РЕАЛИЗАЦИЯ КАСКАДНОЙ ПСЕВДОСЛУЧАЙНОЙ ФУНКЦИИ В ПРОТОКОЛЕ «ДВОЙНОЙ ОПЛАТЫ»

Калмыков И.А., Науменко Д.О., Березкина М.В., Макарова А.В., Калмыков М.И.

Северо-Кавказский федеральный университет.

Институт информационных технологий и телекоммуникаций

г. Ставрополь, Россия

Электронные деньги, выступая как универсальное платежное средство, являются более удобными в обращении и лишены недостатков присущих бумажным финансам, среди которых можно выделить:

- фальсификация;
- использование металлической мелочи;
- очереди при взаиморасчетах.

Электронные деньги устраняют вышеупомянутые недостатки традиционных платежных систем, предоставляя удобный механизм для осуществления выплат.

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

В настоящее время вопросам электронной коммерции уделено достаточно много внимания. В работах [1-3] описаны алгоритмы работы систем, использующих электронные деньги. Основным недостатком таких систем является сложность определения ситуации повторного использования нарушителем денежных средств при расчетах без использования доверительного центра. Кроме того, существующие протоколы применения электронных денег требуют значительные объемы памяти для своей программной реализации, тем самым не позволяя обеспечить хранение большого объема электронных денежных средств на компактных носителях типа смарт-карт.

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 [3] для предотвращения повторного использования электронных монет предлагается 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.

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

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 [4] 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 $\log_2 \ell$ раз меньше умножений. Основным преимуществом данной ПСФ является использование меньшего объема памяти для вычисления значения функция, так как она 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.

В этом случае уравнение «двойной выплаты» примет вид

$$M_i = T_{отк}(F_s(i))^{R_i} = T_{отк}(g^{\frac{1}{\prod_{j=1}^{m}(s+b_j)}})^{R_i} \bmod q.$$

В этом случае для определения секретного ключа злоумышленника банку необходимо вычислить отношение $\left(M_1^{R_2} / M_2^{R_1}\right)^{(R_2-R_1)^{-1}}$.

Выводы. В работе показана целесообразность применения каскадной реализации разработанной псевдослучайной функции. Обладая соответствующей криптографической стойкостью, данная ПСФ позволяет уменьшить временные затраты и сократить размер секретного ключа в $\log_2 \ell$ раз.

Литература

1. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. JACM, Vol. 33, No. 4, October 1986. http://www.wisdom.weizmann.ac.il/~oded/ggm.html

2. Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. In FOCS'97, pages 458–67, 1997. http://www.wisdom.weizmann.ac.il/~naor/PAPERS/gdh_abs.html

3. Калмыков И.А., Дагаева О.И.Разработка псевдослучайной функции повышенной эффективности (статья) Известия ЮФУ. Технические науки, Таганрог: ТРТУ , 2011 г. №12, С. 160-169