Сергиенко Е.Н., Чурилов А.С. Анализ криптостойкости и эффективности протокола электронной наличности T. Nakanihi, M. Shiota, Y. Sugiyama. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XV Междунар. научно-техн. конф. – Пенза: ПДЗ, 2015. – С. 210-215.

УДК 332.1

АНАЛИЗ КРИПТОСТОЙКОСТИ И ЭФФЕКТИВНОСТИ ПРОТОКОЛА ЭЛЕКТРОННОЙ НАЛИЧНОСТИ T. NAKANISHI, M. SHIOTA, Y. SUGIYAMA

Е.Н. Сергиенко, А.С. Чурилов

ANALYSIS OF STRONG CRYPTOGRAPHY AND EFFICIENCY OF THE PROTOCOL OF ELECTRONIC CASH OF T. NAKANISHI, M. SHIOTA, Y. SUGIYAMA

E.N. Sergienko, A.S. Churilov

Аннотация. Проблема анонимности электронных финансовых транзакций с недавнего времени весьма актуальна. В статье проанализирована криптостойкость и «несвязываемость» анонимных электронных платежей в алгоритмах электронных денег, а также предложен способ увеличения эффективности вычислений операций, используемых в протоколах e-cash систем за счет использования быстрых алгоритмов для длинных чисел.

Ключевые слова: криптостойкость, протоколы анонимных e-cash систем, система электронных платежей, длинная арифметика.

Abstract. The anonymity of electronic financial transactions problem is very relevant in recent time. This article analyzes the cryptographic persistence and «unlinkability» of anonymous electronic payments in electronic money algorithms. Based on the fast algorithms for long numbers, the method for increasing computing efficiency for operations in protocols of e-cash is also provided.

Keywords: strong cryptography, anonymous e-cash system protocols, electronic payment system, arbitrary-precision arithmetic.

История анонимных протоколов e-cash началась с опубликования Дэвидом Чаумом в 1982 году алгоритма слепой подписи. Его суть состоит в том, что подписывающая сторона не знает полностью содержимое подписываемого документа [1]. Криптостойкость слепой подписи основывается на сложности факторизации больших составных чисел, используемых алгоритмом RSA. Стоит отметить, что для повышения криптостойкости к атакам Винера на RSA следует использовать длину ключей не менее 2048 бит.

Система онлайн электронной наличности [2] базируется на схеме подписи Camenisch-Lysyanskaya, основанной на криптостойкости алгоритма RSA. Эта схема использует два типа протоколов: протокол подписи и протокол доказательства нулевого разглашения. Обозначим подпись сообщений m_1, m_2, m_3 как $Sign(m_1, m_2, m_3)$. При помощи первого протокола получатель отправляет сообщения m_1, m_2, m_3 подписывающему лицу и получает в ответ подписанное сообщение $Sign(m_1, m_2, m_3)$ без раскрытия его содержания подписывающему лицу. Второй протокол позволяет владельцу подписи доказать содержание сообщений и подписи за счет использования протокола с нулевым разглашением.

Система [2] представляет подпись банка $Sign(x, y, m)$ как монету, где x, y – секрет клиента и m – номинал монеты. При списании банком монеты $Sign(x, y, m)$ клиент получает новую монету $Sign(x, y', m')$ от банка, в то время как разница $d = m' - m$ взымается со счета клиента. При оплате клиент с монетой $Sign(x, y', m')$ получает новую монету $Sign(x, y'', m'')$, оплаченная сумма $d' = m' - m''$ переводится на счет продавца. Эти протоколы позволяют клиенту доказать собственность старой монеты и получить новую, не раскрывая тайн x, y, y', y'' и суммы m, m', m''. Кроме того, равенства $d = m' - m$ и $d' = m' - m''$ доказываются с помощью методов нулевого разглашения, а $m'' \geq 0$ проверяется тем же методом, чтобы защититься от раскрытия секрета.

С другой стороны, протоколы по списанию средств и по оплате вызываются клиентом, чтобы послать $f(y)$ для проверки, где f – односторонняя функция с дискретным логарифмом. Это позволяет банку обнаружить, является ли монета потраченной два или более раз. Кроме того, секрет x характерен для всех монет и привязан к личности плательщика. Эта информация используется для снятия анонимности, которое необходимо для решения конфликтов, связанных с кражей или использованием монеты другим лицом.

Чтобы проверить эффективность протокола, рассматриваемого в данной статье, вычислим затраты на выполнение операций модульного возведения в степень (E), модульного умножения (M), модульного сложения (A) и операции хеширования (H).

Выберем параметры RSA такой длины: $n = 1024$ бит, $p = 512$ бит, $q = 512$ бит. Также будем считать, что в качестве алгоритма симметричного шифрования и хеширования используются AES и SHA1, длина зашифрованного сообщения и хеша 128 и 160 бит соответственно. Для сравнения были выбраны протоколы, изложенные в [2–12]. Согласно [13], $H \approx M, E \approx inv \approx 240M$. Результаты сравнения вычислительной сложности выбранных протоколов представлены в табл. 1.

Таблица 1

Протокол	Количество операций
[2]	$22E + 11M + 4A \approx 5191M$
[3]	$5E + 7M + 7H + 1inv + 1A \approx 1454M$
[4]	$14E + 14M + 1H + 5A \approx 3375M$
[5]	$6E + 8M \approx 1448M$
[6]	$23E + 14M + 1A \approx 5534M$
[7]	$2E + 2M + 2H \approx 966M$
[8]	$5E + 9M + 1H + linv + 2A \approx 1450M$
[9]	$2E \approx 480M$
[10]	$18E + 15M + 2H + 8A \approx 4337M$
[11]	$31E + 22M + 6H + 10A \approx 7468$
[12]	$6E + 8M + 1H \approx 1449M$

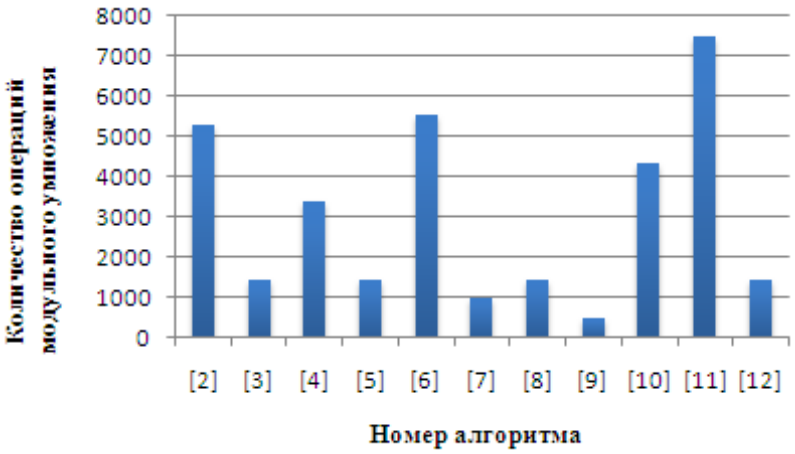
На рисунке представлена гистограмма сложности протоколов [2–12].

Сравним рассмотренные протоколы [2–12] по следующим критериям:

- применение в online/e-cash системах (on/off-line);

- возможность раскрытия личности (Conditional-traceability);
- привязка монеты к владельцу (No-swindling);
- использование доказательства с нулевым разглашением (Formal proof).

Результаты сравнения представлены в табл. 2.



Гистограмма сложности протоколов [2–12]

Таблица 2

Протокол	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
On/off-line	on	off	Off	off	off	on	off	off	off	off	off
Conditional traceability	Да	Да	Да	-	Да	-	Да	Да	Да	Да	-
No-swindling	Да	Да	-	-	-	-	-	Да	-	-	-
Formal proof	Да	Да	Да	-	Да	-	-	Да	Да	Да	-

Сопоставив данные табл. 1 и 2, можно сказать, что, несмотря на большую сложность вычислений, протокол [2] удовлетворяет всем базовым требованиям, а также приведенным выше критериям. Эффективность протоколов электронной наличности можно повысить за счет использования быстрых алгоритмов умножения и возведения в степень, эффективность которых в сравнении с классическими операциями умножения и возведения в степень показана в статье [14].

Классический алгоритм умножения «столбиком» имеет сложность $O(N^2)$, в то время как алгоритм Карацубы, основанный на принципе «разделяй и властвуй», позволяет снизить сложность до $O\left(N^{\log_2 3}\right)$, а алгоритм умножения в классах вычетов – до $O(N \cdot logN)$. Вместо классического алгоритма возведения в степень по модулю, сложность которого $O((logN)^3)$, предлагается использовать бинарный алгоритм возведения в степень сложностью $O(logN)$.

Использование быстрых алгоритмов позволяет сократить расходы не только на вычисления, но и на хранение данных, что, безусловно, сократит расходы на обслуживание анонимной платежной системы.

Использование банками обычных протоколов электронных денег дает возможность злоумышленнику собирать информацию о платежных транзакциях любого человека. Применение же анонимных протоколов электронной наличности позволяет избежать слежки и утечки личных данных.

Библиографический список

1. Chaum D. «Blind signatures for untraceable payments», Proc. CRYPTO'82, pp.199-203, Plenum Press, 1983.

2. Nakanishi T., Shiota M., Sugiyama Y. «An efficient online electronic cash with unlincable exact payments», ISC 2004, pp. 367-378, Springer, 2004.

3. Nakanishi T., Shiota M., Sugiyama Y. "An efficient online electronic cash with unlinkable exact payments," Information Security, vol. 3225, pp. 367–378, 2004.

4. Brands S. "Untraceable off-line cash in wallets with observers (extended abstract)," CRYPTO, pp. 302–318, 1993.

5. Baseri Y., Takhtaei B., Mohajeri J. "Secure untraceable off-line electronic cash system," Scientia Iranica, vol. 20, pp. 637–646, 2012.

6. Camenisch J., Hohenberger S., Lysyanskaya A. "Compact e-cash," in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '05), pp. 302–321, May 2005.

7. Chang C.C., Lai Y.P. "A flexible date-attachment scheme on e-cash," Computers and Security, vol. 22, no. 2, pp. 160–166, 2003.

8. Eslami Z., Talebi M. "A new untraceable off-line electronic cash system," Electronic Commerce Research and Applications, vol. 10, no. 1, pp. 59–66, 2011.

9. Fan C.I., Huang V.S.M., Yu Y.C., "User efficient recoverable off-line e-cash scheme with fast anonymity revoking," Mathematical and Computer Modelling, vol. 58, pp. 227–237, 2013.

10. Hanatani Y., Komano Y., Ohta K., Kunihiro N. "Provably secure electronic cash based on blind multisignature schemes," Financial Cryptography, vol. 4107, pp. 236–250, 2006.

11. Popescu C. "An off-line electronic cash system with revokable anonymity," in Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference, pp. 763–767, May 2004.

12. Wang C., Sun H., Zhang H., Jin Z. "An improved off-line electronic cash scheme," in Proceedings of the 5th International Conference on Computational and Information Sciences (ICCIS '13), p. 438–441, 2013.

13. Menezes A., Oorschot P. van, Vanstone S. Handbook of Applied Cryptography, CRC Press, New York, NY, USA, 1997.

14. Сергиенко Е., Чурилов А., Панарин С., Давыденко Д., Смакаев А., Пригорнев И. Анализ эффективности использования быстрых алгоритмов в длинной арифметике // I Международная научно-практическая конференция «Проблемы информационной безопасности». – Гурзуф, 2015.

Сергиенко Елена Николаевна
Белгородский государственный
технический университет
им. В.Г. Шухова,
г. Белгород, Россия
E-mail: selena07@inbox.ru

Sergienko E.N.
Belgorod StateTechnological
Universitynamed after V.G. Shukhov,
Belgorod, Russia

Чурилов Антон Сергеевич
Белгородский государственный
технический университет
им. В.Г. Шухова,
г. Белгород, Россия
E-mail: bstu@live.ru

Churilov A.S.
Belgorod StateTechnological
Universitynamed after V.G. Shukhov,
Belgorod, Russia