МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет радіоелектроніки

Котух Євген Володимирович

УДК 681.3.06

МЕТОДИ ТА ЗАСОБИ УНІВЕРСАЛЬНОГО ГЕШУВАННЯ ЗА АЛГЕБРИЧНИМИ КРИВИМИ СУДЗУКІ

05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2016

Дисертацією є рукопис.

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Халімов Геннадій Зайдулович,
кафедра «Безпека інформаційних технологій»
Харківського національного університету
радіоелектроніки

Офіційні опоненти: доктор технічних наук, професор
Рудницький Володимир Миколайович,
Черкаський державний технологічний
університет, завідувач кафедри інформаційної
безпеки та комп'ютерної інженерії,

кандидат технічних наук, доцент
Гнатюк Сергій Олександрович,
Національний авіаційний університет,
доцент кафедри безпеки інформаційних
технологій

Захист відбудеться __ _____ 2016 року о ___ годині на засіданні спеціалізованої вченої ради К.64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Науки, 14.

Автореферат розісланий _____

Вчений секретар
спеціалізованої вченої ради Т.В. Носова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Необхідність захисту інформації в інформаційно-телекомунікаційних системах закріплена в Законах України «Про захист персональних даних», «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних». До усіх учасників інформаційного обміну пред'являються високі вимоги щодо забезпечення цілісності та достовірності даних, що передаються між вузлами розподілених інформаційно-телекомунікаційних систем (ІТС) через незахищені канали зв'язку. Відповідно до вимог міжнародних стандартів в області криптографії (ISO 7498, ISO/IEC 10181) базова послуга автентифікації може бути забезпечена за рахунок використання кодів автентифікації (MAC-кодів). Побудова MAC кодів визначається трьома загальними підходами: застосуванням блокових шифрів, на основі безключевої геш-функції, з використанням сімейства універсальних геш-функцій.

Слабка обчислювальна складність, ряд значних недоліків конструкції і математично обгрунтовані атаки на колізійну стійкість дозволили реалізувати для геш-функцій SHA1 і MD5 атаки повного перебору за допустимий час, що стало причиною відмови світових лідерів в області розробки програмного забезпечення від їх використання. Це стало можливим внаслідок значного підвищення продуктивності і доступності GPGPU-процесорів і GRID систем в сукупності з новими методологіями розподільних обчислень.

Результати міжнародних проектів NESSIE (2000 – 2003 рр.) і NIST SHA-3 Competition (2007 – 2012 рр.) підтверджують актуальність вирішення задачі розробки геш-функцій гарантованої стійкості, в тому числі для побудови національного стандарту гешування. Гарантована стійкість до атак реалізується в теорії доказово стійкої автентифікації.

Доказово стійка автентифікація вперше розглянута G.J. Simmons і представлена M.N. Wegman, J.L. Carter в теорії універсального гешування (1979 р.). Універсальне гешування визначається родинами геш-функцій з заданими комбінаторними властивостями. Обчислення гешів за допомогою скалярного множення значення ключа і повідомлення призводить до універсального гешування з ймовірністю колізії $1/|B|$, де B – простір геш-кодів. Основний результат універсального гешування визначає, що розмір ключа дорівнює розміру повідомлення. Універсальне гешування визначає доказово стійку автентифікацію з лічильником, так як кожне повідомлення повинне мати свій ключ автентифікації. У теорії доказово стійкої автентифікації очевидним є протиріччя між витратами ключа на автентифікацію, які визначаються розміром повідомлень, і значенням ймовірності колізії (обману), яка визначається простором геш-кодів.

В Україні перші дослідження з побудови механізмів автентифікації каналів передачі даних розглядаються в роботах І.Д. Горбенко. Ряд фундаментальних результатів з автентифікації і ідентифікації останнім часом отримано

В. К. Задіракою, А.Г. Корченко та ін. Використання алгеброгеометрічних кодів у конструкціях МАС-кодів розглянуто в роботах Г. Кабатіанскі, Т. Йохансона, Б. Сміітса. В роботах В. Столлінгс, Г. Сіммонса, Д. Стинсона запропоновано ряд практичних конструкцій. Ці роботи багато в чому визначили напрямки досліджень дисертаційної роботи.

Таким чином, актуальність дисертаційної роботи обумовлюється необхідністю побудови доказово стійкої автентифікації повідомлень, яка задовольняє вимогам складності і швидкості обчислення, характеристикам і реалізаціям алгоритму для побудови національного стандарту.

Зв'язок з науковими програмами, планами, темами. Основу роботи складають результати теоретичних і практичних досліджень, виконаних автором в науково-дослідницьких роботах за держбюджетними темами ХНУРЕ: «Обґрунтування вимог, розроблення та впровадження інфраструктури електронного цифрового підпису в МОНУ» (№ ДР 0103U001981), «Методи, системи та засоби кріптографічного захисту інформації з гарантованим рівнем стійкості та підвіщеною швидкодією» (№ ДР 0115U002431); за госпдоговорами «Організація та розроблення проекту національного стандарту України та методичних рекомендацій щодо застосування міжнародних стандартів» (шифр «Гармонія» – 2007).

Мета дослідження. Метою роботи є розробка методу універсального гешування за раціональними функціями кривих Судзукі для побудови доказово стійкої автентифікації із забезпеченням гарантованої ймовірності колізії зі зменшеною складністю обчислення.

Для досягнення мети необхідно вирішити такі наукові завдання:

1. Провести аналіз методів побудови МАС-кодів універсального і строго універсального гешування.
2. Розробити метод універсального гешування за раціональними функціями алгебричної кривої Судзукі.
3. Розробити метод швидкого універсального гешування за кривою Судзукі на основі застосування схеми обчислення Горнера.
4. Розробити метод універсального гешування з обмеженням функціонального поля алгебричних кривих зі зменшеною складністю обчислень.
5. Розробити метод каскадного універсального гешування за кривою Судзукі на основі добутку функціональних полів.
6. Розробити практичні рекомендації щодо застосування універсального гешування за кривою Судзукі.

Об'єктом дослідження є процеси автентифікації повідомлень в комп'ютерних системах і мережах на основі сімейства універсального класу геш-функцій з високими вимогами до доказової стійкості і мінімізації витрат на автентифікацію.

Предметом досліджень є методи автентифікації даних на основі універсального гешування, що задовольняють вимогам доказово колізійної стійкості, складності знаходження прообразу і другого прообразу, високої швидкодії, простоти реалізації з мінімізацією витрат на ключовий простір.

Методи досліджень. При виконанні дисертаційної роботи використовувалися:

- теорія груп Судзукі, теорія алгебричних кривих і кривих Судзукі, теорія лінійного простору над функціональним полем проективного різноманіття – для побудови методу універсального гешування за кривими Судзукі;
- теорема Рімана – Роха – для обчислення розмірності лінійного базисного простору і оцінювання параметрів універсального гешування;
- теорія композиційного гешування Стинсона – для розробки методів каскадного універсального гешування;
- теорія ймовірності – для оцінки колізійних властивостей універсального гешування.

Наукова новизна отриманих результатів. Отримано нові наукові результати:

1. Вперше запропоновано метод універсального гешування за раціональними функціями кривої Судзукі, що дозволило зменшити ймовірність колізії в корінь шостого ступеня від розмірності поля обчислення і збільшити довжину даних, що гешуються, в корінь квадратний від розмірності поля обчислення у порівнянні з гешуванням за максимальними плоскими кривими.
2. Вперше запропоновано метод обчислення геш-функцій за кривою Судзукі на основі чотирьохпараметричної схеми Горнера, в якій враховується розмірність раціональних функцій кривих, що дозволило зменшити складність обчислення в два рази у порівнянні із загальним підходом.
3. Набув подальшого розвитку метод універсального гешування за раціональними функціями алгебричних кривих, який, на відміну від відомих, використовує обчислення геш-функцій з обмеженням функціонального поля алгебричних кривих, що дозволило зменшити складність обчислень пропорційно підмножині раціональних функцій, які використовуються для гешування.
4. Набув подальшого розвитку метод каскадного універсального гешування на основі добутку функціональних полів, який, на відміну від відомих, передбачає застосування гешування в каскаді за кривою Судзукі, що дозволило зменшити ймовірність колізії в корінь ступеня числа, що визначається кількістю каскадів від кореня кубічного числа слів даних, і збільшити розмір даних, що гешуються.

Практичне значення отриманих результатів полягає в наступному:

1. Побудовано функціональне поле кривої, асоційованої з підгрупою групи Судзукі над кінцевим полем довільного ступеня розширення. Отримано оцінки алгеброгеометрічних параметрів кривих Судзукі над кінцевими полями.
2. Побудовано алгоритм гешування за кривою Судзукі за методом обчислення геш-коду на основі чотирьохпараметричної схеми Горнера, що дозволило отримати найменшу складність обчислень (акт впровадження).
3. Розроблено практичні рекомендації щодо використання універсального гешування за кривою Судзукі в схемах багаторазового, багатокаскадного, композиційного гешування доказово стійкої і безумовної автентифікації повідомлень, що дозволило мінімізувати ймовірність колізії,

складність обчислень і оптимізувати витрати на ключовий простір (акт впровадження).

4. Отримано оцінки універсального гешування, складності обчислення геш-коду для двохкаскадного гешування і багатокаскадного гешування з гешуванням за кривою Судзукі в схемі, коли у внутрішньому каскаді використовується гешування за проективною прямою.

5. Розроблено програмні засоби для побудови кривих, обчислень їх точок і властивостей (кратності), моделювання лінійного базисного простору з раціональними функціями кривих і статистичного оцінювання ймовірності колізії гешування шляхом обчислення кратності перетину гіперповерхонь лінійного простору з точками кривої (акт впровадження).

Результати дисертаційної роботи впроваджено в дослідницьких і конструкторських роботах в НТК ДП «Імпульс» (акт впровадження), в навчальному процесі кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки при вивченні дисципліни «Системи і засоби автентифікації», в курсовому і дипломному проектуванні (акт впровадження).

Особистий внесок здобувача. Всі положення дисертації, що виносяться на захист, основні результати теоретичних і експериментальних досліджень отримані автором самостійно. У наукових статтях, опублікованих у співавторстві, здобувачеві належать: оцінки складності і секретності алгоритма Whirpool [1]; оцінки безпеки MAC алгоритмів стандарту ISO/IEC 9797-2 [2]; оцінки безпеки MAC алгоритмів стандарту ISO/IEC 9797-1 [3], метод універсального гешування за раціональними функціями кривої Судзукі, доказ твердження про порядки полюсів раціональних функцій кривої Судзукі [4]; метод обчислення геш-функцій на основі чотирьохпараметричної схеми Горнера, практичний алгоритм універсального гешування за раціональними функціями кривої Судзукі на основі схеми Горнера з обчисленням по підгрупі Вейерштрасса розмірності чотири, оцінки для ймовірності колізії та складності гешування [5]; метод каскадного універсального гешування за кривою Судзукі на основі добутку функціональних полів [6]; метод універсального гешування на основі скалярного добутку за раціональними функціями лінійного базисного простору з обмеженням функціонального поля алгебричних кривих [7]; вимоги до криптографічних примітивів нового покоління [8]; оцінки універсального гешування на основі багатопотокових обчислень [9]; алгеброгеометрічні параметри кривих Судзукі над кінцевими полями і оцінки параметрів універсального гешування за кривими Судзукі [10].

Апробація результатів дисертації. Основні наукові результати і положення дисертаційної роботи доповідалися і обговорювалися на міжнародних та національних науково-технічних конференціях: Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах», Київ, 20 – 23 травня 2008 р.; Друга Міжнародна науково-технічна конференція «Комп'ютерні науки та технології КНіТ-2011», Бєлгород, 2011 р.; XV Міжнародна науково-практична конференція «Безпека інформації в інформа-

ційно-телекомунікаційних системах», Київ, 22 – 25 травня 2012 р.; Міжнародна науково-практична конференція «Застосування інформаційніх технологій у підготовці та діяльності сил охорони правопорядку», Академія внутрішніх військ МВС України, 17 – 18 березня 2011 р.; Всеукраїнська науково-практична конференція «Інформаційна безпека держави, суспільства та особистості», Кіровоград, КНТУ, 16 квітня 2015 р.; студентська наукова конференція фізико-технічного факультету ДонНУ, 2015 р.

Публікації. За результатами дисертаційної роботи опубліковано 10 статей у виданнях, що входять до переліків фахових видань України з технічних наук, та 6 матеріалів і тез наукових конференцій.

Структура і обсяг дисертації. Дисертація складається із вступу, п’яти розділів і висновків, має загальний обсяг 209 сторінок, з яких 169 сторінок основного тексту, містить 16 рисунків, 25 таблиць, список використаних джерел з 164 найменувань на 17 сторінках.

ОСНОВНА ЧАСТИНА

У **вступі** надається загальна характеристика роботи, обґрунтовується актуальність теми, формулюються мета і основні завдання дисертаційної роботи, визначаються об’єкт, предмет і методи дослідження, наукова і практична значущість отриманих результатів, наводяться дані про публікації та особистий внесок автора в роботах, виконаних у співавторстві, відомості про апробацію результатів дисертації, обгрунтовуються наукова новизна, практичне значення та впровадження одержаних результатів.

У **першому розділі** «Аналіз сучасних вимог до криптографічних примітивів» виконаний аналіз існуючих алгоритмів вироблення MAC-кодів і обгрунтування шляхів підвищення колізійної стійкості, зменшення обчислювальної складності.

Якість рішення задач автентифікації в каналах передачі інформації значною мірою визначається використовуваними криптографічними алгоритмами гешування і формування MAC-кодів. Основними показниками автентифікації на основі MAC-кодів є: ймовірність хибної інформації, ймовірність колізії, довжина повідомлення, розмір ключа, розмір і обчислювальна складність MAC-коду. Результати алгоритмів-фіналістів конкурсу NIST щодо швидкості алгоритмів представлені в табл. 1.

Більшість кандидатів NIST другого раунду змагань показали композитну схему реалізації. Функція стиснення як основний елемент архітектури геш-функції була заявлена більшістю кандидатів. З точки зору вимог до архітектури важливими атрибутами є: особливості реалізації структури SPN і блоків підстановок (S-box) або блоків перестановок (P-box), схеми Фейстеля для перетворень функцій F (Li, Ki), математична складність функції ключового розширення (функції розгортання подключей раунду з основного ключа), структури Merkle-Damgard, Wide Pipe, розмірність MDS-матриці. Деякі з них були представлені парою функцій для різної довжини виходів (224, 256, 384,

512-біт). Fugue і Lufa складалися з трьох функцій, а Keccak – з чотирьох, хоча і з ядром, що розділяється. У свою чергу, такий підхід в архітектурі має негативні наслідки для продуктивності: реалізація сімейства функцій вимагає більше ресурсів для розробки, ніж для оптимізації; збільшується розмір коду; проблеми продуктивності та безпеки більш не є взаємозалежними.

Таблиця 1 – Порівняльний аналіз алгоритмів-фіналістів NIST

SHA-256/512	Blake-256/512	Grostl-256/512	JH-256/512	Keccak-256/512	Skein-256/512
продуктивність геш-функцій (cpb, 32 -біт)					
29.3/55.2	28.3/61.7	22.9/37.5	21.3/21.3	35.4/68.9	21.6/20.1
продуктивність геш-функцій (cpb, 64-біт)					
20.1/13.1	16.7/12.3	22.4/30.1	16.8/16.8	10.1/20.3	7.6/6.1

Практичні MAC-алгоритми є багаторівневими схемами, адаптованими до швидкісного гешування даних різної довжини. Найбільш високошвидкісним алгоритмом MAC-кодів є UMAC алгоритм. Рішення задач забезпечення високої швидкості обчислення і доказової секретності виявилося можливим на основі застосування композиційної схеми з багаторазовим універсальним гешуванням і криптографічним обчисленням MAC-коду. Недоліком UMAC алгоритму є необхідність генерації 1024 чотирьохбайтних підключів, що призводить до зниження продуктивності алгоритму. Архітектура сучасних телекомунікаційних систем передбачає використання x86 (32-, 64-бітових процесорів), SPARC / RISC високопродуктивних серверів. UMAC підтримує 32- і 64-розрядні обчислення, що на сучасному етапі недостатньо для автентифікації з ймовірністю колізії. Незалежний порівняльний аналіз (в рамках проекту NESSIE) показав, що найбільш потужним MAC примітивом є TTMAC алгоритм, який має найвищий рівень захисту, але при цьому низьку швидкість.

Ідея універсального гешування була запропонована Картером і Вегманом для побудови колізійно стійких і високошвидкісних кодів автентифікації. Геш-сімейство в поданні Картера і Вегмана є множина $(N; n, m)$ з N функцій H таких, що $h: A \to B$, де $h \in H$, $|A| = n$ та $|B| = m$, $n \geq m$.

Геш-сімейство $(N; n, m)$ є ε-універсальнім, якщо для будь-яких двох різних елементів $x_1, x_2 \in A$ існує найбільше εN функцій $h \in H$ таких, що $h(x_1) = h(x_2)$. Абревіатура $\varepsilon - U$ використовується для позначення ε-універсальних геш-функцій. Якщо h вибирається випадково з заданого $\varepsilon - U(N; n, m)$ геш-сімейства, то ймовірність колізії геш-значень для двох різних вхідних повідомлень $x_1, x_2 \in A$ не перевищує ε:

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

Аналіз методів універсального гешування показує, що основними шляхами побудови доказово стійкої автентифікації є універсальне гешування за

лінійним векторним простором Рімана – Роха за раціональними функціями функціонального поля, асоційованого з алгебричною кривою на проектному різноманітті її точок.

Основний результат залежить від того, що ймовірність колізії випливає з відношення значення полюса раціональних функцій функціонального поля до числа точок алгебричної кривої. Імовірність колізії зв'язується з довжиною повідомлення, ключа і полем обчислення гешів, а також з функціональним полем алгебричної кривої. Ключовий простір визначається числом точок алгебричної кривої. Вибір алгебричної кривої і асоційованого з нею функціонального поля дозволяє оптимізувати витрати на автентифікацію. Найкращий результат щодо значення полюса раціональних функцій до потужності точок кривої отримано для кривих Судзукі.

Функція мети (Z) складається з забезпечення гарантованої ймовірності колізії P_{col} функції гешування, мінімізації витрат на ключовий простір $|K|$, складності обчислень N в умовах фіксованої довжини повідомлень $\log|M|$, поля обчислення F_q характеристики 2 непарного ступеня розширення і проективного різноманіття за кривою Судзукі $F_q(C)$:

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

У **другому розділі** «Доказово стійка автентифікація на основі методів універсального гешування» розглянуто методи універсального гешування на основі алгебричного кодування, за раціональними функціями алгебричних кривих, властивості універсальних геш-функцій, асимптотичні межі для ймовірності колізії, а також безумовна автентифікація на основі строго універсального гешування.

Універсальне гешування реалізується на основі методів: скалярного добутку, поліноміального гешування, гешування на основі алгебричних кодів, скалярного добутку за раціональними функціями алгебричних кривих.

Строго універсальне гешування визначає безумовну автентифікацію. Колізійні оцінки майже строго універсального гешування зв'язуються з розподілами гешів для пар повідомлень по ключовому простору, що визначає безумовну автентифікацію на масивах автентифікаторів. У загальному випадку можна говорити про розподіли t гешів повідомлень, що визначає t пов'язану автентифікацію. Для побудови строго універсального гешування використовують методи на основі ортогональних масивів, на основі майже незалежних масивів (almost independent arrays) і на основі слабозміщених (biased) масивів.

Алгоритми обчислення геш-кодів універсальних класів і їх властивості представлено в табл. 2.

Таблиця 2 – Алгоритми побудови універсальних геш-класів і їх властивості

Назва методу	Алгоритм обчислення	Властивость геш-класу $\varepsilon - U\left(N; n, m\right)$
Метод скалярного добутку	$y = \sum_{i=1}^{k} x_i m_i ,\ y, x_i, m_i \in F_q$	$1/q - U(q^k, q^k, q)$
Метод поліноміального гешування	$y = \sum_{i=1}^{k} m_i x^i ,\ y, x, m_i \in F_q$	$k/q - U(q, q^k, q)$
Метод на основі алгебричного кодування	$y = c_i(x),\ c(x) \in (n, k, d)_q$	$(1 - d/n) - U(n, q^k, q)$
Метод на основі скалярного добутку за раціональними функціями алгебричних кривих	$y = \sum_{i=1}^{k} f_i\left(P_j\right) m_i$	$\rho_k / N - U\left(N, q^k, q\right)$

$y, x_i, m_i \in F_q$, F_q – поле обчислень, m_i – слова повідомлення, x_i – слова ключа, k – кількість слов повідомлення, ε – верхня межа ймовірності колізії.

Універсальне гешування на основі скалярного добутку вимагає, щоб розмір ключового простору був не менший простору повідомлення.

Поліноміальне універсальне гешування запропоноване для зняття обмеження на простір ключів. Недоліком є вимога – розмір простору повідомлень обмежується умовою для ймовірності колізії $\varepsilon = k/q$ і розміром поля обчислень. Обмеження на розмір простору повідомлень знімається в методі на основі алгебричного кодування. Для практичної автентифікації слід використовувати $\left(n, k, d\right)_q$ коди великої розмірності і з великою відносною кодовою відстанню. Найкращими алгебричними кодами для побудови універсальних геш-функцій є коди Ріда – Соломона, Ерміта і Судзукі. Залежності ймовірності колізій для універсального гешування на кодах РС (RSh), Ерміта (HCh) і Судзукі (SCh) від довжини повідомлення, що гешується, представлені на рис. 1.

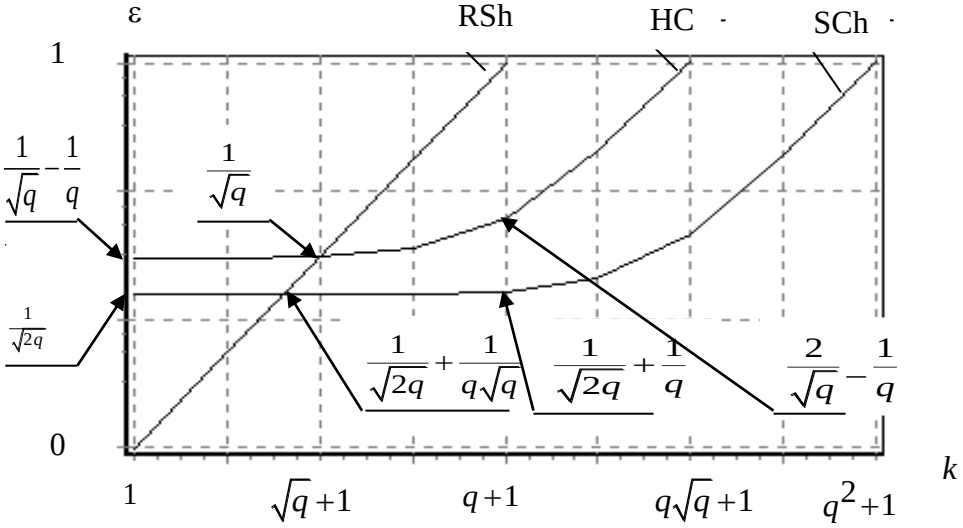

Рис. 1. Залежності ймовірності колізій універсального гешування з кодами РС, Ерміта і Судзукі від довжини повідомлення

Універсальне гешування за раціональними функціями алгебричних кривих визначається властивостями лінійного базисного простору, асоційованого з функціональним полем кривої. Асимптотичні оцінки ймовірності колізії для гешування за кращими алгебричними максимальними кривими представлені в табл. 3. Найкраща асимптотична оцінка ймовірності колізії $\varepsilon_{q\to\infty}(k)$ досягається при гешуванні за кривою Ерміта $y^q + y = x^{q+1}$.

Основне протиріччя універсального гешування за алгебричними кривими полягає в тому, що для забезпечення гарантованої ймовірності обману на нижньому рівні необхідно побудувати обчислення за раціональними функціями алгебричних кривих з якомога меншим відношенням значення максимального полюса раціональних функцій до числа точок кривої для фіксованої довжини даних.

Таблиця 3 – Колізійні оцінки універсального гешування за максимальними кривими

Рівняння кривої над F_{q^2}	Параметри $\varepsilon - U(N, q^{2k}, q^2)$	Асимптотична оцінка $\varepsilon_{q\to\infty}(k)$
$y^q + y = x^{q+1}$,	$U(q^3, q^{2k}, q^2)$	$\sqrt{2}k^{1/2}/q^2$
$y^q + y = x^d$, $d \mid q+1$	$U(q^2 + (d-1)(q-1)q, q^{2k}, q^2)$	$\sqrt{2(q+1)/d}$, $k^{1/2}/q^2$
$\sum_{i=1}^{t} y^{q/p^i} + \omega x^{q+1} = 0$, $q = p^t$, $\omega^{q-1} = -1$	$U(q^3/p, q^{2k}, q^2)$	$\sqrt{2p}k^{1/2}/q^2$
$x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$	$U(q^3 + 2q^2 + 4q + 3, q^{2k}, q^2)$	$\sqrt{6}k^{1/2}/q^2$
$\alpha^{(q+1)/2}x^{(q-1)/3} + \alpha^{(q^2-1)/2}yx^{2(q-1)/3} + y^q = 0$	$U(q^3 + 2q^2 - q - 2, q^{2k}, q^2)$	$\sqrt{6}k^{1/2}/q^2$

Криві, асоційовані з групою Судзукі, мають суттєво більшу кількість точок і потенційно менше відношення значення полюса раціональних функцій до числа точок кривої.

У **третьому розділі** «Універсальне гешування за кривою Судзукі» надані оцінка властивостей групи Судзукі, алгебричної кривої, асоційованої з групою Судзукі, побудова її функціонального поля кривої, універсального гешування за раціональними функціями і оцінка параметрів.

Параметризація групи Судзукі має уявлення через добуток матриць розмірності 4×4:

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

де $|Sz(q)| = q^2(q^2+1)(q-1)$, $q = 2^{2m+1}$.

Група Судзукі містить підгрупи $S(a,b)$, $M(c)$, підгрупи Холла і підгрупи по дільниках їх порядків q^2+1, $q-1$, $2^u r$, $2r$, $2s$, $4s$, де $r\big|(q-1)$, $s\big|(q\pm 2q_0+1), q_0=2^m$.

Крива Судзукі з точністю до F_q ізоморфізму, асоційована з підгрупою $S(a,b)$, має вигляд

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

де $q=2q_0^2$ и $q_0=2^s$, род кривої $g=q_0(q-1)$ та число F_q раціональних точок дорівнює q^2+1.

Крива Судзукі над полем F_q є оптимальною для кривої роду $g=q_0(q-1)$, по числу точок лежить близько до межі Хассе – Вейля, у квадратичному і кубічному полях є неоптимальною і максимальною в полі F_{q^4}. Криві по інших підгрупах мають число точок, відповідних порядкам цих підгруп, що менше числа точок кривої, асоційованої з підгрупою $S(a,b)$.

Раціональний морфізм кривої Судзукі в проектному просторі є відображенням $\pi := (1: x: y: v: w)$, де x, y, v, w визначаються рівняннями

$$y^q - y = x^{q_0}\left(x^q - x\right),\ v := x^{2q_0+1} + y^{2q_0},\ w := xy^{2q_0} + x^{2q+2q_0} + y^{2q},$$

і порядки полюсів

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

Крива Судзукі може бути представлена в P^4 множиною точок виду

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

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

Підгрупа Вейерштрасса $H(P_\infty)$, $P \in C(F_q)$ функціонального поля кривої містить підгрупу $H(P_\infty) = \langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$.

Розроблено метод універсального гешування за раціональними функціями кривої Судзукі, який визначається побудовою базисного простору $L(\rho_k P_0)$, асоційованого з кривою Судзукі, ранжируванням раціональних функцій за зростанням полюсів $0<\rho_1<\rho_2<\ldots<\rho_k$ і обчисленням геш-значень за функціями виду $y=\sum_{i=1}^{k} f_i(P_j)m_i$.

Функціональне поле, асоційоване з кривою Судзукі над полем F_q, визначається чотирьохпараметричними функціями базису $L(kD)\,S \coloneqq \left\{x^r y^t v^i w^j\right\}$. Формула для геш-обчислень буде мати вигляд

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

де $r \le q-1,\ 0 \le t \le 1,\ i \le q_0 - 1,\ j \le q_0 - 1,$
$r \cdot q + t(q+q_0) + i(q+2q_0) + j(q+2q_0+1) \le \rho_k, \rho_k$ – полюс підгрупи Вейерштрасса $H(P_\infty)$ для слів даних $m_{i,j,t,r}$.

Гешування за раціональними функціями кривої Судзукі над полем F_q визначає універсальний геш-клас $\varepsilon - U\left(q^2, q^k, q\right)$, де q^2 – число геш-функцій (обсяг ключового простору), q^k – обсяг простору повідомлень, q – обсяг простору геш-кодів. Імовірність колізії визначається відношенням

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

$$\varepsilon = \left(k + q_0(q-1)\right)/q^2, \text{ якщо } k \ge q_0(q-1).$$

Універсальне гешування за максимальною кривою Судзукі над кінцевим полем F_{q^4} обчислюється за п’ятьма параметричними функціями базису $S \coloneqq \left\{x^a y^b v^c w^d \left(x^q + x\right)^r\right\}$. Раціональні функції шикуються за порядком зростання полюсів $f = x^a y^b v^c w^d \left(x^q + x\right)^r$. Для числа слів даних $k < q(q-1)^2$ обчислення раціональних функцій здійснюється за параметрами x, y, v, w.

Для числа слів даних $k = q_0(q-1)$ маємо оцінку ймовірності колізії гешування над полем F_{q^4}, $\varepsilon \approx 1/(q^2 q_0)$. Обгрунтовано, що гешування за кривою Судзукі над полем F_p з параметрами $p_0 = 2^s$, $p = 2p_0^{\,2}$ та $p \approx q^4$ для $k = q_0(q-1)$ слів даних має оцінку ймовірності колізії $\varepsilon \approx \rho_k / p^2 \approx 1/(q^6 q_0)$, що суттєво краще у порівнянні з гешуванням в розширеному полі F_{q^4}.

Показано, що гешування за кривою Судзукі над кінцевим полем F_q має виграш в $q^{1/6}$ раз за ймовірністю колізії і в $q^{1/2}$ раз – по числу слів даних у порівнянні з універсальним гешуванням за кривою Ерміта. Гешування за кривою з параметрами $q = 2q_0^{\,2}$ и $q_0 = 2^s$ має перевагу по ймовірності колізії, довжині даних, складності обчислень у порівнянні з гешуванням за похідними кривим Судзукі і кривої над полем четвертого ступеня розширення.

У **четвертому розділі** «Швидке універсальне гешування за кривою Судзукі» запропоновано метод універсального гешування за кривою Судзукі на основі схеми Горнера зі зменшеною складністю обчислення, метод універсального гешування з обмеженням функціонального поля за алгебричної кривої Судзукі і багатопотокове універсальне гешування.

Запропоновано метод універсального гешування за кривою Судзукі на основі схеми Горнера, який дозволяє зменшити складність обчислень і структурувати алгоритм для довільного значення. Метод визначається наступною послідовністю дій:

1) фіксується базис простору $L\left(\rho_k P_\infty\right)$, асоційований з кривою Судзукі;

2) складається масив мономів $h_{x,\,y}(m)$ для раціональних функцій в порядку зростання їх полюсів по підгрупі Вейерштрасса;

3) формуються групи мономів із загальним коефіцієнтом і поліноміальним гешуванням всередині групи по кожній раціональній функції;

4) групи мономів із загальним коефіцієнтом і поліноміальним гешуванням всередині групи об'єднуються в каскадну схему з гешуванням по одній раціональній функції;

5) на кожнім каскаді з поліноміальним гешуванням будується схема обчислення Горнера.

Застосування методу універсального гешування за кривою Судзукі над кінцевим полем F_q на основі схеми Горнера призводить до результуючої формули

$$h_{x,\,y}(m)=\sum_{i=1}^{k}\ \sum_{t=0}^{1} y^t \sum_{i=0}^{s-t} v^s \sum_{r=0}^{\min(s-t,\,q_0-t)} (x/v)^r \sum_{j=0}^{\min(s-r,\,q_0-1)} (w/v)^j,$$

де s – число рівнів для k інформаційних слів.

Швидке універсальне гешування за кривою Судзукі над полем F_{q^4} в базисі $L(kD)$ призводить до п'ятипараметричної схеми обчислення Горнера. До співвідношення для $h_{x,\,y}(m)$ слід додати зовнішню суму з індексом l і множенням на $\left(x^q + x\right)^l$.

Показано, що асимптотика оцінки складності швидкого універсального гешування за кривими Судзукі (число операцій додавань і множень в поле) дорівнює $N_{\text{îïåð}} = 2k + (3k)^{2/3}/2 + 2(3k)^{1/3} - 1$, що в два рази швидше у порівнянні з базовим методом. Простір ключів дорівнює $q^2 - 4q$. Асимптотика ймовірності колізії універсального гешування за кривою над F_q для $k < g$ при великих значеннях розмірності поля $q \to \infty$ має вигляд $\varepsilon_{q\to\infty} = (3k)^{1/2}/q$.

Геш-обчислення в проективних просторах великої розмірності призводять до структурної складності алгоритмів і складності їх практичної реалізації.

Метод універсального гешування з обмеженням функціонального поля алгебричних кривих передбачає наступний порядок дій:

– побудова алгебричної кривої χ над полем F_q, обчислення точок кривої $P_1, P_2, \ldots, P_n$;

– обчислення функціонального поля $F_q(\chi)\setminus\{0\}$, асоційованого з алгебричною кривою χ;

– обмеження функціонального поля підмножиною раціональних функцій $f_i \in G_q(\chi)$ з упорядкованими порядками полюсів;

– побудова алгоритму обчислення геш-функції на обмеженій підмножині раціональних функцій.

Універсальне гешування за кривою Судзукі над F_q, $q = 2q_0^2$, $q_0 = 2^s$ з обмеженням функціонального поля в базисі лінійного простору $L(mP_\infty) = L(\rho_l P_\infty)$, $\rho_l \le m \le \rho_{l+1}$ раціональних функцій $\left\{x^i \cdot y^j : iq + j(q + 2q_0) \le m\right\}$ визначає $U(q^2, q^k, q)$ сімейство геш-функцій з ймовірністю колізії $\varepsilon = k/(2qq_0) + s/q - s(s-1)/(4qq_0)$, якщо $\rho_k \le 2q_0(q-1)$, та складністю гешування $N_{xy} = k + s$, де k – число слів даних, $s = \left|(2k + 1/4)^{1/2} - 1/2\right|$, $\lceil\cdot\rceil$ округлення до більшого цілого числа.

Багатопотокова обробка даних будується на принципах паралелізму і визначається структурними можливостями процесорів. Для реалізації потокового обчислення слід структурувати алгоритм так, щоб з'явилась послідовна ділянка, що допускає розпаралелювання. Показано, що застосування методу швидкого універсального гешування за кривою Судзукі на основі схеми Горнера дозволяє це зробити. На кожнім каскаді реалізується обчислення поліноміального виду $y = \sum_{i=1}^{n} m_i x^i$. В загальному випадку поліноміальний вираз можна представити за допомогою p однорідних груп. Геш-обчислення в кожній підгрупі можна виконати паралельно з об'єднанням результатів на другому каскаді:

$$y = \sum_{j=0}^{p=1} x^{nj/p} \sum_{i=1}^{n/p} m_{i+jn/p} x^i .$$

На першому каскаді обчислення геш-функції $\sum_{i=1}^{n/p} m_{i+jn/p} x^i$ можна здійснити за ітераційною схемою Горнера, з однією операцією множення і складання в кінцевому полі. Застосування до поліноміальних обчислень за

кожною сумою ітераційної схеми Горнера зі складністю $k/p+p$ практично в p раз підвищує швидкодію поліноміального гешування.

У **п'ятому розділі** «Розробка методу багатокаскадного універсального гешування за кривої Судзукі» представлено метод багатокаскадного універсального гешування за раціональними функціями кривої Судзукі, виконана оцінка параметрів багатокаскадного універсального гешування за алгебричними кривими, порівняння за обчислювальними витратами, витратами ключа складності обчислення точок алгебричних кривих, надані практичні рекомендації. Розглянуто багаторазове каскадне універсальне гешування за алгебричними кривими, універсальне гешування за раціональними функціями алгебричних кривих і композиційне універсальне гешування з оцінкою параметрів. Параметри багатокаскадного універсального гешування за алгебричними кривими представлено в табл. 4.

Таблиця 4 – Параметри багатокаскадного універсального гешування за алгебричними кривими

Схеми каскадного включення	Параметри універсального гешування	Оцінки складності обчислень
$Ch_t(M)$, $PSh_q - PSh_q$	$\varepsilon - U\left(q^2, q^k, q\right)$, $\varepsilon = k^{1/2}/q,\ 0 < k \le q^2$	$k + k^{1/2}$
$Ch_t(M)$, $PSh_q - Hh_q$	$\varepsilon - U\left(q^2\sqrt{q}, q^k, q\right)$, $\varepsilon = (2k)^{1/3}/q,\ 0 < k \le q\sqrt{q}/2$	$k + k^{2/3}/2^{1/3} + k^{1/3}/2^{1/6}$
$Ch_t(M)$, $PSh_q - Sh_q$	$\varepsilon - U\left(q^3, q^k, q\right),\ \varepsilon = (3k)^{1/4}/q,$ $0 < k \le q^2$	$k + 1,52k^{3/4} + 0,87k^{1/2} + 2,63k^{1/4}$
$Ch_t(M)$, $Hh_q - Sh_q$	$\varepsilon - U\left(q^3\sqrt{q}, q^k, q\right)$, $\varepsilon = 1,43k^{1/5}/q, 0 < k \le q^2\sqrt{q}$	$k + k^{4/5} + 2k^{3/5} + k^{2/5} + 2,88k^{1/5}$
$l - Ch_t(M)$, $PSh_q - PSh_q - \ldots$	$\varepsilon - U\left(q^l, q^k, q\right)$, $\varepsilon = k^{1/l}/q, 0 < k \le q^l$	$k + k^{l-1/l} + k^{l-2/l} + \ldots + k^{1/l}$
$l - Ch_t(M)$, $Hh_q - Hh_q - \ldots$	$\varepsilon - U\left(q^{l+l/2}, q^k, q\right)$, $\varepsilon = \sqrt{2k^{1/l}}/q,\ 0 < k \le q^l$	$k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} +$ $+ \ldots + k^{1/l} + k^{1/2l}$
$l - Ch_t(M)$, $Sh_q - Sh_q - \ldots$	$\varepsilon - U\left(q^{2l}, q^k, q\right), \varepsilon = \sqrt[3]{3}k^{1/3l}/q,$ $0 < k \le q^{l+l/2}$	$2k + 1,04k^{(3l-1)/3l} + 2,88t^{(3l-2)/3l} +$ $+ 2k^{(l-1)/l} + 1,04k^{(3l-4)/3l} + 2,88k^{(3l-5)/3l} + \ldots$

$*$ PSh_q, Hh_q, Sh_q – гешування за прямою, кривими Ерміта і Судзукі відповідно.

Метод каскадного гешування за алгебричними кривими $Ch_t(M)$ на основі добутку функціональних полів визначається розбиттям даних на t блоків однакової довжини з реалізацією універсального гешування на кожнім блоці по функціональному полю, асоційованому з кривою. Вибір універсального гешування для кожного каскаду визначається рішенням завдання мінімізації ймовірності колізії і складності обчислень при гешуванні заданого числа слів даних за рахунок оптимізації вибору числа каскадів і базисних функцій алгебричних кривих. Для двохкаскадної схеми маємо конструкцію гешування у вигляді

$$Ch_t(M) = AGh_2\left(Agh_1(M_1)\|AGh_1(M_2)\|\ldots\|AGh_1(M_t)\right),$$

де Agh_1, AGh_2 – універсальні схеми гешування за алгебричними кривими, $Ch_t(M)$ визначає універсальне сімейство геш-функцій $\varepsilon - AU$, де $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/|H^2|$, $\varepsilon_1, \varepsilon_2$ – відповідно ймовірності колізій для ADh_1 і AGh_2 гешування.

Оцінки ймовірності колізії і складності обчислень для багатокаскадного гешування в кінцевому полі представлені в табл. 5.

Таблиця 5 – Оцінки ймовірності колізії і складності обчислень для багатокаскадного гешування за алгебричними кривими над полем F_q

Схеми каскадів	F_q	Імовірність колізії для даних розміром L / складність обчислень			Розмір ключів (біт)	Розмір геш-кода (біт)
		1 Кбт	1 Мбт	1 Гбт		
$Ch_t(M)$, $PSh_q - PSh_q$	$q = 2^{32} - 99$	$2^{-28} / 2^8+2^4$	$2^{-23} / 2^{18}+2^9$	$2^{-18} / 2^{28}+2^{14}$	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

Оцінки ймовірності колізії і складності обчислень для кратного гешування представлені в табл. 6.

Таблиця 6 – Оцінки ймовірності колізії і складності обчислень для багаторазового гешування за алгебричними кривими над полем F_q

Рівняння кривої над F_q	t	Імовірність колізії для даних розміром L / складність обчислень			Розмір ключів (біт)	Розмір геш-кода (біт)
		1 Кбт	1 Мбт	1 Гбт		
Проективна пряма $X+Y+Z=0$ $q=2^{32}-99$	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
Крива Ерміта $y^{\sqrt{q}}+y=x^{\sqrt{q}+1}$ $\sqrt{q}=2^{16}+1$	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
Крива 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

ВИСНОВКИ

Дисертаційна робота присвячена вирішенню наукової задачі – розробці методу універсального гешування за раціональними функціями алгебричної кривої Судзукі для побудови доказово стійкої автентифікації повідомлень з гарантованою ймовірністю колізії та мінімізацією витрат на ключовий простір і складність обчислень.

Запропоновано метод універсального гешування за раціональними функціями кривої Судзукі, який дозволяє зменшити ймовірність колізії пропорційно кореню шостого ступеня від розмірності поля обчислення і збільшити максимальну довжину даних, що гешуються, в корінь квадратний від розмірності поля обчислення в порівнянні з гешуванням за кривою Ерміта. В порівнянні з гешуванням за похідними кривими Судзукі і іншими

розширеннями кінцевого поля гешування за кривою над полем F_q є абсолютно кращим.

Запропоновано метод обчислення геш-функцій за кривою Судзукі на основі багатопараметричної схеми Горнера, який призводить до чотирьохпараметричної схеми обчислень та дозволяє зменшити складність обчислення в два рази у порівнянні з базовим методом. Чотирьохпараметричне геш-обчислення визначає найменшу складність обчислень для схем гешування по функціональному простору похідних кривих Судзукі.

Набув подальшого розвитку метод універсального гешування з обмеженням функціонального поля алгебричних кривих за раціональними функціями, який, на відміну від відомих, використовує обчислення геш-функцій по підмножині раціональних функцій з впорядкованими порядками полюсів, що дозволило зменшити складність обчислень пропорційно підмножині використовуваних для гешування раціональних функцій.

Набув подальшого розвитку метод каскадного універсального гешування на основі добутку функціональних полів, який, на відміну від відомих, передбачає застосування гешування в каскаді за кривою Судзукі, що дозволило зменшити ймовірність колізії в корінь ступеня числа, яке визначається кількістю каскадів від кореня кубічного числа слів даних, і збільшити розмір даних, що гешуються.

Практичне значення результатів дисертаційної роботи полягає в оцінці алгеброгеометрічних параметрів кривих Судзукі над кінцевими полями, побудові алгоритму гешування за кривою Судзукі, розробці практичних рекомендацій для універсального гешування за кривою Судзукі в схемах багаторазового, багатокаскадного, композиційного гешування доказово стійкої і безумовної автентифікації повідомлень, розробці програмних засобів для побудови кривих, обчислень їх точок і властивостей (кратності), моделювання лінійного базисного простору з раціональними функціями кривих і статистичного оцінювання ймовірності колізії гешування шляхом обчислення кратності перетину гіперповерхонь лінійного простору з точками кривої.

Результати роботи впроваджено в дослідницьких і конструкторських роботах в НТК ДП «Імпульс», в навчальний процес Харківського національного університету радіоелектроніки.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Халимов Г.З. Стойкий к коллизиям алгоритм WHIRLPOOL / Г.З. Халимов, Е.В. Котух // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – Київ, 2005. – № 10. – С. 159-165.

2. Халімов Г.З. Аналіз безпеки MAC-алгоритмів стандарту ISO/IEC 9797-2 / Г.З. Халімов, О.В. Потій, О.В. Дунь, Є.В. Котух // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2007. – Вип. 1(14). – С. 99-105.

3. Горбенко И. Д. Анализ безопасности международного стандарта ISO/IEC 9797-1 / И. Д. Горбенко, А. В. Потий, Е. В. Котух, А. В. Дунь // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 250-256.

4. Халимов Г. З. Универсальное хеширование по кривой Судзуки / Г.З. Халимов, Е.В. Котух // Прикладная радиоэлектроника. – 2011. – Т. 10. – № 2. – С. 164-170.

5. 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.

6. 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.

7. Котух Е. В. Универсальное хеширование с ограничением функционального поля алгебраических кривых // Радиотехника. – 2012. – Вып. 171. – С. 109-115.

8. 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 .

9. Котух Е.В. Скоростное универсальное хеширование на основе многопотоковых вычислений / Е.В. Котух, В.М. Карташов, Д.П. Цапко, О.Г. Халимов, А.В. Самойлова // Захист інформації. – 2015. – Т. 17. – № 2. – 181-188 с.

10. 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.

11. Котух Е.В. 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.

12. Халимов Г.З. Каскадное универсальное хеширование / Г.З. Халимов, А.А. Бойко, Е.В. Котух // Сб. тр. Второй Междунар. науч.-техн. конф. «Компьютерные науки и технологии КНиТ-2011». – Белгород, 2011. – С. 541-544.

13. Котух Е.В. Метод универсального хеширования по алгебраическим кривым / Е.В. Котух, Г.З. Халимов, А.А. Бойко, А.В. Герцог // XV Междунар. науч.-практ. конф. «Безопасность информации в информационно-телекомуникационных системах», Киев, 22–25 мая 2012 г. : тезисы докладов. – Киев, 2012. – С. 36.

14. 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.

15. 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. 60-61.

16. Котух Е. В. Оценка параметров композиционного универсального хеширования по кривым Судзуки / Е. В. Котух // Праці студентської наук. конф. фізико-технічного факультету. – ДонНУ, 2015. – С. 73-74.

АНОТАЦІЯ

Котух Є.В. Методи та засоби універсального гешування за алгебричними кривими Судзукі. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2016.

Дисертаційна робота присвячена вирішенню важливої науково-технічної задачі, яка полягає в розробці методу та засобів універсального гешування за раціональними функціями кривих Судзукі для побудови доказово стійкої автентифікації із забезпеченням гарантованої ймовірності колізії зі зменшеною складністю обчислення.

Розроблено метод універсального гешування за раціональними функціями кривої Судзукі та метод обчислення геш-функцій за кривою Судзукі на основі багатопараметричної схеми Горнера. Побудовано функціональні поля кривих, що асоційовані з підгрупами групи Судзукі над кінцевим полем довільного ступеня розширення. Отримано оцінки алгеброгеометричних параметрів кривих Судзукі над кінцевими полями. Отримано оцінки універсального гешування за кривою Судзукі, складності обчислення геш-коду, ключові витрати.

Набув подальшого розвитку метод універсального гешування з обмеженням функціонального поля за раціональними функціями алгебричних кривих та метод каскадного універсального гешування на основі добутку функціональних полів.

Ключові слова: гешування універсальне, гешування багатокаскадне, криві Судзукі, поля кінцеві, Горнера схема, функції раціональні.

АННОТАЦИЯ

Котух Е.В. Методы и средства универсального хеширования по алгебраическим кривым Судзуки. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. – Харьковский национальный университет радиоэлектроники, Министерство образования и науки Украины, Харьков, 2016.

Диссертация посвящена решению важной научно-технической задачи, которая заключается в разработке метода и средств универсального хеширования по рациональным функциям кривых Судзуки для построения доказуемо стойкой аутентификации с обеспечением гарантированной вероятности коллизии с уменьшенной сложностью вычисления.

Разработаны метод универсального хеширования по рациональным функциям кривой Судзуки и метод вычислений хеш-функций по кривой Судзуки на основе многопараметрической схемы Горнера. Построены функциональные поля кривых, ассоциированные с подгруппами группы Судзуки над конечным полем произвольной степени расширения. Получены оценки алгеброгеометрических параметров кривых Судзуки над конечными полями. Получены оценки универсального хеширования по кривой Судзуки, сложности высчисления хеш-кода, затраты на ключ.

Получили дальнейшее развитие метод универсального хеширования с ограничением функционального поля по рациональным функциям алгебраических кривых и метод каскадного универсального хеширования на основе произведения функциональных полей.

Ключевые слова: хеширование универсальное, хеширование многокаскадное, кривые Судзуки, поля конечные, Горнера схема, функции рациональные.

ABSTRACT

Kotukh Y.V. Methods and means of universal hashing by algebraic Suzuki curves. – As the Manuscript.

Thesis for scientific degree of candidate of technical sciences, major is 05.13.21 – Systems of information security. – Kharkiv National University of Radio Electronics, Ministry of Education and Science of Ukraine, Kharkiv, 2016.

The thesis is devoted to solution of important scientific and technical problem, which consists in the development of the methods and means of universal hashing by the rational functions of Suzuki curves to build authentication scheme with provable security to ensure the guaranteed probability of collision with reduced computational complexity.

Method of universal hashing based on rational functions of the Suzuki curve and the method of hash function computing based on Horner multiparameter scheme were developed. Functional field for curves associated with subgroups of the Suzuki group over the finite field with arbitrary power of expansion was built. The parameters of algebraic Suzuki curves over finite fields were estimated. The complexity of hash code computing and key space cost for universal hashing on Suzuki curve were obtained.

Method of universal hashing with Suzuki functional field limitation and method of bucket hashing based on function fields product were further elaborated.

The main solution for building authentication with proven security is the universal hashing by a linear vector space of Riemann – Roch, built on the rational

functions of the functional field associated with the algebraic curve in the projective manifold of diversity points. The likelihood of the confusion is associated with the length of the message, the key and the field of hash computing, and the function field of the algebraic curve. The key space was determined by the number of points of algebraical curve. The choice of the algebraic curve and the functional field associated with makes it possible to optimize the authentication costs. The best result was obtained with respect to the values of the pole of the rational functions to the power of curve points for the Suzuki curves.

The functional fields of curves, associated with subgroups of the Suzuki group over a finite field of an arbitrary power of expansion, were considered to take advantage of the universal hashing by the constructions with the algebraic curves. It made it possible to develop the method of the universal hashing functions by the rational functions of the Suzuki curve. The method was developed for fast hashing on the Suzuki curve based on the multivariate Horner scheme to solve the problem of constructing a hash algorithm. The estimates of the universal hashing by the Suzuki curve, the probability of a conflict, the complexity of computing the hash code, the key space costs were received.

The method was further developed for the bucket universal hashing based on the product of the functional fields, which was determined by dividing the data into blocks of equal length with the implementation of the universal hashing at each level of the blocks over the functional field associated with the curve. Selection of the universal hashing for each cascade was determined by the solution to the problem of minimizing the probability of a collision and computational complexity when hashing a given number of words of data at the expense of optimizing the choice of the number of cascades and the basic functions of the algebraic curves.

Practical results consist in the evaluation of algebro-geometric parameters of the Suzuki curves over the finite fields, building the hash algorithm on the Suzuki curve, the development of practical recommendations for the universal hashing by the Suzuki curve in the shemes of the multiple, multicascade, composite hashing provably resistant and unconditional message authentication, the development of software tools for constructing curves, computing of their points and characteristics (multiplicity), modeling of the linear basis space with rational functions of curves and for statistical estimation of the probability of collisions of the hash by computing multiplicity of intersection of hypersurfaces of the linear space with points of the curve.

Key words: universal hashing, bucket hashing, Suzuki curves, finite fields, Horner scheme, rational function.

Підписано до друку 03.10.2016. Формат 60×84 1/16.
Папір офсетний. Друк цифровий.
Ум. друк. арк. 0,9. Наклад 100 примірників.
Замовлення №1408.

Надруковано у друкарні ФОП Тарасенко В. П.
Свідоцтво № 24800170000043751 від 21.02.2002 р.
61124, м. Харків, вул. Зернова, 6/267.
Тел./факс: (0572) 52-82-11, (097) 273-11-77