УДК 681.3

ЗАЩИТА ДАННЫХ В ЭЛЕКТРОННЫХ КОММЕРЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ МОДУЛЯРНЫХ СТРУКТУР

[1]Степанова Е.П., [1]Калмыков М.И., [2]Ананьев А.А., [2]Путинцев С.С.

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

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

Целью исследований является разработка новых протоколов для дальнейшего усовершенствования технологии «электронных денег» таких что, их применение позволяет обеспечить увеличение свободного объема памяти носителя электронной наличности за счет многократного использования псевдослучайной функции повышенной эффективности. Реализация итеративных протоколов на основе разработанной ПСФ является одним из основных путей достижения поставленных перед системами электронных платежей требований по обеспечению высокой степени криптографической защиты.

Ключевые слова: Системы электронных платежей, криптографические протоколы защиты данных, псевдослучайная функция, протокол доказательства *с* нулевым разглашением

DATA PROTECTION IN ELECTRONIC COMMERCIAL SYSTEMS BASED ON THE MODULAR STRUCTURE

[1]Stepanova E.P., [1]Kalmykov M.I., [2]Ananiev A.A., [2]Putintsev S.S.

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

[2]Filial Moscow state University of instrument engineering and informatic, Stavropol, e-mail:kia762@yandex.ru

The purpose of this research is to develop new protocols for further perfected technology-tence of «electronic money» such that their use allows for an increase in its memory the free-carrier electronic cash by reusing pseudowords-random function of increased efficiency. The implementation of iterative protocols developed on the basis of the RPA is one of the main ways to achieve its electronic payment systems requirements to ensure a high degree of cryptographic protection.

Keywords: Electronic payment systems, cryptographic protocols to protect data, pseudo-random function, the protocol Zero-knowledge proof

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.

Как правило, вопросы защиты денежных средств электронных коммерческих систем возлагается на протоколы криптографической защиты. Именно их стойкость во многом определяет степень защищенности электронных денег. В работе рассмотрены вопросы защита данных в электронных коммерческих системах на основе использования модулярных структур.

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 [1-3]:

• 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:

– сложность обеспечения вопросов сохранения анонимности пользователя – владельца электронных денежных средств;

– необходимость постоянной защиты передаваемых данных между пользователями протокола обмена от несанкционированного доступа;

– сложность протоколов, используемых в системах электронной коммерции.

Для решения отмеченных проблем в ряде работ предлагается использовать алгебраические модулярные структуры. Проведенные исследования показали, что такие системы обладают более широкими возможностями по реализации различных линейных и нелинейных криптографических функций [4]

$$A(z)+k(z)\equiv F(z)\bmod\pi(z), \qquad (1)$$

$$A(z)k(z)\equiv F(z)\bmod\pi(z), \qquad (2)$$

$$A(z)^{k(z)}\equiv F(z)\bmod\pi(z), \qquad (3)$$

где $\pi(z)$ – неприводимый полином, порождающей поле $GF(q)$; $q = p^v$; p – простое число; $A(z)$ – блок открытого текста длиной v разрядов; $F(z)$ – блок зашифрованного текста длиной v разрядов; $\{k(z)\}$ – множество ключевых данных.

В работах [5-8] представлен алгоритм нелинейного шифрования потока данных, использующий операцию возведения в степень символов конечного поля. При этом с целью сокращения времени зашифрования потока открытых данных предлагается использовать полиномиальную систему классов вычетов (ПСКВ). В данной непозиционной системе в качестве оснований используются неприводимые полиномы $p_i(z),\ i=1,2,...,n$, произведение которых дает рабочий диапазон системы

$$P(z)=\prod_{i=1}^{n}p_i(z). \qquad (4)$$

Для реализации алгоритма входной поток битов разбивается на отдельные блоки, двоичный код которых представляется в полиномиальной форме A*(z)*. В этом случае размер блока выбирается из условия

$$\deg A(z)<\deg P(z). \qquad (5)$$

Так как рабочий диапазон $P(z)$ представляет собой кольцо неприводимых полиномов, то на основе изоморфизма, порожденного китайской теоремой об остатках, что каждый блок *A(z)*, можно однозначно представить в виде

$$A(z)=(\alpha_1(z),\alpha_2(z),...,\alpha_n(z)). \qquad (6)$$

Так как сравнения по одному и тому же модулю можно почленно умножать, то последнее выражение представляется в виде:

$$F_j(z)=((\alpha_1^j)^{K_j}(z),...,(\alpha_n^j)^{K_j}(z))\bmod P(z). \qquad (8)$$

Представленные результаты исследования показали, что использование ПСКВ для реализации защиты информации от НСД позволяет повысить быстродействие более чем на 9% по сравнению с выполнением метода шифрования с возведением в степень по модулю в поле Галуа $GF(2^3)$. При этом при увеличении разрядности обрабатываемых данных возрастает эффективность применения ПСКВ для реализации нелинейных криптографических процедур защиты данных от НСД.

С целью решения первого и третьего недостатков 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 электронными монетами [2].

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 [1-3], 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 [1] 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 $K_{отк}$. При этом значение последнего определяется

В этом случае выражение (3) можно представить следующим образом

$$F_j(z)=\left|A_j^{K_j}(z)\right|_{P(z)}^{+}=\left|(\alpha_1^j(z),\alpha_2^j(z),...,\alpha_n^j(z))^{K_j}\right|_{P(z)}^{+}=(\beta_1^j(z),...,\beta_n^j(z)), \qquad (7)$$

где $\beta_i^j(z)\equiv F_j(z)\bmod p_i(z)$; $\alpha_i^j(z)\equiv A_j(z)\bmod p_i(z)$.

$$K_{отк} = g^{\text{К}_{\text{секр}}} \bmod q, \qquad (9)$$

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

Для этого пользователь выбирает некоторое случайное число r, вычисляет значение

$$Y = g^r \bmod q. \qquad (10)$$

Вычисленное значение пересылается банку. Проверяющая сторона выбирает число В из мультипликативной группы и пересылает его пользователю, т.е. «задает ему вопрос *B*». Получив «вопрос» с, пользователь должен на него вычислить «ответ» согласно равенства

$$Z = r - BK_{секр} (\bmod \varphi(q)). \qquad (11)$$

Полученный результат пересылается банку, который осуществляет проверку полномочий пользователя согласно

$$\overline{Y} = (\text{К}_{\text{отк}})^B g^Z (\bmod q) =$$

$$= (g^{K_{секр}})^B g^{r-BK_{секр}} (\bmod q) = g^r. \qquad (12)$$

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.

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 проблему можно за счет применения псевдослучайной функции (ПСФ) повышенной эффективности.

В работах [1-3] приведены примеры реализации псевдослучайной функции обладающей повышенной эффективностью. Следует отметить, что ПСФ нашли широкое применение и в других сферах. Так в работах [9,10] показано применение псевдослучайных функций в системах опознавания статуса спутника системы космической связи, используемой при управлении удаленным экологически-опасными объектами. Проведенные исследования показали, что применение разработанной псевдослучайной функции позволяет обеспечить сложность решения λ-DDH проблемы. Кроме того, одним из основных преимуществ 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.

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 $Y = g^{\text{r}} \bmod q$. Затем пользователь сам задает себе «вопрос» B

$$B = \text{F}_{\text{S}}(\text{Y}) = (\text{g}^{\frac{1}{\prod_{j=1}^{m}(r_j + y_j)}}) \bmod q, \qquad (13)$$

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

На поставленный вопрос пользователь вычисляет ответ согласно (11). 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 $\text{К}_{\text{отк}}$.

Пример. Пусть задана мультипликативная группа G_{11}. В данной группе существует первообразный элемент $g = 2$. В качестве секретного ключа пользователь выбираем $\text{К}_{\text{секр}} = 3$. Тогда открытый ключ определяется согласно (1) и составит

$$K_{отк} = g^{\text{К}_{\text{секр}}} \bmod q = 2^3 \bmod 11 = 8.$$

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

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

Разбиваем вычисленное число на два подблока $y_1 = 10_2 = 2$ 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 $s_1 = 01_2 = 1_{10}$ и $s_1 = 10_2 = 2_{10}$. Затем пользовате-

лю, используя полученные выше числа, необходимо вычислить вопрос B согласно (11). Имеем

$$B = \mathrm{F}_6(10) = (\mathrm{g}^{\frac{1}{(s_1+y_1)}\frac{1}{(s_2+y_2)}}) \bmod q = (2^{\frac{1}{(1+2)}\frac{1}{(2+2)}}) \bmod 11 = 2^2 = 4\,.$$

Таким образом, значение вопроса B = 2.

Вычислив свой вопрос, пользователь приступает к вычислениям ответа на данный вопрос, используя $r = 5$ и $\mathrm{K}_{\text{секр}} = 3$. При этом используется выражение (11). Тогда

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

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 $\mathrm{K}_{\text{отк}}$ и получает все зашифрованные значения чисел. Эти значения позволят получателю убедиться в правильности данной подписи. При этом используется выражение (12)

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

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

Выводы

В работе рассмотрены вопросы связанные с обеспечением защиты передаваемых в системах электронной коммерции. Представлен алгоритм нелинейного шифрования с использованием полиномиальной системы классов вычетов. Использование непозиционной системы класса вычетов позволяет повысить скорость выполнения операции зашифрования. Показана целесообразность применения псевдослучайной функции в протоколе аутентификации пользователя в банке. В статье рассмотрен пример реализации протокола с нулевым доказательством на основе псевдослучайной функции.

Список литературы

1. Калмыков И.А., Саркисов А.Б., Макарова А.В., Калмыков М.И. Расширение методов защиты систем электронной коммерции на основе модулярных алгебраических схем // Известия Южного федерального университета. Технические науки. – 2014. – № 2 (151). – С.218-225.

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

3. Калмыков И.А., Дагаева О.И. Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции // Известия Южного федерального университета. Технические науки. – 2012. – № 12 (137). – С.218-224

4. Калмыков И.А., Чипига А.Ф., Кихтенко О.А., Барильская А.В. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем // Известия ЮФУ Технические науки. – 2009. – № 11 (100). – С.210-220.

5. Зюзякин Г.И., Калмыков М.И., Петрова Е.В. Математическая модель системы защиты информации, функционирующей в полиномиальной системе класса вычетов // Современные наукоёмкие технологии. – 2014. – №3. – С.128-132.

6. Юртаев М.В., Калмыков М.И. Применение нелинейных алгоритмов шифрования в системах защиты информации от несанкционированного доступа // Успехи современного естествознания. – 2014. – №3. – С. 131-135.

7. 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.

8. Калмыков И.А., Чипига А.А. Алгоритм обеспечения информационной скрытности для адаптивных средст передачи информации // Инфокоммуникационные технологии. – 2007. – Т.5. – № 3. – С. 159-162.

9. Калмыков И.А., Пашинцев В.П., Вельц О.В., Калмыков М.И. Методы защиты передаваемой информации для систем удаленного контроля и управления высокотехнологическими объектами // Вестник Северо-Кавказского федерального университета. – 2014. – № 4 (43). – С.38-43.

10. Калмыков И.А., Вельц О.В., Калмыков М.И., Науменко Д.О. Алгоритм имитозащиты для систем удаленного мониторинга и управления критическими технология // Известия Южного федерального университета. Технические науки. – 2014. – № 2 (151). – С.181-187.