Раздел V. Прикладные вопросы информационной безопасности

УДК 631.8

И.А. Калмыков, О.И. Дагаева, Д.О. Науменко, О.В. Вельц

СИСТЕМНЫЙ ПОДХОД К ПРИМЕНЕНИЮ ПСЕВДОСЛУЧАЙНЫХ ФУНКЦИЙ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрены протоколы, используемые в системах электронных платежей (СЭП), в которых применение разработанной псевдослучайной функции (ПСФ) повышенной эффективности обеспечивает требуемый уровень защиты информации при меньшей длине ключа. Данная разработанная псевдослучайная функция, за счет уменьшения количества умножений и сокращения размерности обрабатываемых аргументов, позволяет снизить требования к объему памяти, используемой для вычисления ее значений. Дальнейшее повышение эффективности разработанной ПСФ возможно за счет применение системного подхода к расширению числа протоколов, в которых возможно применять эту функцию.

Целью исследований является сокращение объема памяти, которое занимает программное обеспечение, необходимое для эффективной работы носителя электронных денежных средств (смарт-карты) за счет системного подхода к увеличению числа протоколов, реализованных с помощью разработанной псевдослучайной функции. Это позволит увеличить объем свободной памяти носителя, в которой будет храниться электронная наличность.

Системы электронных платежей; криптографические протоколы защиты данных; псевдослучайная функция; протокол доказательства с нулевым разглашением.

I.A. Kalmykov, O.I. Dagayeva, D.O. Naumenko, O.V. Velts

A SYSTEM APPROACH TO USAGE OF PSEUDORANDOM FUNCTION IN THE DATA PROTECTION SYSTEMS

The paper deals with the protocols used in electronic payment systems (EPS), in which the use of the developed pseudo-random function (PRF) increased efficiency provides the required level of security with a smaller key length. This developed pseudo-random function, by reducing the number of multiplications and dimensionality reduction process arguments to reduce the memory requirements used to calculate its value. Improving the effectiveness of the developed PRF is possible due to the use of a systematic approach to expanding the number of protocols in which it is possible to use this feature.

The aim of this research is reducing of the volume occupied by the software which is needed for the effective operation of the e-money carrier (smart card) by system approach to increase the number of protocols implemented by the developed pseudorandom function. This will increase the amount of free memory medium in which to store electronic cash.

Electronic payment systems; cryptographic protocols data protection; pseudorandom function; the zero-knowledge proof protocol.

Лавинообразный рост числа пользователей сети Интернет стал одной из главных предпосылок создания и бурного развития электронного бизнеса. Электронный бизнес характеризуется высокой динамикой изменения среды, в которой осуществляется экономическая деятельность. При этом его организация и ведение

в электронной форме ставят ряд специфических проблем, связанных с корректным функционированием и обеспечением его безопасности. Существенное увеличение числа участников экономической деятельности и перенесение ее части в информационное пространство приводит к тому, что вопросы безопасности организации бизнеса приобретают весьма актуальное содержание. Особенно высокие требования предъявляются к организации системам электронных платежей (СЭП). Основным требованием к системам, обеспечивающим электронные платежи по сделкам, является надежность и безопасность их использования [1].

Анализ отечественного рынка платежных систем, который еще находится на этапе своего развития, показывает, что в нем реально работают несколько различных решений, начиная от традиционных платежных карт и заканчивая – электронной наличностью. При этом последние становятся универсальным платежным средством, благодаря низкой стоимости выполнения транзакций, простотой делимости и объединяемости, более высокой степени защищенности от хищения, подделки, изменения номинала.

Очевидно, что одним из основных свойств любой системы безналичных расчетов является обеспечение безопасности всех ее компонентов на всех этапах функционирования этой системы. При этом покупатель, использующий электронную наличность, продавец, эмитент и эквайер должны быть уверены в защите своих вложений. К сожалению, всестороннее развитие Интернета и мобильной связи, как показал анализ, не позволяют в полной мере обеспечить требуемый уровень защиты данных. Поэтому разработка протоколов, обладающих высокой степенью защиты данных от несанкционированного доступа (НСД), является актуальной задачей.

Проведенный анализ работ [1–3] позволил выделить ряд протоколов, реализация которых позволит обеспечить эффективную работу автономной системы электронных платежей. В работе [4] показано, что вопросы защиты электронной наличности, используемой современными СЭП, возлагается на протоколы криптографической защиты. При этом для организации эффективного функционирования таких систем применяются различные криптографические алгоритмы. Очевидно, что такой подход способствует увеличению размеров программного обеспечения, применяемом на электронном носителе наличности «электронном кошельке». Это приводит к значительному уменьшению свободного объема памяти, которое может использовать пользователь для хранения электронных денег.

Разрешить сложившуюся ситуацию, когда, с одной стороны, в работе СЭП используются несколько криптографических протоколов для обеспечения высокого уровня защиты информации, а, с другой стороны, возрастают требования к свободному объему энергонезависимой памяти смарт-карты, которая используется в качестве хранилища электронных средств платежа, возможно лишь на основе системного подхода.

Известно, что системный анализ (СА) - наиболее конструктивное направление, используемое для практических приложений теории систем к задачам управления, обработки информации. Конструктивность системного анализа связана с тем, что он предлагает методику проведения работ, позволяющую не упустить из рассмотрения существенные факторы, определяющие построение эффективных систем управления в конкретных условиях. При этом современный системный анализ представляет собой совокупность методов и средств, позволяющих исследовать свойства, структуру и функции объектов, явлений или процессов в целом, представив их в качестве систем со всеми сложными межэлементными взаимосвязями, взаимовлиянием элементов на систему и на окружающую среду, а также влиянием самой системы на ее структурные элементы [5].

Применяя методы системного анализа, было проведено исследование основных видов протоколов, которые используются в современных СЭП, работающих с электронными деньгами. На основе полученных результатов был сделан вывод, суть которого состоит в следующем. Для обеспечения эффективной работы носителя электронных денежных средств (смарт-карты) необходимо использовать в различных протоколах одну псевдослучайную функцию.

В настоящее время псевдослучайны функции стали неотъемлемым элементом практически любой системы обработки и передачи информации, независимо от ее сложности и назначения. Как правило, для их реализации используются программные и программно-аппаратные средства генерации. Основными сферами применения ПСФ являются системы космической связи и навигации, помехоустойчивое кодирование техническое диагностирование компонентов компьютерных систем, защита информации [6–8].

Во всех вышеперечисленных случаях ПСФ используются либо непосредственно, либо на их основе строятся алгоритмы хеширования информации. Но при этом каждая из областей применения ПСФ предъявляет к псевдослучайным функциям свои требования. Так при реализации процедур кодировании и защиты информации качество операций генерации псевдослучайных функций и хеширования определяется в первую очередь эффективностью ПСФ. Таким образом, именно от свойств псевдослучайных функций, особенно в тех случаях, когда необходимо обеспечить устойчивую работу системы при наличии случайных и умышленных деструктивных воздействий, будет в значительной степени зависит эффективность работы СЭП. Поэтому задача разработки высокоэффективных ПСФ является актуальной.

На основе системного подхода при проведении исследований основных алгоритмов формирования ПСФ была разработана псевдослучайная функция, удовлетворяющая отмеченным выше требованиям. Как показано в работе [9] была разработана ПСФ, принимающая на входную последовательность $(x_1,\ldots,x_n)$ и ключ $(g,s_1,\ldots,s_n)$, обеспечивает выполнение равенства

$$F((s_1,\ldots,s_n),(g,x_1,\ldots,x_n)) = g^{\left(\frac{1}{\prod_{i=1}^{n}(s_i+x_i)}\right)}, \qquad (1)$$

где g – первообразный элемент мультипликативной группы.

Представленные в работе [9] теоремы, позволили показать, что для области определения размером 2^m значение $n = m/\log_2 l$. Вследствие этого при вычислении данной функции требуется в $\log_2 l$ раз меньше умножений. При этом при сравнении с псевдослучайной функцией Наора-Рейнголда разработанная ПСФ использует меньший объем памяти для вычисления конечного за счет уменьшения в $\log_2 l$ раз размера ключа. Но при этом, стойкость данной ПСФ основывается на доказательстве о сложности решения λ-DDH проблемы.

Вопросы применения разработанной псевдослучайной функции в протоколах определения двойной оплаты и протоколе снятия со счета подробно рассмотрены в работе [10]. Однако наряду с данными протоколами для эффективной работы системы электронных платежей используются и другие. Особое внимание хотелось бы обратить на протокол «выплаты одной монеты».

Для организации протокола выплаты электронной наличности пользователь имеет два ключа – открытый $К_{отк}$ и секретный $К_{секр}$. Открытый ключ применяется банком при выдаче электронного кошелька своему абоненту-покупателю. Секретный ключ покупателя $К_{секр}$ участвует в процессе выплаты электронных денег.

Но при этом $К_{секр}$ должен быть в таком виде, чтобы продавец не смог его вычислитель самостоятельно.

В данной системе электронных платежей покупатель, будучи легальным пользователем системы, вычисляет свой открытый ключ согласно

$$K_{отк} = g^{К_{секр}} \bmod q, \tag{2}$$

где q – порядок мультипликативной группы с порождающим элементом g.

Для осуществления процедуры выплаты у покупателя должен быть в наличии электронный кошелек W, который содержит секретный ключ владельца $К_{секр}$, параметр S для генерации номера электронной купюры, параметр T для проведения протокола «двойной выплаты», $\sigma_{K_{БС}}(C)$ − подпись банка на вручение C, которое использовал покупатель при получении кошелька в банке, J – показатель счетчика электронных монет

$$W = (K_{секр}, S, T, \sigma_{K_{БС}}(C), J). \tag{3}$$

Для осуществления покупки владелец электронного кошелька обращается к продавцу. При этом он должен доказать последнему следующие моменты:

в кошельке W есть подпись банка $\sigma_{K_{БС}}(C)$ на вручение C, т.е.

$$\sigma_{K_{БС}}(C) = \sigma_{K_{БС}}(K_{секр}, S, T); \tag{4}$$

покупатель правильно сгенерировал S_J номер J-ой электронной купюры, т.е.

$$S_J = g^{\frac{1}{S+J+1}}; \tag{5}$$

покупатель правильно сгенерировал число T_J , которое используется в уравнении двойной выплаты электронной купюры, т.е.

$$T_J = K_{отк} g^{\frac{1}{T+J+1}}. \tag{6}$$

Рассмотрим более подробно каждый этап протокола «выплаты одной монеты». На первом этапе, для того чтобы доказать продавцу, что в электронном кошельке присутствует подпись банка, выдавшего электронные купюры, покупатель вычисляет вручение

$$C = (\mathrm{g}^{\left(\prod_{j=1}^{m}(K_i+S_i+T_i)\right)^{-1}}) \bmod q, \tag{7}$$

где K_i , S_i и T_i – i-й блок, полученный при разбиении чисел секретного ключа $К_{секр}$, параметров S и T на m частей; q – порядок мультипликативной группы с порождающим элементом g.

Затем, используя свой секретный ключ, покупатель закрывает данные $E_{K_{секр}}(C, \sigma_{K_{БС}}(C))$ и пересылает зашифрованный текст продавцу. Продавец, зная открытый ключ покупателя, расшифровывает данное сообщение $D_{K_{отк}}(C, \sigma_{K_{БС}}(C))$ и получает в открытом виде вручение C и подпись банка на это вручение $\sigma_{K_{БС}}(C)$.

После этого продавец обращается в банк и, получив его открытый ключ, расшифровывает его подпись. Результатом данной процедуры является вручение C, которое представил покупатель в банк для получения кошелька. Продавец сравнивает эти значения. При совпадении этих значений продавец убеждается, что у покупателя есть электронный кошелек.

На втором этапе выполнения протокола «выплаты одной монеты» продавец должен убедиться, что покупатель правильно сгенерировал S_J номер J-й электронной купюры и число T_J, которое используется в уравнении двойной выплаты электронной купюры.

При использовании разработанной псевдослучайной функции повышенной эффективности процедура генерации S_J номера J-ой электронной купюры имеет вид

$$S_J = g^{\prod_i \frac{1}{S_i + J_j + 1}}, \quad (8)$$

где S_i и J_i – *i*-й блок, полученный при разбиении параметров S и J на m частей.

При этом генерация числа T_J , которое используется в уравнении двойной выплаты электронной купюры, определяется

$$T_J = K_{отк} g^{\prod_i \frac{1}{T_i + J_j + 1}}, \quad (9)$$

где T_i и J_i – *i*-й блок, полученный при разбиении параметров T и J на m частей

Для удобства введем обозначения

$$a_s = \prod_{i=1}^{m} \frac{1}{S_i + J_i + 1} \bmod q; \quad a_T = \prod_{i=1}^{m} \frac{1}{T_i + J_i + 1} \bmod q.$$

Продавец пересылает покупателю случайное число, которое $r \in Z_q$.

После этого покупатель вычисляет ответы на вопрос r, заданный продавцом

$$a_s^* = (a_s - r) \bmod q, \quad (10)$$

$$a_T^* = (a_T - r) \bmod q. \quad (11)$$

Полученные значения покупатель использует для вычисления затемненных образов серийного номера купюры и параметра для уравнения двойной выплаты

$$S_J^* = g^{a_S^*} \bmod q, \quad (12)$$

$$T_J^* = g^{a_T^*} \bmod q. \quad (13)$$

После этого покупатель определяет произведение истинных и затемненных образов

$$S_J T_J \bmod q = g^{a_S} K_{отк} g^{a_T} \bmod q = K_{отк} g^{(a_S + a_T) \bmod \varphi(q)} \bmod q, \quad (14)$$

$$S_J^* T_J^* = g^{a_S^*} K_{отк} g^{a_T^*} \bmod q = K_{отк} g^{(a_S^* + a_T^*) \bmod \varphi(q)} \bmod q. \quad (15)$$

Полученные результаты с помощью выражений (14) и (15) в зашифрованном виде $E_{K_{сеар}}(S_J T_J, S_J^* T_J^*)$ пересылаются продавцу.

После этого продавец, используя открытый ключ покупателя $K_{отк}$, расшифровывает его подпись $D_{K_{отк}}(S_J T_J, S_J^* T_J^*)$. Затем продавец вычисляет отношение

$$A = \frac{S_J T_J}{S_J^* T_J^*} = \frac{K_{отк} g^{(a_S + a_T) \bmod \varphi(q)}}{K_{отк} g^{(a_S^* + a_T^*) \bmod \varphi(q)}} = g^{((a_S + a_T) - (a_S^* + a_T^*)) \bmod \varphi(q)} \bmod q = g^{2r} \bmod q. \quad (16)$$

Если вычисленное значение, согласно равенства (16), соответствует

$$A = (g^r)^2 \bmod q, \quad (17)$$

то это свидетельствует о том, что представленные электронной S_J номер J-й электронной купюры и соответствующей ему параметр T_J , который используется в уравнении двойной выплаты, сгенерированы правильно.

Обобщая полученные результаты, можно отметить, что благодаря использованию методов системного анализа был разработан протокол «выплаты одной монеты», который применяет предлагаемую ПСФ.

Выводы. На основе системного подхода осуществлено расширение области применения разработанной псевдослучайной функции повышенной эффективности в системах электронных платежей. В работе показана возможность использования ПСФ в новом протоколе «выплаты одной монеты» автономной системы

электронных денег. Следует отметить, что данная функция может быть использована при работе с протоколом выплаты электронных монет, не позволяя злоумышленнику повторно использовать одни и те же электронные монеты, а также в протоколе доказательства с нулевым разглашением. Благодаря своим свойствам, разработанная ПСФ характеризуется высокой криптографической стойкостью. Таким образом, за счет многократного использования одной и той же математической ПСФ, освобождается объем памяти необходимый для хранения электронных денежных средств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Пярин В.А., Кузьмин А.С., Смирнов С.М*. Безопасность электронного бизнеса. – М.: Гелиоас АРВ, 2009. – 432 с.
2. *Панасенко С.В.* Алгоритмы шифрования. – М.- БХВ-Петербург, 2009. – 576 с.
3. *Девятов В.А.* Электронные деньги и платежные системы. Краткий справочник. – М.: АСТ-Пресс. – 2008. – 319 с.
4. *Калмыков И.А., Дагаева О.И.* Разработка псевдослучайной функции повышенной эффективности // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 160-169.
5. *Емарлукова Я.В., Калмыков И.А., Яковлева Е.М.* Системное проектирование отказоустойчивых устройств цифровой обработки сигналов // Современные наукоемкие технологии. − 2011. – № 3. − С. 32-35.
6. *Пашинцев В.П., Чипига А.Ф., Галкина В.А., Смирнов А.А.* Решение проблемы обеспечения энергетической скрытности в системах спутниковой связи при близком размещении приемника радиоперехвата // Наукоемкие технологии. – 2012. – Т. 13, № 7. – С. 30-34.
7. *Катков К.А.* Адаптивный алгоритм определения вектора пространственно-временных координат // Известия ОрелГТУ. Информационные системы и технологии. – 2011. – № 1 (63) – С. 5-14
8. *Чипига А.Ф.* Обоснование возможности сохранения конфиденциальности данных в симметричных криптосистемах в случае компрометации ключа шифрования // Известия ЮФУ. Технические науки. – 2010. – № 11 (112). – С. 124-129.
9. *Калмыков И.А., Дагаева О.И.* Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции // Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 218-224.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Калмыков Игорь Анатольевич – Институт информационных технологий и телекоммуникаций Северо-Кавказского федерального университета, г. Ставрополь; e-mail: kia762@yandex.ru; 355040 г. Ставрополь, ул. Шпаковская, 92, кор. 1, кв. 28; тел.: 88652731380, 89034163533; кафедра информационной безопасности автоматизированных систем; д.т.н.; профессор.

Дагаева Ольга Игоревна – e-mail: scorpio@bk.ru; 355040 г. Ставрополь, пр. Кулакова, 33, кв. 56; тел.: 88652956546; кафедра информационной безопасности автоматизированных систем; аспирантка.

Науменко Даниил Олегович – e-mail: dante603@gmail.com; 355040, г. Ставрополь, ул. Семашко, 8, кв. 23; тел.: 89197362888; кафедра информационной безопасности автоматизированных систем; аспирант.

Вельц Оксана Владимировна – e-mail: velts-yatsenco@yandex.ru; 355013, г. Ставрополь, ул. Чехова, 33, кв. 66; тел.: 88652944241; кафедра информатики; старший преподаватель.

Kalmykov Igor Anatolyevich – Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol; e-mail: kia762@yandex.ru; 92, Shpakovskaya street, k. 1, fl. 28, Stavropol, 355000, Russia; phones: +78652731380, +79034163533; the department of information security of automated systems; dr. of eng. sc.; professor.

Dagayeva Olga Igorevna – e-mail: scorpio@bk.ru; 33, pr. Kulakova, fl. 56, Stavropol, 355000, Russia; phone: +79197389273; the department of information security of automated systems; postgraduate student.

Naumenko Daniil Olegovich – e-mail: dante603@gmail.com; 8, Semashko street, fl. 23, Stavropol, 355000, Russia; phone: +79197362888; the department of information security of automated systems; postgraduate student.

Velts Oksana Vladimirovna – e-mail: velts-yatsenco@yandex.ru; 33, Chehova street, fl. 66, Stavropol, 355000, Russia; phone: +78652944241; the department of information science; senior lecturer.

УДК 631.8

И.А. Калмыков, А.Б. Саркисов, А.В. Макарова

ТЕХНОЛОГИЯ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ МОДУЛЯРНОГО ПОЛИНОМИАЛЬНОГО КОДА

Целью исследований является разработка новой технологии цифровой обработки сигналов (ЦОС), применение которой позволяет, за счет использования целочисленной непозиционной математической модели ЦОС, обеспечить высокоскоростную обработку сигналов в условиях воздействия помех и отказа оборудования. Возрастание требований к временным характеристикам современных систем ЦОС привело к созданию вычислительных устройств (ВУ), использующих параллельные вычисления. Однако при этом возникает следующая проблема: с одной стороны, постоянный рост требований к скоростным характеристикам ВУ приводит к необходимости организации параллельных вычислений, а с другой стороны, при этом увеличивается частота возникновения отказов и возрастает время простоя, вызванное трудностью отыскания неисправности.

Для решения данной проблемы в работе предлагается использовать математическую модель ЦОС, использующую модулярный полиномиальный код (МПК), который за счет распараллеливания на уровне операций и обработки малоразрядных данных позволяет не только увеличить скорость вычислений, но и обеспечивает получение корректного результата в условиях воздействия помех при передаче и отказа оборудования.

Цифровая обработка сигналов; ортогональные преобразования сигналов в кольце полиномов; модулярный полиномиальный код; коррекция ошибки; позиционные характеристики.

I.A. Kalmykov, A.B. Sarkisov, A.V. Makarova

TECHNOLOGY OF THE DIGITAL PROCESSING SIGNAL WITH USE MODULAR POLYNOMIAL CODE

The aim of research is a development to new technology of the digital processing signal (COS), which using allows, through the use of integer no positional mathematical model COS, provide speediest processing a signal in condition of the influence of the hindrances and refusal of the equipment. Increasing of requirements to the temporal characteristics of modern systems of COS led to the creation of computing devices (VU), using parallel computing. However, this raises the following problem: on the one hand, steady growth of requirements for high-speed characteristics of VU leads to the necessity of organization of parallel computations and on the other hand, this increases the frequency of occurrence of failures and increases downtime caused by the difficulty of finding fault.

To solve this problem it is suggested to use a mathematical model of a COS that uses modular polynomial code (MPC), which is due to parallelization at the level of operations and processing of small category data allows not only to increase speed of calculations, and ensures obtaining the correct result in the conditions of influence of interference during transmission and equipment failure.

Digital signal processing; the orthogonal transformation of signals in the ring of polynomials; modular polynomial code; correction of errors; positive institutional characteristics.

Введение. На современном этапе развития цивилизации информация играет ключевую роль в функционировании общественных и государственных институтов. Информационная среда, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности государства.