УДК 681.3

РАЗРАБОТКА ПРОТОКОЛА ВЫПЛАТЫ ЭЛЕКТРОННОЙ НАЛИЧНОСТИ С ИСПОЛЬЗОВАНИЕМ МОДУЛЯРНОЙ АРИФМЕТИКИ

[1]Топоркова Е.В., [1]Калмыков М.И., [2]Борода Н.П., [2]Сирота С.А.

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

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

В современных системах электронных платежей используется целый ряд протоколов, реализация которых позволит обеспечить эффективную работу автономной системы электронных платежей. При этом защита электронной наличности от несанкционированного доступа и модификации возлагается на протоколы криптографической защиты данных. В работе представлен протокол выплаты электронной наличности, реализованный на основе модулярной арифметики.

Ключевые слова: системы электронных платежей, криптографические протоколы защиты данных, псевдослучайная функция, протокол выплаты электронной наличности

PROTOCOL DEVELOPMENT OF THE PAYMENT ELECTRONIC CASH USING MODULAR ARITHMETIC

[1]Toporkova E.V., [1]Kalmykov M.I., [2]Boroda N.P., [2]Sirota S.A.

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

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

In modern electronic payment systems uses a number of protocols, implementation of which will ensure the effective operation of the Autonomous system of electronic payments. The protection of electronic cash from unauthorized access and modification is vested in the protocols, cryptographic protection of data. This paper presents the Protocol of the payment electronic cash, implemented based on modular arithmetic.

Keywords: Electronic payment systems, cryptographic data security protocols, pseudorandom function, the Protocol of the payment electronic cash

На современном этапе развития электронных коммерческих систем электронные деньги находят все большее распространение. Такая ситуация определяется достоинства, которыми обладает электронная наличность. В то же самое время для эффективного функционирования систем электронных платежей (СЭП) необходимо разрабатывать и использовать протоколы, обеспечивающие обмен данными между покупателем и продавцом в реальном масштабе времени и с высокой степенью защиты от несанкционированного доступа (НСД) и модификации.

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 (эмитент) и продавец (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, является актуальной задачей.

Обеспечить высокую степень защиты от НСД передаваемых данных можно за счет применения различных алгоритмов шифрования. При этом для обеспечения интерактивного обмена данными между двумя сторонами, участвующими в работе СЭП, такие алгоритмы должны работать в реальном масштабе времени. Одним из решений данной проблемы является использование в системах электронной платежей поточных шифров, на основе псевдослучайных последовательностей (ПСП).

Однако процедура обеспечения конфиденциальности и целостности информации на основе сложения потока псевдослучайных битов с битами исходного текста по модулю два не отличается стойкостью и может быть раскрыта при наличии определенного количества символов исходного и шифрованного текста. Несмотря на то, что такой шифр считается теоретически нераспознаваем, то с помощью системы уравнений можно раскрыть структуру генератора ПСП, имея в наличии $2k$ символов открытого и зашифрованного текста, где k – степень порождающего полинома.

Одним из путей решения является использование нелинейных алгоритмов шифрования, которые реализуются с использованием непозиционных модулярных структур [1-4]. В данных алгоритмах нашли широкое применение операции сложения, умножения и возведения в степень элементов конечного поля, а также их комбинаций. Так в работе [5] с целью повышения скорости выполнения нелинейных операций предлагается перейти к использованию полиномиальной системы классов вычетов. Параллельная независимая обработка малоразрядных остатков позволяет повысить скорость базовых операций алгоритмов нелинейного шифрования. В работе [6] предлагается использовать индексное представление элементов конечного поля Галуа. Переход к индексам позволил заменить низкоскоростную операцию возведения в степень по модулю на операцию умножения индексов.

Однако использование криптографических преобразований целесообразно при закрытии передачи данных по открытому каналу связи между пользователями СЭП. В то же самое время в протоколе выплаты электронной наличности в прямом виде нельзя использовать процедуры нелинейного шифрования. Как правило, для обеспечения требуемого уровня защиты от НСД в таких протоколах применяются псевдослучайные функции (ПСФ). В работах [7-8] представлена псевдослучайная функция, которая при меньшей длине ключа обеспечивает высокую криптостойкость, которая соответствует сложности решения l-DDH проблемы. Применение данной псевдослучайной функции в системах электронных платежей приведено в работах [9,10]. Использование одной ПСФ в различных протоколах позволяет сократить объем памяти носителя электронного кошелька, который будет использоваться для хранения программного обеспечения.

Рассмотрим использование этой ПСФ в протоколе «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

$$K_{отк} = g^{К_{секр}} \bmod q, \qquad (1)$$

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 Т для проведения протокола «двойной выплаты», $\sigma_{K_{БС}}(C)$ – подпись банка на вручение C, которое использовал покупатель при получении кошелька в банке; $К_{БС}$ – секретный ключ банка; J – показатель счетчика электронных монет

$$W = (K_{секр}, S, T, \sigma_{K_{БС}}(C), J). \qquad (2)$$

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

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

$$\sigma_{K_{БС}}(C) = \sigma_{K_{БС}}(K_{секр}, S, T); \qquad (3)$$

– покупатель правильно сгенерировал S_J номер J-й электронной купюры, используя при этом псевдослучайную функцию

$$S_J = g^{\frac{1}{S+J+1}}. \qquad (4)$$

Рассмотрим более подробно каждый этап протокола «выплаты одной монеты». При обращении в банк за электронным кошельком, покупатель доказывал банку в протоколе «снятия электронных денег со счета», что он является авторизованным пользователем этой наличности. Для этого покупатель вычислял вручение согласно следующего равенства

$$C = (\mathrm{g}^{\left(\prod_{j=1}^{m}(K_i+S_i+T_i)\right)^{-1}}) \bmod q, \qquad (5)$$

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; g –порождающий элемент мультипликативной группы; q – порядок мультипликативной группы с порождающим элементом g.

Затем после проверки подлинности покупателя банк подписывает вручение C и передает свою подпись в электронном кошельке его владельцу.

На первом этапе покупки с помощью электронной наличности , для того чтобы доказать продавцу, что в электронном кошельке присутствует подпись банка, выдавшего электронные купюры, покупатель производит вычисление вручение

$$B = g^{\left(\sigma_{K_{БС}}(C)\right)^{-1}} \bmod q = g^{\sigma_{обр}(C)} \bmod q, \quad (6)$$

где $\sigma_{обр}(C) = \left(\sigma_{K_{БС}}(C)\right)^{-1} \bmod q$ – обратная величина подписи вручения банку.

Затем покупатель затемняет значение вручения банка

$$\sigma^{*}_{обр}(C) = \left(\sigma_{обр}(C) + \Delta\sigma\right) \bmod q, \quad (7)$$

где $1 \le \Delta\sigma \le q-1$ – случайная величина.

После этого покупатель вычисляет затемненное вручение продавцу

$$B^{*} = \mathrm{g}^{\sigma^{*}_{обр}(C)} \bmod q. \quad (8)$$

Эти значения пересылаются продавцу, который в ответ высылает случайное число, которое принадлежит мультипликативной группе $1 < d < q$. Владелец электронного кошелька, получив вопрос *d*, производит ответ на поставленный вопрос

$$r = \sigma^{*}_{\text{обр}}(C) - d\sigma_{обр}(C) \bmod \varphi(q). \quad (9)$$

Далее покупатель передает ответ на поставленный вопрос продавцу. Затем продавец производит проверку полученного ответа

$$B^{d} g^{r} = \left(\mathrm{g}^{\sigma_{обр}(C)}\right)^{d} g^{r} \bmod q =$$

$$= g^{d\sigma_{обр}(C) + \sigma^{*}_{обр}(C) - d\sigma_{обр}(C)} \bmod q =$$

$$= g^{\sigma^{*}_{обр}(C)} \bmod q = B^{*} \quad (10)$$

Если выражение (10) будет истинным, то это свидетельствует о том, что покупатель обладает электронным кошельком, который подписан банком. Другими, словами, покупатель является платежеспособным.

Данную процедуру проверку наличия у покупателя электронного кошелька можно провести применяя другой алгоритм. В этом случае, используя свой секретный ключ, покупатель закрывает данные $E_{K_{секр}}(C, \sigma_{K_{БС}}(C))$ и пересылает зашифрованный текст продавцу товара.

Продавец, зная открытый ключ покупателя, расшифровывает данное сообщение $D_{K_{отк}}(C, \sigma_{K_{БС}}(C))$ и получает в открытом виде вручение С покупателя 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 С, которое представил покупатель в банк для получения кошелька. Продавец сравнивает эти значения. При совпадении этих значений продавец убеждается, что у покупателя есть электронный кошелек.

Реализация последнего алгоритма возможна только в том случае, когда продавец может интерактивно обращаться в банк. При этом первый алгоритм проверки электронного кошелька у покупателя позволяет обеспечить автономную работу двух субъектов «купли-продажи», не увеличивая при этом трафик между банком и его клиентами.

Выводы

Использование в системах электронной коммерции криптографических протоколов аутентификации покупателя позволяет обеспечить высокую надежность работы такой системы. Применение разработанного протокола выплаты электронной наличности с использованием модулярной арифметики позволяет продавцу в интерактивном режиме провести проверку наличности покупателя. При этом применение единой псевдослучайной функции позволит сократить затраты на память в носителе электронного кошелька за счет использования ПСФ в нескольких протоколах.

Список литературы

1. 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.

2. 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.

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

4. Калмыков И.А., Стрекалов Ю.А., Щелкунова Ю.О., Кихтенко О.А., Барильская А.В. Технология нелинейного шифрования данных в высокоскоростных сетях связи // Инфокоммуникационные технологии. 2010. Т. 8. № 2. С.14-22.

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., Дагаева О.И. Разработка псевдослучайной функции повышенной эффективности // Известия Южного федерального университета. Технические науки. – 2011. –№ 12 (125). – С. 160-169.

8. 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.

9. 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.

10. 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.