Раздел VI. Прикладные вопросы информационной безопасности

УДК 631.8

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

РАСШИРЕНИЕ МЕТОДОВ ЗАЩИТЫ СИСТЕМ ЭЛЕКТРОННОЙ КОММЕРЦИИ НА ОСНОВЕ МОДУЛЯРНЫХ АЛГЕБРАИЧЕСКИХ СХЕМ

Целью исследований является разработка новых протоколов для усовершенствования технологии «электронных денег» таких что, их применение позволяет обеспечить увеличение свободного объема памяти носителя электронной наличности за счет многократного использования псевдослучайной функции (ПСФ) повышенной эффективности. Реализация итеративных протоколов на основе разработанной ПСФ является одним из основных путей достижения поставленных перед системами электронных платежей (СЭП) требований по обеспечению высокой степени криптографической защиты. С целью повышения эффективности обмена электронной наличностью разработан протокол, способный обеспечить выплату всей наличности электронного кошелька. Протокол позволяет осуществлять передачу продавцу данных, составляющих основу электронного кошелька пользователя. В результате этого обеспечивается ускорение всего процесса выплаты для больших сумм и уменьшается количество транзакции по сравнению с протоколом «выплаты одной монеты». Разработка данного протокола стало результатом системного подхода к решению поставленной задачи исследований по разработке эффективной системы, использующей «электронные деньги».

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

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

ENHANCED PROTECTION METHODS OF ELECTRONIC COMMERCE ON THE BASIS OF MODULAR ALGEBRAIC SCHEME

The purpose of this research is to develop new protocols to further improve the technology of "electronic money" such that their use allows for an increase in the free volume of the storage media of electronic cash by reusing pseudo-random function (PRF) to improve efficiency. Implementation of iterative -based protocols developed PRF is one of the main ways of achieving before the electronic payment systems (EPS) requirements to ensure a high degree of cryptographic protection. To improve the efficiency of the exchange of e-cash develop a Protocol capable of ensuring the payment of all cash electronic purse. This Protocol allows transmitting the seller of the data constituting the basis of the electronic wallet user. As a result of the speed of the entire process of payment for large amounts and decreases in the number of transactions in comparison with the Protocol «payment of the same coin». The development of this Protocol was the result of a systematic approach to the task of research to develop an efficient system, using the «electronic money».

Electronic payment systems; cryptographic protocols for the protection of data; pseudo-random function; the protocol zero-knowledge proof.

Введение. Эффективное развитие современного информационного общества невозможно без широкого применения информационных технологий. В настоящее время в основу систем, обеспечивающих безопасность и оборону страны, положе-

ны компьютерные и телекоммуникационные системы. Они реализуют современные информационные технологии, обеспечивая обработку, передачу и хранение больших объемов данных. Массовое использование вычислительной техники позволяет эффективно решать проблему автоматизации процедур обработки и хранения информации. Однако при этом возникает новая проблема, связанная с обеспечением информационной безопасности компьютерных систем. При этом обеспечение информационной безопасности требует комплексного и системного подхода к своему решению.

Одним из наиболее перспективных направлений развития информационных технологий является широкое проникновение систем электронных платежей (СЭП) практически во все сферы деятельности современного государства. Однако при этом использование таких информационных технологий непосредственно связано с определенной совокупностью рисков, основой причиной которых являются уязвимости информационных технологий и систем.

В настоящее время криптографические протоколы нашли свое применение во многих областях деятельности человека. Расширение сфер их применения во многом определяется необходимостью обеспечения требуемого уровня защиты данных, которые являются объектом обработки, передачи и хранения.

Как правило, вопросы защиты денежных средств электронных коммерческих систем возлагается на протоколы криптографической защиты. Именно их стойкость во многом определяет степень защищенности электронных денег. Проведенный системный анализ предметной области позволил выделить следующие три области применения криптографических методов защиты информации:

- обеспечение информационной безопасности государства;
- защиты обмена информацией между органами власти и юридическими и физическими лицами;
- защита систем, работающих с электронной наличностью.

Основу первой области составляет все многообразие сфер деятельности человека, связанных с повышенными требованиями к защите информации, включая военные применения, деятельность спецслужб, дипломатию. Основу второй области применения криптографических методов защиты составляют протоколы, которые используются в системах дистанционного взаимодействия органов государственной власти и отдельных юридических и физических лиц. Качественный скачок в данной области был дан в момент принятия решения о создании в стране электронного правительства. По мере расширения сфер взаимодействия между различными органами государственной власти будут внедряться новые методы защиты данных от НСД, обладающие разной степенью криптографической стойкости. Появившаяся относительно недавно третья область напрямую связана с разработкой способов дистанционного осуществления коммерческих отношений между субъектами экономической деятельности.

Первопричиной создания третьей области применения криптографических методов защиты информации является стремление государства уменьшить денежные потоки бумажной наличности. Всестороннее и постоянное расширение сферы применения электронной наличности обусловлено достоинствами последних, среди которых можно выделить [1, 2]:

- очень низкую стоимость эмиссии электронных денег;
- превосходную делимость и объединяемость;
- высокую портативность;
- более высокую степень защищенности от хищения, подделки, изменения номинала.

В настоящее время для эффективной работы автономной системы электронных денег предлагается использовать ряд криптографических протоколов. Математическую основу большинства этих протоколов составляют, так называемые, алгоритмы «слепой подписи» [2]. К сожалению, данные алгоритмы не позволяют в полной мере использовать все достоинства электронных платежных средств. Кроме того, для большинства известных платежных систем характерен один недостаток, который выражается в сложности размещения достаточно большого количества электронных денежных знаков на носителях информации, таких как смарт-карты. Это обусловлено, прежде всего, тем, что такой носитель имеет малый объем памяти чипа.

Постановка задачи исследования: Для эффективного функционирования систем, работающих с электронной наличностью, используется несколько различных криптографических протоколов. Среди них можно выделить основные:

- протокол снятия со счета;
- протокол выплаты одной монеты;
- протокол определения двойной выплаты;
- протокол выплаты всего кошелька;
- протокол проверки наличия электронных денег в кошельке покупателя;
- протокол проверки сгенерированных номеров электронных монет.

Для реализации отмеченных выше протоколов предлагается использовать псевдослучайные функции (ПСФ). В настоящее время ПСФ нашли широкое применение в самых различных сферах, начиная от космических технологий и закачивая криптографией [3–5]. При этом каждая область применения выдвигает свои требования к свойствам ПСФ. В работах [6–10] довольно подробно рассмотрены вопросы применения псевдослучайных функций повышенной эффективности для реализации протоколов «снятие со счета», «выплаты одной монеты» и «определение двойной выплаты».

Рассмотрим более подробно протокол «выплаты всего кошелька». Данный протокол позволяет осуществлять передачу продавцу данных, составляющих основу электронного кошелька пользователя. Это позволяет ускорить процесс выплаты для больших сумм, уменьшая количество транзакции по сравнению с протоколом «выплаты одной монеты».

Для реализации данного протокола банк добавляет в электронный кошелек покупателя дополнительный параметр V, где $V < q$. Чтобы обеспечить правильную выплату электронной наличности в кошелек пользователя вводятся числа S и T. Число S применяется для вычисления номеров электронных купюр, которыми расплачивается покупатель. Число T используется для вычисления параметра безопасности как для всего кошелька, так и для отдельной монеты. Это необходимо для осуществления проверки «двойной выплаты», чтобы определить недобросовестного пользователя, который пытается дважды использовать электронную наличность.

Пользователь доказывает продавцу правильность имеющегося параметра V и раскрывает ему свои инициализирующие значения (S, T), которые используются в качестве исходных данных для генерации номера j-й электронной банкноты S_j и соответствующего ей параметра для проверки двойной выплаты T_i.

Для получения наличности продавец предоставляет в банк, переданные пользователем значения (S, T). Банк самостоятельно производит генерацию всех номеров j-й электронной банкноты S_i и соответствующего ей параметра для проверки двойной выплаты T_i. Это необходимо для того, чтобы предотвратить ситуацию, когда недобросовестный пользователь попытается воспользоваться отдельными монетами «уплаченного кошелька» по отдельности.

Для эффективной работы этого протокола необходимо, чтобы продавец убедился, что у пользователя есть параметр V, позволяющий уплатить весь кошелек сразу, и при этом значение счетчика выплат равно $J = 1$. Это соответствует ситуации, когда из кошелька еще «не тратилась» электронная наличность. Для обеспечения высокого уровня защиты данных от НСД воспользуемся ПСФ, приведенной в работах [6–10].

Проверка параметров пользователя осуществляется выполнением следующих действий.

1. Продавец передает пользователю вопрос, в качестве которого выступает случайное число $d_к$.

2. Пользователь вычисляет значение параметра

$$L = g^{JV} \bmod q, \tag{1}$$

где g – первообразный корень по модулю q.

Если из кошелька не было потрачено ни одной монеты, то $J = 1$. Тогда

$$L = g^{V} \bmod q. \tag{2}$$

3. После получения вопроса, в виде числа $d_к$, пользователь вычисляет ответы на вопросы

$$J^* = \left|J - d_k\right|_{q-1}^{+} = \left|1 - d_k\right|_{q-1}^{+}, \tag{3}$$

$$V^* = \left|V - d_k\right|_{q-1}^{+}. \tag{4}$$

4. Полученные ответы участвуют в получении значения по модулю

$$L^* = g^{J^*} g^{V^*} \, mod \, q. \tag{5}$$

5. Пользователь передает в зашифрованном виде, используя свой секретный ключ $К_{ПС}$, значение $E_{К_{ПС}}(L, L^*)$.

6. Продавец, используя открытый ключ пользователя $К_{ПО}$, расшифровывает принятое сообщение

$$D_{К_{ПО}}\left(E_{К_{ПС}}\left(L, L^*\right)\right).$$

7. Затем продавец осуществляет проверку доказательства

$$M = \frac{L}{L^*} \bmod q = g^{2d_К - 1} \bmod q. \tag{6}$$

Если выражение (6) является истинным, то это означает, что значение счетчика выплат равно $J = 1$. Эта ситуация возможна в случае, когда пользователь не истратил ни одной электронной монеты из своего кошелька.

В противном случае, пользователь обманывает продавца, что его кошелек является полным.

Пример. Пусть для работы системы задана мультипликативная группа и значение $q = 11$. В данной группе существует первообразный корень $g = 2$. В качестве секретного ключа пользователя выбираем $К_{ПС} = 3$. Тогда открытый ключ определяется

$$К_{ПО} = g^{К_{ПС}} \bmod q = 8.$$

Пусть параметр, дающий возможность пользователю потратить весь кошелек за одну покупку, равен $V = 6$.

Чтобы доказать продавцу, что он владеет «полным» кошельком электронной наличности, пользователь использует выражение (2). Тогда

$$L = g^{V} \bmod q = 2^6 \bmod 11 = 9.$$

Продавец выбирает число $d_к = 5$ и пересылает его пользователю в качестве вопроса.

Тот вычисляет ответ на вопрос согласно (3)

$$J^* = \left|J - d_k\right|_{q-1}^{+} = \left|1 - d_k\right|_{q-1}^{+}, = \left|1-5\right|_{10}^{+} = 6.$$

$$V^* = \left|V - d_k\right|_{q-1}^{+} = \left|6-5\right|_{10}^{+} = 1.$$

Затем пользователь использует выражение (4) и получает

$$L^* = g^{J^*} g^{V^*} \bmod q = 2^1 2^6 \bmod 11 = 7.$$

Зашифрованная пара значений (9, 7) передается продавцу. Последний, проведя процедуру расшифрования, производит вычисления согласно (6)

$$M = \frac{L}{L^*} \bmod q = \frac{9}{7} \bmod 11 = 6 \cdot$$

После этого продавец приступает к проверке правильности ответа на поставленный вопрос $d_к = 5$

$$M^* = g^{2d_K - 1} \bmod q = 2^{2 \cdot 5 - 1} \bmod 11 = 6.$$

Так как полученные значения совпали, то продавец делает вывод о том, что кошелек пользователь является полным, и его можно принять к оплате.

Применение данного протокола позволит сократить время на выполнение транзакции по сравнению с последовательно процедурой, определяемой протоколом «выплаты одной монеты».

Чтобы начать транзакцию по выплате электронной наличности покупатель должен доказать продавцу, что он обладает «свободной наличностью», т.е. значение счетчика выплаченных монет J не превысил предельного значения N. Для осуществления доказательства с нулевым разглашением он должен вычислить ряд вспомогательных параметров.

Проверка параметров пользователя осуществляется выполнением следующих действий.

1. Продавец передает пользователю случайное число-вопрос d_1.

2. Пользователь вычисляет значение параметров

$$a_1 = N - (J - 2) - d_1 = N - J - d_1 + 2, \quad (7)$$

$$a_2 = N - (J - 1) - d_1 = N - J - d_1 + 1, \quad (8)$$

$$a_3 = N - J - d_1, \quad (9)$$

где J – текущее значение счетчика потраченных электронных монет.

Если из кошелька не было потрачено ни одной монеты, то $J = 1$.

3. После полученных значений ответа на вопрос d_1 пользователь вычисляет значение

$$n = g^{a_1} g^{a_2} g^{a_3} \bmod q. \quad (10)$$

4. Пользователь передает в зашифрованном виде, используя свой секретный ключ $K_{ПС}$, значение $E_{K_{ПС}}(n)$.

5. Продавец, используя открытый ключ пользователя, расшифровывает принятое сообщение

$$D_{K_{ПО}}\left(E_{K_{ПС}}(n)\right).$$

6. Затем продавец осуществляет проверку доказательства

$$ng^{3d_1} \bmod q = g^{a_1} g^{a_2} g^{a_{31}} g^{3d_1} \bmod q = g^{3N-3J+3} \bmod q. \quad (11)$$

Анализ выражения (11) показывает, что последнее будет равно единице только в том случае, когда текущее значение счетчика будет равно $J = N + 1$. Такая ситуация соответствует попытке пользователя получить очередной серийный номер *J + 1*-й монеты, которая отсутствует в электронном кошельке. Таким образом, покупатель пытается сгенерировать номер банкноты в момент, когда у него полностью закончилась электронная наличность предоставленная банком.

Если выражение (11) не равняется единице, то это соответствует ситуации, когда у покупателя есть электронная наличность в кошельке, и он может совершить покупку.

Для реализации последней процедуры пользователь вычисляет серийный номер очередной монеты

$$S_J = g^{\frac{1}{S+J+1}} \bmod q. \tag{12}$$

Кроме этого пользователь определяет значение параметра безопасности, который используется в уравнениях двойной выплаты

$$T_J = K_{ПО} g^{\frac{1}{T+J+1}} \bmod q. \tag{13}$$

Полученные значения пересылаются продавцу.

Затем покупатель должен доказать продавцу, что значения $S_J = g^{\frac{1}{S+J+1}} \bmod q$ и $T_J = K_{ПО} g^{\frac{1}{T+J+1}} \bmod q$ вычислены правильно с использованием исходных значений S и T входящих в состав вручения, подписанного банком

Для удобства представим значения в виде

$$S_J = g^{\frac{1}{S+J+1}} \bmod q = g^{a_S^{обр}} \bmod q, \tag{13}$$

где $a_S^{обр} = \dfrac{1}{S+J+1} \bmod q.$

$$T_J = K_{ПО} g^{\frac{1}{T+J+1}} \bmod q = K_{ПО} g^{a_T^{обр}} \bmod q, \tag{14}$$

где $a_T^{обр} = \dfrac{1}{T+J+1} \bmod q.$

Для проверки серийного номера электронной монеты, которой будет расплачиваться покупатель, продавец пересылает последнему случайное число $d_2 \in Z_q$. После этого покупатель вычисляет затемненные значения

$$a_S^* = \left(a_S^{обр} - d_2\right) \bmod q - 1, \tag{15}$$

$$a_T^* = \left(a_T^{обр} - d_2\right) \bmod q - 1. \tag{16}$$

Затем вычисляется затемненные значения

$$S_J^* = g^{a_S^*} \bmod q. \tag{17}$$

$$T_J^* = K_{ПО} g^{a_T^*} \bmod q. \tag{18}$$

После этого покупатель находит значения произведений $S_J T_J$ и $S_J^* T_J^*$. Полученные значения произведений пересылаются продавцу, который проверяет доказательство

$$A = \frac{S_J T_J}{S_J^* T_J^*} \bmod q = \frac{K_{ПО} g^{\left(a_S^{обр} + a_T^{обр}\right)}}{K_{ПО} g^{\left(a_S^* + a_T^*\right)}} \bmod q = g^{2d_2} \bmod q = \left(g^{d_2}\right)^2 \bmod q. \tag{19}$$

Если выражение (19) является истинным, то это означает, что порядковые значения S_J, T_J вычислены правильно. В противном случае, пользователь обманывает продавца, что его электронные монеты имеют правильные номера.

Выводы. В работе показаны результаты расширения интерфейса пользователя электронной наличности. Для повышения эффективности работы систем электронных платежей были разработаны протоколы выплаты всего кошелька, проверки наличия электронных денег в кошельке покупателя и проверки сгенерированных номеров электронных монет. Использование данных протокол позволит повысить качество проведения транзакций в СЭП и обеспечить более высокую степень защиты продавца от навязывания ложных данных при проведении процедуры покупки. В разработанных протоколах предлагается использовать разработанную псевдослучайную функцию, что в конечном итоге, позволит уменьшить объемы памяти носителя кошелька, необходимой для хранения программного обеспечения СЭП.

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. *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.
4. *Катков К.А.* Адаптивный алгоритм определения вектора пространственно-временных координат // Известия ОрелГТУ. Информационные системы и технологии. – 2011 – № 1 (63). – С. 5-14
5. *Katkov K.A., Kalmykov I.A.* Application of Parallel Technologies in Navigation Management under the Conditions of Artificial Ionospheric Disturbances World Applied Sciences Journal 26 (1): 108-113, 2013, Nov 10, 2013. http://www.idosi.org/wasj/wasj26%281%292013.htm.
6. *Калмыков И.А., Дагаева О.И.* Разработка псевдослучайной функции повышенной эффективности // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 160-169.
7. *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.
8. *Калмыков И.А., Кихтенко О.А., Барильская А.В., Дагаева О.И.* Криптографическая система на базе непозиционных полиномиальных алгебраических структур // Вестник Северо-Кавказского федерального университета. – 2010. – № 2. – С. 51-57.
9. *Калмыков И.А., Дагаева О.И., Науменко Д.О., Вельц О.В.* Системный подход к применению псевдослучайных функций в системах защиты информации // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 228-234..
10. *Калмыков И.А., Дагаева О.И.* Применение системы остаточных классов для формирования псевдослучайной функции повышенной эффективности // Вестник Северо-Кавказского федерального университета. – 2012. – № 3 (32). – С. 26-34

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

Калмыков Игорь Анатольевич – Институт информационных технологий и телекоммуникаций Северо-Кавказского федерального университета; 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.

Макарова Алена Васильевна – e-mail: alyonchikmav@yandex.ru; 355040, г. Ставрополь, ул. Краснофлотская, 14, кв. 7; тел.: 89187647533; кафедра информационной безопасности автоматизированных систем; аспирантка.

Саркисов Артем Брониславович – e-mail: samael68@yandex.ru; 355040, г. Ставрополь, ул. Ленина, 118, кв. 25; тел.: 89064716706; кафедра информационной безопасности автоматизированных систем; аспирант.

Калмыков Максим Игоревич – e-mail: kmi762@yandex.ru; 355040, г. Ставрополь, пр. Кулакова, 33, кв. 56; тел.: 88652956546; кафедра информационной безопасности автоматизированных систем; аспирант.

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

Makarova Alena Vasilyevna – e-mail: alyonchikmav@yandex.ru; 14, Krasnoflotskay street, kv. 7, Stavropol, 355000, Russia; phone: +79187647533; the department of information security of automated systems; postgraduate student.

Sarkisov Artem Bronislavovich – e-mail: samael68@yandex.ru; 118, Lenina street, kv. 25, Stavropol, 355000, Russia; phone: +79064716706; the department of information security of automated systems; postgraduate student.

Kalmykov Maksim Igorevich – e-mail: kmi762@yandex.ru; 33, pr. Kulakova, kv. 56, Stavropol, 355000, Russia; phone: +79064710242; the department of information security of automated systems; postgraduate student.

УДК 14.35.07

Л.В. Толмачёва, Е.Н. Каменская

АНАЛИЗ ВОЗДЕЙСТВИЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ НА СТУДЕНТА ТЕХНИЧЕСКОГО ВУЗА

Информационно-образовательная среда рассматривается как сложное, многокомпонентное системное образование, насыщенное разнообразными ресурсами. Целью исследования является изучение основных видов воздействий информационно-образовательной среды на студента технического вуза. В качестве метода использован теоретический анализ. Рассмотрены положительные (сокращение времени на обучение, возможность дистантного образования, комплекс личностных новообразований – формирование способности и готовности взаимодействовать с современными информационными системами, развитие мышления, расширение диапазона активности человека: предметного содержания намеченных целей, значимость целей и результатов) и негативные (чрезмерная формализация мышления, нарушение адекватности восприятия окружающего мира, стремление уйти от объективной реальности, погрузиться в виртуальную среду) воздействия информационных технологий на студентов в образовательном пространстве технического вуза. К негативным личностным изменениям студентов, вызванным особенностями образовательной среды технического вуза относятся: символизация образа мира, обеднение эмоциональной сферы, утрата креативности, что приводит к падению личностной успешности, снижению уровня социальной мобильности, неблагоприятным эмоционально-волевым, мотивационно-ценностным и психосоматическим изменениям.

Информатизация; двойное опосредование; компьютерные каналы коммуникации; информационно-образовательная среда; виртуальная среда.

L.V. Tolmacheva, E.N. Kamenskaya

IMPACT ANALYSIS OF INFORMATION EDUCATIONAL ENVIRONMENT FOR A STUDENT OF A TECHNICAL UNIVERSITY

Information and educational environment is considered as a complex, multi-component system of education, a rich variety of resources. The purpose of our research is to study the main types of impacts information and learning environment for a student of a technical College. As a method we use theoretical analysis. We have considered positive (reduction of time for training, the possibility of distant education, complex personal tumors – forming ability and willingness to