http://dx.doi.org/10.35596/1729-7648-2024-22-5-80-88

Оригинальная статья
Original paper

УДК 004.832, 519.6

ОСОБЕННОСТИ СТРУКТУРНО-АППАРАТНОГО ОБЕСПЕЧЕНИЯ ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ В КРИПТОСИСТЕМАХ

А. Ф. ЧЕРНЯВСКИЙ[1], Е. И. КОЗЛОВА[1], Ю. А. ЧЕРНЯВСКИЙ[2]

[1]Белорусский государственный университет (г. Минск, Республика Беларусь)
[2]Белорусский государственный университет информатики и радиоэлектроники (г. Минск, Республика Беларусь)

Поступила в редакцию 30.04.2024

Аннотация. Рассмотрены виды, функции и некоторые особенности криптосистем, а также схемотехнические варианты расширения их функциональных возможностей. Представлены варианты формирования ключей и шифров, используемых в криптосистемах с типовой структурной организацией, и технологии создания цепочек шифрования. Описана схема шифрования, в рекуррентной формуле алгоритма которой задействованы предыдущие блоки как шифрования, так и открытого текста. Данная схема надежно защищает от любой несанкционированной модификации зашифрованного текста. Приведены структурные схемы организации криптосистем симметричного и асимметричного типов. Предложен вариант реализации декодирующей процедуры в пороговом МИМА-криптомодуле разделения секрета с маскирующим преобразованием, в котором минимизируются необходимые временные и аппаратные затраты на выполнение процедуры реконструкции секрет-оригинала. Представленный материал может быть частью исходных разделов необходимого и достаточно обеспеченного в математическом плане учебного пособия по основам и современным проблемам криптографии.

Ключевые слова: криптосистема, шифр, ключ, хеш-функция, генератор случайных чисел, минимально избыточное модулярное кодирование, криптостойкость, преобразование, транспортное кодирование, МИМА-криптомодуль.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Благодарность. Работа выполнена в рамках Государственной программы научных исследований «Цифровые и космические технологии, безопасность общества и государства» (подпрограмма «Цифровые технологии и космическая информатика», задание 5.1.6.3).

Для цитирования. Чернявский, А. Ф. Особенности структурно-аппаратного обеспечения преобразования информации в криптосистемах / А. Ф. Чернявский, Е. И. Козлова, Ю. А. Чернявский // Доклады БГУИР. 2024. Т. 22, № 5. С. 80–88. http://dx.doi.org/10.35596/1729-7648-2024-22-5-80-88.

FEATURES OF STRUCTURAL HARDWARE TRANSFORMATION OF INFORMATION IN CRYPTOSYSTEMS

ALEXANDER F. CHERNYAVSKIY[1], ELENA I. KOZLOVA[1], YURI A. CHERNYAVSKIY[2]

[1]*Belarusian State University (Minsk, Republic of Belarus)*
[2]*Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)*

Submitted 30.04.2024

Abstract. The article considers types, functions and some features of cryptosystems, as well as circuit design options for expanding their functionality. Options for generating keys and ciphers used in cryptosystems with a typical structural organization, and technologies for creating encryption chains are presented. An encryption scheme is described, in the recurrent formula of the algorithm of which the previous blocks of both encryption and plaintext are used. This scheme reliably protects against any unauthorized modification of the encrypted text. Structural diagrams of the organization of symmetric and asymmetric cryptosystems are given. A variant of implementing a decoding procedure in a threshold MIMA cryptomodule for sharing a secret with a masking transformation is proposed, in which the necessary time and hardware costs for performing the procedure of reconstructing the original secret are minimized. The presented material can be the part of the original sections of a necessary and sufficiently provided in mathematical terms textbook on the basics and modern problems of cryptography.

Keywords: cryptosystem, cipher, key, hash function, random number generator, minimum redundant modular coding, cryptographic strength, conversion, transport coding, MIMA cryptomodule.

Conflict of interests. The authors declare no conflict of interests.

Gratitude. This work was carried out in the frames of the State Programme of Scientific Research “Digital and Space Technologies, Security of Society and the State” (Subprogramme “Digital Technologies and Space Informatics”, assignment 5.1.6.3).

For citation. Chernyavskiy A. F., Kozlova E. I., Chernyavskiy Yu. A. (2024) Features of Structural Hardware Transformation of Information in Cryptosystems. *Doklady BGUIR*. 22 (5), 80–88. http://dx.doi.org/10.35596/1729-7648-2024-22-5-80-88 (in Russian).

Введение

Криптосистема – это система, представляющая собой программно-аппаратный комплекс, объединяющий в единое целое набор криптосхем, шифров и средств обеспечения оперативного криптографического преобразования информации [1]. Методы и средства криптографического преобразования информации изучаются в криптографии, а проблемы практической стойкости шифров – в криптоанализе. Криптография и криптоанализ развиваются параллельно. Криптографы всегда пытаются создать такую криптосистему, которая была бы стойкой ко всем известным методам криптоанализа. Исследованием совместного применения методов криптографии и криптоанализа занимается криптология.

В основу любой криптосистемы положен шифр. К криптосистемам с типовой структурной организацией относят системы, основанные на симметричных и асимметричных алгоритмах шифрования. По типам схем обработки потоков информации симметричные криптосистемы делятся на поточные и блочные, а асимметричные – на двухключевые и алгоритмы электронной цифровой подписи (ЭЦП). Существенную значимость для криптосистем имеют алгоритмы формирования временной последовательности с блочной схемой разбиения, при которой длина каждого блока соответствует интервалу шифрования. При этом криптопреобразование над каждым блоком осуществляется независимо.

Простейший вариант формирования последовательности интервалов шифрования недостаточно устойчив к таким известным методам криптоанализа, как «атака на основе известного открытого текста» и «атака на основе выбранного открытого текста», что не позволяет широко его использовать в криптосистемах. В настоящее время данный метод шифрования существенно модернизирован.

Современные криптосистемы обладают специальной функцией защиты от внешних атак, позволяющей обнаружить несанкционированные изменения информации посредством осуществления программно-аппаратного контроля за параметрами информационных потоков как в преде-

лах криптосистемы, так и напрямую с ней не связанных. Стойкость современных криптосистем обусловлена устойчивостью их алгоритмов к применению методов криптоанализа (криптостойкостью) и конфиденциальностью относительно небольшого блока информации, называемой секретным ключом.

Изложенный в статье материал может быть частью исходных разделов необходимого и достаточно обеспеченного в математическом плане учебного пособия по проблемам криптографии «Особенности структурного и аппаратного обеспечения криптографического преобразования информации в криптосистемах».

Варианты ключей, используемых в криптосистемах с типовой структурной организацией

Если алгоритм шифрования является долгосрочным и устойчивым элементом криптосистемы, то ключ используется для управления процессом криптографического преобразования (шифрования) и является легко сменяемым элементом криптосистемы. Мастер-ключ формируется системой управления или пользователем из парольной фразы. Ключ сеанса генерируется системой управления для шифрования каждого нового сообщения на основе использования последовательности случайных или псевдослучайных чисел. Ключ сеанса шифруется мастер-ключом пользователя и помещается в заголовок сообщения.

На сегодняшний день разработаны как простые, так и относительно сложные схемы создания ключа [1]. В простых схемах ключ может сформировать самостоятельно отправитель сообщения, в более сложных – ключ формируется автоматически программным обеспечением, либо запрашивается у базы данных ключей. Ввиду того, что ключ представляет собой большую последовательность целых чисел, которую трудно запомнить обычному человеку, пользователю предлагается вводить пароль – конкретную заданную последовательность, состоящую, например, из текста, символов и цифр.

Ключ каждого сеанса используется для шифрования только одного сообщения, поэтому при получении злоумышленником значения такого ключа нарушается конфиденциальность лишь одного сообщения. Таким образом обеспечивается дополнительная криптостойкость системы и исключается необходимость обмениваться мастер-ключом по защищенному каналу.

Технология обработки потоков информации

По технологии обработки потоков информации симметричные криптоалгоритмы подразделяются на поточные и блочные шифры. Поточный шифр обрабатывает информацию побитно и применяется прежде всего тогда, когда информацию невозможно разбить на блоки (например – потоковое видео). В блочных шифрах для обработки информация делится на блоки заданного объема (64, 128, 256 или 512 бит). Асимметричные криптоалгоритмы всегда являются блочными. Для криптосистем, основанных на блочных криптоалгоритмах, могут применяться две различные технологии обработки потоков информации.

Простейшая схема блочного шифрования позволяет из текста (*M*) произвольной длины сформировать блоки (*Mi*), которые затем шифруются (*Encrypt*) независимо друг от друга, при этом длина формируемого блочного шифра (*Ci*) равняется длине шифруемого участка сообщения, как показано на рис. 1.

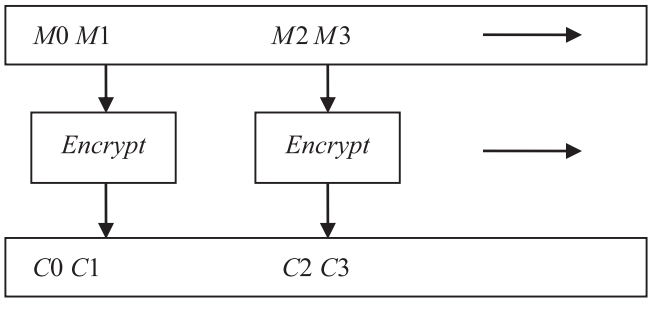

Рис. 1. Простейшая схема шифрования
Fig. 1. Simplest encryption scheme

Существенный недостаток данной схемы обусловлен тем, что при шифровании двух одинаковых блоков на выходе формируются два идентичных блока шифрованного текста. Наличие указанного недостатка создает уязвимость с точки зрения возможности модификации шифрованного текста. Недостаток устраняется относительно простой модификацией такой схемы путем применения схемы шифрования «со сцеплением блоков». Благодаря введению рекуррентной формулы в схеме шифрования «со сцеплением блоков» результат шифрования текущего блока данных будет зависеть от значения предыдущего блока, связывая таким образом воедино весь документ. Как показано на рис. 2, текущий блок *M*1 открытого текста инициирует операцию «исключающее ИЛИ» (*XOR*) на шифротекст предыдущего блока *C*0 и только потом производится его шифрование. Таким образом при искажении одного блока шифротекста полностью повреждаются модифицированные измененные биты в схеме блока. Эта схема достаточно надежно защищает от модификации зашифрованного потока [1].

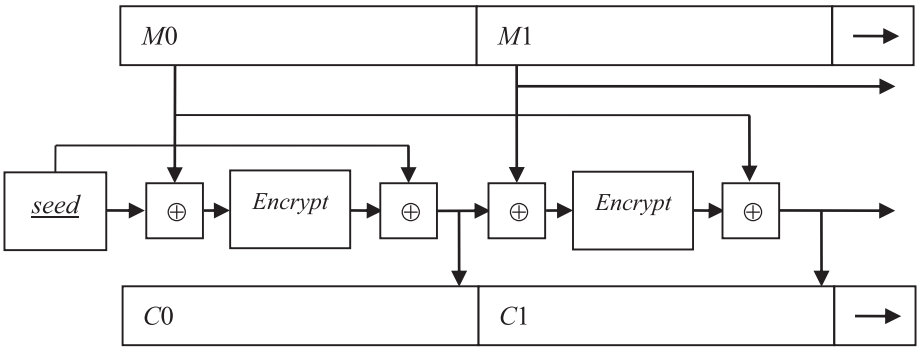

Рис. 2. Схема шифрования «со сцеплением блоков»:
⊕ – *XOR* («исключающее ИЛИ»); *seed* – генератор случайных чисел
Fig. 2. Block chaining encryption scheme: ⊕ – *XOR* (“exclusive OR”); s*eed* – random number generator

Структурная организация криптосистем

Все криптоалгоритмы с ключом подразделяются на симметричные и асимметричные. При симметричном шифровании используется один и тот же ключ ($K_с$), называемый секретным ключом, как для шифрования, так и для дешифрования информации. Для данных схем также допускается различие ключей для шифрования и дешифрования при условии существования криптоалгоритма их взаимного вычисления. Секретный ключ не должен быть известен никому, кроме отправителя и получателя сообщения, поскольку позволяет получить полный доступ к информации, содержащейся в шифрограмме. Алгоритмы симметричных криптосхем должны быть практически стойкими, чтобы исключить наличие слабых мест, для которых прослеживается взаимосвязь между незашифрованным и зашифрованным сообщениями, а также не позволить узнать ключ по множеству пар (зашифрованное сообщение – незашифрованное сообщение).

В асимметричном варианте при применении криптосхемы для шифрования сообщения (идентификации лица, подписавшего документ, в случае выработки ЭЦП ($K_з$)) применяется один ключ ($K_о$), а для дешифрования (аутентификации лица, подписавшего документ, в случае выработки ЭЦП ($K_о$)) – другой ($K_з$). Процедура шифрования в асимметричных системах реализуется таким образом, чтобы злоумышленник не смог восстановить исходный текст, даже зная зашифрованный текст *C* и открытый ключ шифрования $K_о$. Такие криптосистемы закрывают возможность осуществления злоумышленником попыток выяснить либо исходный текст *M*, либо закрытый ключ шифрования $K_з$ по определенному, достаточно большому объему зашифрованных данных *C*, а также узнать закрытый ключ шифрования $K_з$ по известному исходному *Mi*, соответствующему зашифрованному тексту *Ci* и открытому ключу $K_о$.

В состав криптосистем входят схемы шифрования и управления ключами. Схема шифрования, как правило, включает в себя алгоритм первоначального преобразования, в том числе алгоритм сжатия, непосредственно алгоритм шифрования, алгоритм заключительной перестановки и схему транспортного кодирования. Схема управления ключами в большинстве случаев включает в себя алгоритм преобразования парольной фразы в мастер-ключ, алгоритм вычисления хеш-функции ключа, генератор случайных чисел, систему управления цифровыми сертификата-

ми и алгоритм выработки ключа сеанса. Общая структура криптосистемы симметричного типа представлена на рис. 3 (где ГСЧ – генератор случайных чисел) [2].

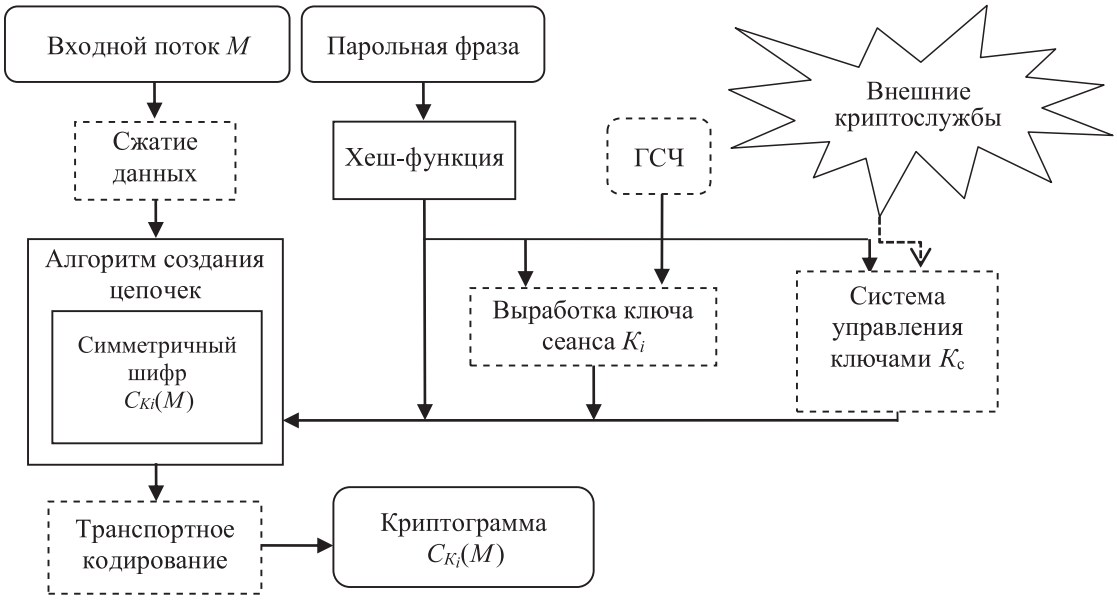

Рис. 3. Структура криптосистемы симметричного типа
Fig. 3. Structure of a symmetric type cryptosystem

Асимметричные криптосистемы в качестве своего основного элемента используют алгоритмы шифрования на открытом ключе. По своей криптостойкости они сравнимы с симметричными алгоритмами, однако, ввиду особенности функционирования самого процесса шифрования, быстродействие у асимметричных алгоритмов существенно ниже. В силу этого свойства они находят применение в схемах, где необходимо надежно зашифровать блоки данных небольших размеров, например, хеш-функцию документа при его подписании ЭЦП, либо ключ сеанса для алгоритма симметрического шифрования, как представлено на рис. 4 [2].

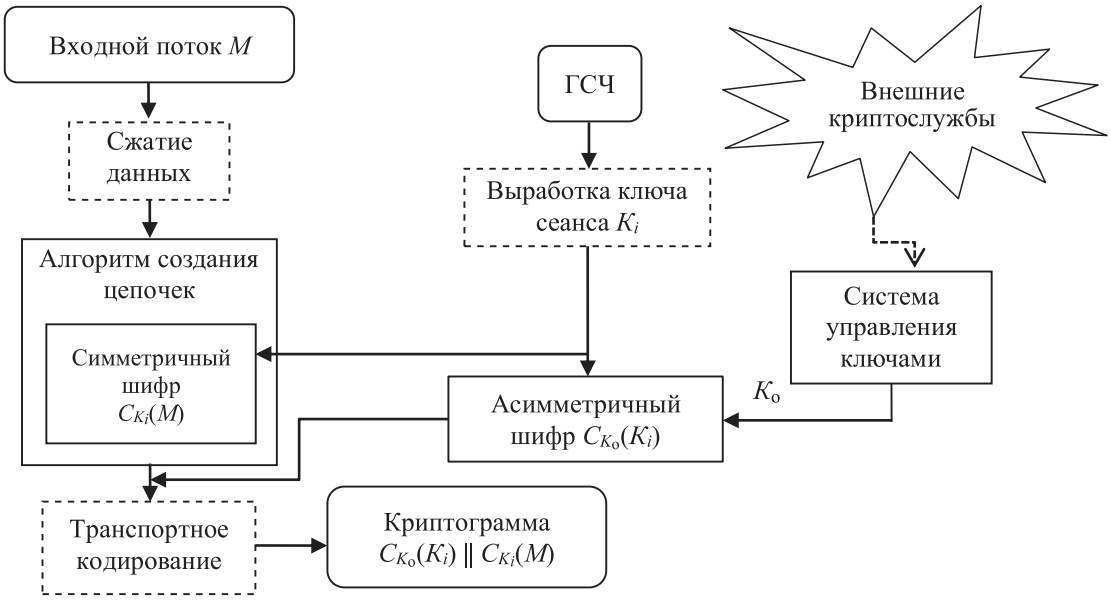

Рис. 4. Структура криптосистемы асимметричного типа
Fig. 4. Structure of an asymmetric type cryptosystem

В случае применения асимметричной криптосистемы текст сообщения M шифруется блочным шифром с использованием ключей сеанса. Открытым ключом K_o шифруется только ключ сеанса K_i, формируемый передающей стороной. Сообщение в целом состоит из зашифрованного

ключа сеанса $C_{K_o}(K_i)$ и собственно основной шифрограммы $C_{K_i}(M)$. После завершения шифрования, как и в любой другой криптосхеме, ключ сеанса уничтожается, а криптограмма отправляется получателю. На приемной стороне с помощью закрытого ключа дешифруется ключ сеанса, а затем уже и само сообщение [2].

Назначение блока «транспортное кодирование» на выходе – превращать исходный поток сигналов в поток большего объема, состоящий только из печатных символов ASCII. Такой блок необходим вследствие того, что во многих случаях криптосистемы являются прозрачной прослойкой систем передачи данных. Например, если система проектировалась для передачи текстовых сообщений по электронной почте, то соглашение, формируемое при встраивании криптопрослоек, не должно нарушать исходного разрешенного набора символов.

Способная необратимо изменять данные хеш-функция получила широкое распространение в алгоритмах быстрого поиска информации. В настоящее время она ничуть не в меньшей мере используется в криптографии. Вычисление «неподделываемых» контрольных сумм документов $HASH(M)$ является основным, но не единственным назначением хеш-функции в криптографии.

При использовании алгоритма хеширования в условиях невозможности подобрать иной документ с той же хеш-суммой и два документа $M1$ и $M2$ с произвольной одинаковой хеш-суммой $HASH(M1) = HASH(M2)$ хеш-сумма становится уникальной характеристикой документа. Именно такое свойство позволило свести проблему защиты большого блока данных к решению задачи защиты маленького блока данных заранее известной длины, что нашло широкое применение в алгоритмах формирования ЭЦП.

В системах электронной цифровой подписи ключи асимметричных алгоритмов применяются в обратном порядке. На стороне лица, подписывающего документ (отправителя), закрытым ключом отправителя $K_з$ шифруется не сам электронный документ M, а только его хеш-сумма $HASH(M)$. Документ M в открытом виде и зашифрованное значение хеш-суммы $C_{K_з}(HASH(M))$ отправляют получателю. Получатель на своей стороне проверяет ЭЦП путем самостоятельного вычисления значения хеш-суммы и сверки его со значением хеш, извлеченным из ЭЦП и расшифрованным с помощью открытого ключа отправителя K_o. При совпадении значений хеш-сумм весь документ признается целостным и аутентичным.

Случайные числа применяются при создании ключей сеанса симметричных схем и закрытых ключей асимметричных схем, при подписании документов и в схемах разделения секрета. Криптографические алгоритмы генерации псевдослучайных чисел установлены СТБ 34.101.47–2017. Алгоритмы стандарта могут применяться для построения ключей, синхропосылок, одноразовых паролей, других непредсказуемых или уникальных параметров криптографических алгоритмов и протоколов [3].

ГСЧ создаются либо на основе использования информации из физических процессов, либо из самой ЭВМ. Фотоприемники, работающие в режиме одноквантовой регистрации, детекторы событий ионизирующей радиации, высокоточные измерители теплового шума полупроводниковых устройств или космическое излучение – основные устройства либо источники, используемые для этих целей. На современных компьютерах генерация случайных чисел затруднительна, поскольку компьютеры по своей конструкции являются детерминированными системами. С учетом этого проблема генерации случайной последовательности с произвольным законом распределения вероятностей сводится к задаче генерации равномерно распределенной случайной последовательности (РРСП). Стойкость криптосистем во многом определяется уровнем соответствия модели РРСП применяемых в таких системах псевдослучайных последовательностей, поэтому важно оценивать этот уровень с помощью универсального алгоритма тестирования случайных и псевдослучайных последовательностей [1].

Генераторы РРСП – устройства, позволяющие по запросу получать некоторую случайную последовательность чисел $(x_1, \ldots, x_n) \in A$ длиной $n \in N$, элементы которой $x_1, \ldots, x_n$ называются случайными числами и распределены по равномерному закону. Существуют табличный, физический и программный генераторы РРСП. Программные генераторы РРСП наиболее известны.

Итак, РРСП – это случайная последовательность $x_1, \ldots, x_t, x_{t+1}\ldots$ со значениями в дискретном множестве A, определенная на вероятностном пространстве (Ω, F, P) и удовлетворяющая следующим свойствам [1]:

– для любого $n \in N$ и произвольных значений индексов $1 \le (t_1 < \ldots < t_n)$ случайные величины $(x_{t1}, \ldots, x_{tn}) \in A$ независимы в совокупности;

– для любого номера $t \in N$ случайная величина x_t является бернуллиевой и имеет дискретное, равномерное на A распределение вероятностей:

$$P(X_t = I) = 1/2,\ i \in V = \{0,1\}.$$

В современных криптосистемах широко используются равномерно распределенные случайные последовательности или имитирующие их псевдослучайные последовательности. Для программирования обычно применяются псевдослучайные числа, полученные детерминированным алгоритмом из некоторого начального значения *seed*. Последовательность $\{x_t\}$ называется псевдослучайной, когда она вычисляется по некоторому известному детерминированному соотношению и обладает статистическими свойствами, схожими с РРСП. Поскольку стойкость криптосистем во многом определяется уровнем соответствия модели РРСП и используемых последовательностей $x_t \in A$ (t = 1, 2, …), важно на практике оценивать этот уровень. В [1] предложен универсальный алгоритм тестирования случайных и псевдослучайных последовательностей.

Реализация декодирующей процедуры в пороговом криптомодуле разделения секрета с маскирующим преобразованием, основанным на базе избыточных модулярных вычислительных структур

Применяемая технология управления криптографическими ключами выполняет особую роль при решении актуальной задачи обеспечения необходимого уровня безопасности при хранении, обработке и передаче данных. В качестве компьютерно-арифметической основы для криптографических приложений рассматриваемого класса целесообразно принять модулярную арифметику – арифметику модулярных систем счисления (МСС). Фундаментальные преимущества МСС наиболее полно удается реализовать в рамках так называемого минимально избыточного кодирования [4, 5].

Введение в модулярный код минимальной избыточности существенно упрощает расчет интервально-индексных характеристик и связанных с ними форм представления целого числа при реализации ряда немодульных операций [6]. Отмеченное обстоятельство обуславливает целесообразность использования минимально избыточной модулярной арифметики (МИМА) в решении задач преобразования информации в криптосистемах. Приведенные в [7] исследования привели к формированию принципиально новой основы для создания пороговых криптосхем разделения секрета с применением минимально избыточного модулярного кодирования.

Наиболее перспективными технологиями, расширяющими функциональные возможности криптосхем и повышающими их устойчивость к применению методов криптоанализа, считаются технологии так называемой активной безопасности. Такие технологии предусматривают периодическое обновление ключей, одноразовых паролей и пространственное разделение секрета. Пространственное разделение секрета между n абонентами с возможностью его восстановления по компонентам любого абонента ($2 \le t \le l \le n$; t – пороговое число абонентов) обеспечивается решающим правилом, реализуемым (t, n) – пороговой системой. Концептуальную базу (t, n) – пороговой МИМА-схемы разделения секрета, которая рассчитана на полное число n и пороговое число t абонентов распределенной системы, составляют следующие определяющие положения [7]:

1) исходный секрет, разделяемый n сторонами, представляет собой целое число $S \in Z_p$, где p – большой модуль, взаимно простой с $p_1, p_2, \ldots, p_n$;

2) над S в МСС с базисом P выполняется маскирующее преобразование вида $\hat{S} = S + C_p$ (C_p – псевдослучайная целочисленная величина). Цифровые значения $\tilde{\sigma}_i = \left|\tilde{S}\right|_{p_i} = \left|\sigma_i + \left|C_p\right|_{p_i}\right|_{p_i}$; $\sigma_i = \left|S\right|_{p_i}$; $i = \overline{1,n}$, получаемого кода (σ_1, σ_2, …, σ_n) рассматриваются как долевые (частичные) секреты, принадлежащие одноименным абонентам;

3) любые t или более абонентов могут восстановить секрет-оригинал S по принадлежащим им маскирующим частичным секретам. Но никакая группа абонентов числом менее t сделать этого не может;

4) область (диапазон) изменения маскирующего секрета $\tilde{S}$ согласуется с принципом минимально избыточного модулярного кодирования, что обеспечивает возможность выполнения декодирующей операции (операции восстановления секрета-оригинала) по упрощенным МИМА-процедурам.

Реконструкция секрет-оригинала группой абонентов численностью $k < t$ невозможна. Исходный и долевые секреты представляют собой большие целые числа. В связи с этим эффективность выполняемых в пороговых криптосистемах преобразований определяется свойствами используемой технологии перевода реализуемых вычислений из диапазонов больших чисел в диапазоны целых чисел стандартной разрядности. Наиболее трудоемкой операцией в пороговых криптосистемах рассматриваемого типа является реконструкция секрета-оригинала по модулярным кодам маскирующего аналога. В [8] представлен метод выполнения декодирующей операции в пороговом криптомодуле разделения секрета. Его основой также является МИМА. Фундаментальные преимущества МСС наиболее полно реализуются в рамках применения минимально избыточного модулярного кодирования и ассоциированной с ним интервально-модулярной формой представления чисел. В этом варианте минимизируются необходимые временные и аппаратные затраты на выполнение процедуры реконструкции секрет-оригинала.

Заключение

1. Представлена схема шифрования, в рекуррентной формуле алгоритма которой задействован не только предыдущий блок шифрования, но и предыдущий открытый блок. Эта схема надежно защищает от любой несанкционированной модификации зашифрованного текста.

2. Обозначены ограничения на диапазон изменения маскирующего аналога секрет-оригинала, обеспечивающие возможность применения минимально избыточной модулярной арифметики в пороговой схеме рассматриваемого класса без снижения ее криптостойкости [8].

3. Разработана концептуальная база (t, n) пороговой минимально избыточной модулярной арифметики – схемы разделения секрета, которая рассчитана на полное число абонентов n и пороговое число t.

Список литературы

1. Харин, Ю. С. Математические и компьютерные основы криптологии / Ю. С. Харин. Минск: Новое знание, 2003.
2. Конев, И. Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. СПб.: БХВ-Петербург, 2003.
3. Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел: СТБ 34.101.47–2017.
4. Чернявский, А. Ф. Особенности машинной арифметики высокопроизводительных модулярных вычислительных структур / А. Ф. Чернявский, Е. И. Козлова, А. А. Коляда // Журнал Белорусского государственного университета. Математика. Информатика. 2023. № 2. С. 94–101.
5. Червяков, Н. И. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Н. И. Червяков, А. А. Коляда, П. А. Ляхов. М.: Физматлит, 2017.
6. Коляда, А. А. Модулярная интерпретация сообщений в системах защиты информации / А. А. Коляда, С. Ю. Протасеня, Н. И. Червяков // Инфокоммуникационные технологии. 2015. Т. 13, № 3. С. 245–252.
7. Коляда, А. А. Пороговый метод разделения секрета на базе избыточных модулярных вычислительных структур / А. А. Коляда, П. В. Кучинский, Н. И. Червяков // Информационные технологии. 2019. Т. 25, № 9. С. 553–561.
8. Чернявский, А. Ф. Метод деления на двоичную экспоненту для выполнения декодирующей операции в пороговом мини-криптомодуле разделения секрета в маскирующем преобразовании / А. Ф. Чернявский, А. А. Коляда, С. Ф. Протасеня // Теоретическая и прикладная криптография: матер. Междунар. науч. конф. Минск: Белор. гос. ун-т, 2020. С. 99–104.

References

1. Kharin Yu. S. (2003) *Mathematical and Computer Foundations of Cryptology.* Minsk, Novoe Znanie Publ. (in Russian).
2. Konev I. R., Belyaev A. V. (2003) *Information Security of an Enterprise*. St. Petersburg, BHV-Petersburg Publ. (in Russian).

3. State Standard of the Republic of Belarus STB 34.101.47–2017. *Information Technology and Security. Cryptographic Algorithms for Generating Pseudorandom Numbers* (in Russian).
4. Chernyavsky A. F., Kozlova E. I., Kolyada A. A. (2023) Features of Machine Arithmetic of High-Performance Modular Computing Structures. *Journal of the Belarusian State University. Mathematics. Computer Science*. (2), 94–101 (in Russian).
5. Chervyakov N. I., Kolyada A. A., Lyakhov P. A. (2017) *Modular Arithmetic and Its Applications in Infocommunication Technologies*. Moscow, Fizmatlit Pabl. (in Russian).
6. Kolyada A. A., Protasenya S. Yu., Chervyakov N. I. (2015) Modular Interpretation of Messages in Information Security Systems. *Infocommunication Technologies*. 13 (3), 245–252 (in Russian).
7. Kolyada A. A., Kuchinsky P. V., Chervyakov N. I. (2019) Threshold Method of Secret Sharing Based on Redundant Modular Computing Structures. *Information Technologies*. 25 (9), 553–561 (in Russian).
8. Chernyavsky A. F., Kolyada A. A., Protasenya S. F. (2020) Method of Division by Binary Exponent for Performing a Decoding Operation in a Threshold Mini-Cryptomodule for Sharing a Secret in a Masking Transformation. *Theoretical and Applied Cryptography: Proceedings of the International Scientific Conference*. Minsk, Belarusian State University. 99–104 (in Russian).

Вклад авторов / Authors' contribution

Авторы внесли равный вклад в написание статьи / The authors contributed equally to the writing of the article.

Сведения об авторах

Чернявский А. Ф., д-р техн. наук, акад. Нац. акад. наук Беларуси, проф., проф. каф. интеллектуальных систем, Белорусский государственный университет (БГУ)

Козлова Е. И., канд. физ.-мат. наук, доц., зав. каф. интеллектуальных систем, БГУ

Чернявский Ю. А., канд. техн. наук, доц., доц. каф. информатики, Белорусский государственный университет информатики и радиоэлектроники

Адрес для корреспонденции

220030, Республика Беларусь,
г. Минск, просп. Независимости, 4
Белорусский государственный университет
Тел.: +375 17 209-58-36
E-mail: kozlova@bsu.by
Козлова Елена Ивановна

Information about the authors

Chernyavskiy A. F., Dr. of Sci. (Tech.), Academician of the National Academy of Sciences of Belarus, Professor, Professor at the Department of Intelligent Systems, Belarusian State University (BSU)

Kozlova E. I., Cand. of Sci., Associate Professor, Head of the Intelligent Systems Department, BSU

Chernyavskiy Yu. A., Cand. of Sci., Associate Professor, Associate Professor at the Department of Informatics, Belarusian State University of Informatics and Radioelectronics

Address for correspondence

220030, Republic of Belarus,
Minsk, Nezavisimosti Ave, 4
Belarusian State University
Tel.: +375 17 209-58-36
E-mail: kozlova@bsu.by
Kozlova Elena Ivanovna