УДК 621. 3.06

В.И. ДОЛГОВ, д-р техн. наук, И.В. ЛИСИЦКАЯ, д-р техн. наук, К.Е. ЛИСИЦКИЙ

НОВАЯ КОНЦЕПЦИЯ ПРОЕКТИРОВАНИЯ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Введение

В первой части работы представлены результаты, связанные с изучением истоков современных наиболее перспективных разработок и решений по построению блочных симметричных шифров, с анализом и освоением идей и принципов, использованных при их построении, позволивших признать эти решения лидерами современных технологий блочного симметричного шифрования.

В числе лидеров технологий блочного симметричного шифрования, как отмечено в [1], можно назвать две разработки: шифр Rijndael, ставший победителем конкурсов AES и NESSIE [2], и шифр IDEA NXT, родившийся на основе шифра IDEA (International Data Encryption Algorithm – Международный алгоритм шифрования данных [3]), разработанного в свое время в качестве предлагаемого стандарта шифрования [4]. В книге Б. Шнаера [5] отмечается, что в основе алгоритма IDEA лежат некоторые впечатляющие теоретические положения, и, по его мнению, IDEA является самым лучшим и надежным блочным алгоритмом, опубликованным к моменту написания им книги.

Компания MediaCrypt AG – собственник технологии IDEA NXT – считает, что IDEA NXT является семейством блочных симметричных алгоритмов шифрования следующего поколения, что и определило включение этого семейства шифров в круг перспективных разработок.

Остановимся также на трех последних разработках по построению блочных шифров: шифре «Мухомор», разработанном сотрудниками ИИТ (г. Харьков), блочном шифре из белорусского стандарта СТБ 34.101. 31-2011, появившемся сравнительно недавно, и новом стандарте блочного симметричного шифрования Украины.

Сегодня, оглядываясь на прошедший период освоения технологий блочного симметричного шифрования, связанных с Rijndael и IDEA NXT, можно отметить, что уже накопился критический материал, позволяющий считать, что не все решения, использованные разработчиками Rijndael и IDEA NXT, являются самыми совершенными. Формулируется новая, на взгляд авторов, (уточненная) концепция проектирования блочных симметричных шифров.

Во второй части работы предложена конструкция шифра, построенного в соответствии с предлагаемыми новыми принципами проектирования, приведены результаты анализа динамических показателей прихода нового шифра к состоянию случайной подстановки. За основу принят новый подход к оценке стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, развитый в последнее время в работах И.В. Лисицкой и В.И. Долгова. Показано, что существующая концепция проектирования и разработки блочных симметричных шифров может быть уточнена и доработана (пересмотрена).

1. Современные методы проектирования БСШ

AES – передовой стандарт 21-го века. Шифр Rijndael считается последним достижением в технологиях проектирования и разработки блочных симметричных шифров. Уместно напомнить мысли, представленные в работе Susan Landau [6], посвященной изучению алгебраических аспектов разработки Rijndael (AES).

В цитируемой работе внимание сосредоточено как раз на проектировании блочных шифров. Автор прослеживает пути, которые привели к шифру Rijndael, который считается

последним словом в проектных и конструкторских решениях. Акцентируется, что эта разработка стала закономерным итогом развития мировой криптографической мысли.

Так, в [6] отмечается ряд работ и предложений, выполненных на пути к Rijndael. Напомним их здесь.

Willi Meier и Othmar Staffelbach предположили, что определенные примеры нелинейностей, используемых математиками, могут подходить для криптографического системного проекта [7]. Основываясь на этих идеях, Josef Pieprzyk предложил алгебраические методы для строительства нелинейных функций [8, 9]. Kaisa Nyberg исследовала S-блоки и применила некоторые из идей Pieprzyk при проектировании S-блоков [10]. Joan Daemen изучил цикловые функции с точки зрения дифференциального и линейного криптоанализа шифра и предложил новую парадигму – подход широкого следа [11]. С другими исследователями он использовал широкий след и S-блоки Nyberg в криптосистеме SHARK [12]. Thomas Jakobsen и Lars Knudsen нашли «интерполяционную атаку» против простых алгебраических шифров, таких как SHARK [13]. Двум разработчикам SHARK Daemen и Vincent Rijmen противопоставили криптосистему Square [14]. Knudsen взломал Square, используя различные атакующие методы [14]. Rijndael, отмечает автор цитируемой работы, поднялся из праха Square. Далее в работе отслеживается, как эти нити ткали Rijndael.

При анализе методов проектирования Rijndael значительное внимание уделено новой парадигме, подходу, считающемуся развитым Joan Daemen и получившему название стратегии широкого следа.

Говоря о стратегии широкого следа, Susan Landau отмечает, что криптоанализ выполнить легче всего, когда в каждом цикле активен единственный (один) S-блок. Поэтому проектировщик криптографического алгоритма должен стремиться избежать худшего случая диффузии, когда встречается единственный активный S-блок. Очевидно, лучшее, что может быть сделано проектировщиком, с точки зрения достижения верхней границы, – это чтобы число ветвлений $\mathcal{B}$[1] было равно $n + 1$, где n – число связок (каждая связка состоит из m битов). Обратимое линейное отображение, которое достигает этого эффекта, названо оптимальным. Daemen и Rijmen удалось построить такое отображение. Они показали, что сепарабельные коды с максимальным минимальным расстоянием обеспечивают путь строительства таких оптимальных линейных преобразований. Это отображение оказалось существенно эффективнее многих других используемых в шифрах линейных преобразований. В последнее время найден путь реализации стратегии широкого следа и без сепарабельных кодов [15].

Цели проекта Rijndael. Заслуживают внимания также цели проекта Rijndael в интерпретации Susan Landau. Для проектировщиков Rijndael безопасность была основным выбором, эффективность была вторым беспокойством, отмечает она. Daemen и Rijmen искали простоту – простоту спецификации и простоту анализа [16, с. 65]. Не каждый криптограф видит простоту как важную цель. Два финалиста AES, MARS и Twofish имеют намного более сложные проекты (некоторые наблюдатели посчитали, что эта сложность стала частью причин, по которым эти два алгоритма не были выбраны как Продвинутый Стандарт Шифрования, поскольку их цикловые функции были просто трудными, чтобы их проанализировать полностью). Стратегия широкого следа – простая парадигма, чтобы защититься от атак дифференциального и линейного криптоанализа. Во всех вариантах алгоритмов, которые применяли эту стратегию – SHARK, Square и Rijndael, Daemen и Rijmen использовали простые примитивы. Таким образом, шаг Square для доказательства достаточности оказался не совсем хорошим, транспозиция была естественным и простым путем осуществить смешивание колонок. В Rijndael, следующем экземпляре широкого следа, этот шаг был заменен перестановкой строк, немного более сложной функцией, которая позволяет достигнуть цели.

[1] число ветвлений $\mathcal{B}$ ($\mathcal{B}_L$ –линейное и $\mathcal{B}_D$ – дифференциальное) – нижняя граница для числа активных S-блоков в смежных циклах для дифференциальной или линейной характеристики.

Простота порождает другие критерии, в том числе симметрию. Rijndael обладает симметрией между циклами и в пределах их.

Daemen и Rijmen, пишет Susan Landau, имели незаявленную цель в разработке своего алгоритма: прозрачность. Они не захотели, чтобы имелись подозрения о наличии в шифре лазеек. Многочлен, определяющий поле, – первый в таблице неприводимых полиномов в поле $GF(2^8)$ Lidl и Niederreiter [17]. В использованном открытом списке выбора параметров проектировщики Rijndael показали, что у них нет ничего в запасе. Простота $x^8 + 1$ и $x^4 + 1$ – другая демонстрация отсутствия скрытых параметров.

Daemen и Rijmen предпочли, чтобы перемешивание столбцов (колонок), было обратимым и линейным в поле $GF(2)$, и чтобы диффузия была хорошей и в то же время, чтобы оно было быстрым на восьмиразрядных процессорах. Многочленное умножение удовлетворяет обратимости, линейности в $GF(2)$ и простоте для описания – это было естественным выбором. Получение мультипликативных коэффициентов в $GF(2^8)$ быстрее всего на восьмиразрядных процессорах. Соответственно умножение на полином $3x^3 + x^2 + x + 2$ работает хорошо, отмечает Susan Landau. Многочлены $x^7 + x^6 + x^2 + x$, $x^7 + x^6 + x^5 + x^4 + 1$ и $3x^3 + x^2 + x + 2$ не имеют элегантного объяснения для выбора полиномов $x^8 + 1$ и $x^4 + 1$. Тем не менее, аргументы – самый "простой среди всех многочленов, взаимно простых с модулем", и "линейный в $GF(2)$), сильно разреженный, быстро реализуемый на восьмиразрядных процессорах" – делают ясным, что ничего скрытого здесь также нет.

Проектировщики Rijndael достигли эффективности. Алгоритм оказался значительно быстрее, чем все другие финалисты в ключевых настройках, и был посередине пакета для шифрований.

Расшифрование для Rijndael оказалось более медленным, потому что ключевая настройка берет больше времени, но замедление не чрезмерное. Анализ Агентства национальной безопасности аппаратных выполнений показал, что Rijndael является разумным и по его макетному размеру, и по имеющейся превосходной "производительности" (объему работы, проделанной в течение определенного периода) [18].

Daemen и Rijmen удалось создать конструкцию, которая сумела завоевать доверие и поддержку большинства экспертов и специалистов мирового уровня.

Конечно, заслуживает безусловного одобрения и поддержки принципы проектирования, примененные разработчиками AES, такие как:

- простота спецификации и простота анализа;
- прозрачность использованных решений;
- эффективность.

IDEA NXT – новый подход в технологиях блочного симметричного шифрования. Еще одно направление развития технологий блочного симметричного шифрования, которое заслуживает отдельного внимания, – это так называемое "гибкое шифрование", появившееся в связи с разработками, связанными с шифром FOX, задуманном в период 2001 – 2003 гг. и опубликованном в 2004 г. [19]. Этот шифр стал усовершенствованием европейского стандарта IDEA, который уже прошел значительный период испытаний временем и обеспечил в течение всего этого периода задекларированный уровень стойкости. В мае 2005 г. шифр FOX был анонсирован компанией MediaCrypt под названием IDEA NXT. Здесь вспоминаются результаты обсуждения особенностей этого предложения, представленные в работе [20].

Сегодня, отмечается в этой работе, IDEA NXT выступает как универсальное семейство алгоритмов блочного симметричного шифрования, которое обеспечивает защиту электронных сред, данных, которые передаются в телекоммуникационных системах, и хранящихся данных. Семейство представлено набором двух модификаций шифров с различными размерами шифруемых блоков и ключей: Standard NXT64 (64-битный блок, 128-битный ключ, 12 раундов шифрования) и Standard NXT128 (128-битный блок, 256-битный ключ, 12 раундов шифрования). Могут также быть построены версии Standard с размерами ключей от двух до

256 бит и числами циклов от 2 до 255. В шифрах предусмотрена загрузка индивидуальных таблиц (S-блоков и перестановочных матриц) для замены стандартных.

Главными особенностями (свойствами) этой разработки, как отмечается в публикациях, является высокий уровень защиты, высокая эффективность и беспрецедентный уровень гибкости реализации.

Как заявляет компания-собственник разработки, IDEA NXT имеет способность применения в динамической системе обновления, в результате чего защита может переустанавливаться после успешной атаки. Такая система позволяет пользователям (собственникам) и операторам осуществлять быстрое возвращение в нормальное рабочее состояние и продолжать поддерживать рентабельное производство без необходимости выполнения трудоемкого аппаратного свопинга. IDEA NXT характеризуется гибким и масштабированным диапазоном операционных режимов, что позволяет динамично оптимизировать компромисс между эффективностью и безопасностью с одновременной поддержкой согласованности и эффективной функциональности в широком разнообразии устройств.

Математическая структура разработки построена на базе схемы X. Lai и J. Massey. В качестве табличных преобразований используются раундовые (цикловые) функции и элементы Замены-Перестановки (SPN). Кроме того, разработана новая структура стойких и эффективных алгоритмов разворачивания ключей.

IDEA NXT обеспечивает необходимый уровень управления настройками, включая простое и надежное создание уникальных собственных версий алгоритмов. Такие версии создают дополнительную степень защиты для применений, которые требуют особенной обработки.

Кроме того:

- стандарт допускает эволюционную миграцию с существующими алгоритмами, такими как IDEA, AES и 3DES;
- настраиваемость позволяет заказчикам выбирать размеры ключей, число раундов для достижения компромиссного решения между эффективностью и степенью защищенности;
- заказной характер обеспечивает достижение максимального уровня защиты, с выдачей гарантийных уникальных таблиц, на базе которых создается собственный алгоритм;
- индивидуализация способствует адаптации IDEA NXT продукта к целевым процессорам или к заказанным сервисным требованиям.

Таким образом, судя по заявлениям компании-собственника разработки, предлагаемая технология обладает следующими преимуществами:

- высокий уровень защиты;
- высокая эффективность;
- гибкость и масштабируемость;
- разнообразие в применениях;
- динамическое обновление;
- настраиваемость для разных приложений;
- эволюционную миграцию с существующими алгоритмами;
- правовую защиту.

Уместно напомнить три конструкции блочных симметричных шифров, появившиеся в последние годы, которые можно рассматривать как развитие рассмотренных выше подходов.

Шифр «Мухомор» [21] разработан для украинского конкурса Институтом Информационных Технологий (ИИТ, г. Харьков). Он тоже построен на основе схемы X. Lai и J. Massey. В этом шифре в функциях усложнения, как и в шифрах серии IDEA NXT также используется дополнительный слой S-блоков (SL преобразований) цикловой функции. За счет использования управляемых SL преобразований шифр приходит к случайной подстановке по дифференциальным и линейным показателям за два цикла. С применением управляемых SL преобразований удается сделать активными все S-блоки второго слоя SL преобразований. Описание этой разработки приведено далее.

Шифр из белорусского стандарта СТБ 34.101. 31-2011 [22]**.** Этот шифр относится к последним («свежим») разработкам. Его особенностью является также увеличенное число S-блоков, используемых в каждой цикловой функции и уменьшенное по сравнению с традиционными подходами к построению блочных шифров число циклов зашифрования (восемь). Для 128-битного шифра в каждом цикле используются 28 S-блоков. Шифр построен по не традиционной SPN схеме. В нем применяются вложенные многомодульные фестель подобные преобразования 32-битных слов с различными сдвигами слов на выходах линеек байтовых S-блоков. Можно искать недостатки в этом шифре в сложности его анализа (отсутствии прозрачности) и усложненной спецификации, но он получился эффективным по динамическим показателям (становится случайной подстановкой на втором цикле). Заслуживает одобрения и простая схема формирования подключей зашифрования этого шифра.

Шифр Калина-2. Шифр Калина-2 принят в этом году в качестве национального стандарта Украины [23]. Это Rijndael подобный шифр. Основные его отличия от шифра Rijndael состоят в том, что в нем выполняется умножение выходов восьмерок байтовых S-блоков на МДР матрицы размером 8×8. Сами S-блоки здесь взяты случайно сгенерированными с последующим дополнительным отбором. Кроме того, ключ забеливания и сложение с последним цикловым подключом выполняется по модулю 2^{64}. В шифре применена также усовершенствованная схема формирования цикловых подключей. Позднее остановимся на свойствах отмеченных шифров более обстоятельно.

Представленный обзор принципов построения современных шифров позволяет выделить следующие существенные результаты [24]:

1. Безусловным достижением современных конструкторских решений по построению шифров следует считать реализацию стратегии широкого следа, строящуюся на основе матричного умножения в расширениях полей.

2. Заслуживают одобрения и поддержки принципы проектирования, примененные разработчиками AES, такие как:

- простота спецификации и простота анализа;
- прозрачность;
- эффективность.

3. Пропагандируемая новая концепция гибкого шифрования безусловно является шагом вперед в технологиях блочного симметричного шифрования и при желании легко может быть реализована с использованием многих других разработок, а не только с помощью семейства шифров IDEA NXT.

4. Приведенные в публикациях подходы и результаты оценки показателей стойкости шифров к атакам дифференциального и линейного криптоанализа являются приближенными и нуждаются в уточнении.

5. Сегодня уже существует подход, позволяющий вычислительным путем определить точные показатели стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. В соответствии с этим подходом отмеченные здесь шифры семейства IDEA NXT по своим показателям стойкости находятся на уровне показателей стойкости, реализуемых многими другими шифрами. Тем не менее, рассмотренная разработка, так же как и шифр Калина-2, в этом отношении имеет некоторое преимущество по сравнению со многими другими (здесь имеются в виду Rijndael и шифры, представленные на украинский конкурс). В трех отмеченных разработках удается реализовать динамические показатели прихода шифра к состоянию случайной подстановки, уменьшенные на один цикл по сравнению с другими известными решениями.

6. Структура X. Lai и J. Massey (архитектура верхнего уровня) не создает сколько-нибудь ощутимых преимуществ по сравнению с конструкцией цикловой функции, примененной в шифре Калина-2.

7. В последних разработках просматривается стремление улучшить динамические характеристики прихода к установившимся (стационарным) значениям максимумов полных

дифференциалов и линейных корпусов на основе увеличения числа S-блоков, используемых в цикловых функциях, и создания механизмов увеличения минимального числа активизируемых S-блоков первого цикла. Это позволило привести лавинные показатели шифров последних разработок к глубине лавинного эффекта до двух циклов.

Далее приведены предложения, направленные на дальнейшее совершенствование технологий проектирования и разработки блочных симметричных шифров.

2. Результаты анализа проектных решений шифров Rijndael и IDEA NXT

Прежде всего, следует обратить внимание на то, что, несмотря на прогрессивность решений, принятых разработчиками рассмотренных шифров, в них реализованы далеко не все потенциальные возможности обеспечения эффективности выполнения начальных цикловых преобразований. Так, по динамическим показателям прихода шифра Rijndael к случайной подстановке он становится случайной подстановкой по дифференциальным показателям на третьем цикле, а по линейным показателям – лишь на четвертом. Это связано с тем, что при активизации одного байта входа в цикловую функцию активизируется лишь один S-блок, который на втором цикле активизирует четыре S-блока, и на третьем цикле активизируются уже все 16 S-блоков. В результате на трех циклах получается активным минимум 21 S-блок, что позволяет по дифференциальным показателям прийти шифру к состоянию случайной подстановки на третьем цикле [24]. Для прихода шифра к состоянию случайной подстановки по линейным показателям ему необходим дополнительный четвертый цикл [25].

При активизации же четырех байтов входа минимальное число активизируемых S-блоков первого цикла равно четырем. МДР преобразование, хоть и с весьма малой вероятностью, переводит результат в один активный байт на выходе МДР преобразования и в результате на втором цикле активизируется один S-блок, который на следующем цикле активизирует четыре S-блока, и активизации 16 S-блоков можно ожидать лишь на четвертом цикле. Приходим к выводу, что и в этом случае шифр Rijndael и по дифференциальным и по линейным показателям приходит к случайной подстановке на четвертом цикле. Таким образом, стратегия широкого следа, реализованная в шифре Rijndael, имеет слабость (происходит активизация лишь части S-блоков первого цикла), приводящую к затягиванию процесса перехода шифра к состоянию случайной подстановке.

К наиболее прогрессивным из рассмотренных конструкций можно отнести шифры Калина-2, «Мухомор» и шифр из белорусского стандарта. Эти шифры реализуют показатели прихода к состоянию случайной подстановки, близкие к предельным.

Напомним теперь, что в соответствии с новой методологией оценки показателей доказуемой стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, предложенной в последнее время [1, 24], все шифры (в том числе и Rijndael) асимптотически становятся случайными подстановками, и их стойкость не связана со свойствами S-блоков, входящих в шифр. S-блоки влияют (не всегда) лишь на динамику прихода шифра к состоянию случайной подстановки (на число циклов необходимых шифру для прихода по дифференциальным и линейным показателям к показателям случайной подстановки).

Отметим далее, что в ходе разработки новой методики оценки стойкости блочных симметричных шифров был введен дополнительный показатель эффективности шифрующих преобразований в виде числа циклов, требующихся для прихода шифра к состоянию случайной подстановки [24]. Тот шифр полагается более совершенным, для которого число циклов прихода к случайной подстановке оказывается меньшим.

Обратим здесь внимание также на практику проектирования современных шифров – число циклов шифрования в них выбирается в три-четыре раза превосходящим число циклов, требующихся для прихода шифра по дифференциальным и линейным свойствам к показателям случайной подстановки (запас стойкости).

Для конкурса AES в соответствии с его требованиями авторы зафиксировали длину шифруемого блока 128 битами (в виде квадрата размером 4×4 байта) и для 128-битного ключа количество раундов шифра взято равным 10, т.е. на грани запаса стойкости. Использование S-блоков с худшими дифференциальными и линейными показателями выводит шифр за границы установленного запаса стойкости. Увеличение длины входного блока и ключей приводит к решениям с увеличенным числом циклов шифрования (12 и 14 циклов соответственно). В шифре IDEA NXT используется 12 циклов зашифрования.

Линейное преобразование в виде матричного произведения, ставшее основой реализации новой стратегии широкого следа, как оказалось, не является единственным совершенным преобразованием (с максимальным числом ветвлений), а это значит, что динамические показатели шифров могут быть улучшены.

К еще одному недостатку можно отнести и усложненные схемы разворачивания ключей в рассмотренных шифрах. Стремление сделать схемы разворачивания ключей подобными по лавинным характеристикам самим шифрам, на наш взгляд, не оправдано, так как наши эксперименты с уменьшенными моделями шифров [26] показали, что шифры и с нулевыми цикловыми подключами приходят к случайным подстановкам за то же число циклов, что и с ненулевыми цикловыми подключами (в штатном режиме работы). Показателей случайности самих S-блоков оказывается вполне достаточно, чтобы шифр стал случайной подстановкой независимо от значений ключевых битов.

Представленные результаты позволяют охарактеризовать состояние современных технологий проектирования БСШ (ориентируясь на наиболее прогрессивные из них) следующими основными положениями:

1. Полагается, что показатели стойкости шифров к атакам дифференциального и линейного криптоанализа непосредственно связаны со значениями дифференциальных и линейных вероятностей входящих в шифры нелинейных преобразований (S-блоков). Поэтому в криптографической литературе давно и интенсивно развивается научное направление исследований, связанное с разработкой и поиском S-блоков с улучшенными криптографическими показателями;

2. Наиболее прогрессивные решения по построению БСШ связаны с реализацией итеративной многоцикловой процедуры с использованием линейного преобразования, реализующего стратегию широкого следа (Rijndael, IDEA NXT, Лабиринт, Камелия, Калина, «Мухомор», Grand Cru и др.).

3. Практика построения блочных шифров определила число используемых циклов зашифрования (запас стойкости), в три-четыре раза превышающее глубину лавинного эффекта (число циклов, необходимых для прихода шифра к состоянию случайной подстановки);

4. Примененные в известных шифрах конструкции цикловых преобразований обеспечивают приход шифров к состоянию случайной подстановки за минимальное число циклов, превосходящее два-три (исключение составляет алгоритм блочного шифрования из белорусского стандарта и шифры Калина-2 и «Мухомор»);

5. Практически все известные разработки ориентированы на использование S-блоков с предельными и близкими к ним значениями дифференциальных и линейных показателей;

6. Достигнутые показатели по быстродействию шифров характеризуются предельным значением удельных затрат XOR операций (тактов), приходящихся на один S-блок, близким к единице (без учета затрат на выполнение процедуры разворачивания ключей);

7. Существующая концепция построения схем разворачивания ключей для блочных симметричных шифров ориентирована на реализацию процедур, приближающихся по своим свойствам к дополнительному шифрующему преобразованию.

В последних разработках (алгоритм блочного шифрования из белорусского стандарта, а также шифр «Мухомор») просматривается стремление увеличить минимальное число активизируемых S-блоков цикловой функции за счет увеличения числа слоев S-блоков входящих

в нее, однако все они ориентированы на использование S-блоков со значениями дифференциальных и линейных вероятностей близкими к предельным.

3. Новая концепция проектирования БСШ

Тяжело конкурировать с мировыми авторитетами, но здесь предпринимаются шаги сделать это.

Подход, о котором идет речь далее, строится на изначально новых идеях, позволяющих его трактовать как новую концепцию в проектировании БСШ.

Результаты исследований [1, 24, 25, 27-29 и др.] позволяют сформулировать исходные положения этой концепции в виде следующих положений:

1. Все современные итеративные шифры независимо от используемых в них S-блоков (подстановочных преобразований) на полноцикловой длине по комбинаторным показателям, а также по дифференциальным и линейным показателям (по значениям максимумов дифференциальных и линейных вероятностей) становятся случайными подстановками. Подстановочные преобразования влияют лишь на динамику (число цилов) перехода шифра к состоянию случайной подстановки.

2. Динамические показатели прихода шифра к случайной подстановке определяются минимальным числом активных S-блоков, приходящихся на первые циклы преобразований, при этом минимальное число активных S-блоков первого цикла в большинстве известных конструкций блочных симметричных шифров равно одному. Линейные преобразования, строящиеся на основе МДР преобразований, не обеспечивают активизацию всех S-блоков второго и третьего циклов.

3. Предельное число ветвлений (когда один S-блок активизирует все последующие S-блоки цикла) может быть реализовано на основе конструкции линейного преобразования, в которой обеспечивается принцип последовательной активизации S-блоков цикловой функции одного за другим.

4. Для получения шифрующего преобразования, которое становится случайной подстановкой с первого цикла, необходимо увеличить число S-блоков первого цикла до заданного их количества $k_{\min}$ и, кроме того, создать условия, при которых активизация любого байта входа шифра приводит к активизации всех S-блоков первого цикла, причем последующие циклы могут быть построены с помощью стандартных (известных) методов.

5. Конструкция цикловой функции должна позволять сделать участие всех байтов входа в шифр в активизации S-блоков сбалансированным в том смысле, что после двух циклов, а в предельном случае – после одного цикла преобразований, все байты входа должны проходить набор активных S-блоков по возможности одинаковое число раз.

7. Схемы разворачивания ключей могут быть построены с использованием существенно упрощенных подходов. Основное требование к схемам разворачивания ключей − отсутствие самоподобия в последовательности цикловых подключей.

Далее ставится задача построить цикловое преобразование шифра, позволяющее активизировать сразу все (почти все) S-блоки первого и последующих циклов.

Такая возможность уже отмечалась в работе [28] для преобразований М-64, М-128 шифра «Мухомор». Сегодня, развивая идеи построения функции усложнения М-256, можем обосновать новый подход более обстоятельно. А весь секрет в свойствах конструкции циклового преобразования, которое строится на основе скорее не параллельной, а последовательной активизации S-блоков циклового преобразования с одновременным обеспечением взаимосвязи соседних S-блоков так, чтобы каждый текущий S-блок зависел от результатов активизации предыдущего (предыдущих) S-блоков.

4. Блочный симметричный шифр с управляемыми подстановками

Возвратимся к идее использования при построении цикловой функции блочного симметричного шифра принципов управления с помощью текущих данных шифрования процессами (результатами) выполнения подстановочных преобразований. Мы назвали этот принцип недетерминированным криптографическим преобразованием [30]. Предложенное тогда решение оказалось далеко не совершенным. Много внимания пришлось уделить перекрытию обнаруженных в процессе исследования его слабостей. Дальнейшим развитием отмеченных принципов стало наше очередное предложение – шифр «Мухомор» [30], представленный на украинский конкурс, в котором удалось на основе введения в процессы формирования входов в S-блоки дополнительных обратных связей с выходов других S-блоков устранить слабости первого предложения. Этот шифр прошел экспертизу авторитетных специалистов и был признан одним из лидеров современных алгоритмов шифрования.

Развитый в [30] подход в своей основе был ориентирован на использование двухэтапного принципа формирования цикловой функции, когда на верхнем (внешнем) уровне преобразования использовалась известная схема Lai – Massey [4], а динамическое управление подстановочными преобразованиями выполнялось на нижнем уровне схемами усложнения. Тогда мы посчитали такую двухэтапную процедуру перемешивания битов данных более эффективной с точки зрения обеспечения высокого уровня криптографической стойкости шифра. Проведенные к сегодняшнему дню исследования [25, 28] показали, что введенный внешний уровень перемешивания цикловой функции является как бы лишним. Приход шифра к случайной подстановке за один-два цикла удается реализовать и без внешнего уровня перемешивания цикловой функции (схемы Lai – Massey) несмотря на то, что он позволяет вдвое увеличить число активных S-блоков. Цикловое преобразование нижнего уровня оказывается самодостаточным для реализации предельных показателей динамики перехода шифра к состоянию случайной подстановки. Кроме того, сама функция усложнения представляется несколько утяжеленной из-за того, что некоторые преобразования цикловых функций получились дублирующими друг друга (избыточными) и к тому же сложными для математического анализа. Здесь имеются в виду связи через суммирование по модулю 2 текущих выходов SL преобразований с предыдущими и последующими линейками входных блоков данных. Таким образом, задача нахождения разумного компромисса между стойкостью и быстродействием сохраняет актуальность.

В этой работе предлагаем шифр, использующий в своей конструкции принципы построения нижнего уровня шифра «Мухомор», из которого мы сохранили только идею управления текущими значениями выходов SL преобразований значениями выходов предыдущих SL преобразований. Это реализуется с помощью сложения по модулю 2 текущих 32-битных входных блоков данных (SL преобразований) с предыдущими результатами выполнения нелинейных преобразований блоков данных (SL преобразований). Первая из предлагаемых конструкций шифров, названная нами «Шифром с управляемыми подстановками» 1-й версии (ШУП-1), обеспечивает шифрование блоков данных размером 256 бит.

При разработке этого решения в основу были положены следующие критерии:

- шифр должен приходить к случайной подстановке за минимально возможное число циклов (в данном случае за один-два цикла);

- приход к состоянию случайной подстановки обозначает, что изменение любого бита на входе шифра приводит в среднем к изменению половины битов на выходе циклового преобразования;

- конструкция цикловой функции должна в известной мере быть простой и прозрачной;

- вычислительная сложность выполнения операций зашифрования и расшифрования должна быть выше, чем у известных конструкций шифров с таким же размером битового входа;

- схема разворачивания ключей должна быть простой и быстродействующей. Основное требование для этой схемы отсутствие самоподобия цикловых подключей.

При построении нового шифра устранены все отмеченные недостатки и слабости шифра «Мухомор».

Представляется, что логично было бы сразу пойти по пути применения цикловой функции, использованной в шифре «Мухомор».

Напомним конструкцию цикловой функции шифра «Мухомор».

На вход циклового преобразования шифра «Мухомор» подается блок данных, совпадающих по размеру с открытым текстом (128, 256 или 512 битов). Входной блок разбивается на четыре равных подблока, разность (XOR) между которыми подается на вход функции усложнения (М-64, М-128, М-256 для размеров блока 128, 256 и 512 битов соответственно) вместе со значением очередного циклового подключа (K_i). Выходное значение функции складывается по модулю 2 с входными значениями, после чего первый и третий подблоки обрабатываются операцией ортогонального преобразования (ОП). Схема циклового преобразования шифра «Мухомор» представлена на рис. 1. На рис. 2 приведена схема преобразования М-256.

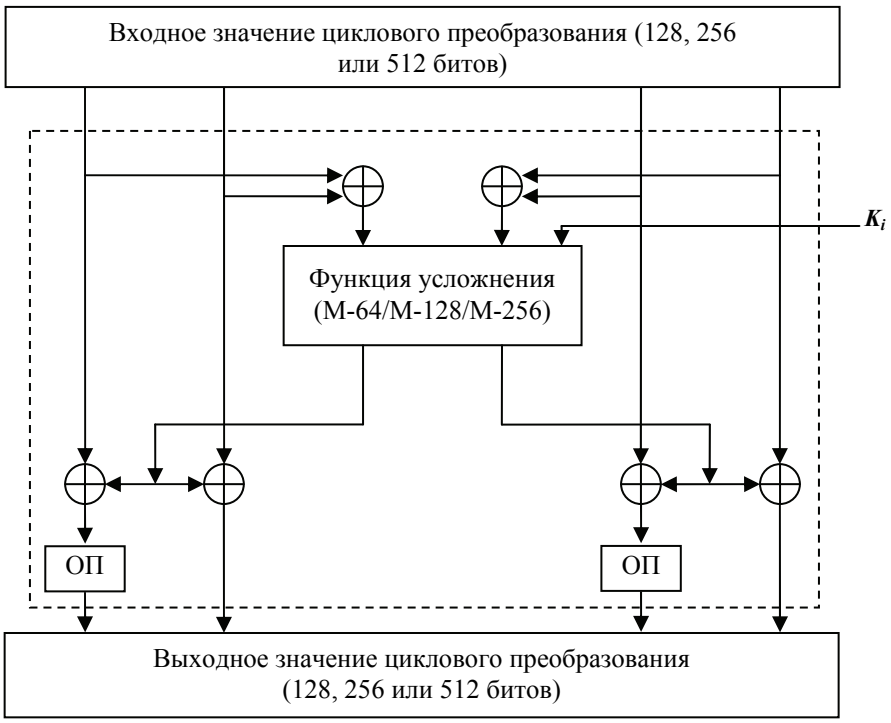

Рис. 1

При размере блока открытого текста 512 битов функция усложнения М-512 принимает очередной 256-битовый подключ K_i и два 128-битовых значения, первое из которых вычисляется как разность по модулю 2 между первым и вторым подблоками данных на входе цикла, соответственно второе входное значение – разность между третьим и четвертым подблоками на входе цикла.

Каждое из 32-битных входных значений функции М-256 складывается по модулю 2^{32} с соответствующей частью очередного подключа, поданного на вход функции. Затем каждое полученное 32-битное слово проходит через SL преобразование, причем результат преобразования складывается по модулю 2 со всеми остальными словами.

Описанная операция выполняется два раза (два слоя *SL*-преобразований). Левое выходное 128-битное слово формируется как результат конкатенации четырех левых 32-битовых слов, правое 128-битное слово – как результат конкатенации четырех правых 32-битных слов.

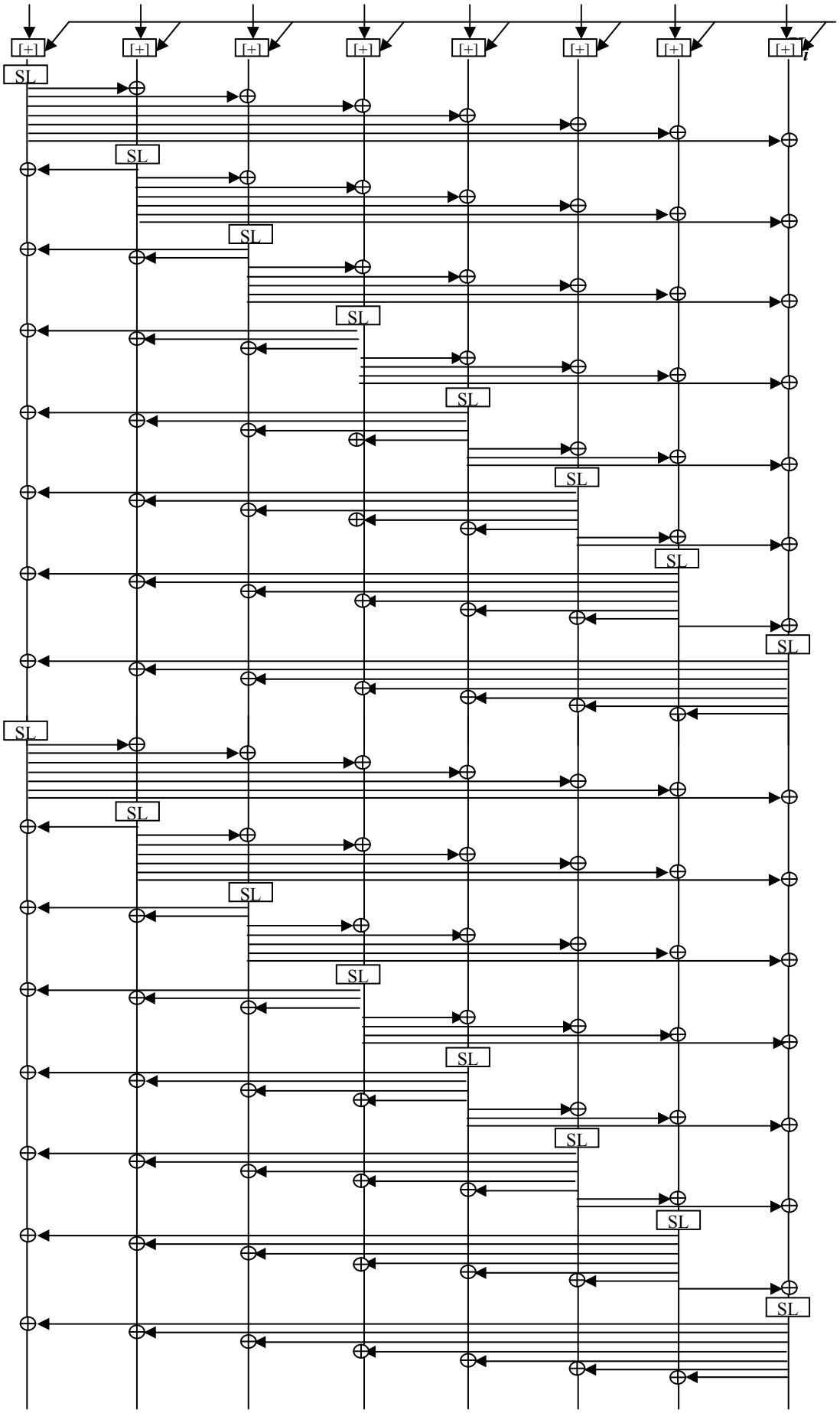

Рис. 2

Возвратимся к обсуждению нашего предложения.

Действительно, если повторять цикловую функцию усложнения шифра «Мухомор» М-256, то надо было бы ее строить с двумя слоями SL преобразований. Мы действительно, как увидим из дальнейшего, получили бы шифр с управляемыми подстановками, который приходил бы к случайной подстановке за один цикл (в шифре «Мухомор-256» в первом цикле используются два слоя SL преобразований, при этом активизируется максимум 36 S-блоков (одно SL преобразование в первом слое и 8 SL преобразований во втором), и это число удваивается за счет схемы Lai – Massey). Но уж очень такая конструкция похожа на шифр с удвоенными цикловыми преобразованиями. Эффекта увеличения числа активных S-блоков первого цикла можно было бы добиться и в шифре AES (если его четырехцикловую конструкцию переформатировать в двухцикловую). Поэтому, чтобы обойти возможные критические замечания в отношении неоригинальности конструкции, мы представляем версию шифра, которая повторяет классический подход к построению цикловых функций (в каждом цикле будет использоваться один слой SL преобразований). Основное ее достоинство состоит в том, что в отличие от шифра AES она будет приходить к случайной подстановке за два цикла вместо четырех за счет того, что в циклах, начиная с первого, в шифре будут активизироваться, по-возможности, все S-блоки цикловых функций. Подчеркнем, что мы оставляем за собой возможность построить преобразование первого цикла с двумя слоями SL преобразований, что открывает, как будет видно из дальнейшего, возможность построения шифра, который становится случайной подстановкой уже после первого цикла. Далее представляется описание одной из первых наших разработок, которую мы назвали, как уже было отмечено выше, шифром с управляемыми подстановками (ШУП-1).

4.1. Описание шифра ШУП-1

При изложении материала воспользовались описанием шифра «Мухомор» [21], ставшего в определенной степени прототипом предложения. Нам потребовалось выделить из него часть, связанную с описанием функции усложнения М-256, как раз составляющую основу построения цикловой функции ШУП.

4.1.1. *Параметры алгоритма*. Алгоритм шифрования ШУП-1 поддерживает длину блока 256 битов и ключи шифрования длиной 256 и 512 битов.

4.1.2. *Процедура зашифрования*. На вход процедуры подается открытый текст и подключи шифрования. Входной блок данных заданное количество раз (восемь) обрабатывается цикловой функцией, и в завершение производится финальная рандомизация с помощью операции XOR с дополнительным (девятым) цикловым подключом. Полученный в результате блок данных является шифртекстом.

4.1.3. *Цикловое преобразование*. Мы не стали излишне усложнять конструкцию циклового преобразования шифра, полагая, что решение по построению шифра должно обладать определенной элегантностью и простотой. Поэтому при построении цикловой функции ШУП-1 из базовой конструкции шифра «Мухомор» исключили второй слой SL преобразований, а также ряд суммирований результатов прохождения SL преобразований с последующими и предыдущими блоками данных, так как они дублировали операции, реализуемые последовательностью SL преобразований. Кроме того, эти цепи усложняли анализ процессов активизации S-блоков. Мы сохранили лишь суммирование по модулю 2 выхода текущего слоя SL преобразований, а именно – последней колонки входных блоков данных со входом следующего слоя SL преобразований (первой колонки входных блоков данных), чтобы обеспечить при формировании выхода цикловой функции эффект прохождения каждым байтом входа всех SL преобразований (получить максимально возможное количество активных S-блоков) для каждой четверки байтов входа.

Особое внимание при построении циклового преобразования шифра было уделено конструкции первого цикла. Здесь поставлена задача построить их так, чтобы была обеспечена активизация входными блоками данных (колонками) одновременно и сбалансировано, по-

возможности, всех S-блоков этой цикловой функции. В результате в качестве циклового преобразования используется несколько измененная функция усложнения М-256 шифра «Мухомор». Во-первых, цикл ШУП-1 практически включает только первую (верхнюю) половину преобразования функции усложнения М-256. Практически один цикл функции усложнения М-256 шифра «Мухомор» разбивается на два цикла (ко второй части функции усложнения добавляется в самом начале сложение с цикловым подключем, аналогичное операции введения циклового подключа в верхней части цикловой функции, и из одного циклового преобразования функции М-256 получается два цикловых преобразования ШУП. Во-вторых, – кроме указанных выше исключений ряда суммирований *для обеспечения активизации любым* 32-*битным словом* (*сегментом*) *входа первого SL преобразования в линейке динамично управляемых переходов других SL преобразований, в первом цикле после операции сложения с цикловыми подключами* (*по модулю* 2^{32}) *перед заходом в первое SL преобразование вводится дополнительное сложение по модулю* 2 (*XOR*) *всех* 32-*битных сегментов.* Эта операция является принципиальной и имеет смысл только для выбранного способа запуска SL преобразований, когда SL преобразования включены в цепочку с последовательным запуском друг друга. Для других (известных) конструкций шифров эта процедура не имеет смысла, так как в других шифрах S-блоки в цикловую функцию входят независимо друг от друга или независимыми группами.

4.1.3.1. SL-преобразование. На вход циклового преобразования шифра подается блок данных, совпадающий по размеру с открытым текстом (256 битов). Входной блок разбивается на восемь равных по длительности подблоков, которые подаются на вход цикловой функции вместе со значениями очередного циклового подключа K_i , также представленного в виде последовательности четырехбайтовых блоков.

Входное 32-битовое значение делится на 4 байта, каждый из которых заменяется в соответствии с заданной таблицей подстановки. В преобразовании используются четыре разные таблицы, по одной на каждый байт.

После операции замены в S-блоках 4 байта (a_0,a_1,a_2,a_3) подаются на вход МДР преобразования, которое выполняет матричное умножение следующего вида:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 02 \cdot a_0 \oplus 03 \cdot a_1 \oplus 01 \cdot a_2 \oplus 01 \cdot a_3 \\ 01 \cdot a_0 \oplus 02 \cdot a_1 \oplus 03 \cdot a_2 \oplus 01 \cdot a_3 \\ 01 \cdot a_0 \oplus 01 \cdot a_1 \oplus 02 \cdot a_2 \oplus 03 \cdot a_3 \\ 03 \cdot a_0 \oplus 01 \cdot a_1 \oplus 01 \cdot a_2 \oplus 02 \cdot a_3 \end{bmatrix}$$

Таблицы подстановок алгоритма ШУП-1 повторяют таблицы подстановок шифра «Мухомор».

Основным элементом цикловой функции является SL преобразование, выполняющее преобразование 32-битовых блоков данных. Схема SL преобразования приведена на рис. 3. Она повторяет схему SL преобразования шифра «Мухомор».

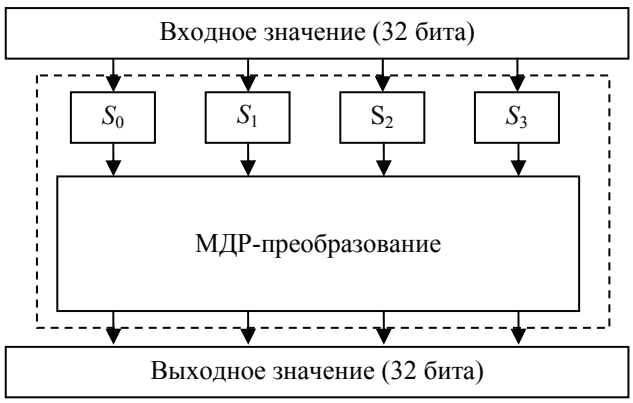

Рис. 3

Матрица МДР преобразования ШУП-1 совпадает с матрицей преобразования шифра «Мухомор» (совпадает с матрицей линейного преобразования алгоритма Rijndael/AES), но при вычислении произведения элементов вектора на матричные коэффициенты в шифрах ШУП-1 и «Мухомор» используется другой полином:

$$m(x) = x^8 + x^4 + x^3 + x^2 + 1,$$

или {01}{1d} в шестнадцатеричном представлении.

Выходной 32-битовый вектор МДР преобразования (b_0,b_1,b_2,b_3) является выходным значением SL преобразования.

4.1.3.2. Схема циклового преобразования. Схема циклового преобразования ШУП-1 предельно проста и приведена на рис. 4. При такой схеме запуска SL преобразований получается, что фактически в качестве укрупненных S-блоков (SL преобразований) выступают как бы латинские квадраты [31]. Если считать, что SL преобразование является подстановкой, то строками латинского квадрата выступают циклические сдвиги второй строки матрицы исходной 4-байтовой подстановки, т.е. вместо одной исходной подстановки используется 2^{32} различных подстановок (строк латинского квадрата). При этом строка (столбец) входа в латинский квадрат задается выходом предыдущего SL преобразования, а столбец (строка) подстановки задается ее первичным входом цикла, а остальные семь циклов строятся без сложений по модулю 2 на входе первого SL преобразования и без сложений по модулю 2 выхода последнего SL преобразования с выходами остальных SL преобразований.

4.1.3.3. Процедура расшифрования**.** Алгоритм расшифрования является обратным к алгоритму зашифрования. На вход алгоритма подаются блоки зашифрованного текста и подключи разшифрования. В самом начале процедуры расшифрования осуществляется снятие финальной рандомизации шифртекста, после чего полученный блок данных необходимое число раз (восемь) в обратном порядке обрабатывается цикловыми функциями. Полученный блок данных является блоком открытого текста. Остается отметить, что при расшифровании:

- в обратном порядке также подаются подключи расшифрования;
- в качестве подстановок используются инверсные S-блоки.

4.1.3.4. Процедура разворачивания ключей. В шифре «Мухомор» используется сложная схема разворачивания мастер-ключа. В нашем шифре мы хотим воспользоваться более простым решением. При его формировании мы постарались обеспечить отсутствие периодичности в построении цикловых подключей. Используется мастер ключ, в котором отсутствует повторение байтов. Сама процедура разворачивания мастер-ключа включает его разделение на отдельные байты с последующим выполнением циклического сдвига мастер-ключа на величину, задаваемую значениями смежных (соседних) байтов, которые и используются как очередные подключи. В этом случае для формирования всего набора цикловых подключей потребуется девять последовательных байтов. Выбор байтов для разворачивания ключей может стать дополнительным секретным параметром шифра ($C_{32}^{11} = 2^{27}$ вариантов выбора байтов). Для ключа длиной 512 бит значением байта можно задавать число бит, которые отбрасываются от мастер-ключа. Текущий подключ определяется 256 битами, идущими после отброшенных (в этом случае $C_{64}^{11} = 2^{39,4}$).

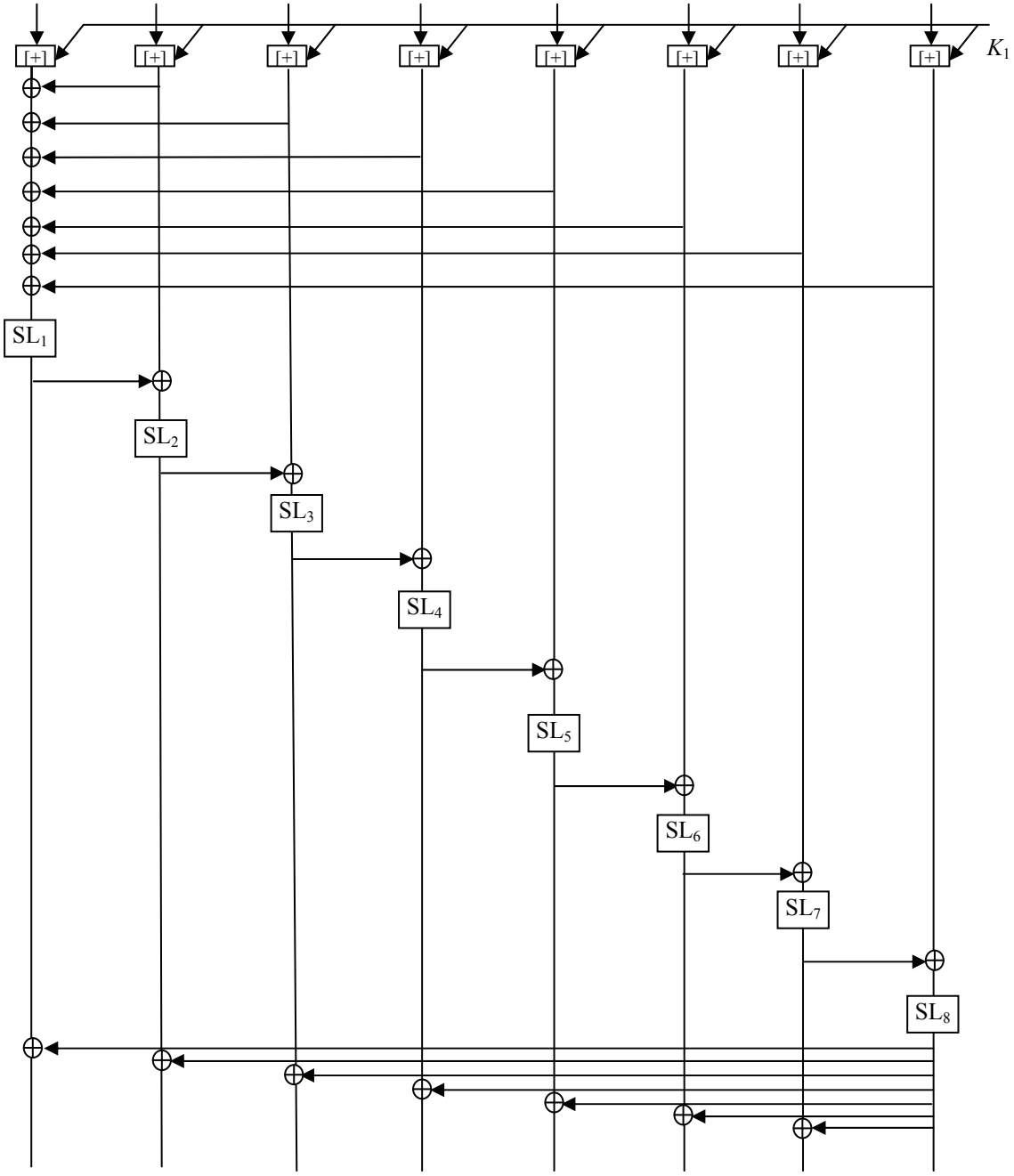

Рис. 4

4.2. Эффективность преобразования

Далее приводим результаты экспериментов по оценке эффективности предлагаемого решения.

В табл. 1 представлены результаты вычислительного эксперимента по определению закона распределения числа активизируемых S-блоков первого цикла (в процентах).

Подсчет количества активизируемых S-блоков производился для каждого из 32 байт, при этом для каждой разности из множества 2^8 битовых сегментов перебирались все возможные пары сегментов. Во второй колонке (количество повторений) сумма $2^{21} = 2\ 097\ 152$. Нулей получилось 8192 (это нулевые входные разности).

Таблица 1

Количество активных S-блоков первого цикла	Доля от общего числа переходов
0	0,0039
1	0
. . .	. . .
27	0
28	0,0000057
29	0,000279
30	0,0070
31	0,1094
32	0,879

Как следует из представленных результатов, на первом цикле с большой вероятностью активизируются все 32 S-блока. Такой эффективностью перемешивания не обладает ни один из известных шифров.

4.3. Показатели случайности ШУП-1

В этом подразделе приведем результаты оценки ожидаемых параметров перехода ШУП-1 к состоянию случайной подстановки.

В соответствии с идеей развиваемого в [24] подхода необходимо выполнить оценку минимального числа активных (задействованных S-блоков), после прохождения которых шифр становится случайной подстановкой. Это минимальное число определяется дифференциальными и линейными показателями самих S-блоков, применяемых в шифре, конструкциями и свойствами его цикловых преобразований, а также значениями показателей доказуемой стойкости шифра, зависящими от размера его битового входа. В работе [24] эта связь между отмеченными показателями определена в виде двух соотношений:

$$IPS_D = (\,DP^{\pi}_{\max}\,)^k,\ IPS_L = 2^{k-1}\cdot\left(LP^{\pi}_{\max}\right)^k.$$

Здесь $DP^{\pi}_{\max}$ и $LP^{\pi}_{\max}$ – максимальные значения дифференциальной и линейной вероятностей подстановочных преобразований $\pi(x)$. IPS_D (Differential Indicator of Provable Security) – дифференциальный показатель доказуемой безопасности и IPS_L (Linear Indicator of Provable Security) – линейный показатель доказуемой безопасности, $k = k_{\min}$ – минимальное число активных S-блоков, участвующих в формировании перехода шифра к случайной подстановке.

Пользуясь расчетными соотношениями, установленными в работе [28], можно прийти к выводу, что для прихода шифра к случайной подстановке ожидаемое значение максимума числа дифференциальных переходов для шифра с 256-битным входом оказывается близким к 190, а ожидаемое значение максимума смещения линейного корпуса для шифра с 256-битным входом оказывается близким к 2^{130}. Соответственно получим, что максимальные значения линейной и дифференциальной вероятности для шифра с 256-битным входом получаются близкими друг к другу и равными приблизительно $2^{-248} \div 2^{-250}$.

Исходя из приведенных выше соотношений можно сделать вывод, что для шифра с 256-битным входом для прихода к состоянию случайной подстановки по дифференциальным показателям при использовании S-блоков с предельными показателями δ-равномерности, равными $DP^{\pi}_{\max} = 2^{-6}$ (в соответствии с равенством $2^{-248} = (2^{-6})^k$), потребуется $k_{\min} = 41$ S-блок.

Аналогично, для прихода к состоянию случайной подстановки по линейным показателям при использовании S-блоков с предельными показателями нелинейности, равными

$LP^{\pi}_{\max} = 2^{-6}$, потребуется ($2^{-250} = 2^{k-1} \cdot \left(2^{-6}\right)^k$) $k_{\min}$ = 50 S-блоков (для «родных» S-блоков с показателем нелинейности $LP^{\pi}_{\max} = 2^{-5}$ имеем в этом случае $k_{\min}$ = 62,25).

В соответствии со структурой циклового преобразовании рис. 1 в первом цикле каждый 32-битный блок входных данных попадает на выход цикловой функции, проходя восемь SL преобразований. Это значит, в лучшем случае активизируются 32 S-блока, кроме возможных одного-двух переходов МДР преобразований в один-два или три активных байта с вероятностью меньшей 2^{-59}. В худшем случае это будет 29-31 S-блок. Затем во втором цикле входные блоки данных проходят уже через все 32 S-блока.

Получается, что два цикла зашифрования вполне достаточно (с запасом) для того, чтобы ШУП-1 пришел к состоянию случайной подстановки и при использовании S-блоков с предельными дифференциальными и линейными показателями и при использовании S-блоков шифра «Мухомор».

4.4. Использование случайных S-блоков

Оценим перспективы использования в ШУП случайных S-блоков. Методика выполнения расчетов представлена в работе [24].

Для нашего шифра на первом цикле с ненулевой разностью на входе одного байта входа активизируются практически все 32 S-блока этого цикла, причем входы в S-блоки являются всегда случайными (за счет сложения с ключевыми битами).

В табл. 2 представлены результаты расчетов числа переходов разного типа в 48 строках дифференциальной таблицы случайной подстановки. В своих расчетах методом перебора мы выбрали сразу такое максимальное число активных S-блоков, которое позволяет реализовать приход шифра к случайной подстановке. Для дифференциальных показателей оно равно 48.

Таблица 2

Значение перехода таблицы	Число переходов дифференциальной таблицы	Число переходов в строке	Число переходов в 48 строках
12	1	0,003906	0,19
10	10	0,039065	1,87
8	104	0,40625	19,5
6	830	3,24218	155,62

Из представленных результатов следует, что 48 S-блоков (активных переходов) можно выбрать при случайных входах в S-блоки активных на основе использования:

- двух переходов со значением 10;
- двадцати переходов со значением 8;
- двадцати шести переходов со значением 6;

(используются максимально вероятные переходы). Всего 48 переходов (48 активных S-блока). Вычисления в этом случае приводят к нужному результату:

$$\left(\frac{10}{256}\right)^2 \times \left(\frac{8}{256}\right)^{20} \times \left(\frac{6}{256}\right)^{26} = 2^{-250}.$$

Это означает, что и случайные S-блоки по дифференциальным показателям обеспечивают приход шифра ШУП-1 к состоянию случайной подстановки за два цикла.

Приведем закон распределения переходов для смещений линейной аппроксимационной таблицы. В общее число переходов входят и положительные, и отрицательные смещения. Пользуясь результатами работы [24], можем рассчитать числа переходов разного типа в 64 строках линейной аппроксимационной таблицы случайной подстановки, итоги расчетов которых представлены в табл. 3.

Таблица 3

Значение перехода	Число переходов в таблице ЛАТ	Число переходов в строке таблицы ЛАТ	Число переходов в 64 случайно взятых строках таблицы ЛАТ
±34	1,998	0,0078	0,4992
±32	4	0,0156	0,9984
±30	10	0,0392	2,5089
±28	28	0,1098	7,0272
±26	65	0,2588	16,5632
±24	146	0,572	36,808,
±22	298	1,164	74,498

Опять будем считать, что за счет введения цикловых подсключей входы в S-блоки будут случайными и статистически независимыми. Методика расчетов представлена в работе [24].

В таблице представлены результаты оценки числа переходов и их значений в 64 случайно взятых строках таблицы ЛАТ. Из результатов следует, что для 64 активных S-блоков при использовании в них максимально вероятных переходов можно ожидать при случайных входах в случайные S-блоки:

- один переход со значением 32;
- три перехода со значением 30;
- семь переходов со значением 28;
- семнадцать переходов со значением 26;
- тридцать шесть переходов со значением 24.

Полагая далее, что строки в S-блок выбираются из всего множества 256 строк, при этом переходы по S-блокам идут в произвольном порядке и осуществляются по наиболее вероятному пути, можем выполнить оценку вероятности прихода шифра к состоянию случайной подстановки со случайными S-блоками. Вычисления для значения $k = 64$ приводят к результату

$$2^{63}\times\left(\frac{32}{128}\right)^2\left(\left(\frac{30}{128}\right)^2\right)^3\times\left(\left(\frac{28}{128}\right)^2\right)^7\times\left(\left(\frac{26}{128}\right)^2\right)^{17}\times\left(\left(\frac{24}{128}\right)^2\right)^{36}=2^{-236}.$$

Здесь уже вроде бы 64 случайных S-блоков недостаточно, чтобы шифр стал случайной подстановкой. Однако значение линейной вероятности 2^{-236} все равно оказывается приемлемым показателем стойкости двухциклового преобразования, хотя и для гарантированного прихода ШУП к случайной подстановке по линейным показателям требуется уже три цикла. Практически же можно будет считать шифр стойким против атак линейного криптоанализа и при двух циклах зашифрования.

В заключение напомним, что шифр Rijndael приходит к состоянию случайной подстановки по дифференциальным и линейным показателям лишь на третьем-четвертом циклах.

Заметим, что если бы первое цикловое преобразование мы сделали двухслойным (использовали бы две линейки SL преобразований), то шифр ШУП стал бы случайной подстановкой уже на первом цикле. Назовем эту модификацию решения шифром ШУП-2. Для этого шифра отпадают все ограничения на дифференциальные и линейные показатели используемых в шифре S-блоков.

4.5. Показатели вычислительной сложности

Как и в работе [32], при оценке вычислительной сложности будем ориентироваться на число XOR операций, выполняемых шифром в процессе зашифрования и расшифрования. Будем исходить из того, что для выполнения SL-преобразования (матричного умножения) требуется выполнить три XOR операции.

Тогда в соответствии со структурой циклового преобразования, представленной на рис. 2, в первом цикле ШУП-1 потребуется выполнить 8 + 3×7 + 3×8 = 53 XOR (тактов). На 8-цикловой шифр, если на остальных циклах, кроме первого использовать только одну линейку SL преобразований без сложений по модулю два на входе и выходе линейки, приходится 53 + 3×8×7 + 8 = 229 XOR.

В AES-256 на 14 циклов приходится 32×14 = 448 XOR, т.е. ШУП-1 будет быстрее AES.

Здесь еще не учитываются затраты на процедуру разворачивания мастер-ключа.

Приведем, наконец, результаты экспериментальной оценки вычислительной сложности ШУП-1. Применялся процессор Intel (ore i 7@2,4 GHz. Оперативная память 8 Гб. Получены такие характеристики быстродействия ШУП-1:

зашифрование: ≈ 15 Мбайт/с;

расшифрование: ≈ 2 Мбайт/с.

В дальнейшем предполагаем предложить и другие конструкции шифров с улучшенными динамическими показателями их прихода к состоянию случайной подстановки, чем дополнительно подтвердить плодотворность развиваемого подхода к проектированию блочных симметричных шифров.

4.6. Конвейерная обработка данных

Цикловые функции, которые используются в обоих шифрах (ШУП-1 и ШУП-2) с особым первым циклом на оставшихся семи циклах допускают конвейерную обработку данных.

Действительно, после формирования выхода первого SL преобразования второго цикла можно сразу же с формированием выхода второго SL преобразования данного цикла формировать выход первого SL преобразования третьего цикла. После формирования выхода второго SL преобразования третьего цикла формировать и выход первого SL преобразования четвертого цикла и т.д.

Если считать, что для 32-битной платформы для выполнения операции SL преобразования необходимо затратить время T, то для отдельной линейки (цикла) из m SL преобразований необходимо будет затратить mT с.

При конвейерной обработке каждый очередной s-й цикл будет начинаться с задержкой $(s-1)T$ с, $1 \le s \le r$. В результате, если для обработки r циклов при зашифровании одним потоком будет необходимо затратить rm с, то при параллельной обработке r циклов достаточно будет затратить $m + r - 1$ с.

Если шифр строится с использованием 32-битных SL преобразований, то для $r = 7$, $m = 8$ имеем выигрыш в быстродействии вычисления семи последних циклов зашифрования:

$$\frac{mr}{m+r-1} = \frac{8\times 7}{8+6} = \frac{56}{14} = 4$$

раза, а с учетом первого цикла:

$$\frac{mr+m}{m+r-1+m} = \frac{8\times 8}{2\times 8+6} = \frac{64}{22} = 2{,}9\,.$$

В итоге выигрыш получается почти в три раза.

Таким образом, описанные шифры, названные ШУП, представляются как наиболее перспективные решения по построению современных шифров.

Выводы

Предложены две конструкции шифров ШУП-1 и ШУП-2, в которых обеспечивается активизация практически всех S-блоков цикловой функции уже на первом цикле.

Установлено, что шифры предлагаемой конструкции обладают наилучшими из известных шифров динамическими показателями прихода к случайной подстановке. Практически они стают случайными подстановками уже с первого цикла, чего не позволяет ни один из известных шифров, что означает их повышенную стойкость к атакам дифференциального и линейного криптоанализа (позволяют уменьшить число циклов зашифрования). По показателям вычислительной сложности шифры могут работать существенно быстрее AES. Важной особенностью шифров является то, что они допускают конвейерную обработку блоков данных, при этом открывается возможность дальнейшего повышения их быстродействия до трех раз.

По другим показателям стойкости эти шифры унаследовали все высокие показатели стойкости, свойственные шифру «Мухомор» [30]. Замечательным свойством этих шифров является то, что они становятся случайными подстановками за один-два цикла и при использовании случайных S-блоков, т.е. получаются шифры, свойства которых практически не зависят от свойств входящих в них S-блоков.

Самый полезный результат развиваемого подхода состоит в том, что удается построить шифры с уменьшенным числом цикловых преобразований без потери стойкости, что позволяет добиться дальнейшего повышения производительности алгоритмов шифрования.

Дополнительным полезным результатом работы является предложенная простая схема разворачивания ключей, не привязанная к процедуре шифрования, которая позволяет обеспечить отсутствие самоподобия цикловых подключей при их формировании.

В заключение следует заметить, что в существующих конструкциях шифров число S-блоков цикловой функции обычно привязано к размеру битового входа в шифр и их число, приходящееся на цикл, оказывается, как правило, существенно меньше количества активных S-боков, необходимых для прихода шифра за один цикл к состоянию случайной подстановки. Поэтому одним из реальных путей улучшения динамических показателей шифров является увеличение числа S-блоков, приходящихся на первое цикловое преобразование, с одновременным использованием принципов их последовательной активизации, начиная с первого S-блока. Это и реальный путь снижения зависимости свойств шифров от свойств, входящих в них S-блоков.

На шифр ШУП-1 получен патент [33].

Список литературы: 1. *Лисицкая, И.В*. Методология оценки стойкости блочных симметричных криптопреобразований на основе уменьшенных моделей: дис. … д-ра техн. наук : 05.13.05 / Ирина Викторовна Лисицкая. – 2012. – 293 с. – Библиогр.: 294–319. 2. *Daemen, J.* AES submission, Document on Rijndael, Version 2 / J. Daemen, V. Rijmen // September 1999, p. 1-45. 3. *Lai, X.* On the design and security of block ciphers / X. Lai // volume 1 of ETH Series in Information Processing. Hartung-Gorre Verlag, 1992. 4. *Lai, X.* A proposal for a new block encryption standard / X Lai and J. Massey // In I. Damgard, editor, Advances in Cryptology – EUROCRYPT'90, volume 473 of Lecture Notes in Computer Science, pages 389–404. Springer-Verlag, 1991. 5. *Шнаер, Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнаер. – М. : Триумф, 2002. – 727 с. 6. *Landau, S.* Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard / S. Landau // February, 2004. 7. *Meier, W*. Nonlinearity criteria for cryptographic functions, in Advances in Cryptology / W. Meier, O. Staffelbach: Eurocrypt '89, J.-J Quisquater and J. Vandewalle, eds., Springer-Verlag, Berlin, 1989. 8. *Pieprzyk, J.* Nonlinearity of exponent permutations, in Advances in Cryptology: Eurocrypt '89, J.-J Quisquater and J. Vandewalle, eds., Springer-Verlag, Berlin, 1990, pp. 89-92 9. *Pieprzyk, J.* On Bent Permutations / J. Pieprzyk // Technical Report CS91/11, Department of Computer Science, University of New South Wales; presented at International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing, Las Vegas, 1991. 10. *Nyberg, K.* Differentially uniform mappings for cryptography, in Advances in Cryptology / K. Nyberg // Eurocrypt '93, T. Helleseth, ed., Springer-Verlag, Berlin, 1994, pp. 53-

64. 11. *Daemen, J.* Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis / J. Daemen // Ph.D. thesis, Katholieke Universiteit, Leuven, Belgium, 1995. 12. *Ridjmen, V.* The cipher SHARK, in Fast Software Encryption / V. Ridjmen, J. Daemen, B. Preneel and outhers // Third International Workshop, D. Gollman, ed., Springer-Verlag, Berlin, 1996, pp. 99-112. 13. *Jakobsen and L. Knudsen.* Attacks on block ciphers of low algebraic degree / T. Jakobsen and L. Knudsen // J. Cryptology 14 (2001), pp. 197-210. 14. *Daemen, J., Knudsen, L.* and *Ridjmen*, *V.* The Block Cipher Square, in Fast Software Encryption, E. Biham ed., LNCS 1267, Springer-Verlag, Berlin, 1997. 15. *Rodinko, M.YU*. The wide trail strategy without separable codes / M.YU. Rodinko, K.E. Lisitskiy // Радиотехника. – 2015. – Вип.181. – С. 40-45. 16. *Daemen, J.* The Design of Rijndael: AES — the Advanced Encryption Standard / J. Daemen and V. Ridjmen.// Springer-Verlag, Berlin, 2002. 17. *Lidl, R.* Introduction to Finite Fields and Their Applications / R. Lidl, H. Niederreiter, Cambridge University Press, Cambridge, 1986. 18. *Weeks, B*. Hardware Performance Simulation of Round 2 Advanced Encryption Standard Algorithms / B. Weeks, M. Bean, T. Rozylowicz, and C. Ficke, (May 15, 2000); available at http://csrc.nist.gov/encryption/aes/ round2/r2anlsys.htm. 19. *Junod, P.* FOX: a new family of block ciphers. In H. Handschuh and A. Hasan, editors, Selected Areas in Cryptography / P. Junod, S. Vaudenay // 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004. Revised Selected Papers, volume 3357 of Lecture Notes in Computer Science, pages 114-129. Springer-Verlag, 2004. 20. *Горбенко, І.Д.* Принципи побудування та властивості блокових симетричних IDEA подібних шифрів / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та інші // Прикладная радиоэлектроника. – Харьков : ХНУРЭ. – 2007. – Т. 6, № 2. – С. 158-173. 21. *Горбенко, І.Д.* Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов, Р.В. Олійников та інші // Прикладная радиоэлектроника. – Харьков : ХТУРЭ. – 2007. – Т. 6, №2. – С. 147-157. 22. *Государственный с*тандарт республики Беларусь. СТБ 34.101.31-2011. Информационные технологии. Защита информации Криптографические алгоритмы шифрования и контроля целостности. Введен в действие постановлением Госстандарта Республики Беларусь от 31 января 2011 г. № 5. – Минск : Изд-во Госстандарт – 2011. – 35 с. 23. *Стандарт* блочного симметричного преобразования ДСТУ 7624:2014. 24. *Долгов, В. И.* Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа : монография / В.И. Долгов, И.В. Лисицкая. – Харьков : Форт, 2013. – 420 с. 25. *Gorbenko, I.D*. On Ciphers Coming to a Stationary State of Random Substitution / I.D. Gorbenko, K.E. Lisitskiy, D.S. Denisov // Copyright © 2013 Horizon Research Publishing. 26. *Лисицкая, И.В.* О криптографической значимости схем разворачивания ключей в обеспечении стойкости блочних симметричных шифров к атакам линейного и дифференциального криптоанализа / И.В. Лисицкая, А.А. Настенко, К.Е. Лисицкий // Радиоэлектроника и информатика. – 2012. -№3(58). 27. *Лисицкая, И.В.* Современные методы проектирования БСШ. От конкурсов к стандартам / И.В. Лисицкая // Радиотехника. – 2011. – Вып. 165. – С. 226-239. 28. *Горбенко, И.Д.* О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным / И.Д. Горбенко, К.Е. Лисицкий // Радиотехника. – 2014. – Вып. № 176. – С. 27-39. 29. *Lisitskiy, K.E.* On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers [Text] / K.E. Lisitskiy // I.J. Computer Network and Information Security, 2014, 1, 11-18 Published Online November 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis. 2014.01.02. 30. *Бондаренко, М.Ф.* Обґрунтування вимог та розробка основних рішень з побудування та властивості перспективного БСШ «Мухомор» / М.Ф. Бондаренко, І.Д. Горбенко, В.І. Долгов та інші // Прикладная радиоэлектроника. – Харьков : ХНУРЭ. – 2007. – Т. 6, № 2. – С. 174-185. 31. *Деклараційний* патент на винахід № 53949. 17.02.2003. Бюл. № 2. 32. *Горбенко, И.Д.* Свойства и возможности оптимизации криптографических преобразований в AES – RIJNDAEL / И.Д. Горбенко, Д.А. Чекалин // Радиотехника. – 2001. – Вып 119. – С. 36-42. 33. *Пат. 111547* Україна, МПК (2016.01) G09C 1/00 H04L 9/06 (2006.01). Спосіб криптографічного перетворення двійкових даних (варіанти) / Горбенко І.Д., Долгов В.І., Лисицька І.В. та інші (Україна); заявник АО ІІТ м. Харків. № a201500942 ; заявл. 06.02.2015 ; опубл. 10.05.2016, Бюл. № 9. – 20 с.

Харьковский национальный
университет радиоэлектроники
Харьковский национальный университет
имени В.Н.Каразина

Поступила в редколлегию 07.09.2016