УДК 004.052.2

ИСПОЛЬЗОВАНИЕ МОДУЛЯРНЫХ АЛГЕБРАИЧЕСКИХ СИСТЕМ КОЛЬЦА И ПОЛЯ В СИСТЕМАХ ЭЛЕКТРОННОЙ КОММЕРЦИИ

[1]Попов А.И., [1]Калмыков И.А., [1]Атуев К.Р., [1]Санян Э.А., [2]Харечкина Ю.О., [3]Ряднов С.А.

[1]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;

[2]ФГБОУ ВО «Ставропольский государственный аграрный университет» Ставрополь, e-mail: kia762@yandex.ru;

[3]Филиал Московского государственного университета приборостроения и информатики, Ставрополь, e-mail: kia762@yandex.ru

Увеличение числа пользователей, работающих в сети Интернет, способствовало созданию и развитию электронного бизнеса. При этом эффективность реализации электронного бизнеса во многом определяется безопасностью его проведения. Актуальность обеспечения безопасности в области организации электронного бизнеса напрямую зависит от увеличения числа участников экономической деятельности, а также от переноса ее части в информационное пространство. Особенно это наглядно проявляется в системах электронных платежей. Системы электронных платежей относятся к сложным информационным системам. Поэтому они обладают целым рядом уязвимостей, используя которые злоумышленник может нарушить нормальную работу одной из подсистем электронных платежей. Это может привести к дестабилизации работы всей системы электронных платежей и способствовать значительным финансовым потерям участникам. Поэтому разработка теоретических и практических решений, построенных на основе модулярных алгебраических систем кольца и поля, применение которых позволит снизить число уязвимостей систем электронных платежей, является актуальной задачей. В работе рассмотрены протоколы, применение которых позволит обеспечить требуемый уровень защиты от несанкционированного доступа.

Ключевые слова: системы электронных платежей, протоколы, электронные деньги, псевдослучайная функция, модулярные коды, алгебраическая система кольца и поля

THE USE OF MODULAR ALGEBRAIC SYSTEMS OF RINGS AND FIELDS IN THE E-COMMERCE SYSTEMS

[1]Popov A.I., [1]Kalmykov I.A., [1]Atuev K.R., [1]Sanya E.A., [2]Kharechkina Y.O., [3]Ryadnov S.A.

[1]North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru;

[2]Stavropol State Agrarian University, Stavropol, e-mail: kia762@yandex.ru;

[3]Branch of Moscow state University of instrument engineering and informatics in the city of Stavropol, e-mail: kia762@yandex.ru

The increase in the number of users in the Internet, contributed to the creation and development of e-business. The effectiveness of the implementation of e-business is largely determined by without the risk of holding it. The relevance of security in the field of e-business depends on the increase in the number of participants of economic activities, as well as from the transfer part of the information space. This is especially evident in the electronic payment systems. The electronic payment system are to complex information systems. Therefore, they have a number of vulnerabilities that an attacker can disrupt the normal operation of one of the subsystems of electronic payments. This can lead to destabilization of the whole system of electronic payments and result in significant financial losses to the participants. Therefore, the development of theoretical and practical solutions based on modular systems of algebraic rings and fields, the use of which will reduce the number of vulnerabilities of systems of electronic payments, is an urgent task. In operation the protocols, the application of which will allow to provide the required level of protection from unauthorized access.

Keywords: electronic payment protocols, electronic cash, pseudorandom function, modular codes, and algebraic system of rings and fields

В настоящее время для эффективной работы автономной системы электронных денег, а также для предотвращения несанкционированного доступа (НСД) широко используются криптографические методы. Особое место среди данных средств защиты данных от НСД занимают протоколы, используемые в электронной коммерции [4]. Эффективность работы систем электронной коммерции во многом определяется тем, чтобы используемые протоколы использовали единую алгебраическую систему. Такой подход позволит увеличить объем свободной памяти носителя, которую может использовать пользователь для хранения электронных денег.

Цель исследования. Как и все сложные информационные системы, системы электронных платежей, имеют целый ряд уязвимостей, использование которых может привести к нарушению работы одной из подсистем СЭП. Это может способствовать дестабилизации работы всей системы электронных платежей, что, в конечном

итоге, приведет к значительным финансовым потерям участникам СЭП. Решить данную задачу можно за счет разработки эффективных протоколов, которые могут быть использованы при работе с электронной наличностью. Поэтому целью работы является разработка теоретических и практических решений, построенных на основе модулярных алгебраических структур кольца и поля, применение которых позволит снизить число уязвимостей системы электронных платежей.

Материалы и методы исследования

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 при реализации защиты систем электронных платежей используют различные криптографические методы защиты информации. Это приводит к значительному уменьшению свободного объема памяти, которое может использовать пользователь для хранения электронных денег. для решения данной проблемы целесообразно использовать модулярные алгебраические системы кольца и поля, применение которых позволит использовать единую базу при разработке протоколов электронной наличности.

Одним из протоколов, поддерживающих систему электронной коммерции в актуальном состоянии, является протокол «снятия со счета», приведенный в [3]. Используя данный протокол, пользователь, обратившийся в банк, должен доказать последнему, что обладает рядом секретных параметров. Эти параметры включают в себя – секретный ключ пользователя $K_{пс}$, число S, которое используется для определения текущего номера электронной банкноты, а также число T, применяемое в уравнение «двойной оплаты».

Наличие данных параметров позволит пользователю снять со счета в банке N электронных монет. При использовании протокола снятия со счета в современных системах электронной коммерции должна обеспечиваться высокая анонимность пользователя. для обеспечения этого требования в таких системах нашли широкое применение протоколы доказательства с нулевым разглашением [2]. Применение таких протоколов позволяет владельцу электронной наличности доказать банку свою правомочность использования электронных денег и получить от него кошелек с ними. 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.

Известно, что классические протоколы доказательства с нулевым разглашением имеют итерационный характер. В работе [3] представлен протокол, позволяющий пользователю осуществить снятие наличности в банке. Рассмотрим более подробно разработанный протокол.

На первом этапе протокола пользователь вычисляет значение параметра, который называется «вручением». для этого он вычисляет значение

$$Cs = g^{K_{ПС}} g^{ST} g \mod q, \qquad (1)$$

где C – вручение; q – мультипликативная группа.

Данное «вручение» пересылается банку. При этом пользователь не раскрывает перед банком свои секретные данные.

Затем пользователь проводит «зашумление» своих секретных данных, т.е. изменяет значения секретного ключа $K_{пс}$, чисел S и T. В результате получаются следующие значения $K^*_{ПС} \neq K_{ПС}, S^* \neq S, T^* \neq T$. После этого пользователь вычисляет новое «зашумленное вручение»

$$C^* = g^{K^*_{GC}} g^{S^*} g^{T^*} \mod q, \qquad (2)$$

где C^* – зашумленное вручение.

Полученное значение пересылается в банк. Внесенные изменения не позволяют банку узнать секретные значения ключа $K_{ПС}$, чисел S и T.

На следующем этапе банк пересылает пользователю число $d \in Z_q$. Данное число выступает в качестве вопроса, на который должен ответить пользователь. Если он знает секретные значения ключа $K_{ПС}$, чисел S и T, то сможет правильно ответить на «поставленный вопрос».

Пользователь приступает к вычислению ответа на вопрос d согласно

$$\begin{aligned} r_1 &= K^*_{ПС} - dK_{ПС}, \\ r_2 &= S^* - dS, \\ r_3 &= T^* - dT. \end{aligned} \qquad (3)$$

Полученные ответы на поставленный вопрос d передаются банку. Последний приступает к проверке доказательства истинности пользователя. для этого вычисляется

$$A = C^d g^{r_1} g^{r_2} g^{r_3} \mod q. \qquad (4)$$

Если пользователя является действительным владельцем секретных параметров секретного ключа $K_{ПС}$, чисел S и T, то справедливо равенство

$$A = C^* \mod q. \qquad (5)$$

В противном случае банк откажет пользователю в получении электронной наличности.

Основным недостатком данного протокола является необходимость передачи продавцу истинного вручения, зашумленного вручения и трех ответов на поставленный вопрос, что при значительном увеличении числа пользователей электронными деньгами может привести к существенной временной задержке. Решить данную задачу можно за счет применения псевдослучайной функции.

С целью повышения эффективности в работе [1] была разработана каскадная псевдослучайная функций. Эта функция принимает в качестве входной последовательности $(x_1,...,x_n)$ и ключ $(g, s_1,...,s_n)$. При этом она реализует

$$F((s_1,...,s_n,g),(x_1,...,x_n)) = g^{\left(\prod_{i=1}^{n}(s_i+x_i)\right)_{-1}}, \qquad (6)$$

где g – элемент, порождающий мультипликативную группу.

Рассмотрим более подробно разработанный протокол «снятия со счета», использующий псевдослучайную функцию, алгоритм получения которой определяется равенством (6).

На первом этапе протокола пользователь перед вычислением вручения представляет параметры K, S и T в двоичном коде и разбивает их на m частей. Затем

производит вычисление самого вручения с использованием выбранной ПСФ повышенной эффективности

$$C = g^{(K_{ПС1}+S_1+T_1)^{-1}} \cdot \ldots \cdot g^{(K_{ПСm}+S_m+T_m)^{-1}} \bmod q. \quad (7)$$

Данное «вручение» пересылается банку.

На втором этапе протокола пользователь проводит «зашумление» своих секретных данных, т.е. изменяет значения секретного ключа $K_{ПС}$, чисел S и T. В результате получаются следующие значения $K^*_{ПС} \neq K_{ПС}, S^* \neq S, T^* \neq T$. Пользователь вычисляет новое «зашумленное вручение»

$$C^* = g^{(K^*_{ПС1}+S^*_1+T^*_1)^{-1}} \cdot \ldots \cdot g^{(K^*_{ПСm}+S^*_m+T^*_m)^{-1}} \bmod q. \quad (8)$$

Полученное значение пересылается в банк. Внесенные изменения не позволяют банку узнать секретные значения ключа $K_{ПС}$, чисел S и T.

На следующем этапе банк пересылает пользователю число $d \in Z_q$. Данное число выступает в качестве вопроса, на который должен ответить пользователь. Если он знает секретные значения ключа $K_{ПС}$, чисел S и T, то сможет правильно ответить на «поставленный вопрос».

Пользователь приступает к вычислению ответа на вопрос d согласно

$$r_1 = l^*_{обр} - dl_{обр}, \bmod \varphi(q). \quad (9)$$

где $l_{обр} = \log_r C \bmod q$ и $l^*_{обр} = \log_r C^* \bmod q$ – степени истинного и зашумленного вручений.

Полученный ответ на поставленный вопрос d передается банку. Последний приступает к проверке доказательства истинности пользователя. для этого вычисляется

$$A = C^d g^{r_1} \bmod q. \quad (10)$$

Если результат совпадает с зашумленным вручением, то есть справедливо равенство $A = C^* \bmod q$, то это свидетельствует, что пользователь является электронного кошелька.

Очевидно, что использование в протоколе псевдослучайной функции, определяемой выражением (6), обеспечивает более высокую скорость выполнения протокола «снятия со счета». Это определяется тем, что пользователь электронной наличности передает не 3 ответа, как это было при выполнении предыдущего протокола, а только один. Это позволяет снизить трафик обмена данными между абонентами.

Результаты исследования и их обсуждение

Пусть для выполнения протокола используется мультипликативная группа порожденная модулем q =43. В данной группе существует порождающий элемент равный g = 3. для совершения процедуры выплаты денежных средств у покупателя должен быть в наличии электронный кошелек, который содержит в себе:

- секретный ключ владельца $K_{ПС} = 7$;
- параметр для генерации номера электронной монеты $S = 8$;
- параметр для проведения проверки «двойной выплаты» одной монетой $T = 9$.

При обращении в банк за электронным кошельком, покупатель доказывал, что он является авторизованным покупателем. для этого он вычислял вручение:

$$C = g^{K_i+S_i+T_i} \bmod q = 3^{7+8+9} \bmod 43 =$$
$$= 3^{24} \bmod 43 = 16.$$

Вносим искажения в значения содержимого кошелька K, S, T. Пусть затемненные значения параметров владельца электронного кошелька равны $K^*_i = 5$, $S^*_i = 7$, $T^*_i = 13$. Затем владелец затемняет значение вручения:

$$C^* = g^{K^*_i+S^*_i+T^*_i} \bmod q = 3^{5+7+13} \bmod 43 =$$
$$= 3^{25} \bmod 43 = 5.$$

Банку передается истинное вручение C и зашумленное вручение C^*. Получив значения C и $C,^*$ он посылает в ответ случайное число – вопрос d = 15. Владелец электронного кошелька, получив вопрос, генерирует ответ

$$r_1 = \left(K^*_i - dK_i\right) \bmod \varphi(q) =$$
$$= \left|5 - 15 \cdot 7\right| \bmod 42 = 26;$$

$$r_2 = \left(S^*_i - dS_i\right) \bmod \varphi(q) =$$
$$= \left|7 - 15 \cdot 8\right| \bmod 42 = 13;$$

$$r_1 = \left(T^*_i - dT_i\right) \bmod \varphi(q) = \left|13 - 15 \cdot 9\right| \bmod 42 = 4.$$

Далее владелец передает ответ $(r_1, r_2, r_3) = (26, 13, 4)$ банку, который в свою очередь проверяет их истинность

$$A = \left(C^d g^{r_1} g^{r_2} g^{r_3}\right) \bmod q =$$
$$= \left(16^{15} \cdot 3^{26+13+4}\right) \bmod 43 = 5.$$

Поскольку вычисленное значение совпало с зашумленным вручением, то это означает, что владелец электронного кошелька доказал, что знает секретные части последнего. Банк подписывает электронный кошелек и передает его владельцу, который может осуществлять покупку.

Рассмотрим выполнение модифицированного протокола, в котором предлагается использовать псевдослучайную функцию повышенной эффективности.

Пусть задана мультипликативная группа G_{11}. В качестве первообразного элемента данной группы возьмем g = 2. В качестве секретного ключа пользователя выбираем $K_{ПС}$= 3. Пусть значения S = 4 и T = 5. Выбранные значения представим в двоичном

четырехразрядном коде. Пусть данный код разбивается на 2 части. В результате получаем, что секретный ключ, представленный в двоичном коде $K_{ПС} = 3_{10} = 0011_2$, будет представлен двумя двухразрядными блоками

$$K_{ПС1} = 00_2 = 0_{10},$$

$$K_{ПС2} = 11_2 = 3_{10}.$$

Аналогично поступаем с параметром S, который используется для выработки номера электронной банкноты. Так как значение $S = 4_{10} = 0100_2$, данное число можно представить в виде двух блоков по 2 разряда каждый

$$S_1 = 01_2 = 1_{10},$$

$$S_2 = 00_2 = 0_{10},$$

Для параметра проверки двоичной уплаты электронной банкноты, который равен $T = 5_{10} = 0101_2$. получаем два блока

$$T_1 = 01_2 = 1_{10};$$

$$T_2 = 01_2 = 1_{10}.$$

Для вычисления «вручения» воспользуемся выражением

$$C = g^{(K_{ПС1}+S_1+T_1)^{-1}} g^{(K_{ПС2}+S_2+T_2)^{-1}} \bmod q =$$

$$= 2^{(0+1+1)^{-1}} 2^{(3+0+1)^{-1}} \bmod 11 = 2^7 \bmod 11 = 7.$$

Обозначим показатель степени первообразного элемента через переменную $l_{обр} = 7$.

Пользователь пересылает истинное вручение банку. Банк полученное истинное вручение хранит для проведения проверки владельца электронного кошелька при следующем обращении.

Пусть пользователь для аутентификации производит зашумление, используемых выше параметров. В результате получаем, что «зашумленный» секретный ключ, представленный в двоичном коде $K^*_{ПС} = 2_{10} = 0010_2$, будет представлен двумя двухразрядными блоками

$$K^*_{ПС1} = 00_2 = 0_{10},$$

$$K^*_{ПС2} = 10_2 = 2_{10}.$$

Аналогично поступаем с параметром S, который используется для выработки номера электронной банкноты. Так как «зашумленное» значение $S^* = 3_{10} = 0011_2$, то данное число можно представить в виде двух блоков по 2 разряда каждый

$$S^*_1 = 00_2 = 0_{10},$$

$$S^*_2 = 11_2 = 3_{10},$$

Для «зашумленного» параметра проверки двоичной уплаты электронной банкноты, который равен $T^* = 6_{10} = 0110_2$. получаем два блока двоичного кода

$$T^*_1 = 01_2 = 1_{10};$$

$$T^*_2 = 10_2 = 2_{10}.$$

Для вычисления «зашумленного» вручения владелец кошелька использует выражением

$$C^* = g^{(K^*_{ПС1}+S^*_1+T^*_1)^{-1}} g^{(K^*_{ПС2}+S^*_2+T^*_2)^{-1}} \bmod q =$$

$$= 2^{(0+0+1)^{-1}} 2^{(2+3+2)^{-1}} \bmod 11 = 2^8 \bmod 11 = 3.$$

Обозначим показатель степени порождающего элемента через переменную $l^*_{обр} = 8$.

Владелец электронного кошелька пересылает банку «зашумленное вручение».

Для проверки пользователя банк прислал в качестве «вопроса» случайное число $d = 7$. Владелец электронного кошелька должен вычислить ответ на поставленный банком вопрос, используя свои секретные параметры кошелька. В результате он использует равенство

$$r_1 = l^*_{обр} - dl_{обр}, \bmod \varphi(q) =$$

$$= (8 - 7 \cdot 7) \bmod 10 = 9.$$

Вычисленный ответ на поставленный вопрос отправляется банку.

Последний приступает к проверке доказательства истинности пользователя

$$A = C^d g^{r_1} \bmod q = (7^7 \cdot 2^9) \bmod 11 =$$

$$= 2^8 \bmod 11 = 3.$$

Так как $A = C^* \bmod q$, то банк делает вывод о том, что пользователь является действительным владельцем секретных параметров секретного ключа $K_{ПС}$, чисел S и T. В результате этого пользователь получает кошелек с электронной наличностью.

Таким образом, применение псевдослучайной функции, определяемой выражением (6) позволило повысить скорость выполнения протокола «снятия со счета». Кроме того, реализация протоколов с использованием единой модулярной алгебраической системы позволит уменьшить требования к объему занимаемым программным обеспечением памяти персональных устройств хранения электронных денег.

Выводы

В работе рассмотрен протокол, позволяющий пользователю осуществить снятие

наличности в банке. Показана его итерационная природа. С целью повышения скорости выполнения протокола предложено использовать псевдослучайную функцию повышенной эффективности. Полученные результаты показали, что усовершенствованный протокол позволяет сократить трафик обмена между сторонами проверки, что влечет за собой повышение производительности СЭП. Кроме того использования единой модулярной алгебраической системы кольца и поля для реализации ПСФ, освобождает объем памяти для хранения электронных денежных средств.

Список литературы

1. Калмыков И.А., Дагаева О.И. Разработка псевдослучайной функции повышенной эффективности // Известия ЮФУ. Технические науки. – 2011. – №12. – С. 160–169.

2. 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. – С. 218–224.

3. Калмыков И.А., Дагаева О.И., Науменко Д.О., Вельц О.В. Системный подход к применению псевдослучайных функций в системах защиты информации // Известия Южного федерального университета. Технические науки. – 2013. – №12 (149). – С. 228–234.

4. Пярин В.А., Кузьмин А.С., Смирнов С.М. Безопасность электронного бизнеса. – М.: Гелиоас АРВ, 2009. – 432 с.