определенным объектом. Модель угроз, представленная в данной работе, позволяет определить необходимые уровни функционирования подсистемы обеспечения безопасности информации в СЗЭД, а именно:

- *первый уровень (превентивный)* – уровень организационно-технических мер, направленных на локализацию и устранение возможных предпосылок к возникновению угроз безопасности информации в СЗЭД;
- *второй уровень (текущего контроля)* – контроль этапов обработки ЭлД (с определенной периодичностью) влияющих на юридическую значимость ЭлД;
- *третий уровень (устранения последствий реализованных угроз)* – обеспечение возможности восстановления юридической значимости ЭлД в минимальные сроки в случае реализации комплексной угрозы потери юридической значимости ЭлД.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *ГОСТ Р ИСО 15489-1-2007*. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования. – Введ. 2007-03-12. – М.: Стандартинформ, 2007. – 23 с.
2. *ГОСТ 2.051-2006*. Единая система конструкторской документации. Электронные документы. Общие положения. – Введ. 2006-09-01. – М.: Изд-во стандартов, 2006. – 12 с.
3. *Елисеев Н.И.. Финько О.А.* Системные основы защищенного гибридного документооборота // Тр. междунар. конф. «Управление развитием крупномасштабных систем» / ИПУ РАН. – М., 2011.
4. *Елисеев Н.И., Финько О.А.* Обеспечение подлинности аналоговых документов в системе электронного документооборота МО РФ// Инфофорум – 2012: Материалы Национального форума информационной безопасности (Москва, 7–8 февраля 2012 г.). URL : http://www.2012.infoforum.ru/2012/program (дата обращения: 11.10.2012 г.).

Статью рекомендовал к опубликованию д.т.н., профессор В.Н. Марков.

Елисеев Николай Иванович – Филиал Военной академии связи (г. Краснодар); e-mail: eliseev_81_09@mail.ru; 350063, г. Краснодар, ул. Красина, 4; тел.: +79094476289; доцент.

Eliseev Nikolay Ivanovich – Branch of the Military Academy of Communications (Krasnodar); e-mail: eliseev_81_09@mail.ru; 4, Krasina, Krasnodar, 350063, Russia; phone: +79094476289; associate professor.

УДК 631.8

И.А. Калмыков, О.И. Дагаева

НОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В ЭЛЕКТРОННЫХ КОММЕРЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПСЕВДОСЛУЧАЙНОЙ ФУНКЦИИ

Целью исследований является сокращение занимаемого программным обеспечением объема, необходимого для эффективной работы носителя электронных денежных средств (смарт-карты) за счет использования разработанной псевдослучайной функции (ПСФ), многократное применение которой в различных протоколах позволит увеличить объем наличности, хранимой в «электронном кошельке».

В работе представлены задачи, решение которых возможно путем применения разработанной ПСФ повышенной эффективности в протоколе определения двойной оплаты и протоколе снятия со счета. Реализация разработанной функции использует ключ в $\log_2 \ell$ *раз меньший размером по сравнения с ПСФ Наора-Рейнголда, при этом стойкость*

данной ПСФ основывается на предположении о сложности решения λ-DDH проблемы. Так как при вычислении этой функции требуется в $\log_2 \ell$ *раз меньше умножений, то основным преимуществом данной ПСФ является использование меньшего объема памяти для вычисления значения функции.*

Псевдослучайная функция; криптографические протоколы защиты данных в электронных коммерческих системах; протокол определения двойной оплаты; протокол доказательства с нулевым разглашением.

I.A. Kalmykov, O.I. Dagaeva

NEW TECHNOLOGIES OF E-COMMERCE SYSTEMS DATA SECURITY BASED ON THE USAGE OF PSEUDORANDOM FUNCTION

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 multiple usage of the designed pseudorandom function (PRF) in different protocols which could increase the amount of cash stored in "electronic purse".

The paper presents the problem which could be possibly solved by usage of the designed effective PRF in the protocol of double payment definition and draw down protocol. The implementation of the developed function uses the key $\log_2 \ell$ *times smaller compared to the Naor-Rheingold PRF and its security relies on the λ-DDH assumption. Since the calculation of the designed function requires* $\log_2 \ell$ *times less multiplications, the main advantage of one is the usage of less memory volume for computing the function value.*

Pseudorandom function, cryptographic protocols data protection in e-commerce systems; the protocol of double payment definition; the zero-knowledge protocol.

Современный этап развития электронных коммерческих систем предопределяет все более широкое применение универсальных платежных средств, таких как электронные деньги. Это обусловлено достоинствами электронных платежных средств, среди которых можно выделить [1]:

- очень низкая стоимость эмиссии электронных денег;
- превосходная делимость и объединяемость;
- высокая портативность;
- снижается воздействие человеческого фактора;
- более высокая степень защищенности от хищения, подделки, изменения номинала.

При постоянно расширяющихся возможностях электронных коммерческих систем широкое внедрение электронных денег пока не наблюдается. Это обусловлено целым рядом причин, основными из которых являются [2]:

- сложность обеспечения вопросов сохранения анонимности пользователя – владельца электронных денежных средств;
- сложность протоколов, используемых в системах электронной коммерции.
- средства криптографической защиты, которыми защищаются системы электронных денег, ещё не имеют длительной истории успешной эксплуатации;
- теоретически, заинтересованные лица могут пытаться отслеживать персональные данные плательщиков и обращение электронных денег вне банковской системы.

Для решения выявленных проблем в работе [3] выработаны требования, предъявляемые к оптимальной автономной системе коммерческих расчетов, использующих электронные деньги:

- безопасность для банка, которая состоит в невозможности пользователем создавать неконтролируемые электронные средства расчета;

- анонимность клиентов при контроле финансовых транзакций;
- невозможность потратить электронную монету дважды.
- возможность восстановления информации при сбое и отказе оборудования.

В настоящее время для эффективной работы автономной системы электронных денег предлагается использовать следующие протоколы:

- протокол снятия со счета;
- протокол выплаты одной монеты;
- протокол выплаты всего кошелька
- протокол выплаты нескольких монет;
- протокол депонирования на счет;
- протокол определения двойной выплаты;
- протокол факта нарушения.

Как правило, вопросы защиты денежных средств электронных коммерческих систем возлагается на протоколы криптографической защиты. Именно их стойкость во многом определяет степень защищенности электронных денег. При этом для эффективного функционирования систем, работающих с электронной наличностью, используется несколько различных криптографических алгоритмов. Это приводит к значительному уменьшению свободного объема памяти, которое может использовать пользователь для хранения электронных денег. Поэтому вопросы разработки новых технологий защиты электронных платежных средств, требующих минимального объема памяти для своего хранения, является актуальным.

Таким образом, очевидно, следующее противоречие. С одной стороны, высокие требования к степени защиты электронных денег предопределяют использование множества криптографических протоколов, что приводит к увеличению объема памяти необходимого для их хранения, а, с другой стороны, накладываются жесткие ограничения на объем энергонезависимой памяти смарт-карты, которая используется в качестве хранилища электронных средств платежа.

Разрешить данное противоречие путем разработки псевдослучайных функции повышенной эффективности, которая может быть применена в различных протоколах защиты информации. В данной работе будут рассмотрены вопросы применения ПСФ в протоколе определения двойной оплаты и протоколе снятия со счета.

Эффективность работы систем электронной коммерции во многом определяется способностью протоколов, применяемых в таких системах, предотвратить коллизии связанные с повторным использованием злоумышленником одних и тех же электронных денежных средств при расчетах. При этом такой протокол должен обеспечить банку возможность самостоятельно идентифицировать такого нарушителя без использования доверительного центра, применение которого является обязательным в классических системах электронных платежей.

Для организации процесса использования электронных денежных средств пользователь наделяется двумя ключами – открытым $К_{отк}$ и секретным $К_{секр}$. Открытый ключ применяется банком при выдаче электронного кошелька своему абоненту. Секретный ключ покупателя $К_{секр}$ участвует в процессе выплаты электронных денег. Это позволяет в случае двойного использования одних и тех же монет установить данный факт. Но при этом должен $К_{секр}$ быть в таком виде, чтобы продавец не смог его вычислитель самостоятельно.

В работе [4] для предотвращения повторного использования электронных монет использовать уравнение «двойной выплаты»

$$M = К_{сек} + T_i R \bmod q, \quad (1)$$

где R – случайное число; T_i – величина связанная с i-м серийным номером монеты; q – порядок мультипликативной группы с элементом g.

При повторном использовании одной и той же монеты злоумышленник получит две случайных величины R_1 и R_2. Тогда выражение (1) преобразуется в систему уравнений, по которой банк и продавец свободно вычислят секретный ключ злоумышленника.

$$\begin{cases} M_1 = \mathrm{K}_{\text{сек}} + T_i R_1 \bmod q \\ M_2 = \mathrm{K}_{\text{сек}} + T_i R_2 \bmod q \end{cases}. \quad (2)$$

В системе применения электронных денежных средств пользователь должен иметь возможность сам генерировать серийные номера монет $S_i = F_s(i)$, где $F_s(i)$ – функция, задаваемая параметром s, полученным из банка. Для эффективной данной процедуры необходимо использовать псевдослучайную функцию, которая должна обладать следующими свойствами:

- для соседних аргументов i и i+1 результаты $F_s(i)$ и $F_s(i+1)$ должны быть некоррелированными;
- функция должна обладать достаточно простой аппаратной и программной реализацией при хороших криптографических свойствах;
- возможность конвейерной организации вычислений.

В качестве такой функции целесообразно использовать разработанную ПСФ повышенной эффективности. В работе [5] на основе анализа основных алгоритмов формирования ПСФ, была разработана псевдослучайная функция, принимающая на входную последовательность $(x_1,...,x_n)$ и ключ $(g, s_1,...,s_n)$ и реализующая

$$F((s_1,...,s_n,h),(x_1,...,x_n)) = g^{\left(\prod_{i=1}^{n}(s_i+x_i)\right)^{-1}}, \quad (3)$$

где h – первообразный элемент мультипликативной группы.

На основе доказанных теорем было показано, 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. Основным преимуществом данной ПСФ является использование меньшего объема памяти для вычисления значения функция, так как она использует ключ в $\log_2 l$ раз меньший размером по сравнения с ПСФ Наора-Рейнголда. Прим этом стойкость данной ПСФ основывается на предположении о сложности решения λ-DDH проблемы.

В этом случае уравнение «двойной выплаты» примет вид

$$M_i = T_{отк}(\mathrm{F_s(i)})^{\mathrm{R_i}} = T_{отк}(\mathrm{g}^{\left(\prod_{j=1}^{n}(\mathrm{s_j}+b_j\right)})^{\mathrm{R_i}} \bmod q, \quad (4)$$

где g – первообразный элемент мультипликативной группы; s_j и b_j – j-й блок, полученный при разбиении чисел s и i на n частей.

В этом случае для определения секретного ключа злоумышленника банку необходимо вычислить отношение

$$K_{\text{сек}} = \left(M_1^{R_2} / M_2^{R_1}\right)^{(R_2-R_1)^{-1}}. \quad (5)$$

Применение разработанной псевдослучайной функции позволяет осуществить эффективную реализацию протокола определения повторной выплаты. Обладая соответствующей криптографической стойкостью, данная ПСФ позволяет сократить размер секретного ключа в $\log_2(m/n)$ раз. Кроме того, разработанная ПСФ может быть использована и в другом протоколе.

При использовании протокола снятия со счета должна обеспечиваться высокая анонимность пользователя. Для обеспечения этого требования в системах электронной коммерции все больше используются различные протоколы доказательства с нулевым разглашением. Применение таких протоколов позволяет владельцу электронной наличности доказать банку свою правомочность использования электронных денег и получить от него кошелек с ними [4]. При этом протоколы доказательства с нулевым разглашением не предоставляют банку никакой информации о секретном ключе пользователя, а только убедить банк, что клиент действительно владеет таким ключом.

Как правило, такие процедуры носят итерационный характер. Такая многоэтапная процедура обмена позволяет банку убедиться в истинности намерений пользователя. Однако при значительном увеличении числа пользователей электронными деньгами это может привести к значительной временной задержке. Решить данную задачу можно за счет применения разработанной псевдослучайной функции.

Известно [6, 7], что основным преимуществом протоколов доказательства с нулевым разглашением является то, что проверяющая сторона не может получить никакой полезной информации о секретном ключе пользователя. Для того чтобы снизить вероятность ошибочного опознания, проверяющая сторона может задавать подряд несколько вопросов. Все это приводит к снижению эффективности работы систем коммерческих расчетов. В работе [6] приведен пример итерационного алгоритма протокола доказательства с нулевым разглашением. Покупатель, будучи легальным пользователем системы, обладает секретным (закрытым) ключом $К_{секр}$ и соответствующим ему открытым ключом $К_{отк}$. При этом значение последнего определяется

$$K_{отк} = g^{К_{секр}} \bmod q, \tag{6}$$

где q – порядок мультипликативной группы с порождающим элементом g. Для того, чтоб убедить банк в том, что он и есть обладатель открытого ключа $К_{отк}$, ему необходимо доказать, что он знает $К_{секр}$.

Для этого пользователь выбирает некоторое случайное число r, вычисляет значение $Y = g^{r} \bmod q$ и пересылает банку это значение. Проверяющая сторона выбирает число B из мультипликативной группы и пересылает его пользователю, т.е. «задает ему вопрос» B. Получив «вопрос» B, пользователь должен на него вычислить «ответ» согласно равенства

$$Z = r - BK_{секр} (\bmod \varphi(q)). \tag{7}$$

Полученный результат пересылается банку, который осуществляет проверку полномочий пользователя согласно

$$\overline{Y} = (К_{отк})^{B} g^{Z} (\bmod q) = (g^{K_{секр}})^{B} g^{r-BK_{секр}} (\bmod q) = g^{r}. \tag{8}$$

Затем производится сравнение с принятым ранее значением Y.

Основным недостатком данного алгоритма является низкая скорость проверки авторизованного пользователя из-за интерактивного обмена сообщениями между сторонами. Решить данную проблему можно за счет применения псевдослучайной функции, которая бы позволила создавать вопрос и находить ответ на одной стороне пользователя. При этом пользователь пересылает только ответы банку.

Алгоритм применения разработанной псевдослучайной функции в протоколе доказательства с нулевым разглашением состоит из следующих этапов. На первом этапе проверяющая сторона пересылает пользователю случайное число S. Затем

последний выбирает случайное число r и вычисляет соответствующее ему значение $Y = g^{\mathrm{r}} \bmod q$. Затем пользователь сам задает себе «вопрос» B

$$B = \mathrm{F_S(Y)} = (\mathrm{g}^{\left(\prod_{j=1}^{m}(r_j+y_j)\right)^{-1}}) \bmod q, \qquad (9)$$

где y_j и r_j – j-й блок, полученный при разбиении чисел Y и R на m частей.

На поставленный вопрос пользователь вычисляет ответ согласно (2). Затем, используя свой секретный ключ, закрывает данные $E_{K_{секр}}(S, Y, B, Z)$ и пересылает полученный зашифрованный текст банку. Банк может убедиться в правильности данной подписи, применяя открытый ключ пользователя $K_{\text{отк}}$.

Пример. Пусть задана мультипликативная группа G_{11}. В данной группе существует первообразный элемент $g = 2$. В качестве секретного ключа пользователя выбираем $K_{\text{секр}} = 3$. Тогда открытый ключ определяется согласно $K_{\text{отк}} = 8$.

Чтобы доказать банку, что он владеет секретным ключом, пользователь выбирает число r = 5 и вычисляет

$$Y = g^{\mathrm{r}} \bmod q = 2^5 \bmod 11 = 10_{10} = 1010_2.$$

Затем производится разделение вычисленного числа на два подблока

$$y_1 = 10_2 = 2 \text{ и } y_2 = 10_2 = 2.$$

Для проверки пользователя банк прислал случайное число S = 6, которое в двоичном коде представляется как 0110. Двоичный код числа $S = 0110_2$ разбивается на два подблока

$$s_1 = 01_2 = 1_{10} \text{ и } s_2 = 10_2 = 2_{10}.$$

Затем пользователю, используя полученные выше числа, необходимо вычислить вопрос B согласно (9). Имеем

$$B = \mathrm{F_6(10)} = (\mathrm{g}^{((s_1+y_1)(s_2+y_2))^{-1}}) \bmod q = (2^{\frac{1}{(1+2)}\frac{1}{(2+2)}}) \bmod 11 = 2^2 = 4.$$

Таким образом, вопрос B = 4.

Вычислив свой вопрос, пользователь приступает к вычислениям ответа на данный вопрос, используя r = 5 и $K_{\text{секр}} = 3$. При этом применяется выражение (2). Тогда

$$Z = r - BK_{секр} (\bmod \phi(q)) = (5 - 2 \cdot 3) \bmod 10 = 9.$$

Затем, используя свой секретный ключ, пользователь закрывает данные $E_{K_{секр}}(6, 10, 4, 9)$ и пересылает полученный зашифрованный текст банку. Банк применяет открытый ключ пользователя $K_{\text{отк}}$ и получает все зашифрованные значения чисел. Эти значения позволят получателю убедиться в правильности данной подписи. При этом используется выражение (8)

$$\overline{Y} = (\mathrm{K_{отк}})^B g^Z (\bmod q) = (8^2 \cdot 2^9) (\bmod 11) = 2^5 \bmod 11 = 10_{10} = Y.$$

Таким образом, применение разработанной псевдослучайной функции позволило выполнить протокол доказательства с нулевым разглашением.

Выводы. В работе показана возможность применения разработанной псевдослучайной функции в различных протоколах 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. *Девятов А.С.* Электронные деньги и платежные системы. Краткий справочник. – М.: АСТ-Пресс, 2008. – 319 с.
3. *Захарченко В.С.* Деньги виртуального мира // Банковский форум Банкир.Ру – 14.03.2005 - http://bankir.ru/analytics/it/3/27881.
4. *Лейман Р.Д.* Электронные деньги. – М.: Дрофа, 2006. – 284 с.
5. *Калмыков И.А., Дагаева О.И.* Разработка псевдослучайной функции повышенной эффективности // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 160-169.
6. *Панасенко С.В.* Алгоритмы шифрования. – М.: БХВ-Петербург, 2009. – 576 с.
7. *Бабаш А.В., Шанкин Г.П.* Криптография / Под ред. В.П. Шерстюка. – М.: СОЛОН-ПРЕСС, 2007. – 512 с.

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; аспирант.

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

Dagaeva Olga Igorevna – e-mail: scorpio@bk.ru; 33, Chehova street, fl. 66, Stavropol, 355013, Russia; phone: +79197389273; the department for information security of automated systems; postgraduate student.

УДК 681. 587.5

А.А. Бошляков, В.В. Ковалев, В.И. Рубцов

ДИАГНОСТИКА ВЫСОКОТОЧНЫХ СКАНИРУЮЩИХ МЕХАТРОННЫХ МОДУЛЕЙ

Качество работы высокоточных сканирующих модулей зависит от большого числа параметров, поэтому их диагностика представляет собой сложную техническую задачу и требует высококвалифицированного персонала. В статье предлагается методика, которая позволяет упростить как контроль мехатронного модуля, так и принятие соответствующего решения о неисправности.

Методика предполагает автоматизированную диагностику изделий на основе анализа сигналов, передаваемых штатным контроллером системы управления мехатнонного модуля, и предоставление персоналу рекомендаций по выявлению и устранению имеющихся дефектов.

Мехатронный модуль; диагностика; математическое моделирование; сканирующая система.