Подстановка значения рода $g=q_0(q-1)$ в выражение Хассе – Вейля дает

$$N_{q^4}(g)=q^4+1+2q_0(q-1)q^2,$$

что равно числу точек кривой в F_{q^4}.

4. Более общий результат получен в [156], где показано, что для расширений $r\equiv 0 \bmod 4$ кривая Судзуки является максимальной. Действительно,

$$N_{q^{4s}}(g)=q^{4s}+1-g(\alpha^{4s}+\beta^{4s})=q^{4s}+1+2\cdot 4^s gq_0{}^{4s}=$$
$$=q^{4s}+1+2q_0(q-1)q^{2s},\quad s\geq 1.$$

5. В работе [156] рассмотрена кривая Судзуки

$$y^q-y=x^{q_0}(x^q-x),$$

где $q_0=2^s$ и $q=2q_0$.

Показано, что кривая имеет род $g = q_0(q-1)$, число точек $N_q(g) = q^2 + 1$ и также является F_q-изоморфной кривой Дэлигнэ – Лустига, ассоциированной с группой Судзуки $Sz(q)$. По сравнению с выражением (3.8), кривая определена над меньшим в q_0 раз конечным полем и содержит в ${q_0}^2$ меньше точек.

6. В работе [158] получены производные кривые по подгруппам группы Судзуки для случая $q = 2{q_0}^2$ и $q_0 = 2^s$.

По циклической подгруппе порядка r, $r \mid q-1$ кривая рода $g = q_0(q-1)/r$ имеет вид

$$V^{(q-1)/r} f(U) = \left(1 + U^{q_0}\right)\left(U^{q-1} + V^{2(q-1)/r}\right),$$

где $f(t) = 1 + \sum_{i=0}^{s-1} t^{2^i(2q_0+1)-(q_0+1)} \left(1+t\right)^{2^i}$.

Кривая по подгруппе Зингера порядка $q + 2q_0 + 1$ имеет род $g = (q + 2q_0 + 1)(q_0 - 1)/r + 1$ и определяется выражением

$$V^{(q+2q_0+1)/r} \tilde{f}(U) = U^{q+2q_0+1} + V^{2(q+2q_0+1)/r},$$

где $\tilde{f}(t) = 1 + \sum_{i=0}^{s-1} t^{2^i q_0} \left(1+t\right)^{2^i(q_0+1)+q_0} + t^{q/2}$.

Кривая по подгруппе Зингера порядка $q - 2q_0 + 1$ имеет род $g = (q - 2q_0 + 1)(q_0 - 1)/r - 1$ и вид

$$bV^{(q-2q_0+1)/r} f(U) = \left(U^{q_0-1} + V^{2q_0-1}\right)\left(U^{q-2q_0+1} + V^{2(q-2q_0+1)/r}\right),$$

где $b = \lambda^{q_0} + \lambda^{q_0-1} + \lambda^{-q_0} + \lambda^{-(q_0-1)}$, $\lambda \in F_{q^4}$, порядка $q - 2q_0 + 1$.

7. В [158] рассмотрены кривые, ассоциированные с подгруппами группы Судзуки порядков $2^u r$, $2r$, $2s$, $4s$, где $r \mid (q-1)$, $s \mid (q \pm 2q_0 + 1)$. Кривые по данным подгруппам имеют число точек, соответствующих порядкам

подгрупп, что меньше числа точек кривой, ассоциированной с подгруппой $S(a,b)$ порядка q^2.

3.3 Функциональное поле кривой Судзуки

Кривая Дэлигнэ – Лустига, ассоциированная с группой Судзуки, определяется полной линейной серией $D=\left|(q+2q_0+1)P_0\right|$ размерности $\dim=4$ и степени $q+2q_0+1$, которая выводится из энумератора дзета-функции [155]. Отображение кривой Судзуки на проективное пространство P^4 и подгруппа Вейерштрасса $H(P)$, $P\in X(F_q)$ рассмотрены в работах [110,155]. Основные результаты обобщены в утверждении 3.1.

Утверждение 3.1 [38]. F_q-рациональный морфизм кривой Судзуки в P^4 есть отображение

$$\pi := (1:x:y:v:w),$$

где x, y, v, w определяются уравнениями [155]

$$y^q - y = x^{q_0}\left(x^q - x\right),$$

$$v := x^{2q_0+1} + y^{2q_0},$$

$$w := xy^{2q_0} + x^{2q+2q_0} + y^{2q},$$

и порядки полюсов

$$\mathrm{div}_\infty(x) = qP_0,\ \mathrm{div}_\infty(y) = (q+q_0)P_0,$$

$$\mathrm{div}_\infty(v) = (q+2q_0)P_0,\ \mathrm{div}_\infty(w) = (q+2q_0+1)P_0.$$

Кривая Судзуки может быть представлена в P^4 множеством точек вида

$$P_{(a,b)} := (1:a:b:f(a,b):af(a,b)+b^2)\bigcup\pi(P_0) = (0:0:0:0:1),$$

где $a,b\in F_q$ и $f(a,b) := a^{2q_0+1} + b^{2q_0}$ [128].

Подгруппа Вейерштрасса $H(P)$, $P \in C(F_q)$ функционального поля кривой содержит подгруппу [126]

$$H(P) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle.$$

Доказательство. Покажем подгруппу Вейерштрасса. Для этого запишем уравнение кривой в проективных координатах:

$$Y^q Z^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1} Z^{q+q_0-1}. \qquad (3.16)$$

На кривой C существуют особая точка на бесконечности $P_0 = (0:1:0)$ кратности q_0 и рациональные точки $P_{\alpha,0} = (\alpha:0:1)$, $P_{0,\beta} = (0:\beta:1)$, где $\alpha, \beta \in F_q$.

Пусть $\aleph$ – линия с уравнением $X = 0$. Тогда $\aleph$ пересекает кривую в точках $P_{0,\beta}$ и P_0. Число точек $P_{0,\beta}$ равно q. Линия $\aleph$ имеет только однократные пересечения в точках $P_{0,\beta}$, так как $X = 0$ не является касательной в этих точках. По теореме Безу кратность пересечения линии $\aleph$ с кривой C равна $q + q_0$. Отсюда следует, что $\aleph \cdot C = \sum_{\beta \in F_q} P_{0,\beta} + q_0 P_0$.

Рассмотрим линию $\Re$ с уравнением $Y = 0$. $\Re$ пересекает кривую C в точках $P_{\alpha,0}$ и в точке $P_{0,0} = (0:0:1)$ является касательной кратности пересечения $q_0 + 1$, следовательно $\Re \cdot C = \sum_{\alpha \in F_q,\, \alpha \neq 0} P_{\alpha,0} + (q_0+1) P_{0,0}$. Для линии $\Im$ с уравнением $Z = 0$ имеем пересечение с кривой только в одной точке $P_0 = (0:1:0)$ и $\Im \cdot C = (q+q_0) P_0$.

Для рациональных функций $x = X/Z$ и $y = Y/Z$ получим следующие дивизоры:

$$\operatorname{div}(x) = \sum_{\beta \in F_q} P_{0,\beta} + qP_0,\ \operatorname{div}(y) = \sum_{\alpha \in F_q,\, \alpha \neq 0} P_{\alpha,0} + (q_0+1) P_{0,0} - (q+q_0) P_0,$$

соответственно $\operatorname{div}_\infty(x) = qP_0$ и $\operatorname{div}_\infty(y) = (q+q_0) P_0$ – значения полюса дивизоров.

Рассмотрим уравнение $v := x^{2q_0+1} + y^{2q_0}$. Имеем

$$y = \left(v - x^{2q_0+1}\right)^{1/2q_0}.$$

Подставим в $y^q - y = x^{q_0}\left(x^q - x\right)$ и после преобразований получим

$$v^q - v = x^{2q_0}\left(x^q - x\right).$$

Запишем уравнение в проективных координатах

$$V^q Z^{2q_0} - VZ^{q+2q_0-1} = X^{q+2q_0} - X^{2q_0+1}Z^{q-1}. \qquad (3.17)$$

Уравнение (3.17) так же, как и уравнение кривой (3.16), имеет q^2+1 число решений в F_q.

Рассмотрим линию Ψ с уравнением $V = 0$. Ψ пересекает кривую C в точках $P_{\alpha,\beta}$, $\alpha^{2q_0+1} + \beta^{2q_0} = 0$ и в точке $P_{0,0} = (0:0:1)$ является касательной кратности пересечения $2q_0 + 1$.

Следовательно, $\Re \cdot C = \sum_{\alpha,\beta \in F_q,\ \alpha^{2q_0+1}+\beta^{2q_0}=0} P_{\alpha,\beta} + (2q_0+1)P_{0,0}$.

Для линии $\Im$ с уравнением $Z = 0$ имеем пересечение с кривой $V^q Z^{2q_0} - VZ^{q+2q_0-1} = X^{q+2q_0} - X^{2q_0+1}Z^{q-1}$ только в одной точке $P_0 = (0:1:0)$ и $\Im \cdot C = (q+2q_0)P_0$. Для рациональной функции $v = V/Z$ получим дивизор

$$\operatorname{div}(y) = \sum_{\alpha \in F_q,\ \alpha \neq 0} P_{\alpha,0} + (2q_0+1)P_{0,0} - (q+2q_0)P_0$$

и $\operatorname{div}_\infty(y) = (q+2q_0)P_0$ – значение полюса дивизора.

Определим $w := y^{2q_0}x + v^{2q_0}$. Уравнение от переменных w, y, x имеет вид

$$w^q - w = y^{2q\cdot q_0}x^q + v^{2q\cdot q_0} - y^{2q_0}x - v^{2q_0} = y^{2q_0}\left(x^q - x\right).$$

Порядок полюса функции w в точке P_0 получим с использованием следующих свойств дискретной оценки ϑ_P для рациональных функций.

Предложение 3.6.

а) $\vartheta_{P_0}(xy) = \vartheta_{P_0}(x) + \vartheta_{P_0}(y)$ [130];

б) оценка ϑ_P рациональных функций x, y в уравнении $y^q + \mu y = f(x)$ над $F_q, q = p^s$ определяется выражением [130]

$$q\vartheta_{P_0}(y)=\vartheta_{P_0}\left(y^q+\mu y\right)=\vartheta_{P_0}\left(f(x)\right).$$

Вычислим оценку ϑ_P для w^q-w

$$\vartheta_{P_0}\left(w^q-w\right)=\vartheta_{P_0}\left(y^{2q_0}\left(x^q-x\right)\right)=\vartheta_{P_0}\left(y^{2q_0}\right)+\vartheta_{P_0}\left(x^q-x\right).$$

Так как $\vartheta_{P_0}(x)=\mathrm{div}_\infty(x)=q$ и $\vartheta_{P_0}(y)=\mathrm{div}_\infty(y)=q+q_0$, получим

$$q\vartheta_{P_0}(w)=(q+q_0)2q_0+q\cdot q=q(q+2q_0+1)$$

и значение полюса дивизора $\mathrm{div}_\infty(w)=q+2q_0+1$.

Отсюда следует, что подгруппа Вейерштрасса $H(P)$, $P\in C\left(F_q\right)$ функционального поля кривой содержит подгруппу

$$H(P)=\langle q, q+q_0, q+2q_0, q+2q_0+1\rangle.$$

Число точек разрыва определяет род кривой $\left|G(P_0)\right|=\#(N\setminus H)=q_0(q-1)$ [126]. Линейная серия $q, q+q_0, q+2q_0, q+2q_0+1$ является полной, размерности $\dim=4$ и определяется рациональными функциями $x, y, v, w\in F_q(C)$.

Рассмотрим представление точек кривой Судзуки. Для $P\in C\left(F_q\right)\setminus P_0$ пусть $a:=x(P), b:=y(P)$ и $f(a,b):=v(a,b)=a^{2q_0+1}+b^{2q_0}$. Уравнение для $w:=y^{2q_0}x+v^{2q_0}$ приводится к виду $w:=xy^{2q_0}+x^{2q+2q_0}+y^{2q}$. Тогда $w(a,b):=af(a,b)+b^2$. ◊

Замечание 3.9.

1. Базис пространства $L(\rho_\ell P_0)$, ассоциированный с кривой

$$y^q-y=x^{q_0}\left(x^q-x\right),$$

задается функциями вида

$$S:=\left\{x^r y^t v^i w^j\right\},$$

где $r\le q-1,\ 0\le t\le 1,\ i\le q_0-1,\ j\le q_0-1,$

$$r\cdot q+t(q+q_0)+i(q+2q_0)+j(q+2q_0+1)\le \rho_l.$$

2. Функциональное поле максимальной кривой Судзуки над конечным полем F_{q^4} рассмотрено в [145]. Основной результат определяется следующей теоремой.

Теорема [145]. Пусть $l \in N$, $l \le q^2 - 1$. Тогда

$$S := \left\{ \begin{array}{ll} x^a y^b v^c w^d \left(x^q + x\right)^r & aq + b\left(q + q_0\right) + c\left(q + 2q_0\right) + \\ & + d\left(q + 2q_0 + 1\right) + rq^2 \le l\left(q^2 + 1\right) \\ & \le a \le q - 1, 0 \le b \le 1, 0 \le c \\ & \le\le q_0 - 1, 0 \le d \le q_0 - 1, 0 \le r \le l \end{array} \right\}$$

является базисом линейного пространства $L(lD)$, рациональные функции которого ассоциированы с кривой Судзуки над расширенным конечным полем степени расширения 4.

Дивизор кривой определяется на точках

$$D = P_\infty + \sum_{\alpha, \beta \in F_q} P_{\alpha, \beta},$$

имеет степень $\deg(D) = q^2 + 1$.

Пусть $f = x^a y^b v^c w^d \left(x^q + x\right)^r$ – одна из рациональных функций из множества S и пусть ν_∞ – ее дискретная оценка в точке P_∞. Тогда

$$\nu_\infty(f) = aq + b\left(q + q_0\right) + c\left(q + 2q_0\right) + d\left(q + 2q_0 + 1\right) + rq^2$$

и f не имеет других полюсов. Рациональные функции множества $S \in L\left(l\left(q^2 + 1\right)P_\infty\right)$. Кодовые конструкции, ассоциированные с дивизором D, определены на точках

$$N = N_{q^4} - \sum_{\alpha, \beta \in F_q} P_{\alpha, \beta},$$

так как $x^q + x = 0$, для $x \in F_q$.

3. Пусть $q_0 = 2^s$ и $q = 2q_0$. Кривая, ассоциированная с группой Судзуки $Sz(q)$ и дивизором $D = \left|\left(q + 2q_0 + 1\right)P_0\right|$, $P_0 \in C\left(F_q\right)$, – точка на бесконечности определяется как F_q рациональный морфизм $\pi := (1 : x : y : v : w)$ в P^4 с

порядками полюсов $\mathrm{div}_\infty(x)=qP_0$, $\mathrm{div}_\infty(y)=(q+q_0)P_0$, $\mathrm{div}_\infty(v)=(q+2q_0)P_0$, $\mathrm{div}_\infty(w)=(q+2q_0+1)P_0$.

3.4 Метод универсального хеширования по рациональным функциям кривой Судзуки

В основе разработанного метода лежат известные результаты, представленные в утверждении 3.1. Уравнение кривой в проективном пространстве P^2

$$Y^q Z^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1}Z^{q+q_0-1}$$

и в аффинном пространстве над F_q

$$y^q - y = x^{q_0}\left(x^q - x\right),$$

где $q=2q_0^2$ и $q_0=2^s$.

Род кривой $g=q_0(q-1)$ и число F_q рациональных точек равно q^2+1. Кривая является максимальной и удовлетворяет границе Хассе – Вейля. Точками кривой являются особая точка на бесконечности $P_0=(0:1:0)$ кратности q_0 и рациональные точки $P_{a,b}=(a:b:1)$, где $a,b\in F_{q^2}$ и $b^q-b=a^{q_0}\left(a^q-a\right)$.

Подгруппа Вейерштрасса функционального поля кривой содержит подгруппу $H(P_\infty)=\langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$. Кривая Судзуки определяется полной линейной серией $D=\left|(q+2q_0+1)P_0\right|$ размерности $\dim=4$.

Базис пространства $L(\rho_\ell P_0)$ задается функциями вида $\left\{w^j\cdot v^i\cdot y^t\cdot x^r : i(q+2q_0)+j(q+2q_0+1)+t(q+q_0)+r\cdot q\le\rho_\ell\right\}$, что следует из подгруппы Вейерштрасса $H(P_0)$, представленной порядками полюсов функций $x=X/Z$, $y=Y/Z$, $v=x^{2q_0+1}+y^{2q_0}$), $w:=xy^{2q_0}+x^{2q+2q_0}+y^{2q}$.

Порядки полюсов: $\mathrm{div}_\infty(x) = qP_0$, $\mathrm{div}_\infty(y) = (q+q_0)P_0$, $\mathrm{div}_\infty(v) = (q+2q_0)P_0$, $\mathrm{div}_\infty(w) = (q+2q_0+1)P_0$.

Кривая Судзуки представляется в P^4 множеством точек вида $P_{(a,b)} := (1:a:b:f(a,b):af(a,b)+b^2) \cup \pi(P_0) = (0:0:0:0:1)$, где $a, b \in F_q$ и $f(a,b) := a^{2q_0+1} + b^{2q_0}$.

Замечание 3.10.

Кривая Судзуки имеет определение в поле характеристики 2 нечетной степени расширения.

Определение 3.8. [38]. Хеш-функция $h_{x,y}(m) \in F_q$, $q = 2q_0^2$, $q_0 = 2^s$ для сообщения m по рациональным функциям в точке x, y кривой $Y^q Z^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1} Z^{q+q_0-1}$ определяется выражением

$$h_{x,y}(m) = \sum m_{i,j,t,r} \cdot w^j \cdot v^i \cdot y^t \cdot x^r , \qquad (3.18)$$

где ρ_k – полюс подгруппы Вейерштрасса $H(P_\infty)$,

$m_{i,j,t,r} \in F_q$ – слова сообщения m,

$i \geq 0$, $0 \leq j \leq 2q_0 - 1$, $0 \leq t \leq 1$, $0 \leq r \leq q_0$,

$i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + rq \leq \rho_k$,

$x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$.

Пример 3.1. Пусть задано F_{2^3}. Кривая Судзуки имеет вид $y^8 - y = x^2(x^8 - x)$. Число точек кривой $N = 65$. Точки кривой в P^4 определяются уравнениями:

$$x = a; \quad y = b,$$

$$v = x^5 + y^4 = a^5 + b^4,$$

$$w = x^6 + y^2 + xy^4 = a^6 + b^2 + ab^4,$$

где $b^8 - b = a^2(a^8 - a)$ (таблица 3.1).

Таблица 3.1 – Точки кривой $y^8 - y = x^2\left(x^8 - x\right)$ над F_{2^3}

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
z	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x	0	0	1	α_1	α_2	α_3	α^4	α_5	α_6	0	1	α_1	α_2	α_3	α^4	α_5	α_6
v	1	0	1	α_5	α_3	α_1	α_6	α^4	α_2	1	0	$\alpha 4$	α_1	α_3	α_2	α_5	α_6
w	1	0	1	α_6	α_5	α^4	α_2	α_1	1	1	α^4	α_1	α_2	α_2		α_1	α_3
	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}	P_{25}	P_{26}	P_{27}	P_{28}	P_{29}	P_{30}	P_{31}	P_{32}	P_{33}
z	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	α_1	α_1	α_1	α_1	α_1	α_1	α_1	α_1	α_2	α_2	α_2	α_2	α_2	α_2	α_2	α_2	α_3
x	0	1	α_1	α_2	α_3	α^4	α_5	α_6	0	1	α_1	α_2	α_3	α^4	α_5	α_6	0
v	α^4	α_5	1	α_6	α_2	α_3	0	α_1	α_1	α_3	α_6	1	0	α_5	α_2	α^4	α_5
w	α_2	α_3	α^4	α^4	α_3	α_6	α_2	α_6	α_5	α_1	α^4	α_1	α^4	α_1	α_5	α_6	α_6
	P_{34}	P_{35}	P_{36}	P_{37}	P_{38}	P_{39}	P_{40}	P_{41}	P_{42}	P_{43}	P_{44}	P_{45}	P_{46}	P_{47}	P_{48}	P_{49}	P_{50}
Z	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
y	α_3	α_3	α_3	α_3	α_3	α_3	α_3	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α_5	α_5
x	1	α_1	α_2	α_3	α^4	α_5	α_6	0	1	α_1	α_2	α_3	α^4	α_5	α_6	0	1
v	α^4	0	α_2	α_6	α_1	1	α_3	α_2	α_6	α_3	α_5	α^4	1	α_1	0	α_6	α_2
w	α_3	α_6	α_3	1	α_1	α_1	1	α_1	α_5	α_2	α_3	α_3	α_2	α_5	α_1	α_3	α_5
	P_{51}	P_{52}	P_{53}	P_{54}	P_{55}	P_{56}	P_{57}	P_{58}	P_{59}	P_{60}	P_{61}	P_{62}	P_{63}	P_{64}			
z	1	1	1	1	1	1	1	1	1	1	1	1	1	1			
y	α_5	α_5	α_5	α_5	α_5	α_5	α_6	α_6	α_6	α_6	α_6	α_6	α_6	α_6			
x	α_1	α_2	α_3	α^4	α_5	α_6	0	1	α_1	α_2	α_3	α^4	α_5	α_6			
v	α_1	α^4	α_5	0	α_3	1	α_3	α_1	α_2	0	1	α^4	α_6	α_5			
w	α_5	α^4	1	α_3	1	α^4	α_5	α_6	α_2	α_5	α_2	α_6	1	1			

Значения полюсов дивизоров $\mathrm{div}_\infty\left(x\right) = 8P_\infty$ и $\mathrm{div}_\infty\left(y\right) = 10P_\infty$, $\mathrm{div}_\infty\left(v\right) = 12P_\infty$, $\mathrm{div}_\infty\left(w\right) = 13P_\infty$. Подгруппа Вейерштрасса точек неразрыва

определяется значениями полюсов $H(P_\infty)=\langle 8,10,12,13\rangle$ и имеет вид $\{0,8,10,12,13,16,18,20,21,22,23,24,25,26,28,\ldots.\}$. Точки разрыва определяются множеством $G(P_\infty)=\{1,2,3,4,5,6,7,9,11,14,15,17,19,27\}$, их число $|G(P_\infty)|=14$ и равняется значению рода $g=q_0(q-1)=14$. Линейная серия 8,10,12,13 является полной, определяется рациональными функциями x, y, v, w.

Базисное пространство кривой $y^8-y=x^2(x^8-x)$ определяется рациональными функциями x, y, $v=x^5+y^4$, $w:=x^6+xy^4+y^2$. Распределение кратности пересечения полиномов базисного пространства и $y^8-y=x^2(x^8-x)$ над F_{2^3} представлено в таблице 3.2. Хеш-вычисления в конечном поле F_{2^3} по полиномиальному базису $L(18P_\infty)$ на кривой $y^8-y=x^2(x^8-x)$ дают оценку вероятности коллизии $\varepsilon=m/N=18/64=0,28$.

Таблица 3.2 – Распределение кратности пересечения полиномов базисного пространства и кривой $y^8-y=x^2(x^8-x)$

Базисное пространство	Число испытаний	Распределение кратности пресечения (значение числа точек пересечения = число опытов)		
x, y, v, w	10000	8:=767 9:=1095	12:=2074	13:=6060
x, y, v, w, x^2	10000	8:=730 9:=138 11:=2904	12:=1479 13:=3781 14:=234	15:=717 16:=17
x, y, v, w, x^2, xy	10000	8:=959 9:=10 10:=2683 11:=1192	12:=2722 13:=577 14:=1136 15:=403	16:=259 17:=21 18:=38
x, y, v, w, x^2, xy, y^2	10000	8:=864 9:=75 10:=2703 11:=897 12:=2969	13:=866 14:=970 15:=307 16:=201	17:=33 18:=108 19:=4 20:=3

Действительно, число точек кривой $N=64$ и число совпадающих хешей при вычислении по полиномиальному базису $L(18P_\infty)$ не превышает значения

18. Число слов данных $k=6$. Хеш-вычисления в конечном поле F_{2^3} для 6 слов данных по полиномиальному базису $L(6P_\infty)$ на проективной прямой $x+y+z=0$ дают оценку вероятности коллизии $\varepsilon = m/N = 6/8 = 0,75$.

Связь значения k с показателями i, j, t, r степеней рациональных функций w, v, y, x определяется леммой 3.1.

Лемма 3.1 [38]. Пусть $k < q_0(q-1)$. Для кривой Судзуки имеет место $i = s-1-r-j-t$, $j = \Delta - t\cdot q_0 - 1$, $r = s - s_2 - dq_0 - t$, $t = t_1 \bmod 2$,

где $s' = \left\lceil (3k)^{1/3} \right\rceil$, $\Sigma = s'(s'+1)(2s'+1)/6$, $s = s' + \lfloor k/\Sigma \rfloor$, $s_1 = s - q_0 - 1$,

$\Sigma_{s-1} = s(s-1)(2s-1)/6 - s_1(s_1-1)(2s_1-1)/3 - s_1(s_1-1)$, $k' = k - \Sigma_{s-1}$, $k_1 = \lceil k'/2 \rceil$,

$d = \lfloor s_2/(s-t) \rfloor$, $k_2 = k_1 + s_1(s_1+1)/2$, $s_2 = \left\lceil (2k_2 + 1/4)^{1/2} - 1/2 \right\rceil$, $s_3 = s_2 - q_0 - 1$,

$\Delta = k' - 2k_3$, $t_1 = \lceil \Delta/q - 1 \rceil$, $k_3 = (s_2-1)s_2/2 - (s_1-1)(s_1+1)/2 - s_3(s_3+1)/2$,

$p = s_2 - (s_2 - t)d$, $\lceil\cdot\rceil$ – округление к большему целому числу, $\lfloor\cdot\rfloor$ – округление к меньшему целому числу, $[\cdot]$ – округление к ближайшему целому числу.

Доказательство. Аддитивная подгруппа Вейерштрасса $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < \ldots\}$ кривой $y^q - y = x^{q_0}(x^q - x)$ определяется значениями полюсов, $\varphi = q$, $\omega = q + q_0$, $\eta = q + 2q_0$ и $\gamma = q + 2q_0 + 1$.

Рассмотрим пример кривой $y^{32} - y = x^4(x^{32} - x)$ над полем F_{2^5}, число точек кривой $N = q^2 + 1 = 1025$ и род $g = q_0(q-1) = 124$. Размещение полюсов в $H(P) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle$ имеет вид, представленный в таблице 3.3.

Полюса подгруппы Вейерштрасса $q_0 = 2^2$, $q = 2^5$, $q + q_0 = 36$, $q + 2q_0 = 40$, $q + 2q_0 + 1 = 41$. Полюса делятся на два слоя. Отличие второго слоя от первого состоит в том, что наряду с комбинаций полюсов 32, 40, 41 функций x, v, w учитывается полюс со значением 36 рациональной функции

y. Каждый слой состоит из уровней с нарастающим числом строк. Число уровней для $k < q_0(q-1) = 124$ будет $2q_0 - 1 = 7$.

Таблица 3.3 – Полюса подгруппы Вейерштрасса $H(P_\infty) = \langle 32, 36, 40, 41 \rangle$

Полюса второго слоя				Полюса первого слоя				№
							ρ_0=0	1
			ρ_2=36				ρ_1=32	
						ρ_4=41	ρ_3=40	2
			ρ_6=68				ρ_5=64	
		ρ_{10}=77	ρ_9=76			ρ_8=73	ρ_7=72	
					ρ_{13}=82	ρ_{12}=81	ρ_{11}=80	3
			ρ_{15}=100				ρ_{14}=96	
		ρ_{19}=109	ρ_{18}=108			ρ_{17}=105	ρ_{16}=104	
	ρ_{25}=118	ρ_{24}=117	ρ_{23}=116		ρ_{22}=114	ρ_{21}=113	ρ_{20}=112	
				ρ_{29}=123	ρ_{28}=122	ρ_{27}=121	ρ_{26}=120	4
			ρ_{31}=132				ρ_{30}=128	
		ρ_{35}=141	ρ_{34}=140			ρ_{33}=137	ρ_{32}=136	
	ρ_{41}=150	ρ_{40}=149	ρ_{39}=148		ρ_{38}=146	ρ_{37}=145	ρ_{36}=144	
ρ_{49}=159	ρ_{48}=158	ρ_{47}=157	ρ_{46}=156	ρ_{45}=155	ρ_{44}=154	ρ_{43}=153	ρ_{42}=152	
			ρ_{54}=164	ρ_{53}=163	ρ_{52}=162	ρ_{51}=161	ρ_{50}=160	5
		ρ_{58}=173	ρ_{57}=172			ρ_{56}=169	ρ_{55}=168	
	ρ_{64}=182	ρ_{63}=181	ρ_{62}=180		ρ_{61}=178	ρ_{60}=177	ρ_{59}=176	
ρ_{72}=191	ρ_{71}=190	ρ_{70}=189	ρ_{69}=188	ρ_{68}=187	ρ_{67}=186	ρ_{66}=185	ρ_{65}=184	
ρ_{80}=199	ρ_{79}=198	ρ_{78}=197	ρ_{77}=196	ρ_{76}=195	ρ_{75}=194	ρ_{74}=193	ρ_{73}=192	
		ρ_{86}=205	ρ_{85}=204	ρ_{84}=203	ρ_{83}=202	ρ_{82}=201	ρ_{81}=200	6
	ρ_{92}=214	ρ_{91}=213	ρ_{90}=212		ρ_{89}=210	ρ_{88}=209	ρ_{87}=208	
ρ_{100}=223	ρ_{99}=222	ρ_{98}=221	ρ_{97}=220	ρ_{96}=219	ρ_{95}=218	ρ_{94}=217	ρ_{93}=216	
ρ_{108}=231	ρ_{107}=230	ρ_{106}=229	ρ_{105}=228	ρ_{104}=227	ρ_{103}=226	ρ_{102}=225	ρ_{101}=224	
ρ_{116}=239	ρ_{115}=238	ρ_{114}=237	ρ_{113}=236	ρ_{112}=235	ρ_{111}=234	ρ_{110}=233	ρ_{109}=232	
	ρ_{123}=246	ρ_{122}=245	ρ_{121}=244	ρ_{120}=243	ρ_{119}=242	ρ_{118}=241	ρ_{117}=240	7
ρ_{131}=255	ρ_{130}=254	ρ_{129}=253	ρ_{128}=252	ρ_{127}=251	ρ_{126}=250	ρ_{125}=249	ρ_{124}=248	
ρ_{139}=263	ρ_{138}=262	ρ_{137}=261	ρ_{136}=260	ρ_{135}=259	ρ_{134}=258	ρ_{133}=257	ρ_{132}=256	
ρ_{147}=271	ρ_{146}=270	ρ_{145}=269	ρ_{144}=268	ρ_{143}=267	ρ_{142}=266	ρ_{141}=265	ρ_{140}=264	
ρ_{155}=279	ρ_{154}=278	ρ_{153}=277	ρ_{152}=276	ρ_{151}=275	ρ_{150}=274	ρ_{149}=273	ρ_{148}=272	
ρ_{163}=287	ρ_{162}=286	ρ_{161}=285	ρ_{160}=284	ρ_{159}=283	ρ_{158}=282	ρ_{157}=281	ρ_{156}=280	8

Число полюсов на каждом уровне определяется следующим образом: пусть s – номер уровня и $s \le q_0 = 4$, тогда в первом слое имеем $\Sigma_1 = s(s+1)/2$, во втором $\Sigma_2 = s(s-1)/2$ и результирующее число полюсов на уровне s будет $\Sigma = s(s+1)/2 + s(s-1)/2 = s^2$. Рассмотрим случай $s > q_0 = 4$. Заметим, что можно использовать выражение для суммы s членов арифметической прогрессии с вычитанием недостающих элементов ряда $1, 2, \ldots, s - q_0 - 1$. В каждом слое таких наборов по два, результирующее выражение для суммы полюсов на уровне s будет $\Sigma = s^2 - 2s_1(s_1+1)$, где $s_1 = s - q_0 - 1$.

Суммарное число полюсов на всех уровнях $1, 2, \ldots, s$

$$\Sigma_s = \sum_{i=1}^{s} i^2 - 2\sum_{j=1}^{s_1} j^2 - 2\sum_{j=1}^{s_1} j = \\ = s(s+1)(2s+1)/6 - s_1(s_1+1)(2s_1+1)/3 - s_1(s_1+1). \qquad (3.19)$$

Размещение полюсов ρ_k в порядке возрастания в подгруппе $H(P_\infty) = \langle q = 32, q + q_0 = 36, q + 2q_0 = 40, q + 2q_0 + 1 = 41 \rangle$, с учетом полюсов рациональных функций представлено в таблице 3.4.

Значение k определяется выражением

$$k = s(s-1)(2s-1)/6 + s_2(s_2-1) - s_1(s_1-1) - s_3(s_3-1) + t_1 q_0 + j + 1. \qquad (3.20)$$

Здесь s – значение уровня, на котором располагается полюс ρ_k, s_2 – номер строки расположения полюса на уровне s, s_1 – номер строки дополнения до полного арифметического ряда s строк, s_3 – номер строки расположения полюсов, которые необходимо вычесть из суммы полного арифметического ряда s строк, t_1 – число строк размера q_0 уровня s, j – месторасположение полюса в последней строке уровня s. Для вычисления значений показателей i, j, t, r степеней рациональных функций w, v, y, x, соответствующих заданному k, следует определить уровень, на котором находится ρ_k полюс, строку расположения полюса на уровне, месторасположение ρ_k в этой строке и принадлежность к первому или второму слою полюсов.

Таблица 3.4 – Размещение полюсов подгруппы Вейерштрасса $H(P_\infty)=\langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$

№	Полюса первого слоя				Полюса второго слоя			
1	$\rho_0=0$							
	$\rho_1=q=\varphi$				$\rho_2=q+q0=\omega$			
2	$\rho_3=q+2q0=\eta$	$\rho_4=q+2q0+1=\gamma$						
	$\rho_5=2\varphi$				$\rho_6=\omega+\varphi$			
	$\rho_7=\eta+\varphi$	$\rho_8=\gamma+\varphi$			$\rho_9=\eta+\omega$	$\rho_{10}=\gamma+\omega$		
3	$\rho_{11}=2\eta$	$\rho_{12}=\gamma+\eta$	$\rho_{13}=2\gamma$					
	$\rho_{14}=3\varphi$				$\rho_{15}=\omega+2\varphi$			
	$\rho_{16}=\eta+2\varphi$	$\rho_{17}=\gamma+2\varphi$			$\rho_{18}=\eta+\omega+\varphi$	$\rho_{19}=\gamma+\omega+\varphi$		
	$\rho_{20}=2\eta+\varphi$	$\rho_{21}=\gamma+\eta+\varphi$	$\rho_{22}=2\gamma+\varphi$		$\rho_{23}=2\eta+\omega$	$\rho_{24}=\gamma+\eta+\omega$	$\rho_{25}=2\gamma+\omega$	
4	$\rho_{26}=3\eta$	$\rho_{27}=\gamma+2\eta$	$\rho_{28}=2\gamma+\eta$	$\rho_{29}=3\gamma$				
	$\rho_{30}=4\varphi$				$\rho_{31}=\omega+3\varphi$			
	$\rho_{32}=\eta+3\varphi$	$\rho_{33}=\gamma+3\varphi$			$\rho_{34}=\eta+\omega+2\varphi$	$\rho_{35}=\gamma+\omega+2\varphi$		
	$\rho_{36}=2\eta+2\varphi$	$\rho_{37}=\gamma+\eta+2\varphi$	$\rho_{38}=2\gamma+2\varphi$		$\rho_{39}=2\eta+\omega+\varphi$	$\rho_{40}=\gamma+\eta+\omega+\varphi$	$\rho_{41}=2\gamma+\omega+\varphi$	
	$\rho_{42}=3\eta+\varphi$	$\rho_{43}=\gamma+2\eta+\varphi$	$\rho_{44}=2\gamma+\eta+\varphi$	$\rho_{45}=3\gamma+\varphi$	$\rho_{46}=3\eta+\omega$	$\rho_{47}=\gamma+2\eta+\omega$	$\rho_{48}=2\gamma+\eta+\omega$	$\rho_{49}=3\gamma+\omega$
5	$\rho_{50}=4\eta$	$\rho_{51}=\gamma+3\eta$	$\rho_{52}=2\gamma+2\eta$	$\rho_{53}=3\gamma+\eta$	$\rho_{54}=4\gamma$			
	$\rho_{55}=\eta+4\varphi$	$\rho_{56}=\gamma+4\varphi$			$\rho_{57}=\eta+\omega+3\varphi$	$\rho_{58}=\gamma+\omega+3\varphi$		
	$\rho_{59}=2\eta+3\varphi$	$\rho_{60}=\gamma+\eta+3\varphi$	$\rho_{61}=2\gamma+3\varphi$		$\rho_{62}=2\eta+\omega+2\varphi$	$\rho_{63}=\gamma+\eta+\omega+2\varphi$	$\rho_{64}=2\gamma+\omega+2\varphi$	
	$\rho_{65}=3\eta+2\varphi$	$\rho_{66}=\gamma+2\eta+2\varphi$	$\rho_{67}=2\gamma+\eta+2\varphi$	$\rho_{68}=3\gamma+2\varphi$	$\rho_{69}=3\eta+\omega+\varphi$	$\rho_{70}=\gamma+2\eta+\omega+\varphi$	$\rho_{71}=2\gamma+\eta+\omega+\varphi$	$\rho_{72}=3\gamma+\omega+\varphi$
	$\rho_{73}=4\eta+\varphi$	$\rho_{74}=\gamma+3\eta+\varphi$	$\rho_{75}=2\gamma+2\eta+\varphi$	$\rho_{76}=3\gamma+\eta+\varphi$	$\rho_{77}=4\eta+\omega$	$\rho_{78}=\gamma+3\eta+\omega$	$\rho_{79}=2\gamma+2\eta+\omega$	$\rho_{80}=3\gamma+\eta+\omega$
6	$\rho_{81}=5\eta$	$\rho_{82}=\gamma+4\eta$	$\rho_{83}=2\gamma+3\eta$	$\rho_{84}=3\gamma+2\eta$	$\rho_{85}=4\gamma+\eta$	$\rho_{86}=5\gamma$		
	…	…	…	…	…	…		
	$\rho_{s(s-1)(2s-1)/6+s_2(s_2-1)-s_1(s_1-1)-s_3(s_3-1)+t_1q_0+j+1}=i(q+2q_0)+j(q+2q_0+1)+t(q+q_0)+rq$							

Нетрудно показать, что значение уровня, на котором находится полюс ρ_k, вычисляется по формулам:

$s=\left[(3k)^{1/3}\right]$ – округление к ближайшему целому,

$\Sigma = s'(s'+1)(2s'+1)/6$ – сумма числа полюсов уровней $1 \div s'$,

$s = s' + \lfloor k/\Sigma \rfloor$ – уточнение значения уровня, $\lfloor \cdot \rfloor$ – округление к наименьшему целому.

Результат следует из кубической зависимости k от s. Для вычисления строки расположения полюса ρ_k на уровне s следует учесть, что число полюсов по строкам на уровне определяется арифметическим рядом. Результирующие выражения имеют вид:

$s_1 = s - q_0 - 1$ – значение числа строк дополнения,

$$\Sigma_{s-1} = \sum_{i=1}^{s-1} i^2 - 2\sum_{j=1}^{s_1-1} j^2 - 2\sum_{j=1}^{s_1-1} j = s(s-1)(2s-1)/6 - s_1(s_1-1)(2s_1-1)/3 - s_1(s_1-1)$$

– число полюсов на уровнях $1, \ldots, s-1$,

$k' = k - \Sigma_{s-1}$ – число полюсов на уровне s,

$k_1 = \lceil k'/2 \rceil$ – число полюсов на уровне s для одного слоя,

$k_2 = k_1 + s_1(s_1+1)/2$ – дополнение числа полюсов на уровне s за счет s_1 строк,

$s_2 = \left\lceil (2k_2 + 1/4)^{1/2} - 1/2 \right\rceil$ – значение строки расположения полюса.

Число строк t_1 размера q_0 на уровне s определяется выражениями:

$s_3 = s_2 - q_0 - 1$ – число строк расположения полюсов, которые необходимо вычесть из суммы полного арифметического ряда,

$k_3 = (s_2 - 1)s_2/2 - (s_1 - 1)(s_1 + 1)/2 - s_3(s_3 + 1)/2$ – число полюсов на уровне s для одного слоя,

$\Delta = k' - 2k_3$ – число полюсов на строке s_2,

$t_1 = \lceil \Delta/q_0 - 1 \rceil$ – число строк размера q_0.

Результирующие выражения для показателей i, j, t, r степеней рациональных функций w, v, y, x определяются по формулам:

$t = t_1 \bmod 2$ – степень y^t (определитель второго слоя),

$j = \Delta - t \cdot q_0 - 1$ – степень w^j,

$d = \lfloor s_2 / (s - t) \rfloor$ – индикатор последней строки s_2 на уровне s,

$r = s - s_2 - dq_0 - t$ – степень x^r,

$i = s - 1 - r - j - t$ – степень v^i.

Пример 3.2. Пусть $y^{32} - y = x^4 \left(x^{32} - x \right)$ над полем F_{2^5}, $q = 2^5$. Полюса представлены таблицей 3.3. Вычислить значение полюса ρ_l.

Пусть $l = 113$. Имеем $k = 113 + 1 = 114$ и вычисления по формулам леммы дают следующее:

$$s' = \left\lceil (3k)^{1/3} \right\rceil = (3 \cdot 114)^{1/3} = 7,$$

$$\Sigma = s'(s' + 1)(2s' + 1)/6 = 7 \cdot 8 \cdot 15/6 = 140,$$

$$s = s' + \lfloor k / \Sigma \rfloor = 7,$$

$$s_1 = s - q_0 - 1 = 7 - 5 = 2,$$

$$\Sigma_{s-1} = s(s-1)(2s-1)/6 - s_1(s_1 - 1)(2s_1 - 1)/3 - s_1(s_1 - 1) = \\ = 7 \cdot 6 \cdot 13/6 - 2 \cdot 1 \cdot 3/3 - 2 \cdot 1 = 87,$$

$$k' = k - \Sigma_{s-1} = 114 - 87 = 27,$$

$$k_1 = \lceil k'/2 \rceil = \lceil 27/2 \rceil = 14,$$

$$k_2 = k_1 + s_1(s_1 + 1)/2 = 14 + 2 \cdot 3/2 = 17,$$

$$s_2 = \left\lceil (2k_2 + 1/4)^{1/2} - 1/2 \right\rceil = \lceil (2 \cdot 17 + 0{,}25) 1/2 - 0{,}5 \rceil = 6,$$

$$s_3 = s_2 - q_0 - 1 = 6 - 4 - 1 = 1,$$

$$k_3 = (s_2 - 1) s_2/2 - s_1(s_1 + 1)/2 - s_3(s_3 + 1)/2 = 5 \cdot 6/2 - 2 \cdot 3/2 - 1 \cdot 2/2 = 11,$$

$$\Delta = k' - 2k_3 = 27 - 2 \cdot 11 = 5,$$

$$t_1 = \lceil \Delta / q_0 - 1 \rceil = \lceil 5/4 - 1 \rceil = 1,$$

$$t = t_1 \bmod 2 = 1,$$

$$j = \Delta t \cdot q_0 - 1 = 5 - 5 - 1 = 0,$$

$$d = \lfloor s_2/(s-t) \rfloor = \lfloor 6/(7-1) \rfloor = 1,$$

$$r = s - s_2 + d \cdot q_0 = 7 - 6 + 1 \cdot 4 = 5.$$

$$r = \varepsilon - \varepsilon_2 d q_0 - t,$$

$$i = \varepsilon - 1 - r - j - t.$$

Получим значение полюса

$$\rho_{113} = i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq = \\ = 1 \cdot 40 + 0 \cdot 41 + 1 \cdot 36 + 5 \cdot 32 = 236,$$

что совпадает со значением в таблице 3.3.

Утверждение 3.2 [38]. Хеширование по рациональным функциям кривой $y^q - y = x^{q_0}\left(x^q - x\right)$, где $q = 2q_0^2$ и $q_0 = 2^s$ над полем F_q, определяет универсальный хеш-класс $\varepsilon - U\left(q^2, q^k, q\right)$, где q^2 – число хеш-функций (объем ключевого пространства), q^k – объем пространства сообщений, q – объем пространства хеш-кодов. Вероятность коллизии ε определяется соотношениями

$$\varepsilon = \left(i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq\right)/q^2, \text{ если } k < q_0(q-1), \quad (3.21)$$

$$\varepsilon = \left(k + q_0(q-1)\right)/q^2, \text{ если } k \geq q_0(q-1), \quad (3.22)$$

где i, j, t, r определяются леммой.

Доказательство. Параметры универсального класса по рациональным функциям кривой Судзуки следуют из определения кривой и числа ее точек в F_q. Вероятность коллизии ε определяется соотношением $\varepsilon = \rho_k / N$, где $\rho_k = i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq$ – значение полюса рациональной функции $f_k = w^i \cdot v^i \cdot y^t \cdot x^r$, $N = q^2$ – число точек кривой.

Пусть $k < q_0(q-1)$. Параметры i, j, t, r определяются леммой, и по подстановке в $\varepsilon = \rho_k / N$ следует (3.21).

В случае $k = q_0(q-1)$ имеем $\rho_k = 2g = 2q_0(q-1)$ и $\varepsilon = 2g/N$, что согласуется с (3.22).

С другой стороны, $\rho_k = i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + rq$. Вычисления по формулам леммы дают $i = q_0 - 1$, $j = 0$, $t = 0$, $r = q_0$ и прямой подстановкой получим проверку:

$$\rho_k = i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + rq = \\ = (q_0-1)(q+2q_0) + q_0 q = 2q_0(q-1)$$

.

Пусть $k > q_0(q-1)$. Заметим, что $\rho_k = k + q_0(q-1)$. Прямое вычисление $\varepsilon = \rho_k / N$ приводит к выражению (3.22).

Замечание 3.11.

1. Пусть $k \approx \sqrt{q}\left(\sqrt{q}-1\right)/2$. По лемме имеем $s \approx \left[(3k)^{1/3}\right] \approx (q)^{1/3}$, значения параметров $i \approx s$, $j = 0$, $t = 0$, $r = 0$ и оценку вероятности коллизии

$$\varepsilon \approx q^{1/3}(q+q_0)/q^2 \approx q^{-1/6}\varepsilon_{HC}, \qquad (3.23)$$

где $\varepsilon_{HC} = 1/\sqrt{q} + 1/q$ – значение вероятности коллизии универсального хеширования по кривой Эрмита в квадратичном поле F_q при $k = \sqrt{q}\left(\sqrt{q}-1\right)/2$. Из оценки (3.23) следует выигрыш в $q^{1/6}$ раз по вероятности коллизии хеширования по кривой Эрмита. Размер ключевых данных $N = q^2$ по сравнению с хешированием по кривой Эрмита больше в $\sqrt{q}$ раз.

2. Для $k = q_0(q-1)$ имеем вероятность коллизии хеширования по кривым Судзуки:

$$\varepsilon = 2q_0(q-1)/q^2 \approx \sqrt{2}q^{-1/2}. \qquad (3.24)$$

Подстановка $k = q_0(q-1)$ в выражение для вероятности коллизии хеширования по кривым Эрмита дает

$$\varepsilon = k/\ \ q^3 + 1/(2q) - 1/\left(2q^2\right) = \\ = \frac{1}{\sqrt{2}}\sqrt{q}(q-1)/q\sqrt{q} + 1/\left(2\sqrt{q}\right) - 1/(2q) \approx 1/\sqrt{2}. \qquad (3.25)$$

3. Универсальное хеширование по кривой Судзуки для случая $q_0 = 2^s$ и $q = 2q_0$, ассоциированное с дивизором $D = \left|\left(q + 2q_0 + 1\right)P_0\right|$, определяется на том же F_q рациональном морфизме $\pi := (1 : x : y : v : w)$ в P^4 с теми же порядками полюсов, как для случая кривой с параметрами $q_0 = 2^s$ и $q = 2{q_0}^2$. Следовательно, справедливо определение (3.18) и соотношения для вероятности коллизии (3.21) и (3.22). Для $k = q_0(q-1)$ получим оценку вероятности коллизии хеширования

$$\varepsilon = 2q_0(q-1)/q^2 \approx \left(4{q_0}^2 - 2q_0\right)/4{q_0}^2 \approx 1,$$

что хуже по сравнению с хешированием с параметрами $q_0 = 2^s$ и $q = 2{q_0}^2$:

$$\varepsilon = 2q_0(q-1)/q^2 \approx 1/q_0 .$$

4. Универсальное хеширование по максимальной кривой Судзуки над конечным полем F_{q^4} вычисляется по пяти параметрическим функциям базиса $L(lD)$:

$$S := \left\{ x^a y^b v^c w^d \left(x^q + x\right)^r \quad \begin{array}{c} aq + b(q + q_0) + c(q + 2q_0) + \\ + d(q + 2q_0 + 1) + rq^2 \le l\left(q^2 + 1\right) \\ 0 \le a \le q - 1, 0 \le b \le 1, 0 \le c \le \\ \le q_0 - 1, 0 \le d \le q_0 - 1, 0 \le r \le l \end{array} \right\}. \qquad (3.26)$$

Функциональное поле выстраивается в порядке возрастания полюсов $f = x^a y^b v^c w^d \left(x^q + x\right)^r$. Для числа слов данных $k < q(q-1)^2$ вычисление рациональных функций осуществляется по параметрам x, y, v, w. Для крайних параметров a, b, c, d из (3.26) будем иметь значение дискретной оценки

$$\nu_\infty(f) = (q-1)q + (q+q_0) + (q_0-1)(q+2q_0) +$$
$$+(q_0-1)(q+2q_0+1) = q^2 + 2g - 1.$$

Для числа слов данных $k > q(q-1)^2$ вычисление рациональных функций следует выполнять по пяти параметрам $x, y, v, w, \left(x^q + x\right)$, что позволяет построить функциональное пространство с непрерывной последовательностью полюсов для больших значений k.

Для $k = q_0(q-1)$ получим оценку вероятности коллизии хеширования над полем F_{q^4}

$$\varepsilon = 2q_0(q-1)/\ q^4 \approx \frac{1}{q^2 q_0}.$$

Хеширование по кривой Судзуки над полем F_p с параметрами $p_0 = 2^s$, $p = 2{p_0}^2$ и $p \approx q^4$ для $k = q_0(q-1)$ слов данных аналогично п.1 замечания будет иметь оценку вероятности коллизии $\varepsilon \approx \rho_k / p^2 \approx \frac{k^{1/3}(q+q_0)}{q^8} \approx \frac{1}{q^6 q_0}$, что существенно лучше по сравнению с хешированием в расширенном поле F_{q^4}.

3.5 Выводы

Результатами раздела являются оценки параметров группы Судзуки, кривых, ассоциированных с подгруппами группы Судзуки, вычисления функционального поля кривой, ассоциированной с подгруппой $S(a,b)$ полной группы Судзуки, построение универсального хеширования по рациональным функциям функционального поля кривой Судзуки, оценки параметров универсального хеширования. Метод универсального хеширования по рациональным функциям кривой Судзуки и его свойства представлен в работах [38,39,40,47,48]. Основные результаты исследований следующие.

1. Кривая Судзуки определена с точностью до F_q изоморфизма, ассоциирована с подгруппой $S(a,b)$ группы Судзуки $Sz(q)$, основана на роде, числе точек и групповом F_q автоморфизме кривой. Кривая имеет относительно своего рода максимальное число точек и над полем F_q, где $q = 2q_0^{\,2}$, $q_0 = 2^s$ и чуть меньше границы Хассе – Вейля. Род кривой $g = q_0(q-1)$ и число F_q рациональных точек равно q^2+1.

2. Кривая Судзуки над конечным полем степени расширения $r \equiv 0 \bmod 4$ является максимальной, имеет малое значение рода и соответственно относительно размера поля малое число точек. Кривая Судзуки над квадратичным и кубическим полем является неоптимальной.

3. Кривая Судзуки над полем F_q, где $q_0 = 2^s$ и $q = 2q_0$ также является F_q- изоморфной кривой Дэлигнэ – Лустига, ассоциированной с группой Судзуки $Sz(q)$, но имеет в q_0^2 меньше точек по сравнению со случаем $q = 2q_0^2$.

4. Классы производных кривых по подгруппам группы Судзуки для случая $q = 2q_0^2$ и $q_0 = 2^s$ определены по циклической подгруппе порядка r, $r \mid q-1$, по подгруппе Зингера порядка $q \pm 2q_0 + 1$, по подгруппам порядков $2^u r$, $2r$, $2s$, $4s$, где $r \mid (q-1)$, $s \mid (q \pm 2q_0 + 1)$. Кривые по данным подгруппам имеют число точек, соответствующих порядкам подгрупп, что меньше числа точек кривой, ассоциированной с подгруппой $S(a,b)$ порядка q^2.

5. Универсальное хеширование по кривой Судзуки строится на основе отображения $\pi := (1 : x : y : v : w)$ в проективном пространстве P^4. Хеширование по рациональным функциям кривой над полем F_q определяет универсальный хеш-класс $\varepsilon - U(q^2, q^k, q)$, где q^2 – число хеш-функций (объем ключевого пространства), ε – верхняя оценка вероятности коллизии, k – число q-х слов данных.

6. Хеширование по кривой Судзуки имеет выигрыш в $q^{1/6}$ раз по вероятности коллизии и в $q^{1/2}$ раз – по числу слов данных по сравнению с универсальным хешированием по кривой Эрмита. Хеширование по кривой с параметрами $q = 2q_0^{\,2}$ и $q_0 = 2^s$ имеет преимущество по вероятности коллизии, длине данных, сложности вычислений по сравнению с хешированием по производным кривым Судзуки и кривой над полем четвертой степени расширения.

РАЗДЕЛ 4
БЫСТРОЕ УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО КРИВОЙ СУДЗУКИ

Вычислительная и алгоритмическая сложность универсального хеширования по рациональным функциям алгебраических кривых зависит от размерности проективного пространства представления кривой. Проективное пространство алгебраической кривой определяется базисом линейного векторного пространства Римана – Роха для функционального поля кривой. В работах [38–40] представлено универсальное хеширование по кривой Судзуки над конечным полем характеристики 2 с нечетной степенью расширения. Кривая Судзуки имеет определение в проективном пространстве P^4 и требует в два раза больше хеш-вычислений по сравнению с хешированием по кривым Эрмита в P^2 для квадратичного поля.

Актуальной задачей является разработка метода универсального хеширования по алгебраическим кривым с уменьшенной сложностью вычислений. В данном разделе предлагается метод универсального хеширования по кривой Судзуки на основе схемы Горнера, метод универсального хеширования с ограничением функционального поля по алгебраической кривой Судзуки и многопотоковое универсальное хеширование. С этой целью в подразделе 4.1 приводится метод универсального хеширования по кривой Судзуки на основе схемы Горнера. В подразделе 4.2 представлен метод универсального хеширования с ограничением функционального поля алгебраических кривых, коллизионные оценки и оценки сложности хеширования. В подразделе 4.3 рассмотрено многопотоковое универсальное хеширование по алгебраическим кривым.

4.1 Метод универсального хеширования по кривой Судзуки на основе схемы Горнера

Сложность универсального хеширования по кривой Судзуки определяется четырех параметрическим выражением для функции хеширования

$$h_{x,y}(m) = \sum m_{i,j,t,r} \cdot w^j \cdot v^i \cdot y^t \cdot x^r . \qquad (4.1)$$

Практическое вычисление $h_{x,y}(m) \in F_q$ требует четырех умножений рациональных функций базиса линейного пространства $L(\rho_k P_0)$ в поле F_q и формирования показателей степеней рациональных функций в порядке возрастания их полюсов. Прямое вычисление выражения (4.1) для произвольного значения числа слов данных k является проблематичным.

Предлагается метод универсального хеширования по кривой Судзуки на основе схемы Горнера, который позволяет уменьшить сложность вычислений и структурировать алгоритм для произвольного значения k. Метод определяется следующей последовательностью действий:

1) фиксируется базис пространства $L(\rho_k P_\infty)$, ассоциированный с кривой Судзуки;

2) составляется массив мономов $h_{x,y}(m)$ для рациональных функций в порядке возрастания их полюсов по подгруппе Вейерштрасса;

3) формируются группы мономов с общим коэффициентом и полиномиальным хешированием внутри группы по каждой рациональной функции;

4) группы мономов с общим коэффициентом и полиномиальным хешированием внутри группы объединяются в каскадную схему с хешированием по одной рациональной функции;

5) на каждом каскаде с полиномиальным хешированием строится схема вычисления Горнера.

Количество каскадов определяется числом базисных функций, и универсальное хеширование со скалярным произведением по рациональным функциям приводится к многопараметрической схеме Горнера по степеням базисных функций.

Применение метода универсального хеширования по кривой Судзуки $y^q - y = x^{q_0}\left(x^q - x\right)$, где $q = 2q_0^2$ и $q_0 = 2^s$ над полем F_q на основе схемы Горнера, приводит к следующему алгоритму.

1. Базис пространства $L\left(\rho_k P_\infty\right)$, ассоциированный с кривой, задается функциями вида $\left\{w^j \cdot v^i \cdot y^t \cdot x^r : i\left(q + 2q_0\right) + j\left(q + 2q_0 + 1\right) + t\left(q + q_0\right) + r \cdot q \le \rho_k\right\}$. Универсальное хеширование определяется выражением

$$h_{x,y}\left(m\right) = \sum m_{i,j,t,r} \cdot w^j \cdot v^i \cdot y^t \cdot x^r ,$$

где $i \ge 0$, $0 \le j \le 2q_0 - 1$, $0 \le t \le 1$, $0 \le r \le q_0$, $i\left(q + 2q_0\right) + j\left(q + 2q_0 + 1\right) + t\left(q + q_0\right) + rq \le \rho_k$, $m_{i,j,t,r} \in F_q$ – слова сообщения m.

2. Подгруппа Вейерштрасса $H\left(P_\infty\right) = \left\langle q, q + q_0, q + 2q_0, q + 2q_0 + 1\right\rangle$ и размещение полюсов имеет представление, подобное $H\left(P_\infty\right) = \left\langle 32, 36, 40, 41\right\rangle$ над F_q, $q_0 = 2^2, q = 2^5, q + q_0 = 36$ (см. таблицу 4.1).

Пусть $k < q_0\left(q - 1\right)$. Члены суммы в выражении $h_{x,y}\left(m\right)$ для F_q, $q = 2^5$ представлены в таблицах 4.1 и 4.2 четырехмерным массивом $H_{w,v,y,x}$ по возрастанию полюсов рациональных функций $w^j \cdot v^i \cdot y^t \cdot x^r$.

В таблице 4.1 представлены рациональные функции с полюсами, соответствующими таблице 4.1 первого слоя и соответственно в таблице 4.2 – рациональные функции с полюсами, соответствующими таблице полюсов второго слоя (таблица 4.2).

Таблица 4.1 – Члены суммы в выражении $h_{x,\,y}(m)$ с учетом возрастания полюсов рациональных функций $w^j \cdot v^i \cdot y^t \cdot x^r$ над F_q, $q = 2^5$

Номер уровней s	Мономы $h_{x,\,y}(m)$ для рациональных функций $w^j \cdot v^i \cdot y^t \cdot x^r$			
1	$w^0v^0y^0x^0m_{0,0,0,0}$			
	$w^0v^0y^0x^1m_{0,0,0,1}$			
2	$w^0v^1y^0x^0m_{0,1,0,0}$	$w^1v^0y^0x^0m_{1,0,0,0}$		
	$w^0v^0y^0x^2m_{0,0,0,2}$			
	$w^0v^1y^0x^1m_{0,1,0,1}$	$w^1v^0y^0x^1m_{1,0,0,1}$		
3	$w^0v^2y^0x^0m_{0,2,0,0}$	$w^1v^1y^0x^0m_{1,1,0,0}$	$w^2v^0y^0x^0m_{2,0,0,0}$	
	$w^0v^0y^0x^3m_{0,0,0,3}$			
	$w^0v^1y^0x^2m_{0,1,0,2}$	$w^1v^0y^0x^2m_{1,0,0,2}$		
	$w^0v^2y^0x^1m_{0,2,0,1}$	$w^1v^1y^0x^1m_{1,1,0,1}$	$w^2v^0y^0x^1m_{2,0,0,1}$	
4	$w^0v^3y^0x^0m_{0,3,0,0}$	$w^1v^2y^0x^0m_{1,2,0,0}$	$w^2v^1y^0x^0m_{2,1,0,0}$	$w^3v^0y^0x^0m_{3,0,0,0}$
	$w^0v^0y^0x^4m_{0,0,0,4}$			
	$w^0v^1y^0x^3m_{0,1,0,3}$	$w^1v^0y^0x^3m_{1,0,0,3}$		
	$w^0v^2y^0x^2m_{0,2,0,2}$	$w^1v^1y^0x^2m_{1,1,0,2}$	$w^2v^0y^0x^2m_{2,0,0,2}$	
	$w^0v^3y^0x^1m_{0,3,0,1}$	$w^1v^2y^0x^1m_{1,2,0,1}$	$w^2v^1y^0x^1m_{2,1,0,1}$	$w^3v^0y^0x^1m_{3,0,0,1}$
5	$w^0v^4y^0x^0m_{0,4,0,0}$	$w^1v^3y^0x^0m_{1,3,0,0}$	$w^2v^2y^0x^0m_{2,2,0,0}$	$w^3v^1y^0x^0m_{3,1,0,0}$
	$w^0v^1y^0x^4m_{0,1,0,4}$	$w^1v^0y^0x^4m_{1,0,0,4}$		
	$w^0v^2y^0x^3m_{0,2,0,3}$	$w^1v^1y^0x^3m_{1,1,0,3}$	$w^2v^0y^0x^3m_{2,0,0,3}$	
	$w^0v^3y^0x^2m_{0,3,0,2}$	$w^1v^2y^0x^2m_{1,2,0,2}$	$w^2v^1y^0x^2m_{2,1,0,2}$	$w^3v^0y^0x^2m_{3,0,0,2}$
	$w^0v^4y^0x^1m_{0,4,0,1}$	$w^1v^3y^0x^1m_{1,3,0,1}$	$w^2v^2y^0x^1m_{2,2,0,1}$	$w^3v^1y^0x^1m_{3,1,0,1}$
6	$w^0v^5y^0x^0m_{0,5,0,0}$	$w^1v^4y^0x^0m_{1,4,0,0}$	$w^2v^3y^0x^0m_{2,3,0,0}$	$w^3v^2y^0x^0m_{3,2,0,0}$
	…	…	…	…

Таблица 4.2 – Члены суммы в выражении $h_{x,\,y}(m)$ с учетом возрастания полюсов рациональных функций $w^j \cdot v^i \cdot y^t \cdot x^r$ над F_q, $q = 2^5$

Номер уровней s	Мономы $h_{x,\,y}(m)$ для рациональных функций $w^j \cdot v^i \cdot y^t \cdot x^r$			
1				
	$w^0v^0y^1x^0m_{0,0,1,0}$			
2				
	$w^0v^0y^1x^1m_{0,0,1,1}$			
	$w^0v^1y^1x^0m_{0,1,1,0}$	$w^1v^0y^1x^0m_{1,0,1,0}$		
3				
	$w^0v^0y^1x^2m_{0,0,1,2}$			
	$w^0v^1y^1x^1m_{0,1,1,1}$	$w^1v^0y^1x^1m_{1,0,1,1}$		
	$w^0v^2y^1x^0m_{0,2,1,0}$	$w^1v^1y^1x^0m_{1,1,1,0}$	$w^2v^0y^1x^0m_{2,0,1,0}$	
4				
	$w^0v^0y^1x^3m_{0,0,1,3}$			
	$w^0v^1y^1x^2m_{0,1,1,2}$	$w^1v^0y^1x^2m_{1,0,1,2}$		
	$w^0v^2y^1x^1m_{0,2,1,1}$	$w^1v^1y^1x^1m_{1,1,1,1}$	$w^2v^0y^1x^1m_{2,0,1,1}$	
	$w^0v^3y^1x^0m_{0,3,1,0}$	$w^1v^2y^1x^0m_{1,2,1,0}$	$w^2v^1y^1x^0m_{2,1,1,0}$	$w^3v^0y^1x^0m_{3,0,1,0}$
5	$w^4v^0y^0x^0m_{4,0,0,0}$			
	$w^0v^1y^1x^3m_{0,1,1,3}$	$w^1v^0y^1x^3m_{1,0,1,3}$		
	$w^0v^2y^1x^2m_{0,2,1,2}$	$w^1v^1y^1x^2m_{1,1,1,2}$	$w^2v^0y^1x^2m_{2,0,1,2}$	
	$w^0v^3y^1x^1m_{0,3,1,1}$	$w^1v^2y^1x^1m_{1,2,1,1}$	$w^2v^1y^1x^1m_{2,1,1,1}$	$w^3v^0y^1x^1m_{3,0,1,1}$
	$w^0v^4y^1x^0m_{0,4,1,0}$	$w^1v^3y^1x^0m_{1,3,1,0}$	$w^2v^2y^1x^0m_{2,2,1,0}$	$w^3v^1y^1x^0m_{3,1,1,0}$
6	$w^4v^1y^0x^0m_{4,1,0,0}$	$w^5v^0y^0x^0m_{5,0,0,0}$		
	…	…		

3. Вычисление $h_{x,y}(m)$ по таблицам 4.1 и 4.2 включает суммы по уровням. Вычисление по рациональным функциям $w^j \cdot v^i \cdot y^t \cdot x^r$ отличается умножением всех коэффициентов на значение y^0 или y^1.

4. Рассмотрим вычисления для первого слоя на уровне $s = 6$ для y^0. Для суммы коэффициентов выражение имеет вид

$$\Sigma_{s=6} = w^1v^0y^0x^4m_{1,0,0,4} + w^0v^1y^0x^4m_{0,1,0,4} +$$
$$+w^2v^0y^0x^3m_{2,0,0,3} + w^1v^1y^0x^3m_{1,1,0,3} + w^0v^2y^0x^3m_{0,2,0,3} +$$
$$+w^3v^0y^0x^2m_{3,0,0,2} + w^2v^1y^0x^2m_{2,1,0,2} + w^1v^2y^0x^2m_{1,2,0,2} +$$
$$+w^0v^3y^0x^2m_{0,3,0,2} + w^3v^1y^0x^1m_{3,1,0,1} + w^2v^2y^0x^1m_{2,2,0,1} +$$
$$+w^1v^3y^0x^1m_{1,3,0,1} + w^0v^4y^0x^1m_{0,4,0,1} + w^3v^2y^0x^0m_{3,2,0,0} +$$
$$+w^2v^3y^0x^0m_{2,3,0,0} + w^1v^4y^0x^0m_{1,4,0,0} + w^0v^5y^0x^0m_{0,5,0,0}.$$

После преобразований получим

$$\Sigma_{s=6} = y^0v^5\sum_{r=1}^{4}(x/v)^r \sum_{j=1}^{\min(5-r,\,3)}(w/v)^j\, m_{0,5,r,j}\,.$$

Обобщение для Σ_s в поле F_q, $q = 2q_0^2$, $q_0 = 2^s$ $q_0 = 2^s$ и произвольном s имеет вид

$$\Sigma_s = y^0v^{s-1}\sum_{r=0}^{\min(s-1,\,q_0)}(x/v)^r \sum_{j=0}^{\min(s-1-r,\,q_0-1)}(w/v)^j\, m_{0,s-1,r,j}\,.$$

5. Результирующая формула $h_{x,y}(m)$ определяется выражением

$$h_{x,y}(m) = \sum_{t=0}^{1}y^t\sum_{i=0}^{s-t}v^i \sum_{r=0}^{\min(s-t,\,q_0-t)}(x/v)^r \sum_{j=0}^{\min(s-r,\,q_0-1)}(w/v)^j\, m_{t,i,r,j}\,, \qquad (4.2)$$

где s – число уровней для k информационных слов. Параметр s определяется по лемме 3.1. В выражении (4.2) значение s уменьшено на 1, так как вычисления по индексу i начинаются с 0.

6. Алгоритм хеширования $h_{x,y}(m)$ определяется схемой вычисления Горнера последовательно для четырех сумм в выражении (4.2).

Замечание 4.1.

1. Универсальное хеширование по кривой Судзуки над полем F_q для случая $q_0 = 2^s$ и $q = 2q_0$ определяется на том же F_q рациональном морфизме $\pi:(1:x:y:v:w)$ в P^4 с теми же порядками полюсов, как в рассмотренном случае для кривой с параметрами $q_0 = 2^s$ и $q = 2q_0^2$. Следовательно, для

параметрического вычисления хеш-значений в схеме Горнера справедливо выражение (4.2).

2. Универсальное хеширование по кривой Судзуки над полем F_q^4 определяется по пятипараметрическим функциям базиса $L(lD)$, что приведет к пятипараметрической схеме вычисления Горнера. В соотношение (4.2) для $h_{x,y}(m)$ нужно добавить внешнюю сумму с индексом l и умножением на $\left(x^q + x\right)^l$

Оценка сложности универсального хеширования по кривой Судзуки в схеме Горнера определяется следующим предложением.

Предложение 4.1. Сложность универсального хеширования по кривым $y^q - y = x^{q_0\left(x^q - x\right)}$, где $q = 2q_0^2$ и $q_0 = 2^s$ над полем F_q определяется выражениями

$$N_{\text{опер}} = k + s^3/3 + s^2/2 + 2s - 1, \text{ если } s \le q_0, \tag{4.3}$$

$$N_{\text{опер}} = k + q_0^3/3 + q_0^2/2 + (s - q_0)(2q_0 - 1) + 2s - 1, \text{ если } s > q_0, \tag{4.4}$$

где $s = (3k)^{1/3}$.

Доказательство. Алгоритм хеширования $h_{x,y}(m)$ определяется схемой вычисления Горнера последовательно для четырех сумм (4.2). Вычисления по внутренней сумме определяются значением $\Sigma_j = k$. Сложность вычисления по индексу r определяются числом уровней и строк на каждом уровне.

В случае $s \le q_0$ имеем

$$\Sigma_{r,\, s \le q_0} = \sum_{\tau=1}^{s \le q_0} \tau(\tau + 1)/2 = s(s+1)(2s+1)/12 + s(s+1)/4. \tag{4.5}$$

Пусть $s > q_0$. На уровнях $q_0 + 1, q_0 + 2, \ldots$ имеем по q_0 умножений на x/v и получим

$$\Sigma_{r,\, s > q_0} = q_0(q_0 + 1)(2q_0 + 1)/12 + q_0(q_0 + 1)/4 + (s - q_0)q_0. \tag{4.6}$$

Для второго слоя в выражениях (4.5) и (4.6) следует сделать замену $s \to s-1$. На уровнях $q_0+1, q_0+2, \ldots$ имеем по q_0-1 умножений на x/v.

Сложность вычислений по индексу i в выражении (4.2) $\Sigma_i = s$, где значение s определяется леммой 3.1.

Если $s \le q_0$, результирующая оценка сложности вычислений $h_{x,\,y}(m)$ по схеме Горнера будет иметь вид

$$N_{\text{опер}} = \Sigma_j + \Sigma_{r,\,y=0} + \Sigma_{i,\,y=0} + \Sigma_{r,\,y=1} + \Sigma_{i,\,y=1} = k + s(s+1)(2s+1)/12 +$$
$$+ s(s+1)/4 + s(s-1)(2s-1)/12 + s(s-1)/4 + s + s - 1 = k + s^3/3 + s^2/2 + 2s - 1.$$

В случае $s > q_0$ применим (4.6) и получим

$$N_{\text{опер}} = k + q_0(q_0+1)(2q_0+1)/12 + q_0(q_0+1)/4 + (s-q_0)q_0 +$$
$$+ q_0(q_0-1)(2q_0-1)/12 + q_0(q_0-1)/4 + (s-q_0)(q_0-1) + s + s - 1 =$$
$$= k + q_0^3/3 + q_0^2/2 + (s-q_0)(2q_0-1) + 2s - 1.$$

где $N_{\text{опер}}$ – сложность хеширования. Полученные выражения определяют (4.3) и (4.4).

Замечание 4.2.

1. Результаты предложения 4.1 являются новыми и представлены впервые в [39].

2. Асимптотика оценки сложности универсального хеширования по кривым Судзуки следует из (4.3). При $s \le q_0$, где $s = (3k)^{1/3}$, число операций сложений и умножений определяется выражением

$$N_{\text{опер}} = k + s^3/3 + s^2/2 + 2s - 1 = 2k + (3k)^{2/3}/2 + 2(3k)^{1/3} - 1. \qquad (4.7)$$

3. Прямое вычисление $h_{x,\,y}(m)$ по формуле (4.1) имеет сложность $N_{опер} = 4k$ без учета возведения в степень рациональных функций базисного пространства.

4. Схема Горнера требует предварительного вычисления w/v и x/v. Выбор точки кривой по ключевым данным реализуется просто, так как

решениями уравнения Судзуки являются рациональные точки $P_{a,b}=(a:b:1)$, где $a,b\in F_{q^2}$. Следует исключить точки $P_{a,0}$, $P_{0,b}$ и $P_{a,b}$, для которых $w=0$ и $v=0$. Число таких точек меньше $4q$. Пространство ключей равно q^2-4q.

Следствие 4.1 [39]. Асимптотика вероятности коллизии универсального хеширования по кривой $y^q-y=x^{q_0}\left(x^q-x\right)$ над F_q при больших значениях размерности поля $q\to\infty$ имеет вид

$$\varepsilon_{q\to\infty}=\left(3k\right)^{1/2}\big/q,\ k<g. \tag{4.8}$$

Доказательство. По лемме 3.1 определим $s\approx\left(3k\right)^{1/3}$ и значения параметров $i\approx s$, $j=0$, $t=0$, $r=0$. Подставим в (4.7) и для больших q получим (4.8).

4.2. Метод универсального хеширования с ограничением функционального поля алгебраических кривых

Сложность вычислений в методе универсального хеширования на основе скалярного произведения по рациональным функциям функционального поля, ассоциированного с алгебраической кривой, определяется параметризацией рациональных функций.

Кривые первой группы кривых Дэлигнэ – Лустига, к которым относится кривая Эрмита, и максимальные кривые второго и третьего рода по классификации имеют подгруппу Вейерштрасса размерности $\dim=2$, функциональное поле определяется двухпараметрическими рациональными функциями вида $\left\{x^i\cdot y^i\right\}$. Некоторые классы максимальных кривых имеют трехмерную параметризацию $\left\{x^i\cdot y^j\cdot v^t\right\}$.

Вторая группа кривых Дэлигнэ – Лустига, которая ассоциируется с группой Судзуки (кривые Судзуки), имеет над полем F_q четырехмерную

параметризацию функционального поля $\left\{x^r y^t v^i w^j\right\}$ и над расширенным полем F_{q^4} – пятимерную $\left\{x^a y^b v^c w^d \left(x^q + x\right)^r\right\}$.

Третья группа кривых Дэлигнэ – Лустига ассоциируется с группой Ри $R(q)$ (кривые Ри). Кривые Ри представлены в [107,121,162]. Кривые определены над полем F_q, характеристики $p = 3$, $q_0 = 3^m$, $q = 3q_0^2$ имеют $q^3 + 1$ точек $F_R := F_q\left(x, y_1, y_2\right)$, которые связаны уравнениями

$$y_1^q - y_1 = x^{q_0}\left(x^q - x\right);$$
$$y_2^q - y_2 = x^{q_0}\left(y_1^q - y_1\right).$$

Кривые Ри являются оптимальными в том смысле, что имеют число F_q рациональных точек относительно рода достаточно близким к границе Хассе – Вейля.

Морфизм $\pi = \left(1 : x : y_1 : y_2 : w_1 : w_2 : w_3 : w_4 : w_5 : w_6 : w_7 : w_8 : w_9 : w_{10}\right)$ассоции рован с линейной серией $D = \left|mP_\infty\right|$, определяет отображение кривой Ри на проективное пространство P^{13} [162]. Уравнения, определяющие координаты w_i, имеют вид

$$w_1 := z^{3q_0+1} - y_1^{2q_0};$$
$$w_2 := zy_1^{3q_0} - y_2^{3q_0};$$
$$w_3 := zy_2^{3q_0} - w_1^{3q_0};$$
$$w_4 := zw_2^{q_0} - y_1 w_2^{q_0};$$
$$v := xw_3^{q_0} - y_2 w_1^{q_0};$$
$$w_5 := y_1 w3_{q_0} - y_2 w_1^{q_0};$$
$$w_6 := v^{3q_0} - w_2^{3q_0} + xw_4^{3q_0};$$
$$w_7 := y_1 w_3^{q_0} - xw_3^{q_0} - w_6^{q_0} = w_2 + v;$$
$$w_8 := w_6^{3q_0} + xw_7^{3q_0};$$

$$w_9 := w_4 w_2^{q_0} - y_1 w_6^{q_0};$$

$$w_{10} := y_2 w_6^{q_0} - w_3^{q_0} w_4.$$

Нули и полюса координатных функций представлены в таблице 4.3.

Таблица 4.3 – Порядки нулей и полюсов рациональных функций кривой Ри

f	$v_0(f)$	$v_\infty(f)$
x	1	$-\left(q^2\right)$
y_1	q_0+1	$-\left(q^2+q_0 q\right)$
y_2	$2q_0+1$	$-\left(q^2+2q_0 q\right)$
w_1	$3q_0+1$	$-\left(q^2+3q_0 q\right)$
w_2	$q+3q_0+1$	$-\left(q^2+3q_0 q+q\right)$
w_3	$2q+3q_0+1$	$-\left(q^2+3q_0 q+2q\right)$
w_4	$q+2q_0+1$	$-\left(q^2+2q_0 q+q\right)$
v	$2q+3q_0+1$	$-\left(q^2+3q_0 q+q\right)$
w_5	$q_0 q+q+3q_0+1$	$-\left(q^2+3q_0 q+q+q_0\right)$
w_6	$3q_0 q+2q+3q_0+1$	$-\left(q^2+3q_0 q+2q+3q_0\right)$
w_7	$q_0 q+q+2q_0+1$	$-\left(q^2+2q_0 q+q+q_0\right)$
w_8	$q^2+3q_0 q+2q+3q_0+1$	$-\left(q^2+3q_0 q+2q+3q_0+1\right)$
w_9	$q_0 q+q+3q_0+1$	$-\left(q^2+3q_0 q+2q+q_0\right)$
w_{10}	$2q_0 q+2q+3q_0+1$	$-\left(q^2+3q_0 q+2q+2q_0\right)$

Таким образом, функциональное поле кривой определяется 13-мерной параметризацией рациональных функций.

Хеш-вычисления в проективных пространствах большой размерности приводят к структурной сложности алгоритмов и сложности их практической реализации. Вычисления над конечным полем фиксированной

характеристики, расширения, условия оптимизации по вероятности коллизии определяют выбор кривой. Для уменьшения структурной сложности алгоритма хеширования по алгебраическим кривым предлагается метод универсального хеширования с ограничением функционального поля алгебраических кривых.

Метод универсального хеширования с ограничением функционального поля алгебраических кривых предусматривает следующий порядок действий [41]:

– задание алгебраической кривой χ над полем F_q, вычисление точек кривой $P_1, P_2, \ldots, P_n$;

– вычисление функционального поля $F_q(\chi)\setminus\{0\}$, ассоциированного с алгебраической кривой χ;

– ограничение функционального поля подмножеством рациональных функций $f_i \in G_q(\chi)$ с упорядоченными порядками полюсов;

– построение алгоритма вычисления хеш-функции на ограниченном подмножестве рациональных функций.

Ограничение функционального поля алгебраических кривых определяется решением задачи минимизации сложности вычислений при хешировании заданного числа слов данных и заданной вероятности коллизии за счет оптимизации выбора базисных функций и размерности функционального пространства.

Рассмотрим решение задачи оптимизации выбора базисных функций и размерности функционального пространства для хеширования по полю рациональных функций кривой Судзуки [41].

Утверждение 4.1. Универсальное хеширование по кривой Судзуки над F_q, $q = 2q_0^2$, $q_0 = 2^s$ с ограничением функционального поля в базисе линейного пространства $L(mP_\infty) = L(\rho_l P_\infty)$, $\rho_l \le m \le \rho_{l+1}$ рациональных функций

$\left\{x^i \cdot y^j : iq + j\left(q + 2q_0\right) \le m\right\}$ определяет $U\left(q^2, q^k, q\right)$ семейство хеш-функций с вероятностью коллизии

$$\varepsilon = k/\left(2qq_0\right) + s/q - s\left(s-1\right)/\left(4qq_0\right), \tag{4.9}$$

если $\rho_k \le 2q_0\left(q-1\right)$ и сложностью хеширования

$$N_{xy} = k + s, \tag{4.10}$$

где k – число слов данных, $s = \left\lceil \left(2k + 1/4\right)^{1/2} - 1/2 \right\rceil$, $\lceil \cdot \rceil$ – округление к большему целому числу.

Доказательство. Кривые Судзуки S являются F_q изоморфными плоской кривой $Y^q Z^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1}Z^{q+q_0-1}$, где $q = 2q_0^2$ и $q_0 = 2^s$. Род кривой $g = q_0\left(q-1\right)$ и число F_q рациональных точек равно $q^2 + 1$. Точками кривой являются особая точка на бесконечности $P_0 = \left(0:1:0\right)$ кратности q_0 и рациональные точки $P_{a,b} = \left(a:b:1\right)$, где $a, b \in F_{q^2}$ и $b^q - b = a^{q_0}\left(a^q - a\right)$. Подгруппа Вейерштрасса функционального поля кривой содержит подгруппу $H\left(P_\infty\right) = \left\langle q, q+q_0, q+2q_0, q+2q_0+1\right\rangle$. Базис пространства $L\left(\rho_\ell P_0\right)$ задается функциями вида $\left\{w^j \cdot v^i \cdot y^t \cdot x^r : i\left(q+2q_0\right) + j\left(q+2q_0+1\right) + t\left(q+q_0\right) + r \cdot q \le \rho_\ell\right\}$, что следует из подгруппы Вейерштрасса $H\left(P_0\right)$, представленной порядками полюсов функций $x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$. Порядки полюсов: $\mathrm{div}_\infty\left(x\right) = qP_0$, $\mathrm{div}_\infty\left(y\right) = \left(q+q_0\right)P_0$, $\mathrm{div}_\infty\left(v\right) = \left(q+2q_0\right)P_0$, $\mathrm{div}_\infty\left(w\right) = \left(q+2q_0+1\right)P_0$.

Хеш-функция $h_{x,y}\left(m\right) \in F_q$ для сообщения m по рациональным функциям кривой Судзуки в точке x, y определяется выражением

$$h_{x,y}\left(m\right) = \sum m_{i,j,t,r} \cdot w^j \cdot v^i \cdot y^t \cdot x^r ,$$

где $m_{i,\,j,\,t,\,r} \in F_q$ – слова сообщения m, $i \ge 0$, $0 \le j \le 2q_0 - 1$, $0 \le t \le 1$, $0 \le r \le q_0$, $i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq \le \rho_k$, $x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$, ρ_k – полюс подгруппы Вейерштрасса $H(P_\infty)$ [38].

Кривая Судзуки при отображении на проективное пространство P^4 представляется точками

$$P_{(a,\,b)} := (1 : a : b : f(a,b) : af(a,b) + b^2) \cup \pi(P_0) = (0:0:0:0:1),$$

где $a, b \in F_q$ и $f(a,b) := a^{2q_0+1} + b^{2q_0}$.

Пусть $L(\rho_\ell P_0)$ определяется базисными функциями $\{x^i \cdot y^j : i \cdot q + j(q + q_0) \le \rho_\ell\}$. Для линейного пространства $L(\rho_\ell P_0)$, построенного по полному функциональному базису кривой Судзуки, имеем

$$\rho_{g+1} = 2g = 2q_0(q-1) = q + (2q_0 - 2)(q + q_0), \qquad (4.11)$$

где g – род кривой.

Из условия (4.11) следует, что $i + j \le 2q_0 - 1$, получим вычисление хеш-кода по двухпараметрической схеме Горнера, эквивалентной схеме вычисления по кривой Эрмита:

$$h_{x,\,y}(m) = \sum_{j=0}^{s} y^j \cdot \sum_{i=0}^{s-j} m_{i,\,j} \cdot x^i ,$$

где $\varepsilon = \left|(2k + 1/4)^{1/2} - 1/2\right|$ – параметр от k слов данных [95,163].

Множество ключей определяется пространством значений x, y. Универсальное хеширование выполняется по базису $\{x^i \cdot y^j : i \cdot q + j(q + q_0) \le \rho_k\}$. Таким образом, получим $U(q^2, q^k, q)$ семейство хеш-функций и вероятность коллизии $\varepsilon = \rho_k / N = \rho_k / q^2$. Нетрудно показать (см. [95]), что $j = k - s(s-1)/2$, $i = s - j$ и $s = \left|(2k + 1/4)^{1/2} - 1/2\right|$ при $\rho_k \le \rho_{g+1}$,

где $\lceil \cdot \rceil$ – округление к большему целому числу. Подставив соотношения i, j, s в выражение для ε, получим

$$\varepsilon = \rho_k / q^2 = \left(i \cdot q + j\left(q + q_0\right)\right) / q^2 = k/\left(2qq_0\right) + s/q - s\left(s-1\right)/\left(4qq_0\right). \qquad (4.12)$$

Оценка сложности универсального хеширования по базису x,y следует из оценки сложности универсального хеширования по двухпараметрической схеме Горнера для кривой Эрмита [163, предложение 2]

$$N_{xy} = k + s, \text{ если } \rho_k \le \rho_{g+1}, \qquad (4.13)$$

где $s = \left|\left(2k + 1/4\right)^{1/2} - 1/2\right|$.

Следствие 4.1. Асимптотическая оценка вероятности коллизии универсального хеширования по кривой Судзуки имеет вид

$$\varepsilon \approx 1/q_0 \text{ , если } k \le \left(2q_0 - 1\right)\left(q_0 + 1\right). \qquad (4.14)$$

Доказательство. Число хешируемых слов данных определяется числом полюсов подгруппы Вейерштрасса $\rho_k \le \rho_{g+1}$. Число пар $i + j \le 2q_0 - 1$ определяется как сумма арифметического ряда вида

$$k_{xy} = 1 + 2 + \ldots + \left(2q_0 - 1\right) + 2q_0 - 1 = \left(2q_0 - 1\right)\left(q_0 + 1\right). \qquad (4.15)$$

Коэффициенты i, j для $k_{xy} = \left(2q_0 - 1\right)\left(q_0 + 1\right)$ слов данных имеют значения $i = 1,\ j = 2q_0 - 2$. Окончательно получим

$$\varepsilon = \rho_k / q^2 = \left(q + \left(2q_0 - 2\right)\left(q + q_0\right)\right) / q^2 = \left(2q_0 - 1\right)/q + 1 - 2/q^2 \approx 1/q_0 .$$

Замечание 4.3.

1. Оценка вероятности коллизии хеширования по кривой Судзуки при полном функциональном базисе для $k_{xy} = \left(2q_0 - 1\right)\left(q_0 + 1\right)$ имеет вид

$$\varepsilon = \left(3k_{xy}\right)^{1/3} / q^2 = \left(\left(2q_0 - 1\right)\left(q_0 + 1\right)\right)^{1/3}\left(q + q_0\right)/q^2 \approx 1{,}6/\left(q_0 q_0^{1/3}\right). \qquad (4.16)$$

Сравнение с асимптотической оценкой (4.13) показывает, что хеширование по двухпараметрическому базису кривой Судзуки в $q_0^{1/3}$ раз проигрывает по вероятности коллизии.

2. Сложность универсального хеширования по кривым Судзуки в полном функциональном базисе определяется выражением

$$N_{xyvw} = k + s^3/3 + s^2/2 + 2s - 1, \text{ если } s \le q_0, \tag{4.17}$$

$$N_{xyvw} = k + q_0^3/3 + q_0^2/2 + (s - q_0)(2q - 1) + 2s - 1, \text{ если } s > q_0, \tag{4.18}$$

где $s = (3k)^{1/3}$.

Асимптотика оценки сложности универсального хеширования по кривым Судзуки следует из (4.3). При $s = (3k)^{1/3}$ и $s \le q_0$ получим

$$N_{xyvw} = 2k + (3k)^{2/3}/2 + 2(3k)^{1/3} - 1.$$

Сравнение с (4.16) показывает, что универсальное хеширование по базису двух рациональных функций в два раза выигрывает по сложности вычислений.

3. Зафиксируем вероятность коллизии значением $\varepsilon = \rho_{g+1}/N = 2g/q^2$. Для условия $\rho_k = \rho_{g+1}$ число слов данных при хешировании по полному функциональному базису определяется родом кривой

$$k_{xyvw} = qq_0 - q_0 + 1. \tag{4.19}$$

При хешировании по двухпараметрическому базису функционального поля кривой Судзуки наибольшее число слов данных $\rho_k \le \rho_{g+1}$ определяется соотношением

$$k_{xy} = (2q_0 - 1)(q_0 + 1). \tag{4.20}$$

Отношение числа хешируемых слов данных при двухпараметрическом хешировании к хешированию по полному базису

$$R = k_{xy}/k_{xyvw} = (2q_0 - 1)(q_0 + 1)/(qq_0 - q_0 + 1) \approx 1/q_0 \tag{4.21}$$

и определяет проигрыш двухпараметрического хеширования при фиксированной вероятности коллизии.

4.3 Многопотоковое универсальное хеширование

Распараллеливание процесса хеш-вычислений является эффективным инструментом увеличения скорости хеширования. Многопотоковая обработка данных строится на принципах параллелизма и определяется структурными возможностями процессоров.

Решение задачи повышения быстродействия универсального хеширования в методе скалярного произведения возможно в реализации с распараллеливанием на графическом процессоре (GPU).

Графический процессор (*GPU*) обладает меньшим набором исполняемых команд (*RISC*-подобные архитектуры), чем *CPU*, но большей производительностью. Технология *GPGPU* позволяет на одном вычислителе достигать достаточно высокого уровня параллелизма без временных затрат на передачу данных между узлами и синхронизацию результатов вычислений. Относительно низкая стоимость, простота добавления вычислительных модулей и удельное энергопотребление в сочетании с высокой удельной производительностью G*P*U позволяют реализовать на практике распределенные параллельные вычисления для решения вычислительно сложных задач в криптографической области.

Модель вычислительного устройства (ядра) GPU-процессора определяется верхним уровнем ядра, который состоит из блоков одинакового размера, которые группируются в сетку (grid) размерностью $N1 \times N2$. При использовании GPU-процессора можно задействовать грид необходимого размера и при помощи CUDA-технологии сконфигурировать блоки под параметры поставленной вычислительной задачи.

Оптимизация производительности, как правило, сводится к следующим шагам:

1) максимальное использование параллелизма задачи;

2) оптимизация доступа в память;

3) оптимизация машинной арифметики.

Каждое ядро *GPU*-процессора может работать одновременно с очень большим числом нитей, поэтому, чтобы ядро могло однозначно определить номер нити, в *CUDA* используются встроенные переменные threadldx и blockldx.

При написании параллельного кода для *GPU*-процессора *CUDA*-технология имеет ряд дополнительных расширений языка С:

– спецификаторы функций, которые показывают, как и откуда будут выполняться функции;

– спецификаторы запуска ядра *GPU*;

– спецификаторы переменных, которые служат для указания типа используемой памяти *GPU*;

– встроенные переменные для идентификации нитей, блоков и других параметров при исполнении кода в ядре *GPU*.

Спецификаторы функций определяют, как и откуда будут вызываться функции. Всего в *CUDA* три таких спецификатора:

– *__host__* – выполняется на *CPU*, вызывается с *CPU*;

– *__global__* – выполняется на *GPU*, вызывается с *CPU*;

– *__device__* – выполняется на *GPU*, вызывается с *GPU*.

Спецификаторы запуска ядра служат для описания количества блоков, нитей и памяти, которые необходимо выделить при расчете на *GPU*-процессоре.

Общим приемом в *CUDA*-технологии является то, что исходная задача разбивается на набор отдельных подзадач, решаемых независимо друг от друга. Каждой такой подзадаче соответствует свой блок нитей. Причем каждой отдельной нити соответствует один элемент вычислительных данных.

Анализ решения задачи повышения быстродействия универсального хеширования в методе скалярного произведения предлагает реализацию следующих действий.

На первом шаге необходимо решить проблему «последовательного участка» параллельного алгоритма. Возможные варианты решения – уменьшение такого участка либо попытка преобразовать его большую часть в параллельный код. Однопотоковый алгоритм универсального хеширования разбивается на многопотоковый на p процессоров. Это в p раз уменьшает сложность вычислений.

Следующий этап заключается в скоростной реализации целочисленных операций умножения и сложения в модулярной арифметике. Известные алгоритмы с вычислениями 64-битных чисел на графических процессорах позволяют повысить быстродействие в 81,1 и более раз [43].

Универсальное хеширование по точкам алгебраической кривой χ для сообщения $m=(m_1,\ldots,m_k)$, $m_i \in F_q$ определяется выражением

$$h_{P_j}(m)=\sum_{i=1}^{k} f_i(P_j)m_i,$$

где $f_i \in F_q(\chi)$ с упорядоченными порядками полюсов $0<\rho_1<\ldots<\rho_k$. Хеш-значение $h_{P_j}(m) \in F_q$ вычисляется в точке $P_j \in F_q$.

Параметризация рациональных функций f_i для многих алгебраических кривых приводит к степенным координатным функциям. Универсальное хеширование по кривой Судзуки определяется вычислением по формуле

$$h_{x,y}(m)=\sum m_{i,j,t,r}\cdot w^j\cdot v^i\cdot y^t\cdot x^r \qquad (4.22)$$

с четырехпараметрическим представлением. Показатели степеней должны удовлетворять условию

$$i(q+2q_0)+j(q+2q_0+1)+t(q+q_0)+rq\le\rho_k.$$

Для реализации потокового вычисления следует структурировать алгоритм так, чтобы появился последовательный участок, допускающий распараллеливание.

Применение метода универсального хеширования по кривой Судзуки на основе схемы Горнера позволяет это сделать.

Результирующая формула $h_{x,\,y}(m)$ определяется выражением (4.2):

$$h_{x,\,y}(m)=\sum_{t=0}^{1} y^t \sum_{i=0}^{s-t} v^i \sum_{r=0}^{\min(s-t,\,q_0-t)} (x/v)^r \sum_{j=0}^{\min(s-r,\,q_0-1)} (w/v)^j\, m_{t,i,r,j},$$

где s – число уровней для k информационных слов. Параметр s определяется по лемме 3.1.

На каждом каскаде реализуется вычисление полиномиального вида

$$y=\sum_{i=1}^{n} m_i x^i .$$

Полиномиальное выражение можно представить через p однородных групп:

$$\begin{aligned} y = m_1x + m_2x^2 + \ldots + m_nx^n = \left(m_1x + m_2x^2 + m_3x^3 + \ldots + m_{n/p}x^{n/p}\right) + \\ + x^{n/p}\left(m_{1+n/p}x + m_{2+n/p}x^2 + m_{3+n/p}x^3 + \ldots + m_{2n/p}x^{n/p}\right) + \\ + x^{2n/p}\left(m_{1+2n/p}x + m_{2+2n/p}x^2 + m_{3+2n/p}x^3 + \ldots + m_{3n/p}x^{n/p}\right) + \ldots + \\ + x^{(p-1)n/p}\left(m_{1+(p-1)n/p}x + m_{2+(p-1)n/p}x^2 + m_{3+(p-1)n/p}x^3 + \ldots + m_nx^{n/p}\right). \end{aligned}$$

Хеш-вычисления в каждой подгруппе можно выполнить параллельно с объединением результатов на втором каскаде:

$$y=\sum_{j=0}^{p-1} x^{nj/p} \sum_{i=1}^{n/p} m_{i+jn/p}x^i .$$

На первом каскаде хеш-функцию $\sum_{i=1}^{n/p} m_{i+jn/p}x^i$ можно вычислить по итерационной схеме Горнера с одной операцией умножения и сложения в конечном поле. Итерационная схема Горнера вычисления хеш-функции предполагает вычисление

$$y \leftarrow xy + m \bmod q .$$

Вычисление на втором каскаде полиномиальное, можно также применить схему Горнера. Результат разбиения – двухпараметрическая схема вычисления. Применение к полиномиальным вычислениям по каждой сумме итерационной схемы Горнера со сложностью $k/p+p$ практически в p раз повышает быстродействие полиномиального хеширования [43].

4.4 Выводы

Основными научными результатами являются метод вычисления хеш-функций на четырехпараметрической схеме Горнера, который основывается на определении хеш-функции по алгебраической кривой Судзуки, ее функционального поля, соотношения между размерностью линейного пространства рациональных функций кривых и размером хешируемых данных и метод универсального хеширования с ограничением функционального поля алгебраических кривых.

Основные результаты исследований.

1. Сложность универсального хеширования по алгебраическим кривым определяется многопараметрическим выражением для функции хеширования. Практическое вычисление хеш-значений включает построение линейного векторного пространства рациональных функций по показателям их степеней в порядке возрастания полюсов. Применение метода построения алгоритмов на основе схемы Горнера приводит к эффективной структуризации хеш-вычислений. Метод вычисления хеш-функций по алгебраической кривой Судзуки на основе четырехпараметрической схемы Горнера позволяет повысить в два раза скорость хеширования по сравнению с общим алгоритмом.

2. Метод универсального хеширования с ограничением функционального поля алгебраических кривых позволяет уменьшить структурную сложность алгоритмов хеширования по алгебраическим кривым.

Универсальное хеширование по базису двух рациональных функций по кривой Судзуки в два раза выигрывает по сложности вычислений. Универсальное хеширование с ограничением функционального поля алгебраических кривых позволяет обойти ограничения для вычислений над конечным полем фиксированной характеристики и расширения, условия оптимизации по вероятности коллизии. Недостатком применения данного метода является уменьшение числа хешируемых данных по сравнению с полным функциональным полем. Требуется оптимизация базиса функционального поля. Наибольший результат достигается на сложных многопараметрических кривых.

3. Универсальное хеширование по алгебраическим кривым допускает эффективное многопотоковое вычисление. Для реализации потокового вычисления следует структурировать алгоритм так, чтобы появился последовательный участок, допускающий распараллеливание. Применение метода универсального хеширования по кривой Судзуки на основе схемы Горнера позволяет выполнить структурирование алгоритма в виде полиномиального каскадного хеширования, что допускает распараллеливание процесса вычислений. Скорость вычислений прямо пропорциональна числу потоковых вычислений.

РАЗДЕЛ 5
РАЗРАБОТКА МЕТОДА МНОГОКАСКАДНОГО УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ ПО КРИВОЙ СУДЗУКИ

Задача раздела – разработка метода и практических рекомендаций многокаскадного универсального хеширования по рациональным функциям кривой Судзуки. С этой целью в подразделе 5.1 выполнена оценка параметров многокаскадного универсального хеширования по алгебраическим кривым со связкой хеш-кода с текстом, сравнения по вероятности коллизии, затратам по ключу и длины хешируемых данных. Определение и свойства каскадного хеширования по алгебраическим кривым на основе произведения функциональных полей рассмотрены в подразделе 5.2. Представлены параметры многокаскадного универсального хеширования по алгебраическим кривым и кривой Судзуки, оценки вероятности коллизии и сложности вычислений для многокаскадного хеширования в конечном поле. Многократное универсальное хеширование по рациональным функциям алгебраических кривых рассмотрено в подразделе 5.3. Представлены свойства универсальности многократного хеширования для хеширования по максимальным кривым и кривой Судзуки, оценки вероятности коллизии, сложности вычислений для многократного хеширования. Композиционное универсальное хеширование по кривой Судзуки рассмотрено в подразделе 5.4. Рассмотрено построение безусловной аутентификации в композиционной конструкции Стинсона, оценки параметров строго универсальной композиционной конструкции по кривой Судзуки.

5.1 Каскадное универсальное хеширование по алгебраическим кривым со связкой хеш-кода с текстом

Каскадное универсальное хеширование по алгебраическим кривым рассмотрено в [137] и представляется двумя основными схемами: каскадное

хеширование со связкой хеша и текста и каскадное хеширование на основе произведения функциональных полей.

Определение каскадной схемы универсального хеширования со связкой хеша и текста имеет следующее определение.

Определение 5.1 [139]. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \| M_2$. Каскадное универсальное хеширование по рациональным функциям алгебраических кривых определяется выражением

$$Ch(M) = AGh_2\left(Agh_1(M_1) \| M_2\right), \tag{5.1}$$

где AGh_1, AGh_2 – универсальные схемы хеширования по рациональным функциям алгебраических кривых, $Ch(M)$ определяет универсальное семейство хеш-функций $\varepsilon - AU$, где $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/|H^2|$, $\varepsilon_1, \varepsilon_2$ – соответственно вероятности коллизий для AGh_1 и AGh_2 хеширования.

Коллизионные свойства каскадной конструкции определяются утверждениями 5.1, 5.2.

Утверждение 5.1 [139]. Если H_1 есть $\varepsilon_1 - U$ универсальный класс и H_2 есть $\varepsilon_2 - U$, тогда $H = H_1 H_2$ есть $\varepsilon - U$, где $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/|H^2|$.

Утверждение 5.2 [139]. Пусть H_1 и H_2 соответственно $\varepsilon_1 - U$ и $\varepsilon_2 - U$ универсальные классы хеш-функций. Каскадная конструкция $H_1 H_2$ имеет наименьшую вероятность коллизии, если $\varepsilon_1 = \varepsilon_2$.

Замечание 5.1.

1. Каскадное хеширование определяется тем, что хеш предыдущего каскада связывается с текстом следующего каскада через конкатенацию. Структурная схема вычислений для двух каскадов представлена на рис. 5.1.

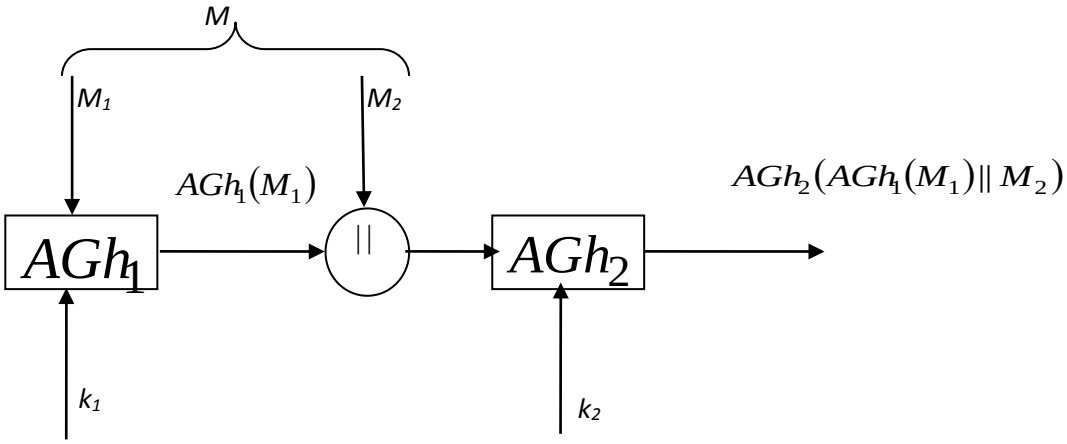


Рис. 5.1. Структурная схема $Ch(M)$ хеширования

2. Каскадное хеширование $Ch(M)$ при фиксированном поле вычислений предполагает разбиение данных на блоки приблизительно равной длины.

3. Вероятность коллизии каскадного хеширования имеет ограничение по наименьшему полю вычисления хеша одного из каскадов.

4. Размер ключевых данных увеличивается пропорционально числу каскадов, с учетом поля вычисления и универсального хеширования каскада.

5. Каскадное хеширование позволяет эффективно увеличить общую длину хешируемых данных и зафиксировать вероятность коллизии на уровне хеша первого каскада, если на втором и последующих каскадах увеличить поле вычислений. Данный метод реализован в алгоритме хеширования *UMAC*(2000). Каскадная схема в *UMAC* применяется с подъёмом поля вычисления сначала 32 бита, затем 64 бита и 128 бит.

При построении двухкаскадного универсального хеширования по алгебраическим кривым рассмотрим каскадирование с универсальным хешированием по проективной кривой, кривой Эрмита и кривой Судзуки.

Утверждение 5.1 определяет, что результирующие параметры универсального хеширования – вероятность коллизии, размер ключевых данных, размер хешируемых данных, сложность вычисления хеша – зависят от выбора схем хеширования в каскадах.

Применение двухкаскадного универсального хеширования с одной и той же функцией хеширования в каждом каскаде приводит к следующим результатам.

Утверждение 5.3. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \| M_2$. Алгоритм вычисления хеш-кода в каскадной конструкции определяется выражением

$$Ch(M) = PSh_q\left(PSh_q(M_1) \| M_2\right),$$

где PSh_q – универсальное хеширование по проективной прямой. Тогда $Ch_q(M)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^2, q^k, q\right)$, $\varepsilon = \max\left(k_1/q, (k_2+1)/q\right)$, k_1, k_2 – число слов данных M_1 и M_2.

Замечание 5.2.

1. Для $Ch(M) = PSh_q\left(PSh_q(M_1) \| M_2\right)$ хеширования справедливо утверждение 5.2. Вероятность коллизии будет минимальной, если $|M_1| = |M_2|$.

2. Вероятность коллизии при хешировании по проективной прямой пропорционально зависит от значения длины данных и в двухкаскадной схеме $Ch_q(M)$ вероятность коллизии уменьшится только в два раза.

3. Применение в каскаде PSh_q хеширования дает преимущество в скорости вычислений, так как PSh_q хеширование имеет определение над простым полем. Практический алгоритм вычислений может учитывать эту особенность. Для малых длин данных по быстродействию целесообразно использовать только PSh_q хеширование.

Утверждение 5.4. Пусть F_q – квадратичное расширенное поле, M – сообщение и $M = M_1 \| M_2$. Алгоритм вычисления хеш-кода в каскадной конструкции определяется выражением

$$Ch(M) = Hh_q\left(Hh_q(M_1) \| M_2\right),$$

где Hh_q – универсальное хеширование по кривой Эрмита. Тогда $Ch_q(M)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^3, q^k, q\right)$, $\varepsilon = \max\left(\sqrt{2k_1}/q, \sqrt{2(k_2+1)}/q\right)$, k_1, k_2 – число слов данных M_1 и M_2, $k < \sqrt{q}\left(\sqrt{q}-1\right)$ – число слов данных M.

Замечание 5.3. Универсальное хеширование по кривой Эрмита для длин данных $k < \sqrt{q}\left(\sqrt{q}-1\right)$ имеет асимптотику $\varepsilon_H = \dfrac{\sqrt{2k}}{q}$. Минимизация вероятности $Ch_q(M)$ требует равенства длин данных на первом и втором каскадах хеширования, что уменьшает вероятность коллизии в $\sqrt{2}$ раз по сравнению с однокаскадным хешированием по кривой Эрмита.

Утверждение 5.5. Пусть F_q – конечное нечетной степени расширения поле, M – сообщение и $M = M_1 \| M_2$. Алгоритм вычисления хеш-кода в каскадной конструкции определяется выражением

$$Ch(M) = Sh_q\left(Sh_q(M_1) \| M_2\right),$$

где Sh_q – универсальное хеширование по кривой Судзуки. Тогда $Ch_q(M)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^4, q^k, q\right)$, $\varepsilon = \max\left((3k_1)^{1/3}/q, (3(k_2+1))^{1/3}/q\right)$, k_1, k_2 – число слов данных M_1 и M_2, $k < (q-1)\sqrt{q/2}$ – число слов данных M.

Замечание 5.4. Универсальное хеширование по кривой Судзуки для длин данных $k < (q-1)\sqrt{q/2}$ имеет асимптотику $\varepsilon_s = (3k)^{1/3}/q$. Двухкаскадное хеширование $Ch_q(M)$ снижает вероятность коллизии в $2^{1/3}$ раз по сравнению с однокаскадным.

Свойства двухкаскадного хеширования по кривой Эрмита и проективной прямой рассмотрены в [137].

Утверждение 5.6 [137]. Пусть F_q, $q = p^2$ – расширенное конечное поле, $M = M_1 \| M_2$, $|M_1| \le \sqrt{q} + 1$, $|M_2| \le q\sqrt{q}$, $0 < k \le q\sqrt{q} + \sqrt{q}$. Тогда $Ch_q(M)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^2\sqrt{q}, q^k, q\right)$, $\varepsilon = \max(\varepsilon_{PS}, \varepsilon_H) + 1/\left|q\sqrt{q}\right|$, $\varepsilon_{PS}, \varepsilon_H$ – соответственно вероятности коллизий для PSh_q и Hh_q хеширования.

Замечание 5.5. Для $Ch_q(M) = Hh_q\left(PSh_q(M_1) \| M_2\right)$ хеширования справедливо утверждение 5.2. Вероятность коллизии будет минимальной, если $\varepsilon_H = \varepsilon_{PS}$.

К подобным результатам приводит каскадное хеширование со связкой хеша по кривым Судзуки во втором каскаде.

Утверждение 5.7. Пусть F_q, $q = 2^{2s+1}$ – расширенное конечное поле, $M = M_1 \| M_2$, $|M_1| \le q$, $|M_2| \le q^2$, $0 < k \le q^2 + q$. Тогда $Ch_q(M) = Sh_q\left(PSh_q(M_1) \| M_2\right)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^3, q^k, q\right)$, $\varepsilon = \max(\varepsilon_{PS}, \varepsilon_S)$, $\varepsilon_{PS}, \varepsilon_S$ – соответственно вероятности коллизий для PSh_q и Sh_q хеширования.

Замечание 5.6. Для $Ch_q(M) = Sh_q\left(PSh_q(M_1) \| M_2\right)$ хеширования вероятность коллизии будет минимальной, если $\varepsilon_S = \varepsilon_{PS}$. Из асимптотики вероятности коллизии $\varepsilon_S = (3k)^{1/3}/q$ для длин данных $k < (q-1)\sqrt{q/2}$ и равенства $\varepsilon_S = \varepsilon_{PS}$ следует $k_2 = k_1^3/3$.

Утверждение 5.8.Пусть F_q, $q = 2^{2s+1}$ – расширенное конечное поле, $M = M_1 \| M_2$, $|M_1| \le q$, $\left|M_2 \le q^2\right|$, $0 < k \le q^2 + q$. Тогда $Ch_q(M) = Sh_q\left(Hh_q(M_1) \| M_2\right)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^{2,5}, q^k, q\right)$, $\varepsilon = \max(\varepsilon_H, \varepsilon_S)$, $\varepsilon_H, \varepsilon_S$ – соответственно вероятности коллизий для Hh_q и Sh_q хеширования.

Замечание 5.7. Для $Ch_q(M)=Sh_q\left(Hh_q(M_1)\|M_2\right)$ хеширования вероятность коллизии будет минимальной, если $\varepsilon_S=\varepsilon_H$. Из асимптотики вероятностей коллизии $\varepsilon_S=(2k_2)^{1/3}/q$, $\varepsilon_H=\sqrt{2k_1}/q$ для длин данных $k_2<(q-1)\sqrt{q/2}$, $k_2<\left(\sqrt{q}-1\right)\sqrt{q}$ и равенства $\varepsilon_S=\varepsilon_H$, следует $k_2\approx k_1^{3/2}/3$.

Параметры универсального каскадного хеширования со связкой хеша и текста представлены в таблице 5.1.

Таблица 5.1 – Оценки вероятности коллизии каскадного универсального хеширования по алгебраическим кривым

Схемы каскадного включения	Параметры универсального хеширования	Условия минимизации вероятности коллизии
$PSh_q\left(PSh_q(M_1)\|M_2\right)$	$\varepsilon-U\left(q^2,q^k,q\right)$, $\varepsilon=\max\left(k_1/q,(k_2+1)/q\right)$	$k_2=k_1=k/2$, $\varepsilon_{PS}=k/(2q)$
$Hh_q\left(Hh_q(M_1)\|M_2\right)$	$\varepsilon-U\left(q^3,q^k,q\right)$, $\varepsilon=\max\left(\sqrt{2k_1}/q,\sqrt{2(k_2+1)}/q\right)$	$k_2=k_1=k/2$, $\varepsilon_H=(k)^{1/2}/q$
$Sh_q\left(Sh_q(M_1)\|M_2\right)$	$\varepsilon-U\left(q^4,q^k,q\right)$. $\varepsilon=\max\left((3k_1)^{1/3}/q,(3(k_2+1))^{1/3}/q\right)$	$k_2=k_1=k/2$, $\varepsilon_S=(3k/2)^{1/3}/q$
$Hh_q\left(PSh_q(M_1)\|M_2\right)$	$\varepsilon-U\left(q^2\sqrt{q},q^k,q\right)$, $\varepsilon=\max(\varepsilon_{PS},\varepsilon_S)+1/\left\|q\sqrt{q}\right\|$	$k_2=k_1^2/2$, $\varepsilon_S=(2k_2)^{1/2}/q$, $\varepsilon_{PS}=k_1/q$
$Sh_q\left(PSh_q(M_1)\|M_2\right)$	$\varepsilon-U\left(q^3,q^k,q\right)$, $\varepsilon=\max(\varepsilon_{PS},\varepsilon_S)$	$k_2=k_1^3/3$, $\varepsilon_S=(3k/2)^{1/3}/q$, $\varepsilon_{PS}=k_1/q$
$Sh_q\left(Hh_q(M_1)\|M_2\right)$	$\varepsilon-U\left(q^{3,5},q^k,q\right)$, $\varepsilon=\max(\varepsilon_H,\varepsilon_S)$	$k_2=k_1^{3/2}/3$, $\varepsilon_S=(2k_2)^{1/3}/q$, $\varepsilon_H=\sqrt{2k_1}/q$

Сравнение каскадного хеширования $PSh_q\left(PSh_q\left(M_1\right)\|M_2\right)$ и $Sh_q\left(PSh_q\left(M_1\right)\|M_2\right)$ показывает, что каскадное универсальное хеширование по кривым Судзуки со связкой хеша с текстом позволяет в куб раз увеличить длину хешируемых данных по сравнению с хешированием по проективной прямой (полиномиальное хеширование) без увеличения вероятности коллизии. Затраты по ключу увеличиваются в q раз. Это абсолютно наилучший результат хеширования по алгебраическим кривым. Хеширование в каскадной схеме $Hh_q\left(PSh_q\left(M_1\right)\|M_2\right)$ реализует увеличение в квадрат раз длины данных, при этом ключевое пространство возрастает в $\sqrt{q}$.

5.2 Каскадное универсальное хеширование по алгебраическим кривым на основе произведения функциональных полей

Определение и свойства каскадного хеширования по алгебраическим кривым на основе произведения функциональных полей представлены в [46,47].

Определение 5.2 [46]. Пусть F_q – конечное поле, M – сообщение и $M = M_1\|M_2\|\ldots\|M_t$. Алгоритм вычисления хеш-кода в каскадной конструкции определяется выражением

$$Ch_t\left(M\right) = AGh_2\left(Agh_1\left(M_1\right)\|AGh_1\left(M_2\right)\|\ldots\|AGh_1\left(M_t\right)\right), \qquad (5.2)$$

где Agh_1, AGh_2 – универсальные схемы хеширования по алгебраическим кривым, $Ch_t\left(M\right)$ определяет универсальное семейство хеш-функций $\varepsilon - AU$, где $\varepsilon = \max\left(\varepsilon_1, \varepsilon_2\right) + 1/\left|H^2\right|$, $\varepsilon_1, \varepsilon_2$ – соответственно вероятности коллизий для ADh_1 и AGh_2 хеширования.

Структурная схема каскадного хеширования по алгебраическим кривым на основе произведения функциональных полей представлена на рис. 5.2.

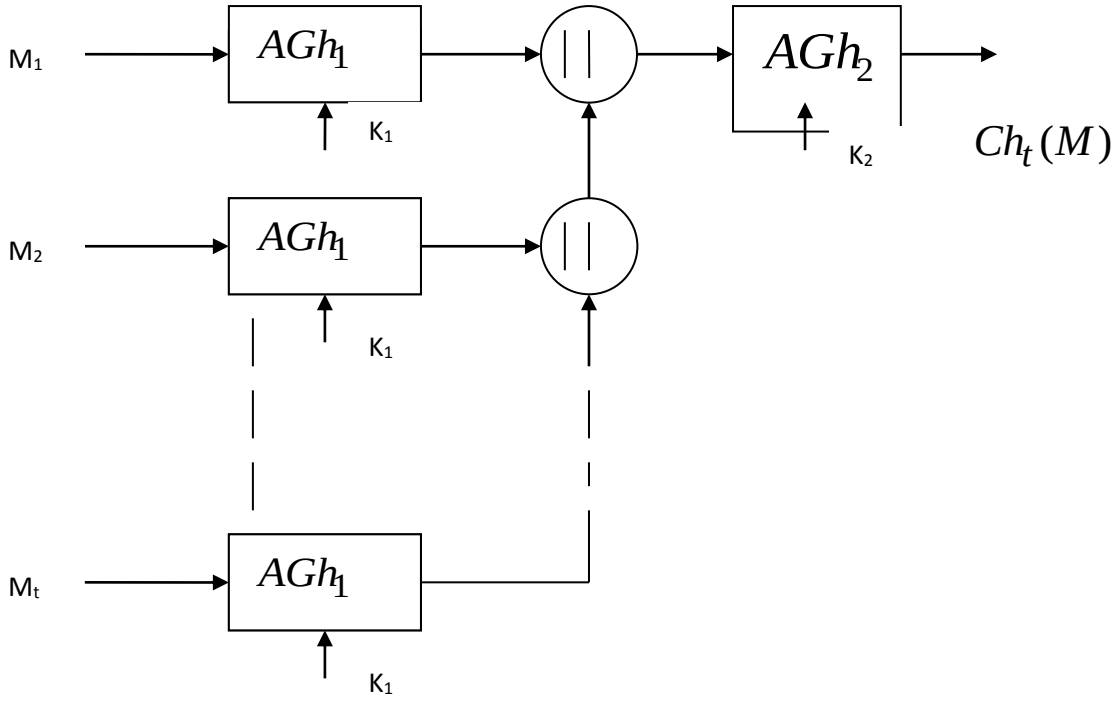


Рис. 5.2. Структурная схема $Ch(M)$ хеширования

Замечание 5.8.

1. Коллизионные свойства каскадного хеширования следуют из утверждения 5.1.

2. Каскадное хеширование $Ch_t(M)$ при фиксированном поле вычислений предполагает разбиение данных на t блоков равной длины. Для первого каскада вероятность коллизии определяется размером блока данных, для второго – значением t – числа блоков данных.

3. Вероятность коллизии каскадного хеширования имеет ограничение по наименьшему полю вычисления хеша одного из каскадов, что следует из выражения для вероятности $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/|H^2|$.

4. Размер ключевых данных определяется произведением пространства ключей первого и второго каскадов с учетом поля вычисления и универсального хеширования каскада.

Каскадное универсальное хеширование $Ch_t(M)$ реализуется по функциональным полям проективной прямой, кривой Эрмита, кривой Судзуки. Для двухкаскадного хеширования ниже представлены следующие результаты.

Определение 5.3 [139]. Пусть F_q, $q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \| M_2 \| \ldots \| M_t$. Алгоритм вычисления хеш-кода в каскадной конструкции определяется выражением

$$Ch_t(M) = Hh_q\left(PSh_q(M_1) \| PSh_q(M_2) \| \ldots \| PSh_q(M_t)\right), \qquad (5.3)$$

где Hh_q, PSh_q PSh_q – универсальные схемы хеширования по кривой Эрмита и проективной прямой.

Утверждение 5.9 [139]. Пусть F_q, $q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \| M_2 \| \ldots \| M_t$, $Ch_t(M)$ – хеширование (5.3). Тогда $Ch_t(M)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^2\sqrt{q}, q^k, q\right)$, $\varepsilon = (2k)^{1/3}/q$, $0 < k \le q\sqrt{q}/2$.

Замечание 5.9.

1. Пространство ключей определяется произведением числа ключей первого и второго каскадов и равно $q^2\sqrt{q}$. Пусть k число слов данных и k' – размер блока данных, $t = k/k'$. Наименьшая вероятность коллизии реализуется в случае $\varepsilon_H = \varepsilon_{PS}$. Подставим в выражения для ε_H и ε_{PS} значения k' и $t = k/k'$, получим $k' = (2k)^{1/3}$ и оценку для вероятности $\varepsilon(2k)^{1/3}/q$.

2. Каскадное хеширование по кривой Эрмита и проективной прямой $PSh_q - Hh_q$ имеет вероятность коллизии $\varepsilon = (2k)^{1/3}/q$, что совпадает с хешированием по кривой Судзуки $\varepsilon = 3k^{1/3}/q$. Затраты по ключу несколько больше – $q^2\sqrt{q}$, в отличие от q^2 – для кривой Судзуки.

3. Вычисления в каскадном хешировании существенно проще. Вычисления по PSh_q каскаду выполняются на одной рациональной функции со сложностью k^t и по Hh_q каскаду на двух рациональных функциях – со сложностью $t+\sqrt{t}$. С учетом $t=k/k'$ и $k'=(2k)^{1/3}$ получим оценку для числа вычислений $k+t+\sqrt{t}=k+k^{2/3}/2^{1/3}+k^{1/3}/2^{1/6}$, что меньше почти в два раза числа вычислений по кривой Судзуки на четырех рациональных функциях – $2k+1,04k^{2/3}+2\sqrt[3]{3}k^{1/3}$ (см. таблицу 5.1).

Интерес представляют комбинации других универсальных хеш-функций в двухкаскадной схеме хеширования. Свойства представлены утверждениями 5.10 – 5.12.

Утверждение 5.10 [139]. Пусть F_q – конечное поле, M – сообщение и $M=M_1\|M_2\|\ldots\|M_t$, $Ch_t(M)$ – хеширование вида (5.2), где $AGh_1=PSh_q$, $AGh_2=Fh_q-$ универсальные схемы хеширования по проективной прямой и кривой Ферма $x^{(q-1)/3}+y^{(q-1)/3}+1=0$ соответственно. Тогда $Ch_t(M)$ определяет универсальное семейство хеш-функций $\varepsilon-U\left(q^3,q^k,q\right)$, $\varepsilon=(9k/2)^{1/3}/q$, $0<k\le q\sqrt{q}$.

Замечание 5.10. Результаты каскадного хеширования PSh_q-Fh_q совпадают по вероятности коллизии с хешированием PSh_q-Hh_q, но требуют больший размер ключа, соответственно q^3 и $q^2\sqrt{q}$.

Утверждение 5.11 [47]. Пусть F_q – конечное поле, M – сообщение и $M=M_1\|M_2\|\ldots\|M_t$, $Ch_t(M)$ – хеширование вида (5.2), где $AGh_1=PSh_q$, $AGh_2=Sh_q-$ универсальные схемы хеширования по проективной прямой и кривой Судзуки соответственно. Тогда $Ch_t(M)$ определяет универсальное семейство хеш-функций $\varepsilon-U\left(q^3,q^k,q\right)$, $\varepsilon=(3k)^{1/4}/q$, $0<k\le q^2$.

Замечание 5.11.

1. Пространство ключей определяется произведением числа ключей первого и второго каскадов и равно q^3. Пусть k – число слов данных и k' – размер блока данных, $t = k/k'$. Наименьшая вероятность коллизии реализуется в случае $\varepsilon_S = \varepsilon_{PS}$. Подставим в выражения для ε_S и ε_{PS} значения k' и $t = k/k'$, получим $\varepsilon_S = \left(3k/k'\right)^{1/3}/q$, $\varepsilon_{PS} = k'/q$, $k' = \left(3k\right)^{1/4}$ и оценку для вероятности $\varepsilon = \left(3k\right)^{1/4}/q$. Результаты каскадного хеширования $PSh_q - Sh_q -$ наилучшие среди схем, где на первом каскаде используется PSh_q хеширование и обеспечивают хеширование наибольшей длины данных.

2. Недостатком каскадного хеширования $PSh_q - Sh_q$ является повышенная сложность. Вычисления по PSh_q каскаду выполняются на одной рациональной функции со сложностью $\sim k^t$ и по Sh_q каскаду на четырех рациональных функциях – со сложностью $\sim 2t + 1{,}04t^{2/3} + 2\sqrt[3]{3}t^{1/3}$ (см. таблицу 5.2). С учетом $t = k/k'$ и $k' = \left(3k\right)^{1/4}$ получим оценку для числа вычислений $k + 2t + 1{,}04t^{2/3} + 2\sqrt[3]{3}t^{1/3} = k + 1{,}5k^{3/4} + 0{,}87k^{1/2} + 2{,}63k^{1/4}$. Относительное увеличение сложности по сравнению с PSh_q хешированием составляет $\sim 1 + 1{,}52k^{-1/4}$.

Утверждение 5.12 [47]. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \| M_2 \| \ldots \| M_t$, $Ch_t\left(M\right)$ – хеширование вида (5.2), где $AGh_1 = Hh_q$, $AGh_2 = Sh_q -$ универсальные схемы хеширования по кривой Эрмита и кривой Судзуки соответственно. Тогда $Ch_t\left(M\right)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^3\sqrt{q}, q^k, q\right)$, $\varepsilon = 1{,}43k^{1/5}/q$, $0 < k \le q^2\sqrt{q}$.

Замечание 5.12.

1. Пространство ключей определяется произведением числа ключей первого и второго каскадов и равно $q^3\sqrt{q}$. Пусть k число слов данных и k' –

размер блока данных, $t = k/k'$. Наименьшая вероятность коллизии реализуется в случае $\varepsilon_S = \varepsilon_H$. Подставим в выражения для ε_S и ε_H значения k' и $t = k/k'$, получим $\varepsilon_S = \left(3k/k'\right)^{1/3}/q$, $\varepsilon_H = \sqrt{2k'}/q$, $k' = \left(3k\right)^{2/5}/2^{3/2}$ и оценку для вероятности $\varepsilon = 1,43k^{1/5}/q$. Результаты каскадного хеширования $Hh_q - Sh_q$ являются абсолютно лучшими среди двухкаскадных схем универсального хеширования по алгебраическим кривым и обеспечивают хеширование наибольшей длины данных.

2. Недостатком каскадного хеширования $Hh_q - Sh_q$ является увеличенная сложность хеширования. Вычисления по Hh_q каскаду выполняются на двух рациональных функциях со сложностью $\le t\left(k' + \sqrt{k'}\right)$ и по Sh_q каскаду на четырех рациональных функциях – со сложностью $\le 2t + 1,04t^{2/3} + 2\sqrt[3]{3}t^{1/3}$ (см. таблицу 5.2). С учетом $t = k/k'$ и $k' = 1,02k^{2/5}$ получим оценку для числа вычислений

$$t\left(k' + \sqrt{k'}\right) + 2t + 1,04t^{2/3} + 2\sqrt[3]{3}t^{1/3} = k + k^{4/5} + 2k^{3/5} + k^{2/5} + 2,88k^{1/5}.$$

Относительное увеличение сложности по сравнению с PSh_q хешированием составляет $\le 1 + k^{-1/5}$.

Оценки многокаскадного универсального хеширования $l - Ch_t\left(M\right)$ представлены утверждениями 5.13 – 5.16.

Утверждение 5.13 [139]. Пусть F_q – конечное поле, $M = M_1 \| M_2 \| \ldots \| M_t$ и $l - Ch_t\left(M\right)$ – l-каскадное универсальное хеширование по проективной прямой. Тогда $l - Ch_t\left(M\right)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^l, q^k, q\right)$, $\varepsilon = k^{1/l}/q$, $0 < k \le q^l$, со сложностью вычислений $k + k^{l-1/l} + k^{l-2/l} + \ldots + k^{1/l}$.

Замечание 5.13.

1. Хеширование на каждом каскаде является универсальным, каскадная хеш-функция также является универсальной.

2. Пространство ключей определяется произведением числа ключей всех каскадов и равно q^l.

3. Наименьшая вероятность коллизии реализуется, если на каждом каскаде значение вероятности коллизии является наименьшим. Это достигается, если размер данных хеширования k' на каждом каскаде является наименьшим $k' = k^{1/l}$. Подставим в выражения для ε_{PS} значения k' получим $\varepsilon = k^{1/l}/q$ и оценку для $0 < k \le q^l$.

4. Оценка сложности вычислений определяется тем, что на каждом каскаде число вычислений уменьшается в $k' = k^{1/l}$. Суммирование по всем каскадам дает результирующее выражение $k + k^{l-1/l} + k^{l-2/l} + \ldots + k^{1/l}$.

Утверждение 5.14 [139]. Пусть F_q, $q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \| M_2 \| \ldots \| M_t$, $l - Ch_t(M)$ – l-каскадное универсальное хеширование по кривой Эрмита.

Тогда $l - Ch_t(M)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^{l+l/2}, q^k, q\right)$, $\varepsilon = \sqrt{2k^{1/l}}/q$, $0, k \le q^l$, со сложностью вычислений $k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} + \ldots + k^{1/l} + k^{1/2l}$. Доказательство аналогично утверждению 5.14.

Утверждение 5.15 [139]. Пусть F_q, $q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \| M_2 \| \ldots \| M_t$, $l - Ch_t(M)$ – l-каскадное универсальное хеширование по кривой Ферма с большим числом точек.

Тогда $l - Ch_t(M)$ определяет универсальное семейство хеш-функций $\varepsilon - U\left(q^{2l}, q^k, q\right)$, $\varepsilon = 3\sqrt{k^{1/l}}/\left(\sqrt{2}q\right)$, $0 < k \le q^l$, со сложностью вычислений $k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} + \ldots + k^{1/l} + k^{1/2l}$.

Утверждение 5.16 [47]. Пусть F_q, $q = 2^{2s+1}$ – расширенное конечное поле, M – сообщение и $M = M_1 \| M_2 \| \ldots \| M_t$, $l - Ch_t(M)$ – l-каскадное универсальное хеширование по кривой Судзуки.

Тогда $l-Ch_t(M)$ определяет универсальное семейство хеш-функций $\varepsilon-U\left(q^{2l},q^k,q\right)$, $\varepsilon=\sqrt[2]{3}k^{1/3l}/q$, $0<k\le q^{l+l/2}$ со сложностью вычислений $2k+1{,}04k^{(3l-1)/3l}+2{,}88t^{(3l-2)/3l}+2k^{(l-1)/l}+1{,}04k^{(3l-4)/3l}+2{,}88k^{(3l-5)/3l}+\ldots$.

Доказательство. Хеширование на каждом каскаде является универсальным, каскадная хеш-функция также является универсальной. Пространство ключей определяется произведением числа ключей всех каскадов и равно q^{2l}. Наименьшая вероятность коллизии в силу утверждения 1 реализуется, если на каждом каскаде значение вероятности коллизии является наименьшим. Это достигается, если размер данных хеширования k' на каждом каскаде является наименьшим $k'=k^{1/l}$. Подставим в выражения для ε_S значения k', получим $\varepsilon_S=\sqrt[3]{3}k^{1/3l}/q$ и оценку для $0<k\le q^{l+l/2}$. Оценка сложности вычислений определяется тем, что на каждом каскаде число вычислений уменьшается в $k'=k^{1/l}$. Суммирование по всем каскадам дает результирующее выражение

$$2k+1{,}04k^{(3l-1)/3l}+2{,}88t^{(3l-2)/3l}+2k^{(l-1)/l}+1{,}04k^{(3l-4)/3l}+2{,}88k^{(3l-5)/3l}+\ldots.$$

Параметры многокаскадного универсального хеширования по алгебраическим кривым представлены в таблице 5.2.

Оценки вероятности коллизии и сложности вычислений для много-каскадного хеширования в конечном поле представлены в таблице 5.3.

Замечание 5.14.

1. Размеры ключей в схеме хеширования следуют из размеров ключей в каждом каскаде.

2. Размер хеш-кода определяется полем определения кривой в последнем каскаде.

3. Оценки сложности вычисления следуют из оценок сложности хеширования по алгебраической кривой каждого каскада по соотношениям таблицы 5.2.

4. Оценки вероятности коллизии вычислены с учетом оптимизации по соотношениям утверждений 5.10 – 5.16.

Таблица 5.2 – Параметры многокаскадного универсального хеширования по алгебраическим кривым

Схемы каскадного включения	Параметры универсального хеширования	Оценки сложности вычислений
$Ch_t(M)$, $PSh_q - PSh_q$	$\varepsilon - U\left(q^2, q^k, q\right)$, $\varepsilon = k^{1/2}/q$, $0 < k \le q^2$	$k + k^{1/2}$
$Ch_t(M)$, $PSh_q - Hh_q$	$\varepsilon - U\left(q^2\sqrt{q}, q^k, q\right)$, $\varepsilon = (2k)^{1/3}/q$, $0 < k \le q\sqrt{q}/2$	$k + k^{2/3}/2^{1/3} + k^{1/3}/2^{1/6}$
$Ch_t(M)$, $PSh_q - Fh_q$	$\varepsilon - U\left(q^3, q^k, q\right)$, $\varepsilon = (9k/2)^{1/3}/q$, $0 < k \le q\sqrt{q}$	$k + k^{2/3}/2^{1/3} + k^{1/3}/2^{1/6}$
$Ch_t(M)$, $PSh_q - Sh_q$	$\varepsilon - U\left(q^3, q^k, q\right)$, $\varepsilon = (3k)^{1/4}/q$, $0 < k \le q^2$	$k + 1{,}52k^{3/4} + 0{,}87k^{1/2} + 2{,}63k^{1/4}$
$Ch_t(M)$, $Hh_q - Sh_q$	$\varepsilon - U\left(q^3\sqrt{q}, q^k, q\right)$, $\varepsilon = 1{,}43k^{1/5}/q$, $0 < k \le q^2\sqrt{q}$	$k + k^{4/5} + 2k^{3/5} + k^{2/5} + 2{,}88k^{1/5}$
$l - Ch_t(M)$, $PSh_q - PSh_q - \ldots$	$\varepsilon - U\left(q^l, q^k, q\right)$, $\varepsilon = k^{1/l}/q$, $0 < k \le q^l$	$k + k^{l-1/l} + k^{l-2/l} + \ldots + k^{1/l}$
$l - Ch_t(M)$, $Hh_q - Hh_q - \ldots$	$\varepsilon - U\left(q^{l+l/2}, q^k, q\right)$, $\varepsilon = \sqrt{2k^{1/l}}/q$, $0 < k \le q^l$	$k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} + \ldots + k^{1/l} + k^{1/2l}$
$l - Ch_t(M)$, $Fh_q - Fh_q - \ldots$	$\varepsilon - U\left(q^{2l}, q^k, q\right)$, $\varepsilon = 3\sqrt{k^{1/l}}/\left(\sqrt{2}q\right)$, $0 < k \le q^l$	$k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} + \ldots + k^{1/l} + k^{1/2l}$
$l - Ch_t(M)$, $Sh_q - Sh_q - \ldots$	$\varepsilon - U\left(q^{2l}, q^k, q\right)$, $\varepsilon = \sqrt[3]{3}k^{1/3l}/q$, $0 < k \le q^{l+l/2}$	$2k + 1{,}04k^{(3l-1)/3l} + 2{,}88t^{(3l-2)/3l} + 2k^{(l-1)/l} + 1{,}04k^{(3l-4)/3l} + 2{,}88k^{(3l-5)/3l} + \ldots$

Таблица 5.3 – Оценки вероятности коллизии и сложности вычислений для многокаскадного хеширования по алгебраическим кривым над полем F_q

Схемы каскадов	F_q	Вероятность коллизии для данных размером L / сложность вычислений			Размер ключей (бит)	Размер хеш-кода (бит)
		1 кБ	1 МБ	1 ГБ		
$Ch_t(M)$, $PSh_q - PSh_q$	$q = 2^{32} - 99$	2^{-28} / 2^8+2^4	2^{-23} / $2^{18}+2^9$	2^{-18} / $2^{28}+2^{14}$	64	32
	$q = 2^{64} - 189$	$2^{-60,5}$ / $2^7+2^{3,5}$	$2^{-55,5}$ / $2^{17}+2^{8,5}$	$2^{-50,5}$ / $2^{27}+2^{13,5}$	128	64
$Ch_t(M)$, $PSh_q - Hh_q$	$\sqrt{q} = 2^{16} + 1$	2^{-29} / 2^8+2^5	2^{-26} / $2^{18}+2^{11,6}$	2^{-23} / $2^{28}+2^{18,3}$	80	32
	$\sqrt{q} = 2^{32} - 5$	$2^{-61,4}$ / $2^7+2^{4,6}$	$2^{-58,4}$ / $2^{17}+2^{11}$	$2^{-55,4}$ / $2^{27}+2^{17,6}$	160	64
$Ch_t(M)$, $PSh_q - Sh_q$	$q = 2^{31}$	$2^{-28,7}$ / 2^8+2^6	$2^{-26,2}$ / $2^{18}+2^{16}$	$2^{-23,7}$ / $2^{28}+2^{20}$	93	31
	$q = 2^{63}$	2^{-61} / 2^7+2^5	$2^{-58,5}$ / $2^{17}+2^{10}$	2^{-56} / $2^{27}+2^{20}$	189	63
$Ch_t(M)$, $Hh_q - Hh_q$	$\sqrt{q} = 2^{16} + 1$	$2^{-29,7}$ / 2^8+2^6	$2^{-27,2}$ / $2^{18}+2^{16}$	$2^{-24,8}$ / $2^{28}+2^{20}$	96	32
	$\sqrt{q} = 2^{32} - 5$	2^{-62} / 2^7+2^5	$2^{-59,5}$ / $2^{17}+2^{10}$	2^{-57} / $2^{27}+2^{20}$	192	64
$Ch_t(M)$, $Hh_q - Sh_q$	$q = 2^{31}$	2^{-29} / 2^8+2^7	2^{-27} / $2^{18}+2^{15}$	2^{-25} / $2^{28}+2^{23}$	109	31
	$q = 2^{63}$	2^{-61} / 2^7+2^6	2^{-59} / $2^{17}+2^{14}$	2^{-57} / $2^{27}+2^{22}$	221	63
$Ch_t(M)$ $Sh_q - Sh_q$	$q = 2^{31}$	2^{-29} / 2^9+2^7	$2^{-27,5}$ / $2^{19}+2^{14}$	2^{-26} / $2^{29}+2^{24}$	124	31
	$q = 2^{63}$	2^{-61} / 2^8+2^6	$2^{-59,5}$ / $2^{18}+2^{13}$	2^{-58} / $2^{28}+2^{23}$	252	63

5.3 Многократное универсальное хеширование по рациональным функциям алгебраических кривых

Эффективным механизмом уменьшения вероятности коллизии является хеширование по нескольким независимо выбранным хеш-функциям.

Определение 5.4 [137]. Пусть $H_1 = \left\{h : \{0,1\}^a \to \{0,1\}^b\right\}$ и $H_2 = \left\{h : \{0,1\}^a \to \{0,1\}^c\right\}$ – классы хеш-функций.

Класс хеш-функций по нескольким независимо выбранным хеш-функциям $H_1 \cap H_2 = \left\{ h : \{0,1\}^a \to \{0,1\}^{b+c} \right\}$ имеет вид

$$(h_1, h_2)(x) = h_1(x) \| h_2(x). \qquad (5.4)$$

Утверждение 5.17 [137]. Если H_1 есть $\varepsilon_1 - U$ универсальный класс и H_2 есть $\varepsilon_2 - U$, тогда $H_q \cap H_2$ есть $\varepsilon_1\varepsilon_2 - U$.

Замечание 5.15.

1. Распространение конструкции (5.4) на m кратное хеширование приводит к схеме с вероятностью коллизии, пропорциональной степени ε^m. Значения хеш-кода увеличиваются в m раз и сложность вычислений увеличивается в m раз.

2. Отличие в вычислении хеш-кода по выражению (5.4) заключается в использовании разных ключей для хеш-функций $h_1(x)$ и $h_2(x)$.

3. Многократное хеширование H_m распространяется на универсальное хеширование по рациональным функциям алгебраических кривых.

Рассмотрим универсальное хеширование по проективной прямой PSh_q.

Определение 5.5 [164]. Пусть F_q – конечное поле, M – сообщение. Алгоритм вычисления хеш-кода с t-кратным PSh_q определяется выражением

$$\left(PSh_{q1}, PSh_{q2}, \ldots, PSh_{qt}\right)(M) = PSh_{q1}(M) \left\| PSh_{q2}(M) \right\| \ldots \left\| PSh_{qt}(M) \right. . \qquad (5.5)$$

Оценки вероятности коллизии для многократного хеширования определяются свойствами универсального класса $\left(PSh_{q1}, PSh_{q2}, \ldots, PSh_{qt}\right)(M)$ конструкции. Справедливо следующее утверждение.

Утверждение 5.18 [164]. Класс хеш-функций $\left(PSh_{q1}, PSh_{q2}, \ldots, PSh_{qt}\right)(M)$ является t-связным $\varepsilon - U$ универсальным, где $\varepsilon = (k-1)/q$, k – число q-значных слов сообщения M.

Оценка вероятности коллизии при многократном хешировании PSh_q определяется следующим утверждением.

Утверждение 5.19 [164]. Для t-связанного $\varepsilon - U$ универсального класса по проективной прямой при равновероятном выборе хеш-функций вероятность коллизии $\Pr\left[h(M_1) = h(M_2)\right] \le \varepsilon^2$, где $\varepsilon = (k-1)/q$.

Доказательство. Хеш-код $PSh_{q1}(M) \| PSh_{q2}(M) \| \ldots \| PSh_{qt}(M)$ представляет конкатенацию хеш-результатов $PSh_{qi}(M)$, $i = 1, \ldots, t$. Для каждого из них существует самое большее εN функций $h_i \in PSh_q$ таких, что $PSh_{qi}(M) = PSh_{qi}(M')$ при $M \neq M'$. Так как h_i выбираются независимо и равновероятно из множества PSh_{qi}, тогда для полного хеш-кода $PSh_{q1}(M) \| PSh_{q2}(M) \| \ldots \| PSh_{qt}(M)$ существует самое большее $(\varepsilon N)^t$ хеш-функций таких, что $PSh_{q1}(M) \| PSh_{q2}(M) \| \ldots \| PSh_{qt}(M)$ и $PSh_{q1}(M') \| PSh_{q2}(M') \| \ldots \| PSh_{qt}(M')$.

Определения многократного хеширования, свойства универсальности для хеширования по максимальным кривым, кривым Ферма и Судзуки являются подобными. Оценки вероятности коллизии и сложности вычислений для многократного хеширования представлены в таблице 5.4.

Замечание 5.16. Кратность хеширования t определяется в двух случаях конечного поля 32 и 64 бит. В графах таблицы, где оценивается сложность вычислений, показаны добавки, которые определяют второй проход за схемой вычисления Горнера, в соответствии с ускоренным алгоритмом хеширования по максимальным кривым.

Таблица 5.4 – Оценки вероятности коллизии и сложности вычислений для многократного хеширования по алгебраическим кривым над полем F_q

Уравнение кривой над F_q	t	Вероятность коллизии для данных размером L/сложность вычислений			Размер ключей (бит)	Размер хеш-кода (бит)
		1 кБ	1 МБ	1 ГБ		
Проективная прямая $X+Y+Z=0$ $q=2^{32}-99$	1	2^{-24} / 2^{8}	2^{-14} / 2^{18}	2^{-4} / 2^{28}	32	32
	2	2^{-48} / 2^{9}	2^{-28} / 2^{19}	2^{-8} / 2^{29}	64	64
	3	2^{-72} / $2^{9,58}$	2^{-42} / $2^{19,58}$	2^{-12} / $2^{29,58}$	96	96
	4	2^{-96} / 2^{10}	2^{-56} / 2^{20}	2^{-16} / 2^{30}	128	128
$q=2^{64}-189$	1	2^{-57} / 2^{7}	2^{-47} / 2^{17}	2^{-37} / 2^{27}	64	64
	2	2^{-114} / 2^{8}	2^{-94} / 2^{18}	2^{-74} / 2^{28}	128	128
Кривая Эрмита $y^{\sqrt{q}}+y=x^{\sqrt{q}+1}$ $\sqrt{q}=2^{16}+1$	1	$2^{-27,5}$ / $2^{8}+2^{4,5}$	$2^{-22,5}$ / $2^{18}+2^{9,5}$	$2^{-17,5}$ / $2^{28}+2^{14,5}$	48	32
	2	2^{-55} / $2^{9}+2^{5,5}$	2^{-45} / $2^{19}+2^{10,5}$	2^{-35} / $2^{29}+2^{15,5}$	96	64
	3	$2^{-82,5}$ / $2^{9,6}+2^{6,1}$	$2^{-67,5}$ / $2^{19,6}+2^{11,1}$	$2^{-52,5}$ / $2^{29,6}+2^{16,1}$	144	96
	4	2^{-110} / $2^{10}+2^{6,5}$	2^{-90} / $2^{20}+2^{11,5}$	2^{-70} / $2^{30}+2^{16,5}$	192	128
$\sqrt{q}=2^{32}-5$	1	2^{-60} / $2^{7}+2^{4}$	2^{-55} / $2^{17}+2^{9}$	2^{-50} / $2^{27}+2^{14}$	96	64
	2	2^{-120} / $2^{8}+2^{5}$	2^{-110} / $2^{18}+2^{10}$	2^{-100} / $2^{28}+2^{15}$	192	128
Кривая Ферма $x^{(q-1)/3}+y^{(q-1)/3}$ $+1=0$ $q=2^{32}-99$	1	$2^{-26,89}$ / $2^{8}+2^{4,5}$	$2^{-21,91}$ / $2^{18}+2^{9,5}$	$2^{-16,9}$ / $2^{28}+2^{14,5}$	62	32
	2	$2^{-53,78}$ / $2^{9}+2^{5,5}$	$2^{-43,82}$ / $2^{19}+2^{10,5}$	$2^{-33,8}$ / $2^{29}+2^{15,5}$	124	64
	3	$2^{-80,67}$ / $2^{9,6}+2^{6,1}$	$2^{-65,73}$ / $2^{19,6}+2^{11,1}$	$2^{-50,7}$ / $2^{29,6}+2^{16,1}$	186	96
	4	$2^{-107,56}$ / $2^{10}+2^{6,5}$	$2^{-87,64}$ / $2^{20}+2^{11,5}$	$2^{-67,6}$ / $2^{30}+2^{16,5}$	248	128
$q=2^{64}-189$	1	$2^{-59,41}$ / $2^{7}+2^{4}$	$2^{-54,41}$ / $2^{17}+2^{9}$	$2^{-49,41}$ / $2^{27}+2^{14}$	126	64
	2	$2^{-118,82}$ / $2^{8}+2^{5}$	$2^{-108,82}$ / $2^{18}+2^{10}$	$2^{-98,82}$ / $2^{28}+2^{15}$	252	128
Кривая Судзуки $y^q-q=$ $=x^{q_0}\left(x^q-x\right)$ $q=2^{31}$	1	$2^{-27,79}$ / $2^{9}+2^{5,4}+2^{4,19}$	$2^{-24,46}$ / $2^{19}+2^{12,05}+2^{7,5}$	$2^{-21,13}$ / $2^{29}+2^{18,7}+2^{10,86}$	62	31
	2	$2^{-55,58}$ / $2^{10}+2^{6,4}+2^{5,19}$	$2^{-48,92}$ / $2^{20}+2^{13,05}+2^{8,5}$	$2^{-42,26}$ / $2^{30}+2^{19,7}+2^{11,86}$	124	62
	3	$2^{-83,37}$ / $2^{10,6}+2^{7}+2^{5,8}$	$2^{-73,38}$ / $2^{20,6}+2^{13,65}+2^{9,1}$	$2^{-63,39}$ / $2^{30,6}+2^{20,3}+2^{12,46}$	186	93
	4	$2^{-111,16}$ / $2^{11}+2^{7,4}+2^{6,19}$	$2^{-97,84}$ / $2^{21}+2^{14,05}+2^{9,5}$	$2^{-84,52}$ / $2^{31}+2^{20,7}+2^{12,86}$	248	124
$q=2^{63}$	1	$2^{-60,13}$ / $2^{8}+2^{4,72}+2^{3,86}$	$2^{-56,8}$ / $2^{18}+2^{11,39}+2^{7,19}$	$2^{-53,47}$ / $2^{28}+2^{18,05}+2^{10,53}$	126	63
	2	$2^{-120,26}$ / $2^{9}+2^{5,72}+2^{4,86}$	$2^{-113,6}$ / $2^{19}+2^{12,39}+2^{8,19}$	$2^{-106,94}$ / $2^{29}+2^{19,05}+2^{11,53}$	252	126

5.4 Композиционное универсальное хеширование по кривой Судзуки

Композиционное универсальное хеширование по алгебраическим кривым состоит из каскада универсального хеширования по кривой и строго универсального хеширования по ортогональным массивам или слабо смещенным массивам. Общая конструкция впервые предложена Стинсоном [74,75]. Общие свойства ортогональных массивов и слабо смещенных массивов рассмотрены в разделе 2.

Композиционное универсальное хеширование определяет безусловную аутентификацию. Коллизионные оценки хеширования связываются с распределениями хешей для пар сообщений по ключевому пространству и определяют значение условной вероятности угадывания MAC кода по результатам одного наблюдения. В более общем случае можно рассматривать распределение t хешей и соответственно вероятность предсказания по $t-1$ предыдущим наблюдениям.

Основной результат композиционной конструкции следует из теоремы 5.1 и определяет, что каскадирование универсального класса хеш-функций $\varepsilon_1 - U(N_1, n, u)$ и строго универсального класса хеш-функций $\varepsilon_2 - SU(N_2, u, m)$ приводит к строго универсальному классу $\varepsilon_1 - SU(N_1, N_2, n, m)$, где $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2$.

Теорема 5.1 [75]. Композиция из универсального класса хеш-функций $\varepsilon_1 - U(N_1, n, u)$ и строго универсального класса хеш-функций $\varepsilon_2 - SU(N_2, n, m)$ является строго универсальным классом с параметрами $\varepsilon - SU(N_1N_2, n, m)$, где $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2$.

Замечание 5.17.

1. Реализация безусловной аутентификации приводит к увеличению ключевого пространства пропорционально t связанности.

2. Нижняя граница для вероятности коллизии ε определяется значением $1/m$, где m – пространство хеш-кодов. Можно говорить об энтропийной избыточности или степени соответствия пространства хеш-кодов и оценки $-\log_2 \varepsilon$.

Для построения строго универсального хеширования применяется метод ортогональных массивов [141,142] и метод сумм экспонент Вейля – Карлитца – Ушиямы (ВКУ) [102,143].

Метод ортогональных массивов включает два шага:

– задание линейного отображения $f(x) = \sum_{j=1}^{t-1} \alpha_j x^j$, $f : F_q^n \to F_q^n$;

– проектирование координат $\varphi = \phi(f(x)) + z$, $\phi : F_q^n \to F_q^m$.

Рассмотрим случай безусловной аутентификации.

Утверждение 5.20. Пусть $t = 2$. Для построения массива аутентификаторов соотношения, по которым вычисляются хеш-значения, имеют вид

$$f(x) = ax,\ a, x \in F_{q^n};$$

$$\varphi = \phi(ax) + z,\ \phi(ax), z \in F_{q^m}.$$

Тогда массив аутентификаторов определяет строго универсальный класс хеш-функций $\frac{1}{q^m} - SU\left(q^{n+m}, q^n, q^m\right)$.

Фиксируем $a = a_1$ и $z = z_1$. Рассмотрим строку массива значений $\varphi = \phi(ax) + z_1$. Число элементов в строке равно q^n. Для прямой $f(x) = ax$, каждое значение $f(x_i)$ встретится только один раз. Проектирование $\phi : F_q^n \to F_q^m$ уменьшит число различных элементов до q^m, число повторений которых равно q^{n-m}. Вероятность коллизии будет $\varepsilon = q^{n-m}/q^n = 1/q^m$.

Рассмотрим столбец массива аутентификаторов $\varphi = \phi(ax_1) + z$, $a \in F_{q^n}$ и $z \in F_{q^m}$. Число элементов в столбце равно q^{n+m}. В выражении $f(x) = ax_1$ каждое значение $f(a_i x_1)$ встретится только один раз. Проектирование $\varphi : F_q^n \to F_q^m$ уменьшит число различных элементов до q^m, число повторений которых равно q^{n-m}. На ключевом пространстве z пробегает q^m значений и при любом фиксированном $x = x_1$, $\varphi = \phi(ax_1) + z$ будет принимать q^n число раз одно и то же значение из F_{q^m}. Имеем вероятность коллизии по ключу $\varepsilon = q^n / q^{n+m} = 1/q^m$.

Замечание 5.18.

1. Рассмотрим ключевое восстановление. Неопределенность по ключу для фиксированного значения $\varphi = \phi(ax) + z$ определяется числом ключей, для которых при фиксированном $x = x_1$ вычисляются одни и те же $\varphi = \phi(ax_1) + z$. Выше определено, что $\varphi = \phi(ax_1) + z$ будет принимать q^n число раз одно и то же значение из F_{q^m}. Вероятность поиска ключа будет $P_1 = 1/q^n$.

2. Рассмотрим случай, когда криптоанализ выполняется для двух текстов и *MAC*-кодов. Множество комбинаций из пар *MAC*-кодов в строке будет равно q^{2m}, число строк q^{n+m}. Вероятность поиска ключа по двум *MAC*-кодам будет $P_2 = 1/q^{n-m}$. Если рассматривать l *MAC*-кодов, вероятность ключевого восстановления будет $P_l = 1/q^{n-(l-1)m}$, $lm \le n$.

3. Рассмотрим линейное отображение $\phi : F_{q_1} \to F_{q_2}$ с функцией $f(x) = \phi(ax) + z$, где q_1 и q_2 – простые числа, $q_1 > q_2$, $a \in F_{q_1}$, $z \in F_{q_1}$. Ключевое пространство равно $q_1 q_2$. В столбце $f(x) = ax_1$ каждое значение $f(a_i x_1)$ встретится только один раз. Проектирование $\varphi : F_{q_1} \to F_{q_2}$ уменьшит число различных элементов до q_2, число повторений которых равно $\lceil q_1 / q_2 \rceil$,

где $\lceil \cdot \rceil$ – округление к большему числу. На ключевом пространстве z пробегает q_2 значений и при любом фиксированном $x = x_1, \varphi = \phi(ax_1) + z$ будет принимать q_1 число раз одно и то же значение из F_{q_2}. Имеем вероятность коллизии по ключу $\varepsilon = q_1 / (q_1 q_2) = 1/q_2$.

Рассмотрим строку массива значений $\varphi = \phi(ax_1) + z_1$. Число элементов в строке равно q_1. Для прямой $f(x) = ax$ каждое значение $f(x_i)$ встретится только один раз. Проектирование $\phi : F_{q_1} \to F_{q_2}$ уменьшит число различных элементов до q_2, число повторений которых равно $\lceil q_1 / q_2 \rceil$. Вероятность коллизии будет $\varepsilon = \lceil q_1 / q_2 \rceil / q_1 < 2/q_2$, что приводит к почти строго универсальному хешированию $\frac{2}{q_2} - ASU(q_1 q_2, q_1, q_2)$.

Утверждение 5.21. Для построения массива аутентификаторов соотношения, по которым вычисляются хеш-значения, имеют вид

$$f(x) = ax^2 + bx,\ a, b, x \in F_{q^n};\ \varphi = \phi(f(x)) + z,\ \phi(f(x)),\ z \in F_{q^m}.$$

Тогда массив аутентификаторов определяет строго универсальный класс хеш-функций $\frac{1}{q^m} - SU(q^{2n+m}, q^n, q^m)$ и является $t = 3$ сильным.

Фиксируем $a = a_1$ и $z = z_1$. Рассмотрим строку массива значений $\varphi = \phi(f(x)) + z$. Число элементов в строке равно q^n. Для $f(x) = ax^2 + bx$ каждое значение $f(x_i)$ встретится самое большее два раза. Проектирование $\varphi : F_q^n \to F_q^m$ уменьшит число различных элементов до q^m, число повторений которых равно q^{n-m}. Вероятность коллизии будет $\varepsilon = q^{n-m} / q^n = 1/q^m$.

Рассмотрим столбец массива аутентификаторов $\varphi = \phi(f(x_1)) + z$, $a, b \in F_{q^n}$ и $z \in F_{q^m}$. Число элементов в столбце равно q^{2n+m}. В выражении $f(x_1) = ax_1^2 + bx_1$ каждое значение встретится q^n раз в q^{2n} записях столбца.

Проектирование $\varphi: F_q^n \to F_q^m$ уменьшит число различных элементов до q^m, число повторений которых равно q^{2n-m}. На ключевом пространстве z пробегает q^m значений и при любом фиксированном $x = x_1$, $\varphi = \phi\left(f\left(x\right)\right) + z$ будет принимать q^{2n} число раз одно и то же значение из F_{q^m}. Имеем вероятность коллизии по ключу $\varepsilon = q^{2n} / q^{2n+m} = 1/q^m$.

Рассмотрим комбинацию из записей для двух столбцов. Число пар записей равно q^{2n+m}, число различных комбинаций q^{2m}. Вероятность появления любой из комбинаций $P = 1/q^{2n-m}$. Соответственно, для комбинаций из трех записей получим $P = 1/q^{2n-2m}$. Так как $n > m$ имеем гарантированно трехсильную аутентификацию.

Замечание 5.19.

1. t-сильная аутентификация определяет, что даже знание $t-1$ аутентификаторов на одном ключе гарантирует равновероятную неопределенность для t-го *MAC*-кода на этом же ключе.

2. Реализация t-сильной аутентификации требует не меньше q^{tm} ключевого пространства.

3. Рассмотрим случай, когда $n = m$ без проектирования $\varphi: F_q^n \to F_q^m$. Имеем наименьшие затраты по ключу. Для функции $f\left(x\right) = ax^2 + bx$ каждое значение $f\left(x_i\right)$ встретится самое большее два раза. Получим почти строгую аутентификацию с вероятностью коллизии $\varepsilon = 2/q^m$.

4. Применение проектирования $\varphi: F_q^n \to F_q^m$, $n > m$ желательно по следующим позициям. Для t-сильной аутентификации избыточность по ключам равняется $q^{(t-1)n-tm}$, что определяет вероятность восстановления ключа при наблюдении t *MAC*-кодов. Вероятность коллизии для t-сильной

аутентификации будет $\varepsilon = 1/q^m$. Длина *MAC*-кодов соответствует энтропийному значению и не является избыточной.

Результаты строго универсального хеширования, построенного на ортогональных массивах, представлены в таблице 5.5.

Таблица 5.5 – Свойства хеш-классов, построенных на ортогональных массивах

Входные параметры	Определение отображения	Свойства $OA_{\lambda}(t,k,\upsilon)$	Свойства хеш-класса
q – простое число, m, n, t – целые числа, $n > m$, $2 \le t \le q^n$	$f = f\left(z, a_1, a_2, \ldots, a_{t-1}\right)$; $\varphi: F_q^n \to F_q^m$ б $z \in F_{q^m}$, $a_j \in F_{q^n}$, $i = \overline{1, t-1}$, $f(x) = \phi\left(\sum_{j=1}^{t-1} a_j x^j\right) + z$	$OA_{q^{(t-1)(n-m)}}\left(t, q^n, q^m\right)$	$\frac{1}{q^m} - SU\left(q^{(t-1)n+m}, q^n, q^m\right)$
q простое число, m, n, t – целые числа, $n > m$, $t = 2$	$f(x) = ax$, $a, x \in F_{q^n}$; $\varphi = \phi(ax) + z$, $\phi(ax)$, $z \in F_{q^m}$, $\varphi: F_q^n \to F_q^m$	$OA_{q^{(n-m)}}\left(2, q^n, q^m\right)$	$\frac{1}{q^m} - SU\left(q^{n+m}, q^n, q^m\right)$
q – простое число, $m = n$, $t = 2$	$\phi: F_{q^m} \to F_{q^m}$, $a, z \in F_{q^m}$, $f(x) = \phi(ax) + z$	$OA_{\lambda-1}\left(2, q^n, q^m\right)$	$\frac{1}{q^m} - SU\left(q^{2m}, q^n, q^m\right)$
q_1, q_2 – простые числа, $q_1 > q_2$, $m = n = 1$, $t = 2$	$f(x) = \phi(ax) + z$, $a \in F_{q_1}$, $z \in F_{q_2}$, $\phi: F_{q_1} \to F_{q_2}$	$OA_{\lambda-q_1/q_2}\left(2, q_1, q_2\right)$	$\frac{2}{q_2} - ASU\left(q_1 q_2, q_1, q_2\right)$
q – простое число, m, n, t – целые числа, $n > m$, $t = 3$	$f(x) = ax^2 + bx$, $a, b, x \in F_{q^n}$ $\varphi = \phi\left(f(x)\right) + z \cdot \phi\left(f(x)\right)$, $z \in F_{q^m}$, $\varphi: F_q^n \to F_q^m$	$OA_{q^{2(n-m)}}\left(3, q^n, q^m\right)$	$\frac{1}{q^m} - SU\left(q^{2n+m}, q^n, q^m\right)$

Метод сумм экспонент Вейля – Карлитца – Ушиямы (ВКУ) рассмотрен в разделе 2. Записи массива аутентификаторов $(s,k)_q$ формируются на основе вычисления следов элементов поля F_q^n. Значение следа лежит в подполе

F_q^m основного поля и определяет отображение $\varphi: F_q^n \to F_q^m$. Основные результаты по массивам ВКУ взяты из [49] и представлены в таблице 5.6.

Таблица 5.6 – Свойства хеш-классов, построенных на ВКУ массивах

Входные параметры	Определение отображения	Свойства массива	Вычисление хеша	Свойства хеш-класса
$\left(p^2, 2\right)_p$, $f=2$, $n=1$	$Y=\sum_{j=1}^{2}\gamma^j Y_j$, $\gamma_j \in F_p$	$bias=0$	$Y+\eta$, строка индексируется α, η, $\alpha \in F_{p^2}$, $\eta \in F_p$.	$1/p-SU\left(p^3, p^2, p\right)$
$\left(p^2, 4\right)_p$, $f=2$, $n=2$	$Y=\sum_{j=1}^{4}\gamma^j Y_j$, $\gamma_j \in F_p$	$bias \le 1/p$	$Y+\eta$, строка индексируется α, η, $\alpha \in F_{p^2}$, $\eta \in F_p$.	$1/p-ASU\left(p^3, p^4, p\right)$

Замечание 5.20.

1. Здесь $p=q^m$. Результаты по первой строке с конструкцией массива $\left(p^2, 2\right)$ и вычислениями по формуле $Y=\sum_{j=1}^{2}\gamma^j Y_j$ приводят к строго универсальному классу $1/p-SU\left(p^3, p^2, p\right)$, что совпадает с конструкцией по ортогональному массиву силы $t=2$.

2. Слабосмещенные массивы определяются элементами частоты, появления которых в столбцах почти равновероятны. Отклонение от равновероятности определяет смещение. В общем случае, когда $p \neq 2$, прямого соответствия между смещением и вероятностью появления символов в столбцах массива нет.

Построение безусловной аутентификации в композиционной конструкции Стинсона определяется двумя каскадами. На первом используется универсальное хеширование по алгебраической кривой, на втором – строго универсальное по ортогональным массивам. Результатом будет строго универсальный класс хеш-функций с вероятностью коллизии

$\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2$, где ε_1 и ε_2 – вероятности коллизии первого и второго каскадов. Пространство ключей будет равно произведению ключевых пространств каскадов.

Пусть $\varepsilon_1 - U\left(N_1, N, q^n\right)$ – универсальное хеширование на первом каскаде. Объединение со вторым каскадом $\frac{1}{q^m} - SU\left(q^{n+m}, q^n, q^m\right)$ приводит к $\varepsilon - SU\left(N_1 q^{n+m}, N, q^n\right)$ строго универсальному хешированию с $\varepsilon < \varepsilon_1 + 1/q^m$.

Минимизируем затраты по ключу для универсального хеширования по кривой Судзуки. Универсальное хеширование имеет параметры $\varepsilon_1 - U\left(2^{2n}, 2^{kn}, 2^n\right)$, $\varepsilon_1 = (3k)^{1/3}/2^n$ – определяется из асимптотики вероятности коллизии для длин данных $k < (q-1)\sqrt{q/2}$, $q = 2^n$. Минимизация вероятности коллизии $\min\varepsilon$ следует из равенства $\varepsilon_1 = 1/q^m$. Так как кривые Судзуки определены над полем характеристики 2, получим

$$(3k)^{1/3}/2^n = 1/2^m;$$

$$m = n - \frac{1}{3}\log 3k.$$

Строго универсальное хеширование будет иметь параметры $2(3k)^{1/3}/2^n - SU\left(2^{4n-\frac{1}{3}\log 3k}, 2^{kn}, 2^{n-\frac{1}{3}\log 3k}\right)$.

Замечание 5.21 [49]. С увеличением числа хешируемых слов данных степень расширения должна уменьшаться $m = n - \frac{1}{3}\log 3k$, при этом будет расти вероятность коллизии $\varepsilon_1 = (3k)^{1/3}/2^n$.

Оценки параметров строго универсальной композиционной конструкции по кривой Судзуки и проективной прямой для хеширования в расширенном поле F_{2^m} показаны в таблице 5.7. Свойства хеш-класса взяты из таблицы 5.6.

Таблица 5.7 – Оценки параметров композиционной конструкции хеширования над полем F_{2^m}

Класс отображения	Универсальный класс $\varepsilon - U(N_1, N, q)$	Строго (почти строго) универсальный класс	Композиционная конструкция
Проективная прямая $X+Y+Z=0$			
$f(x)=ax$, $a, x \in F_{q^n}$; $\varphi = \phi(ax)+z$, $\phi(ax), z \in F_{q^m}$. $\varphi: F_q^n \to F_q^m$	$\frac{k}{q^n} - U\left(2^n, 2^n, 2^n\right)$	$\frac{1}{2^m} - SU\left(2^{n+m}, 2^n, 2^m\right)$	$\varepsilon - SU\left(2^{2n+m}, 2^{kn}, 2^m\right)$ $\varepsilon = k/2^n + 1/2^m$ Безусловная аутентификация силы $t=2$
$f(x)=ax^2+bx$, $a, b, x \in F_{q^n}$; $\varphi = \phi(f(x))+z$, $\phi(f(x)), z \in F_{q^m}$. $\varphi: F_q^n \to F_q^m$	$\frac{k}{q^n} - U\left(2^n, 2^n, 2^n\right)$	$\frac{1}{2^m} - SU\left(2^{n+m}, 2^n, 2^m\right)$	$\varepsilon - SU\left(2^{3n+m}, 2^{kn}, 2^m\right)$ $\varepsilon = k/2^n + 1/2^m$ Безусловная аутентификация силы $t=3$
Кривая Судзуки			
$f(x)=ax$, $a, x \in F_{q^n}$; $\varphi = \phi(ax)+z$, $\phi(ax), z \in F_{q^m}$. $\varphi: F_q^n \to F_q^m$	$\varepsilon_1 - U\left(2^{2n}, 2^{kn}, 2^n\right)$, $\varepsilon_1 = (3k)^{1/3}/2^n$	$\frac{1}{2^m} - SU\left(2^{n+m}, 2^n, 2^m\right)$	$\varepsilon - SU\left(2^{3n+m}, 2^{kn}, 2^m\right)$ $\varepsilon = (3k)^{1/3}/2^n + 1/2^m$ Безусловная аутентификация силы $t=2$
$f(x)=ax^2+bx$, $a, b, x \in F_{q^n}$; $\varphi = \phi(f(x))+z$, $\phi(f(x)), z \in F_{q^m}$. $\varphi: F_q^n \to F_q^m$	$\varepsilon_1 - U\left(2^{2n}, 2^{kn}, 2^n\right)$, $\varepsilon_1 = (3k)^{1/3}/2^n$	$\frac{2}{q^m} - SU\left(q^{2n+m}, q^n, q^m\right)$	$\varepsilon - SU\left(2^{4n+m}, 2^{kn}, 2^m\right)$ $\varepsilon = (3k)^{1/3}/2^n + 1/2^m$ Безусловная аутентификация силы $t=3$

Замечание 5.22.

1. Для фиксированной вероятности коллизии и числа хешируемых слов данных композиционная конструкция с кривыми Судзуки является более эффективной по ключевым затратам по сравнению с хешированием по проективной прямой.

Рассмотрим наименее затратный по длине ключей и сложности вычислений случай, когда $n = m$ – без проектирования $\varphi: F_q^n \to F_q^m$.

Пусть F_{2^m} определяет хеширование по кривой Судзуки и F_{2^ℓ} – хеширование по проективной кривой. Фиксируем вероятность коллизии:

$$\varepsilon = k/2^\ell = (3k)^{1/3}/2_m .$$

Получим

$$2^\ell = 2^m k^{2/3}/3^{1/3} \approx 2^m k^{2/3}.$$

Пусть $k = 2^{m/2}$ и $2^\ell = 2^{m+m/3}$. Рассмотрим строго универсальное хеширование по кривой Судзуки $\varepsilon_1 - SU\left(2^{4m}, 2^{km}, 2^m\right)$, $\varepsilon_1 = (3k)^{1/3}/2^m{}_m$ с отображением $f(x) = ax$, $a, x \in F_{q^m}$; $\varphi = \phi(ax) + z$, $\phi(ax), z \in F_{q^m}$, $\phi: F_{2^m} \to F_{2^m}$. Эквивалентное по вероятности коллизии строго универсальное хеширование по проективной прямой $k/2^\ell - SU\left(2^{3\ell}, 2^{k\ell}, 2^\ell\right)$ имеет параметры $k/2^{m+m/3} - SU\left(2^{4m}, 2^{k(m+m/3)}, 2^{m+m/3}\right)$. Если $k = 2^m$ и $2^\ell = 2^{m+2m/3}$, тогда $k/2^{m+2m/3} - SU\left(2^{5m}, 2^{k(m+2m/3)}, 2^{m+2m/3}\right)$. Чем больше размер хешируемых данных, тем больше выигрыш по ключевому пространству.

2. Для фиксированного поля вычислений и числа хешируемых слов данных композиционная конструкция с кривыми Судзуки имеет меньшую вероятность коллизии по сравнению с хешированием по проективной прямой, за счет универсального хеширования первого каскада.

3. Строгое (почти строгое) универсальное хеширование в расширенном поле F_q^n допускает отображение $\varphi: F_q^n \to F_q^m$. Имеем оптимизацию затрат на размер ключей $3n + m$; значение 2^{-m} определяет нижнюю границу значения вероятности коллизии. Хеширование по разным модулям снимает избыточность размера хеша по коллизионной оценке. С помощью отображения $\varphi: F_q^n \to F_q^m$ размер хеш-кода приводится к энтропийному

значению. Практические оценки по вероятности коллизии для значений модулей 32, 64, 128 бит определяются оценками первого каскада (см. таблицу 5.3).

5.5 Выводы

Основной научный результат раздела состоит в том, что получил дальнейшее развитие метод каскадного универсального хеширования по кривой Судзуки на основе произведения функциональных полей, который, в отличие от известных, предусматривает применение хеширования по кривой Судзуки. Это позволило уменьшить вероятность коллизии в корень степени числа, что определяется количеством каскадов от корня кубического числа слов данных, и увеличить размер хешируемых данных. Данные результаты впервые представлены в работах [46,47].

Основные практические результаты являются следующими.

1. Универсальное хеширование по алгебраическим кривым разрешает основное противоречие доказуемо стойкой аутентификации между вероятностью коллизии, размером хешируемых данных и ключевыми затратами на аутентификацию. Наилучшие результаты универсального хеширования по вероятности коллизии достигаются на максимальных кривых. Оценки для вероятности коллизии в квадратичном поле размерности 64 бит имеют значения $\varepsilon \approx 2^{-60} \div 2^{-50}$ при изменении длины данных от 1 кБ до нескольких ГБ. Оценки для вероятности коллизии хеширования по кривой Судзуки в двоичном расширенном поле размерности 63 бит лежат в диапазоне $\varepsilon \approx 2^{-60} \div 2^{-53}$.

2. Практический аспект реализации универсального хеширования определяется вычислением точек кривой по ключевым данным. Отождествление значение ключа с точкой кривой просто реализуется на проективной прямой и кривой Судзуки. Битовый размер ключевого пространства в полтора раза превышает размер конечного поля для

максимальных плоских кривых и в два раза – для кривой Судзуки. При вычислении в 64-битовом конечном поле соответственно имеем 96 и 126 бит ключи. Наименьшие затраты на размер поля вычислений для фиксированной вероятности коллизии и длины данных реализует универсальное хеширование по кривой Судзуки. Размер конечного поля вычислений, соответственно битовый размер ключа, для универсального хеширования по кривой Судзуки в $k^{2/3}$ раз меньше по сравнению с универсальным хешированием по проективной прямой (k – длина данных).

3. Сложность хеш-вычислений для универсального хеширования по рациональным функциям алгебраических кривых определяется числом вычислений для схемы Горнера по четырем переменным для кривой Судзуки. Относительное увеличение числа вычислений для универсального хеширования по максимальным плоским кривым по сравнению с проективной прямой составляет ~ 5 – 17% на блоках данных малой длины ~1 кБ и ~1 % для данных ≥ 1 МБ. Хеш-вычисления по кривой Судзуки сложнее приблизительно в два раза по сравнению с хешированием по плоским кривым и проективной прямой.

4. Каскадное хеширование эффективно увеличивает размер хешируемых данных и выравнивает вероятность коллизии с изменением длины данных.

5. Многократное хеширование эффективно уменьшает вероятность коллизии. Двукратное универсальное хеширование по проективной прямой над 64 бит конечным полем обеспечивает вероятность коллизии $P_{\text{col}} < 2^{-64}$ для практически всех длин данных и трехкратное хеширование обеспечивает $P_{\text{col}} < 2^{-128}$. Для этом случая двукратное универсальное хеширование по максимальным плоским кривым обеспечивает вероятность коллизии $P_{\text{col}} < 2^{-100}$ и по кривой Судзуки – $P_{\text{êîë}} < 2^{-107}$. По числу вычислений двукратное универсальное хеширование по максимальным плоским кривым имеет в полтора раза меньшую сложность по сравнению с двукратным универсальным хешированием по проективной прямой.

6. Применение многокаскадного универсального хеширования $l - Ch_t(M)$ с одной и той же функцией хеширования на всех каскадах в корень l степени уменьшает вероятность коллизии по сравнению с однокаскадным хешированием. Наименьшая вероятность коллизии реализуется в схеме $Sh_q - Sh_q$. Вычисление в поле ~64 бит обеспечивает доказуемую стойкость $P_{\text{êîë}} < 2^{-57}$ для данных длиной до нескольких Гбт.

7. Двухкаскадные схемы хеширования $PLh_q - Sh_q$ и $Hh_q - Sh_q$ по вероятности коллизии являются эквивалентными. С увеличением размерности поля отличие между схемой хеширования $PLh_q - Sh_q$ и $Hh_q - Sh_q$ становится меньше.

8. Безусловная аутентификация реализуется на основе строго (почти строго) универсального хеширования в композиционной конструкции Стинсона. Хеширование по рациональным функциям алгебраических кривых в первом каскаде является определяющим для оценки вероятности коллизии. Наилучшие результаты достигаются на кривых Судзуки. Строго универсальное хеширование реализуется на основе вычислений по ортогональным массивам и слабо смещенным массивам на втором каскаде. Практические вычисления по ортогональным массивам требуют одно вычисление в каскаде строгого универсального хеширования. Применение строго универсального хеширования по кривой Судзуки позволяет уменьшить размер результирующего хеш-кода до энтропийного значения. Реализация строго (почти строго) универсального хеширования приводит к четырех- и пятикратному увеличению размера ключевого пространства**.**

ЗАКЛЮЧЕНИЕ

Обеспечение информационной безопасности в телекоммуникационных системах и сетях реализуется за счет решения задач защиты информации. В диссертационной работе решена научная задача, которая состоит в разработке метода универсального хеширования по алгебраической кривой Судзуки для построения доказуемо стойкой аутентификации сообщений.

Преимуществом универсальных хэш-функций является то, что они имеют обоснованные комбинаторные свойства и обеспечивают доказуемую вероятность коллизии, которая прямо пропорциональна вероятности навязывания ложной информации. Практические алгоритмы формирования кодов аутентификации сообщений должны включать классы хеш-функций с большим коэффициентом сжатия для данных большого объема, при этом сохраняя свои коллизионные свойства. Проведенный анализ доказуемо стойкой и безусловной аутентификации в теории универсального и строго универсального хеширования, методов универсального и строго универсального хеширования на основе ортогональных массивов, слабо смещённых массивов, линейного алгебраического кодирования позволил определить основное противоречие доказуемо стойкой аутентификации между затратами ключевого пространства и длиной хешируемого сообщения. Данное противоречие имеет разрешение при использовании схем универсального хеширования по рациональным функциям алгебраических кривых, с минимизацией затрат на ключевое пространство, сложности вычислений и обеспечением гарантированной вероятности коллизии, что решает задачу обеспечения безопасности и достоверности данных. Задача построения универсального хеширования по рациональным функциям алгебраических кривых заключается в выборе алгебраических кривых, вычислении их алгеброгеометрических параметров, разработки методов, алгоритмов и оценок универсального хеширования. Верхние оценки

вероятности коллизии универсального хеширования по рациональным функциям алгебраических кривых показывают, что наилучшие результаты достигаются по кривым с большим числом точек.

Основные научные и практические результаты работы:

1. Универсальное хеширование по кривой Судзуки строится на основе отображение $\pi := (1 : x : y : v : w)$ в проективном пространстве P^4. Хеширование по рациональным функциям кривой над полем F_q, определяет универсальный хеш-класс $\varepsilon - U(q^2, q^k, q)$, где q^2 – число хеш-функций (объем ключевого пространства), ε – верхняя оценка вероятности коллизии, k – число q-х слов данных.

2. Хеширование по кривой Судзуки имеет выигрыш в $q^{1/6}$ раз по вероятности коллизии и в $q^{1/2}$ раз – по числу слов данных в сравнении с универсальным хешированием по кривой Эрмита. Хеширование по кривой с параметрами $q = 2q_0^{\,2}$ и $q_0 = 2^s$ имеет преимущество по вероятности коллизии, длине данных, сложности вычислений в сравнении с хешированием по производным кривым Судзуки и кривой над полем четвертой степени расширения.

3. Практический аспект реализации универсального хеширования определяется вычислением точек кривой по ключевым данным. Отождествление значение ключа с точкой кривой просто реализуется на проективной прямой и кривой Судзуки. Битовый размер ключевого пространства в полтора раза превышает размер конечного поля для максимальных плоских кривых и в два раза для кривой Судзуки. При вычислении в 64-битовом конечном поле соответственно имеем 96 и 126 бит ключи. Наименьшие затраты на размер поля вычислений для фиксированной вероятности коллизии и длины данных реализует универсальное хеширование по кривой Судзуки. Размер конечного поля вычислений, соответственно битовый размер ключа, для универсального хеширования по кривой Судзуки

в $k^{2/3}$ раз меньше по сравнению с универсальным хешированием по проективной прямой (k – длина данных). Оценки для вероятности коллизии в квадратичном поле размерности 64 бит имеют значения $\varepsilon \sim 2^{-60} \div 2^{-50}$ при изменении длины данных от 1 Кбт до нескольких Гбт. Оценки для вероятности коллизии хеширования по кривой Судзуки в двоичном расширенном поле размерности 63 бит лежат в диапазоне $\varepsilon \sim 2^{-60} \div 2^{-53}$.

4. В схемах с алгебраическими кодами (n,k,d) вероятность коллизии определяется значением 1-d/n. Для известных к настоящему времени кодов вероятность коллизии ограничивается в лучшем случае значением обратно пропорциональным квадрату размерности поля Z_q. Применение скалярного произведения по рациональным функциям алгебраических кривых определяет метод универсального хеширования. Алгебраические кривые с большим числом точек и плотно упакованным по полюсам функциональным полем рациональных функций реализуют наилучшие результаты универсального хеширования. Универсальное хеширование по кодам Рида Соломона в алгеброгеометрической интерпретации определяется как хеширование по проективной прямой. В параметрической интерпретации является полиномиальным хешированием. Параметрически более сложными кривыми являются максимальные кривые, кривые Судзуки и кривые Ри. Кривые имеют наименьшие отношения значения полюса рациональных функций к числу точек, что определяет наименьшее значение вероятности коллизии в схеме универсального хеширования и являются наилучшими для применения. Практические вычисления показывают, что лучшие результаты для строгой аутентификации достигаются на длинных алгебраических кодах Судзуки, которые относятся к классу алгеброгеометрических кодов определенных над полем рациональных функций, ассоциированным с алгебраической кривой Судзуки, что определяет актуальность построения теории универсального хеширования над функциональным полем алгебраических кривых.

5. Применение метода построения алгоритмов на основе схемы Горнера приводит к эффективной структуризации хеш-вычислений. Разработан метод вычисления хеш-функций на основе многопараметрической схемы Горнера. Метод вычисления хеш-функций по алгебраической кривой Судзуки на основе четырех параметрической схемы Горнера позволяет повысить в два раза скорость хеширования по сравнению с общим алгоритмом. Построены алгоритмы универсального хеширования по рациональным функциям максимальных кривых. Получены оценки параметров универсальных хеш-функций по алгебраическим кривым и оценки сложности универсального хеширования.

6. Универсальное хеширование по алгебраическим кривым допускает эффективное многопотоковое вычисление. Для реализации потокового вычисления следует структурировать алгоритм так, чтобы появился последовательный участок, допускающий распараллеливание. Применение метода универсального хеширования по кривой Судзуки на основе схемы Горнера позволяет выполнить структурирование алгоритма в виде полиномиального каскадного хеширования, что допускает распараллеливание процесса вычислений. Скорость вычислений прямо пропорциональна числу потоковых вычислений.

7. Метод универсального хеширования с ограничением функционального поля алгебраических кривых позволяет уменьшить структурную сложность алгоритмов хеширования по алгебраическим кривым. Универсальное хеширование по базису двух рациональных функций по кривой Судзуки в два раза выигрывает по сложности вычислений. Универсальное хеширование с ограничением функционального поля алгебраических кривых позволяет обойти ограничения для вычислений над конечным полем фиксированной характеристики и расширения, условия оптимизации по вероятности коллизии. Недостатком применения данного метода является уменьшение числа хешируемых данных по сравнению с

полным функциональным полем. Требуется оптимизация базиса функционального поля. Наибольший результат достигается на сложных многопараметрических кривых.

8. Каскадное хеширование эффективно увеличивает размер хешируемых данных и выравнивает вероятность коллизии с изменением длины данных. Многократное хеширование эффективно уменьшает вероятность коллизии. Двукратное универсальное хеширование по проективной прямой над 64 бит конечным полем обеспечивает вероятность коллизии $P_{кол} < 2^{-64}$ для практически всех длин данных и трехкратное хеширование – обеспечивает $P_{кол} < 2^{-128}$. Для этого случая двукратное универсальное хеширование по максимальным плоским кривым обеспечивает вероятность коллизии $P_{кол} < 2^{-100}$ и по кривой Судзуки – $P_{кол} < 2^{-107}$. По числу вычислений двукратное универсальное хеширование по максимальным плоским кривым имеет в полтора раза меньшую сложность по сравнению с двукратным универсальным хешированием по проективной прямой.

9. Применение многокаскадного универсального хеширование $l - Ch_t(M)$ с одной и той же функцией хеширования на всех каскадах в корень l степени уменьшает вероятность коллизии по сравнению с однокаскадным хешированием. Наименьшая вероятность коллизии реализуется в схеме $Sh_q - Sh_q$. Вычисление в поле ~64 бит обеспечивает доказуемую стойкость $P_{кол} < 2^{-57}$ для данных длиной до нескольких Гбт. Двухкаскадные схемы хеширования $PLh_q - Sh_q$ и $Hh_q - Sh_q$ по вероятности коллизии являются эквивалентными. С увеличением размерности поля отличие от $PLh_q - Sh_q$ и $Hh_q - Sh_q$ хеширования становится меньше.

10. Безусловная аутентификация реализуется на основе строго (почти строго) универсального хеширования в композиционной конструкции Стинсона. Хеширование по рациональным функциям алгебраических кривых в первом каскаде является определяющим для оценки вероятности коллизии.

Наилучшие результаты достигаются на кривых Судзуки. $Sh_q(PSh_q(M_1) \| M_2)$ показывает, каскадное универсальное хеширование по кривым Судзуки со связкой хеша с текстом позволяет в куб раз увеличить длину хешируемых данных по сравнению с хешированием по проективной прямой (полиномиальное хеширование) без увеличения вероятности коллизии. Затраты по ключу увеличиваются в q раз. Это абсолютно наилучший результат хеширования по алгебраическим кривым. Недостатком каскадного хеширования $PSh_q - Sh_q$ является повышенная сложность. Вычисления по PSh_q каскаду выполняются на одной рациональной функции со сложностью $\sim k'$ и по Sh_q каскаду на четырех рациональных функциях – со сложностью $\sim 2t + 1.04t^{2/3} + 2\sqrt[3]{3}t^{1/3}$. Результаты каскадного хеширования $Hh_q - Sh_q$ являются абсолютно лучшими среди двухкаскадных схем универсального хеширования по алгебраическим кривым и обеспечивают хеширование наибольшей длины данных. Наименьшая вероятность коллизии реализуется в случае $\varepsilon_S = \varepsilon_H$. Подставим в выражения для ε_S и ε_H значения k' и $t = k / k'$, получим $\varepsilon_S = (3k/k')^{1/3}/q$, $\varepsilon_H = \sqrt{2k'}/q$, $k' = (3k)^{2/5}/2^{3/2}$ и оценку для вероятности $\varepsilon = 1.43k^{1/5}/q$. Недостатком каскадного хеширования $Hh_q - Sh_q$ является увеличенная сложность хеширования. Вычисления по Hh_q каскаду выполняются на двух рациональных функциях со сложностью $\sim t(k' + \sqrt{k'})$ и по Sh_q каскаду на четырех рациональных функциях – со сложностью $\sim 2t + 1.04t^{2/3} + 2\sqrt[3]{3}t^{1/3}$

Научная новизна полученных результатов обусловлена достижением цели исследования, которая состоит в разработке метода универсального хеширования за рациональным функциями кривых Судзуки для построения доказуемо стойкой аутентификации с обеспечением гарантированной

вероятности коллизии с уменьшенной сложностью вычисления. Научная новизна состоит в следующем:

1. Впервые предложен метод универсального хеширования на основе упорядочивания полюсов рациональных функций по кривой Судзуки, что приводит к существенному снижению сложности вычислений и уменьшению числа хешируемых данных; получены коллизионные оценки и оценки сложности хеширования;

2. Впервые предложен метод вычисления хеш-функций на основе четырех параметрической схемы Горнера, в которой учитывается размерность рациональных функций кривых, позволило обеспечить наименьшую сложность вычисления на уровне пропорциональном размеру конечного поля;

3. Получил дальнейшее развитие метод универсального хеширования на основе скалярного произведения по рациональным функциям линейного базисного пространства, с использованием вычисления хеш-функций по подмножеству рациональных функций функционального поля с упорядоченными порядками полюсов.

Практическая значимость полученных результатов состоит в следующем:

1. Построены линейные векторные пространства максимальных кривых на основе вычисления функциональных полей.

2. Построен алгоритм хеширования по кривой Судзуки по методу вычисления хеш-кода на основе четырехпараметрической схемы Горнера, что позволило получить наименьшую сложность вычислений (акт внедрения НТК ГП «Импульс», 17.10.2015).

3. Разработан алгоритм универсального хеширования на основе композиционной схемы.

4. Разработаны практические рекомендации по использованию универсального хеширования по алгебраическими кривыми в схемах многократного, многокаскадного, композиционного хеширования

доказательно-стойкой и безусловной аутентификации сообщений, что позволило минимизировать вероятность коллизии, расходы на ключевой пространство и сложность вычислений (акт внедрения НТК ГП «Импульс», 17.10.2015).

5. Получены оценки универсального хеширования, сложности вычисления хеш-кода для двухкаскадного хеширования и многокаскадного хеширования в схеме, когда во внутреннем каскаде используется хеширование по проективной прямой.

6. Разработаны программные средства для построения кривых, вычислений их точек и свойств (кратности), моделирования линейного базисного пространства с рациональными функциями кривых и статистического оценивания вероятности коллизии хеширования путем вычисления кратности пересечения гиперповерхностей линейного пространства с точками кривой (акт внедрения НТК ГП «Импульс», 17.10.2015).

Результаты диссертационной работы использованы в исследовательских и конструкторских работах в НТК ГП «Импульс» (акт внедрения от 17.10.2015), в учебном процессе кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники при изучении дисциплины «Системы и средства аутентификации», в курсовом и дипломном проектировании (акт внедрения ХНУРЭ). Разработанные программные средства рекомендуется использовать в информационно-телекоммуникационных системах поддержки бизнеса (BSS) для построения схем доказуемо стойкой аутентификации сообщений.

Достоверность полученных результатов подтверждается адекватностью расчетных значений по выведенным аналитическим выражениям, результатам эксперимента, а также совпадением, в некоторых случаях, с известными общетеоретическими положениями.

Достоверность результатов, полученных при разработке метода формирования хэш-кодов, подтверждается сходимостью расчетных значений вероятности коллизий результатам эксперимента по исследованию распределений хэш-кодов.

Достоверность результатов, полученных при разработке алгоритма вычисления хэш-кодов в каскадной конструкции, подтверждается совпадением результатов эксперимента с оценкой временных затрат на формирование хэш-кода с расчетными значениями.

Результаты работы целесообразно использовать:

1. Для построения методов доказуемо стойкой аутентификации на основе применения универсального хеширования с целью обеспечения гарантированной вероятности коллизии и разрешения противоречия между затратами ключевого пространства пропорциональными длине хешируемого сообщения;

2. При проведении конструкторских и научно исследовательских работ построения новых технических и программных средств создания систем защиты информации в компьютерных системах и сетях, автоматизированных системах управления, различных информационных и телекоммуникационных системах, информационно-телекоммуникационных системах, в системах электронного документооборота;

3. В учебном процессе при изучении дисциплин по защите информации при подготовке специалистов по безопасности компьютерных систем и сетей в высших учебных заведениях МОН Украины.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Закон України № 2297-VI «Про захист персональних даних» від 01.06.2010 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17

2. Закон України № 851-IV «Про електронні документи та електронний документообіг» від 22.05.03 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/851-15

3. Закон України № 852-IV «Про електронний цифровий підпис» від 22.05.03 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/852-15

4. Закон України N 2594-IV «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

5. Постанова Кабінету міністрів України № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” від 29.03.2006 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/373-2006-%D0%BF

6. ДСТУ ISO/IEC 9798-1 Методи захисту. Автентифікація об’єктів. Ч. 1: загальні положення (ISO/IEC 9798-1) [Электронный ресурс]. – Режим доступа: www.csm.kiev.ua.

7. ДСТУ ISO/IEC 9798-2 Методи захисту. Автентифікація об’єктів. Ч. 2: механізми, що ґрунтуються на використанні алгоритмів симетричного шифрування. (ISO/IEC 9798-2) [Электронный ресурс]. – Режим доступа: www.csm.kiev.ua.

8. ДСТУ ISO/IEC 9798-3 Інформаційні технології. Методи захисту. Автентифікація об’єктів. Ч. 3: механізми, що ґрунтуються на використанні

алгоритмів цифрового підпису. [Электронный ресурс]. – Режим доступа: www.csm.kiev.ua.

9. ДСТУ ISO/IEC 9798-4 Інформаційні технології. Методи захисту. Автентифікація об’єктів. Ч. 4: протоколи, що ґрунтуються на використанні функцій обчислення криптографічного контрольного значення. (ISO/IEC 9798-4) [Электронний ресурс]. – Режим доступу: www.csm.kiev.ua.

10. ДСТУ ISO/IEC 9798-5 Інформаційні технології. Методи захисту. Автентифікація об’єктів. Ч. 5: протоколи, що використовують методи, які грунтуються на нульових знаннях. (ISO/IEC 9798-5) [Электронный ресурс]. – Режим доступа: www.csm.kiev.ua.

11. ISO/IEC 10118-1. Information technology – Security techniques – Hash-functions – Part 1: General. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber.

12. ISO/IEC 10118-2. Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_ detail.htm.

13. ISO/IEC 10118-3 Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm.

14. ISO/IEC 10118-4 Information technology – Security techniques – Hash-functions. – Part 4: Hash-functions using modular arithmetic [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm.

15. International Organization for Standardization, “ISO/IEC 9797-1: Information Technology – Security Techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher", 1999. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/catalogue_detail.htm? csnumber

16. International Organization for Standardization, \ISO/IEC 9797-2: Information Technology – Security Techniques – Message Authentication Codes (MACs) – Part 2: “Mechanisms using a dedicated hash-function", 2002. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/catalogue.

17. ДСТУ ГОСТ 28147:2009 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». [Электронный ресурс]. – Режим доступа: www.csm.kiev.ua.

18. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» [Электронный ресурс]. – Режим доступа: www.csm.kiev.ua

19. ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» [Электронный ресурс]. – Режим доступа: www.csm.kiev.ua

20. Задірака В. Комп’ютерна криптологія / В.Задірака, О.Олексик. – К., 2002. – 502с.

21. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах. Ч. 1. Криптографічний захист інформації / І.Д. Горбенко, Т.О. Гриненко. – Харків : ХНУРЕ, 2004. – 367с.

22. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія / Ю.І. Горбенко, І.Д. Горбенко. – Харків : Форт, 2010. – 608 с.

23. Горбенко Ю.І. Мета, стан та попередні підсумки проекту SHA-3 / Ю.І. Горбенко, А.В. Бойко, А.М. Герцог // Прикладная радиоэлектроника. – 2009. – Т. 8, № 3. – С. 315-321.

24. Корченко А.Г. Построение систем защиты информации на нечетких множествах / А.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.

25. Simmons G.J. Authentication theory/coding theory, in Advances in Cryptology / G.J. Simmons // Proceedings of Crypto 84, Lecture Notes in Computer Science. – 1985. – V.196. – P.411-431.

26. Симмонс Г.Д. Обзор методов аутентификации информации / Г.Д. Симмонс // ТИИЭР. – 1988. – Т.76, № 5. – С. 105-125.

27. Столингс В. Криптография и защита сетей. Принципы и практика ; 2-е изд. / В.Столингс. – К. : Изд. дом “Вильямс”, 2001. – 669с.

28. Carter J. L. Universal classes of hash functions / J.L. Carter, M.N. Wegman // Journal of Computer and Systems Science. – 1979. – V.18. – P.143-154.

29. Wegman. M. N. New hash functions and their use in authentication and set equality / M.N. Wegman, J.L. Carter // Journal of Computer and Systems Science. – 1981. – V. 22. – P. 265-279.

30. Kabatianskii G. On the Cardinality of Systematic Authentication Codes Via Error-Correcting Codes / G. Kabatianskii, B. Smeets, T. Johansson // IEEE Transactions on Information Theory. – 1991. – Vol. IT-42. – P.583-602.

31. Bierbrauer J. On families of hash functions via geometric codes and concatenation. / J. Bierbrauer, T. Johansson, G. Kabatianskii, B. Smeets // Advances in Cryptology-CRYPTO ’93 Proceedings, Springer-Verlag. – 1994. – P. 331-342.

32. Bierbrauer J. Universal hashing and geometric codes, to appear in Designs / J. Bierbrauer // Designs, Codes and Cryptography. – 1997. – N.11. – P.207-221.

33. Bierbrauer J. Authentication via algebraic-geometric codes / J. Bierbrauer // Recent Progressin Geometry, Supplemento ai Rendicontidel Circolo Matematico di Palermo. – 1998. – N.51. – P.139-152.

34. Milne J.S. Algebraic Geometry / J.S. Milne. – Springer, 2003. – 206 p.

35. Халимов Г. Стойкий к коллизиям алгоритм Whirpool / Г. Халимов, Е. Котух // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – Київ, 2005. – № 10. – С.159-165.

36. Халімов Г.З. Аналіз безпеки MAC алгоритмів стандарту ISO/IEC 9797-2 / Г.З. Халімов, О.В. Потій, О.В. Дунь, Е.В. Котух // Правове,

нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2007. – Вип.1(14). – С. 99-105.

37. Горбенко И.Д. Анализ безопасности международного стандарта ISO/IEC 9797-1 / И.Д. Горбенко, Г.З. Халимов, А.В. Потий, Е.В. Котух, А.В. Дунь // Прикладная радиоэлектроника. – 2007. – Т. 6, №2. – С.250-256.

38. Халимов Г.З. Универсальное хеширование по кривым Сузуки / Г.З. Халимов, Е.В. Котух // Прикладная радиоэлектроника. – 2011. – Т.10, № 2. –С.164-170.

39. Халимов Г.З. Алгоритм универсального хеширования по кривой Судзуки / Г.З. Халимов, Е.В. Котух // Восточно-Европейский журнал передовых технологий. – 2011. – № 3/9 (51). – С. 10-16.

40. Котух Е.В. Универсальное хеширование по кривым, ассоциированным с группой Судзуки / Е.В. Котух, Г.З. Халимов // Прикладная радиоэлектроника. – 2015. – Т.14, №4. – С.361 – 365.

41. Котух Е.В. Универсальное хеширование с ограничением функционального поля алгебраических кривых // Радиотехника. – 2012. – Вып. 171. – С. 109-115.

42. Котух Е.В. Анализ современных требований к криптографическим примитивам нового поколения / Е.В. Котух, В.М. Карташов, О.Г. Халимов, Д.П. Цапко, А.В. Самойлова // Радиотехника. – 2015. – Вып. 181. – С. 133-142 .

43. Котух Е. Скоростное универсальное хеширование на основе многопотоковых вычислений / Е. Котух, В. Карташов, Д. Цапко, О. Халимов, А. Самойлова // Захист інформації. – 2015. – Т.17. – №2. – С.9.

44. Котух Е. Метод универсального хеширования по алгебраическим кривым / Е. Котух, Г. Халимов, А. Бойко, А. Герцог // XV Междунар. науч.-практ. конф. ”Безопасность информации в информационно-телекомуникационных системах”, Киев, 22 – 25 мая 2012 г. : тезисы докладов. – Киев, 2012. – С.36.

45. Котух Е. Высокоскоростное универсальное хеширование по кривым Ферма // XI Междунар. науч.-практ. конф. "Безопасность информации в информационно-телекоммуникационных системах", Киев, 20 – 23 мая 2008 г. : тезисы докладов. – Киев, 2008. – С.31 – 32.

46. Халимов Г. Каскадное универсальное хеширование / Г. Халимов, А. Бойко, Е. Котух // Сб. тр. Второй Междунар. науч.-техн. конф. «Компьютерные науки и технологии КНиТ-2011». – Белгород, 2011. – С. 541 – 544.

47. Корченко А.Г. Многокаскадное универсальное хеширование по рациональным функциям максимальной кривой Судзуки / А. Г. Корченко, Е. В. Котух, А. А. Бойко // Радиотехника. – 2011. – №166. – С. 44-49.

48. Халимов Г.З. Функциональное поле кривой Судзуки для универсального хеширования / Г.З. Халимов, Е.В. Котух // Междунар. науч.-практ. конф. «Застосування інформаційніх технологій у підготовці та діяльності сил охорони правопорядку». Академія внутрішніх військ МВС України 17 – 18.03.2011 : тези доповідей. – 2011. – С.45-48.

49. Котух Е.В. Композиционное универсальное хеширование по кривым Судзуки / Е.В. Котух // Інформаційна безпека держави, суспільства та особистості : зб. тез доповідей Всеукр. наук.-практ. конф. – Кіровоград : КНТУ, 2015. – С.60.

50. Котух Е.В. Оценка параметров композиционного универсального геширования по кривым Судзуки / Е.В. Котух // Праці студентської наук. конф. фізико-технічного факультету. – ДонНУ, 2015. – С.73-74.

51. Google accelerates end of SHA-1 support [Электронный ресурс]. – Режим доступа: http://www.zdnet.com/article/google-accelerates-end-of-sha-1-support-certificate-authorities-nervous/

52. Windows Enforcement of Authenticode Code Signing and Timestamping. [Электронный ресурс]. – Режим доступа: http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx

53. SHA-1 Depreciation Update [Электронный ресурс]. – Режим доступа: https://blogs.windows.com/msedgedev/2015/11/04/sha-1-deprecation-update/

54. Performance of Optimized Implementations of the NESSIE Primitives. NESSIE, Performance Evaluation. V 2.0, Feb 20, 2003 [Электронный ресурс]. – Режим доступа: https://www.cosic.esat.kuleuven.be/nessie/deliverables/D21-v2.pdf

55. Federal Register Notice published on November 2, 2007 [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/groups/ST/hash.

56. NIST Computer security resource center. Announcing request for Candidate algorithm nominations for a new cryptographic hash algorithm nominations for a new cryptographic hash algorithm (SHA-3) family. – 2007 [Электронный ресурс]. – Режим доступа : http://csrc.nist.gov/groups/ST/.

57. Imad Fakhri Alshaikhli. Comparison and analysis study of SHA-3 finalists / Imad Fakhri Alshaikhli, Mohammad A. Alahmad Khanssaa Munthir // International Conferenceon Advanced Computer Science Applications and Technologies, Proceedings. – 2012. – P.366-371.

58. Bellare M. Keying hash functions for message authentication / M. Bellare, R. Canetti, H. Krawczyk // Advances in Cryptology, Proceedings Crypto'96, LNCS 1109, N. Koblitz, Ed., Springer-Verlag. – 1996. – P.1-15.

59. FIPS 180-2 : Secure hash standard – NIST, 2002.

60. ANSI X9.30: American National Standard for Financial Institution Message Authentication (Wholesale) – American Bankers Association, 1986.

61. ANSI X9.31: American National Standard for Financial Institution Message Authentication (Wholesale). – American Bankers Association, 1986.

62. Стандарты хеш-функций. Основные требования [Электронный ресурс]. – Режим доступа: http://vunivere.ru/work23768/page4

63. Горбенко И.Д. TWO-TRACK-MAC алгоритм высокой защиты / И.Д. Горбенко, О.Г. Халимов // Радиотехника. – 2005. – Вып. 141. – С. 161-167.

64. Fleischmann E. Classification of the SHA-3 Candidates / E. Fleischmann, C. Forler, M. Gorski. – 2008 [Электронный ресурс] – Режим доступа: http://eprint.iacr.org/2008/511.pdf.

65. Blake submission package [Електронний ресурс]. – Режим доступа: http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/documents/Blake_FinalRnd.zip

66. SHA-3 Proposal Blake / Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Raphael C.-W. Phan; NIST. Candidatetothe NIST Hash Competition, 2008.

67. Groestl a SHA-3 candidate / Soren Steffen Thomsen, Martin Schlaffer, Christian Rechberger, Florian Mendel, Krystian Matusiewicz, Lars R. Knudsen, Praveen Gauravaram; NIST. Candidate to the NIST Hash Competition, 2011.

68. The Hash Function JH / Hongjun Wu; NIST. Candidate to the NIST Hash Competition, 2008.

69. The Skein Hash Function Family / Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker; NIST. Candidate to the NIST Hash Competition, 2010.

70. Skein submission package [Електронний ресурс]. – Режим доступа: http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/documents/Skein_FinalRnd.zip

71. The Keccak SHA-3 submission / Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche; NIST. Candidate to the NIST Hash Competition, 2011.

72. Pierre-Louis Cayrel, Gerhard Hoffmann, Michael Schneider. GPU Implementation of the Keccak Hash Function Family // Interntaional Journal of Security and Its Applications. – Vol 5. No. 4, October 2011.

73. Халимов Г.З. Асимптотические границы вероятности коллизии для MAC с алгебраическим кодированием / Г.З. Халимов, А.В. Дунь //

Восточно-европейский журнал передовых технологий. – 2007. – Вып. 5/2(29). – С.23-26

74. Stinson D.R. Combinatorial techniques for universal hashing / D.R. Stinson // Journal of Computer and Systems Science. – 1994. – V. 48. – P. 337-346.

75. Stinson D.R. Universal hashing and authentication codes / D.R. Stinson // Designs, Codes and Cryptography. – 1994. – N.4. – P.369–380.

76. Халимов Г.З. Аутентификация и универсальное хеширование/ Г.З. Халимов, А.А. Кузнецов // Радиотехника. – 2001. – Вып. 119. – С. 88-94.

77. Black J. UMAC: Fast and secure message authentication / J. Black, S. Halevi, H. Krawczyk, T. Krovetz and P. Rogaway // In Advances in Cryptology ‘CRYPTO '99, of Lecture Notes in Computer Science, Springer-Verlag. – 1999. – Vol. 1666. – P. 216-233.

78. Krovetz T. UMAC / T. Krovetz, J. Black, S. Halevi, A. Hevia, H. Krawczyk and P. Rogaway // Primitive submitted to NESSIE. – 2000. – Sept. – P. 157-160.

79. Халимов Г.З. Высокоскоростной UMAC алгоритм / Г.З. Халимов // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – НТУУ “КПІ” МОНУ, ДСТСЗІ СБУ. – 2005. – Вип.11. – С.167-173.

80. Stinson D.R. On the connections between universal hashing, combinatorial designes and error-correcting codes / D.R. Stinson // Congressus Numerantium. – 1996. – V.114. – P. 7-27.

81. Гоппа В.Д. Коды на алгебраических кривых / В.Д. Гоппа // Докл. АН СССР. – 1981. – Т.259, № 6. – С. 1289-1290.

82. Krovetz T. Fast universal hashing with small keys and no preprocessing: The PolyR construction. / T. Krovetz, P. Rogaway // In Information Security and Cryptology – ICICS 2000. Springer-Verlag. – 2000. – P.73–89.

83. Krovetz T. Message Authentication on 64-bit Architectures [Электронный ресурс]. – Режим доступа: https://eprint.iacr.org/2006/037.pdf.

84. Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова – Гилберта / М.А. Цфасман // Проблемы передачи информации. – 1982. – Т.18, №3. – С. 3-6.

85. Халимов Г.З. Оценка имитостойкости систем с композиционной схемой аутентификации / Г.З. Халимов, А.А. Кузнецов, А.В. Северинов, А.Д. Буханцов // Зб. наук. праць ХВУ. – Харків : ХВУ, 2001. – Вип. 5(35). – С.113-115.

86. Халимов Г.З. Криптоанализ прямой атаки на универсальное семейство хеш-функций с алгебраическим кодированием / Г.З. Халимов, А.Ю. Иохов, А.В. Северинов // Системи обробки інформації. – Харків : ХВУ, 2004. – Вип. 12(40). – С. 238-247.

87. Халимов Г. З. Методы и средства аутентификации многоадресного источника данных / Г.З. Халимов, А.В. Дунь // Прикладная радиоэлектроника. – 2007. – №3. – С.377-384.

88. Kurosawa K. Almost k-wise independent sample spaces and their cryptologic applications / K. Kurosawa, T. Johansson, D. Stinson // Lecture Notes in Computer Science. – 1997. – N. 1233. – P.409-421.

89. Alon N. Simple constructions of almost k-wise independent random variables / N. Alon, O. Goldreich, J. Hastad, R. Peralta // Random Structures and Algorithms. – 1992. – N.3. – P. 289-304.

90. Bierbrauer J. Weakly biased arrays, almost independent arrays and error-correcting codes / J. Bierbrauer, H. Schellwat // Publication in Proceedings of AMS-DIMACS, 2000. – P.33.

91. Халимов Г.З. Безусловная аутентификация с использованием слабосмещенных массивов / Г.З. Халимов // Радиотехника. – 2003. – №134. – С.165-171.

92. Torres F. Notes on Goppa codes / F. Torres // Report Series: IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-Sp-Brazil. – 2000. – P.17.

93. Халимов Г.З. Коллизионные оценки универсального хеширования на основе схем с алгебраическими кодами / Г.З. Халимов // Прикладная радиоэлектроника. – 2009. – Т. 8, вып. 3. – С.338-342.

94. Халимов Г.З. Аутентификация с применением алгеброгеометрических кодов / Г.З. Халимов, А.А. Кузнецов // Радиотехника. – 2001. – Вып. 119. – С.103-109.

95. Халимов Г.З. Аутентификация с применением эрмитовых кодов / Г.З. Халимов, А.Ю. Иохов // Вестник ХПИ. – Х. : НТУ „ХПИ”, 2005. – Вып. 9. – С. 26-32.

96. Влэдуц С.Г. Алгеброгеометрические коды. Основные понятия / С.Г. Влэдуц, Д.Ю. Ногин, М.А. Цфасман. – М. : МЦНМО, 2003. – 504с.

97. Халимов Г.З. Оценка параметров кривых Ферма для универсального хеширования в простом поле / Г.З. Халимов // Материалы науч.-техн. конф. с международным участием «Компьютерное моделирование в наукоемких технологиях» (Ч. 2). КМНТ. – Харьков, 18–21 мая 2010. – С.266.

98. Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования / Г.З. Халимов // Материалы XI Междунар. науч.-практ. конф. «Информационная безопасность» (Таганрог, Россия, 23–25 июня 2010), ТТИ ЮФУ. – 2010. – Ч. 3. – С. 144-146.

99. Халимов Г.З. Универсальное хеширование по максимальным кривым / Г.З. Халимов // XIII Междунар. науч.-практ. конф. «Безопасность информации в информационно-телекомуникационных системах», Киев, 18–21 мая 2010г. ; тезисы докладов. – С.53.

100. Weil A. Courbes alg´ebrique set vari´et´es abeliennes / A. Weil // Hermann, Paris, 1971. – P.301.

101. Ihara Y. Some remarks on the number of rational points of algebraic curves over finite fields / Y. Ihara // J. Fac. Science. Tokio. – 1981. – N.28. – P. 721-724.

102. Carlitz L. Bounds for exponential sums / L. Carlitz, S. Uchiyama // Duke Mathematical Journal. – 1957. – N.24. – P.37-41.

103. Vladut S.G. Number of points of an algebraic curve / S.G. Vladut ¸ V.G.Drinfeld // Function Analysis. – 1983. – N.17(1). – P.68–69.

104. Giulietti M. A new family of Fq2-maximal curves / M. Giulietti, G. Korchmaros // preprint [Электронный ресурс]. – 2007. – Режим доступа: www.math.u-bordeaux.fr/.../rocher09.pdf

105. Deligne P. Representations of reductive groups over finite fields / P. Deligne, Lusztig // Annatatsiya of Mathematics. – 1976. – N.103. – P.103-161.

106. Lachaud G. d'Eisensteinet nombre de points de certaines courbes algebriques sur les corps finis / G. Lachaud // C.R. Academia Science, Paris, 1987. – V.305, Serie 1. – P.729-732.

107. Hansen, J.P. Deligne-Lusztig varieties and group codes / J.P. Hansen // Lecture Notes of Mathematics. – 1992. – V.1518. – P.63-81.

108. Ruck H.G. A characterization of Hermitian function fields over finite fields / H.G. Ruck, H. Stichtenoth // J. Reineangew. Mathematics. – 1994. – V.457. – P.185-188.

109. Fuhrmann R. The genus of curves over finite fields with many rational points / R. Fuhrmann, F. Torres // Manuscripta Mathematics. – 1996. – N.89. – P.103-106.

110. Torres F. The Deligne-Lusztig curve associated to the Suzuki group / F. Torres // arXiv:alg-geom/9706012v1 26Jun 1997.

111. Hoholdt N. Algebraic geometry codes. In the Handbook of Coding Theory / N. Hoholdt, J.H.van Lint and R. Pellican / V.S. Pless, W.C. Huffman and R.A. Brualdi Eds., Elsevier, Amsterdam. – 1998. – V.1. – P.871-961.

112. Korchmaros G. On the genus of a maximal curve / G. Korchmaros, F. Torres // Mathematics Annatatsiya. – 2002. – V.323(3). – P.589-608.

113. Lauter K. Improved upper bounds for the number of rational points on algebraic curves over finite fields / K. Lauter // C.R. Academy Science Paris. – 1999. – V.328(12), Serie I. – P.1181-1185.

114. Garcia A. On subfields of the Hermitian function field / A. Garcia, H. Stichtenoth and C.P. Xing // Composition Mathematics. – 2000. – V.120. – P.137-170.

115. Cossidente A. On curves covered by the Hermitian curve / A. Cossidente, G. Korchmaros and F. Torres // Algebra. – 1999. – N.216. – P.56-76.

116. Cossidente A. Curves of large genus covered by the Hermitian curve //. A. Cossidente, G. Korchmaros and F. Torres // Commutative Algebra. – 2000. – V.28(10). – P. 4707-4728.

117. Халимов Г.З. Универсальное хеширование по максимальным кривым Гурвица / Г.З. Халимов // Прикладная радиоэлектроника. – 2010. – Т.9, № 3. – С.365-370.

118. Fuhrmann R. On maximal curves / R. Fuhrmann, A. Garcia, F. Torres // Number Theory. – 1997. – V.67(1). – P. 29-51.

119. Халимов Г.З. Универсальное хеширование по максимальной кривой второго рода / Г.З. Халимов // Радиоэлектронные и компьютерные системы. – 2011. – № 1(49). – С.70-76.

120. Garcia A. On curves over finite fields / A. Garcia // Seminaires&Congres. – 2005. – N.11. – P.75-110.

121. Pedersen J.P. A function field related to the Ree group / J.P. Pedersen // Lecture Notes Mathematics. – 1992. – V.1518. – P.122-131.

122. Torres F. Plan maximal curves / F. Torres // Acta Arithmetic. – 2001. – Vol. 98, No. 2. – P. 165-179.

123. Халимов Г.З. Асимптотические оценки максимальных кривых для универсального хеширования / Г.З. Халимов // Междунар. науч.-практ. конф. «Застосування інформаційніх технологій у підготовці та діяльності сил

охорони правопорядку» ; Академія внутрішніх військ МВС України, 17 – 18.03.2011 : зб. тез. доповідей. – 2011. – С.43-44.

124. Халимов Г.З. Универсальное хеширование на функциональном поле алгебраической кривой второго рода / Г.З. Халимов // Спеціальні телекомунікаційні системи та захист інформації : зб. наук. праць. – Київ : ДССЗ та ЗІ. – 2011. – Вип. 1(19). – С.31-39.

125. Халимов Г.З. Универсальное хеширование по максимальной кривой третьего рода / Г.З. Халимов // Науч. ведомости Белгород. гос. ун-та. – 2011. – №1 (96). – Вып. 17/1. – С. 137-145.

126. Халимов Г.З. Универсальное хеширование по рациональным функциям максимальной кривой третьего рода / Г.З. Халимов // Радиотехника. – 2011. – Вып. 165. – С.218-224.

127. Hansen J.P. Group codes on certain algebraic curves with many rational points / J.P.Hansen, H.Stichtenoth // AAECC. – 1990. – N.1. – P.67–77.

128. Tits J. Ovo¨ıdesetgroupes de Suzuki / J. Tits // Archive Mathematics. – 1962. – N.13. – P.187-198.

129. Penttila T. Ovoids of parabolic spaces / T. Penttila, B. Williams // preprint– 1997. – [Электронный ресурс]. Режим доступа: www-ma4.upc.es/.../ovoidsofparabolics.pdf

130. Stichtenoth H. Algebraic function fields and codes / H. Stichtenoth // Springer-Verlag, Berlin. – 1993. – P.132.

131. Халимов Г.З. Универсальное хеширование по алгебраическим кривым в простом поле / Г.З. Халимов // XIV Междунар. науч.-практ. конф. ”Безопасность информации в информационно-телекомуникационных системах”, Киев, 18 – 21 мая 2010 : тезисы докладов. – 2011. – С.22-23.

132. Халимов Г.З. Оценка параметров кривых Ферма для универсального хеширования / Г.З. Халимов // Радіоелектроніка, інформатика, управління. – Запоріжжя : ЗТТУ, 2011. – №1(24). – С.82-86.

133. Халимов Г.З. Универсальное хеширование по максимальным кривым Ферма в квадратичном поле / Г.З. Халимов // XII Міжнар. наук.-практ. конф. «Безпека інформації в інформаційно-телекомунікаційних системах», Київ, 19–22.05.2009 : зб. тез доповідей. – 2009. – С.32.

134. Халимов Г.З. Оценка параметров кривых Ферма в расширенном поле для универсального хеширования / Г.З. Халимов, А.В. Леншин // Защита информация : сб. науч. тр. НАУ. – Киев, 2010. – Вып.17. – С.116-120.

135. Халимов Г.З. Оценка параметров кривых Ферма в расширенном поле для универсального хеширования / Г.З. Халимов, А.В. Леншин // Наук.-практ. конф. «Захист інформації в інформаційно-комунікаційних системах», 24–26.05.2010, Київ : зб. тез доповідей. – 2010. – С.102.

136. Халимов Г.З. Кривые Ферма с большим числом точек в расширенных конечных полях / Г.З. Халимов // Системи обробки інформації. МО України. Харк. ун-т Повітряних Сил ім. Івана Кожедуба. – 2011. – Вип. 4(94). – С.146-150.

137. Халимов Г.З. Двухкаскадное универсальное хеширование с использованием АГ кодов / Г.З. Халимов, А.Ю. Иохов // Восточно-европейский журнал передовых технологий. – 2005. – Вып. 2/2 (14). – С. 115-119.

138. PellikanR. The Klein quartic, the Fanoplanand curves representing design / R. Pellikan // In Codes, Curves and Signals : Common Threads in Communications (A. Vardy Ed.), Kluwer Academy Published, Dordrecht. – 1998. – P.9-20.

139. Халимов Г.З. Каскадное универсальное хеширование по рациональным функциям алгебраических кривых / Г.З. Халимов // Радиотехника. – 2011. – Вып. 166. – С.26-31.

140. Carbonne P. Decomposition de la Jacobienne sur les corps finis / P. Carbonne, T. Henocq // Bull. Polish Academy Science Mathematics. – 1994. – V.42(3). – P.207-215.

141. Mukhopadhyay A.L. Construction of some series of ortogonal array / A.L. Mukhopadhyay // Sankya B43. – 1981. – P. 81-92.

142. Bierbrauer J. Bounds on orthogonal arrays and resilient functions / J. Bierbrauer // Journal of Combinatorial Designs. – 1995. – N.3. – P. – 179-183.

143. Naor J. Small-bias probability spaces: efficient constructions and applications / J. Naor, M. Naor // SIAM Journal on Computing. – 1993. – N.22. – P.838-856.

144. Beelen P. The Newton polygon of plane curves with many rational points. / P. Beelen, R. Pellikan // Designs, Codes and Cryptography. – 2000. – N.21. – P.41-67.

145. Eid A. Suzuki-invariant codes from the Suzuki curve. / A.Eid, H.Hasson, A.Ksir, J.Peachey // arXiv: 1411.6215v2[math.AG] 25 Nov 2014

146. Suzuki M. A new type of simple groups of finite order / M.Suzuki // Proc. Nat. Acad. Sci. U.S.A. – 1960. – V.46. – P.868–870.

147. Suzuki M. On a class of doubly transitive groups / M. Suzuki // Ann. of Math. – 1962. – V. (2)75. – P.105–145.

148. Huppert B. Finite groups. III / B. Huppert, N. Blackburn // Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 243, Springer-Verlag, Berlin. – 1982. – Vol. 243.

149. Carter R.W. Simple groups of Lie type / R.W. Carter // Reprint of the 1972 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York. – 1989. – P.335.

150. Wilson R.A. The finite simple groups / R.A.Wilson // Graduate Texts in Mathematics 251. Springer-Verlag London, Ltd., London. – 2009. – P. 298.

151. Jones G.A. Varieties and simple groups / G.A. Jones // J. Austr. Math. Soc. – 1974. – V.17. – P.163-173.

152. Каргаполов М.И. Основы теории групп / М.И. Каргаполов, Ю.И. Мерзляков ; 3-е изд., перераб. и доп. – М. : Наука, 1982. – 288с

153. Вавилов Н.А. Конкретная теория групп [Електронный ресурс]. – Режим доступа: http://www.twirpx.com/file/1903331/

154. Landazuri V. On the minimal degrees of projective representations of the finite Chevalley groups / V. Landazuri and G. M. Seitz // Algebra. – 1974. – V.32. – P.418-443.

155. Hansen J.P. Group codes on certain algebraic curves with many rational points / J.P. Hansen, H. Stichtenoth // AAECC 1. – 1990. – P.67-77.

156. Hansen J.P. Deligne-Lusztig varieties and group codes / J.P. Hansen // Lect. Notes Math. – 1992. – V. 1518. – P. 63-81.

157. Pedersen J.P. A function field related to the Ree group / J.P. Pedersen // Lect. Notes Math. – 1992. – V. 1518. – P. 122-131.

158. Giulietti M. Quotient curves of the Suzuki curve / M. Giulietti, G. Korchmaŕros, F. Torres // Acta Arith. – 2006. – №3. – P. 245-274.

159. Tits J. Ovo¨ıdesetgroupes de Suzuki / J. Tits // Archive Mathematics. – 1962. – N.13. – P.187-198.

160. Eid A. Suzuki-invariant codes from the Suzuki curve / A. Eid, H. Hasson, A. Ksir, J. Peachey // arXiv: 1411.6215v2[math.AG] 25 Nov 2014.

161. Stichtenoth H. Algebraic function field and code. Springer, Berlin (2009).

162. Eid A., Duursma I. Smooth embeddings for the Suzuki and REE curves [Електронный ресурс]. – Режим доступа: http://arxiv.org/abs/1311.1999

163. Халимов Г.З. Универсальное хеширование по рациональным функциям кривой Эрмита / Г.З. Халимов, А.Ю. Иохов // Міжнар. наук.-практ. конф. «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» ; Академія внутрішніх військ МВС України, 17 – 18.03.2011 ; зб. тези доповідей. – 2011. – С.48-51.

164. Халимов Г.З. Багатократне універсальне гешування / Г.З. Халимов // Спеціальні телекомунікаційні системи та захист інформації : зб. наук. – Київ : ДССЗ та ЗІ, 2010. – Вип. 2(18). – С.43-49.

Приложение

Акты внедрения результатов диссертационной работы

«ЗАТВЕРДЖУЮ»
Т.в.о. ректора Харківського національного
університету радіоелектроніки

_____ Е.Ю. Рубін

«____»_____2016 р.

АКТ
впровадження результатів наукових досліджень
в навчальний процес Харківського національного університету радіоелектроніки
Котуха Євгена Володимировича

Комісія у складі голови комісії, професора кафедри БІТ, кандидата технічних наук, Заболотного В.І та членів комісії, доцента кафедри БІТ, кандидата технічних наук Олешко О.І. старшого викладача кафедри БІТ, кандидата технічних наук Іваненко Д.В., з'ясувала, що у Харківському національному університету радіоелектроніки впроваджені наступні результати при підготовці фахівців в напряму «Інформаційна безпека» у курсі «Системи та засоби автентифікації»:

1. Розроблена за участю Котуха Є.В. лекція «Методи побудови доказово стійкій автентифікації на основі універсального гешування», що базується на результатах, отриманих Котухом Є.В. (статті: «Алгоритм универсального хеширования по кривой Сузуки» // Восточно-Европейский журнал передовых технологий. -2011. -№ 3/9 (51). - стр.10-16., «Универсальное хеширование с ограничением функционального поля алгебраических кривых» /// Радиотехника. Всеукр. межвед. науч.-техн. сб. 2012. Вып. 171. С. 109 — 115.)
2. Розроблена за участю Котуха Є.В лабораторна робота «Дослідження властивостей алгоритмів універсального гешування за алгебричними кривими». Практичною основою лабораторної роботи є розроблена програмна бібліотека для побудови кривих, обчислення їх точок та властивості, моделювання лінійного базисного простору за раціональними функціями кривих та статистичного оцінювання ймовірності колізії гешування за обчисленням кратності перетину гіперповерхонь лінійного простору з точками кривої.

Голова комісії, к..т.н., доц. _____ Заболотний В.І.
Члени комісії:
к.т.н. _____ Олешко О.І.
к.т.н. _____ Іваненко Д.В.

«ЗАТВЕРДЖУЮ»
Генеральний директор
ДП НТК «Імпульс»
м Київ, вул. Горлівська 226/228

_____Погребняк О.Л.

«____»_____2015 р.

АКТ

впровадження результатів досліджень
Котух Євгена Володимировича

Комісія у складі голови комісії, першого заступника генерального директора ДП НТК «Імпульс» Кольнера Є.Я. та члена комісії т.в.о. головного конструктора ДП НТК «Імпульс», Кузьменка І.М, склала дійсний акт, який полягає в тому, що при виконанні дослідно-конструкторських робіт використані наступні результати наукових досліджень:

1. 1) розроблений за участю Котуха Є.В.. метод універсального гешування з обмеженням функціонального поля алгебричних кривих, що використовує гешування за оптимізованим вибором раціональних функцій;

2) розроблений за участю Котуха Є.В. метод універсального гешування за алгебричними кривими Судзукі;

3) розроблені за участю Котуха Є.В. алгоритми обчислення геш кодів за алгебричними кривими Судзукі на основі методу обчислення геш коду з використанням чотирьох параметричної схеми Горнера;

4) розроблена за участю Котуха Є.В. програмна бібліотека для побудови кривих, обчислення їх точок та властивості, моделювання лінійного базисного простору за раціональними функціями кривих та статистичного оцінювання ймовірності колізії гешування за обчисленням кратності перетину гіперповерхонь лінійного простору з точками кривої.

Голова комісії
Перший заступник генерального директора _____Кольнер Є.Я.

Члени комісії:
Т.В.О. Головного конструктора _____Кузьменко І.М.