7. Коблиц, Н. Курс теории чисел и криптография/ Н. Коблиц − М. : ТВП, 2001 − 260 с.
8. Even S., Goldreich O., and Lempel A. A randomized protocol for signing contracts, Communications of the ACM, Volume 28: 1985 — P. 637−647.
9. Фролов А.Б. Эффективные протоколы передачи комбинации сообщений с забыванием/ А.Б. Фролов// Ползуновский вестник,2012.№ 2/1. 2012 — С. 129-133.
10. Frolov, A. Effective Oblivious Transfer Using Probabilistic Encryption/ A. Frolov// In AISC-170. Complex Systems and Dependability. Springer Verlag, 2012 — P. 131-147.
11. Frolov, A. Improving of Non-Interactive Zero-Knowledge Arguments Using Oblivious Transfer. / A.Frolov //In New Results in Dependability and Computer Systems. Advances in Intelligent Systems and Computing, V. 224, Springer, 2013, pp. 153-171.

Профессор кафедры математического моделирования Национального исследовательского университета «МЭИ» д.т.н., проф. ***Фролов А.Б.*** *– abfrolov@mail.ru*

УДК: 519.24

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ НЕИНТЕРАКТИВНЫХ АНАЛОГОВ Σ -ПРОТОКОЛОВ С МНОЖЕСТВЕННЫМИ ЗАПРОСАМИ

А.Б. Фролов

В статье рассматриваются неинтерактивные аналоги интерактивных протоколов идентификации (Σ-протоколов) с множественными запросами. Показано, что для повышения устойчивости к действиям нечестного доказывающего число проверок может быть увеличено при сохранении информационной скорости за счет применения эффективной t+1-из-2t , 1<t≤6, забывающей передачи при многократном использовании единого рандомизатора.

Ключевые слова: протокол с нулевым разглашением секрета, протокол идентификации, множественный запрос, забывающая передача, рандомизатор, информационная скорость.

Введение

Настоящая работа посвящена изучению неинтерактивных протоколов с нулевым разглашением секрета как важных криптографических примитивов современных криптосистем. Функциональность и основные характеристики таких протоколов, их преимущества и недостатки по сравнению с интерактивными протоколами описаны во введении статьи [1] в настоящем журнале. Здесь рассмотрим особенности протоколов доказательства с нулевым разглашением для языков. Протокол доказательства с нулевым разглашением $(P,V)(x)$ исполняется двумя участниками — доказывающим P и проверяющим V, владеющими общей информацией x [2]. Эта общая информация является элементом известного языка L и значением $z= f(s)$ односторонней функции $f(s)$, прообраз s которого является секретом P, язык L характеризуется свидетелем w. Исполняя протокол для языка L, P убеждает проверяющего V, что $z\in L$, не разглашая никакой информации о секрете s. Такие протоколы имеют две вероятностные характеристики: *полнота* σ (нижняя граница вероятности успешного доказательства честным доказывающим P) и *неустойчивость* δ (верхняя граница вероятности успешного доказательства нечестным доказывающим $\widetilde{P}$, что данный элемент $\tilde{z} \notin L$ принадлежит языку L) — граница неустойчивости. Ее понижение означает повышение устойчивости протокола. Протокол (P,V)(x) может использоваться также для доказательства, что доказывающий владеет секретом s, без разглашения информации о секрете. В этом случае протокол является протоколом идентификации.

В настоящей статье предлагаются новые неинтерактивные протоколы идентификации, имитирующие логику интерактивных протоколов с нулевым разглашением секрета (Σ-протоколов) с множественными запросами (примером такого интерактивного протокола является протокол Шнорра [2]), а также рассматриваются особенности неинтерактивных протоколов для языков.

Как и в работе [1], неинтерактивность достигается использованием забывающей передачи [3,4,5]. В таких протоколах неинтерактивной коммуникационной фазе предшествует интерактивная фаза инициализации параметров забывающей передачи. Как и в протоколах с бинарными запросами [1], использование забывающей передачи требует ограничения вычислительных возможностей доказывающего. В связи с этим неинтерак-

тивный аналог интерактивного протокола доказательства с нулевым разглашением является протоколом *аргументации* с нулевым разглашением. При этих недостатках неинтерактивные протоколы этого типа не имеют ограничений на число доказываемых (аргументируемых) теорем для данного языка и, более того, являются «полиязыковыми» в том смысле, что в фазе коммуникаций с использованием однажды инициализированных параметров забывающей передачи можно осуществлять аргументации на основе различных односторонних функций.

Будем использовать следующие обозначения:

- NIOT_n^m - неинтерактивная *m*-из-*n* забывающая передача [4,5].

- NIZKOT_n^m - неинтерактивная аргументация с нулевым разглашением с использованием NIOT_n^m.

- NIEOT_n^m - эффективная (вследствие повторного использования рандомизатора) неинтерактивная *m*-из-*n* забывающая передача [4,5].

- $\mathrm{NIZKEOT}_n^m$ - неинтерактивная аргументация с нулевым разглашением с использованием NIEOT_n^m.

- $e_{\mathrm{NIZKOT}_n^m}$ ($e_{\mathrm{NIZKEOT}_n^m}$) - длина транзакции NIZKOT_n^m ($\mathrm{NIZKEOT}_n^m$).

- $\rho_{\mathrm{NIZKEOT}_n^m}=\dfrac{e_{\mathrm{NIZKOT}_n^m}}{e_{\mathrm{NIZKEOT}_n^m}}$ - коэффициент возрастания информационной скорости протокола $\mathrm{NIZKEOT}_n^m$ относительно протокола NIZKOT_n^m при одинаковой устойчивости (эффективность).

Вероятностные характеристики неустойчивости таких протоколов обозначаются $\delta_{\mathrm{NIZKOT}_n^m}$ и $\delta_{\mathrm{NIZKEOT}_n^m}$ соответственно.

$\mathrm{NIZKEOT}_n^m(p)$ обозначает p итераций протокола $\delta_{\mathrm{NIZKEOT}_n^m}$.

В этой статье описаны новые протоколы $\mathrm{NIZKOT}_{2^t}^{t+1}$ и $\mathrm{NIZKEOT}_{2^t}^{t+1}$, t>1, границы неустойчивости протокола $\mathrm{NIZKEOT}_{2^t}^{t+1}$ сравниваются с границами неустойчивости протоколов $\mathrm{NIZKOT}_{2^t}^{t+1}$ и $\mathrm{NIZKEOT}_2^1(2^t)$ (последние описаны и проанализированы в работе [1]), а также оценивается эффективность $\rho_{\mathrm{NIZKEOT}_{2^t}^{t+1}}$.

Протоколы аргументации $\mathrm{NIZKOT}_{2^t}^{t+1}$ и $\mathrm{NIZKEOT}_{2^t}^{t+1}$, ($t$>1)

Рассмотрим неинтерактивные аналоги интерактивных протоколов с t – битными запросами. Проблема в том, что множество возможных ответов состоит из $n=2^t$ элементов. Применение протокола $NIZKOT_n^1$ наименее эффективно: в этом случае граница устойчивости равна 2^{-t} в то время, как она может быть обеспечена протоколом $\mathrm{NIZKEOT}_2^1(t)$ с гораздо большей информационной скоростью. Рассмотрим реализацию NIZKOT_n^m и $\mathrm{NIZKEOT}_n^m$.

В фазе инициализации проверяющий V и доказывающий P генерируют системные параметры забывающей передачи NIOT_n^m (группу G большого простого порядка q, ее генератор g и элемент U с неизвестным обоим участникам дискретным логарифмом $\log_g U$), Проверяющий V случайно выбирает секретные ключи, вычисляет и публикует соответствующие открытые ключи, позволяющие ему скрытым для доказывающего образом получать m из n передаваемых им сообщений. Способы реализации протокола NIOT_n^m, а также его эффективного варианта NIEOT_n^m описаны и обоснованы в работах[8,9],

Рассмотрим неинтерактивную коммуникационную фазу. Пусть $n=2^t$, $m=t+1$ и P должен убедить проверяющего V в своем владении прообразом s объявленного значения $z=f(s)$ односторонней функции $f(x)$, используя NIZKOT_n^m. Аргументация включает следующие шаги.

Вызов (*commit*): доказывающий случайно выбирает элементы (или числа) l, $l_1,\ldots,l_t$ (committals), вычисляет значения (commits) $c=f(l)$, $c_1=f(l_1),\ldots,c_i=f(l_i),\ldots$, $gf(l_t)$, и посылает c, $c_1,\ldots$, $c_i,\ldots$, c_t проверяющему,

NIOT_n^m: Проверяющий вычисляет набор из $n=2^t$ сообщений

$$r_{(e\_1,\ldots,e\_\{t\})}=l+\sum_{i=1}^{t}e_i l_i+(e_1\vee\cdots\vee e_t)s,\quad e_i\in\{0,1\},$$

сохраняя лексикографический порядок индексов (мы полагаем, что функция $f(x)$ есть функция аддитивного типа. Здесь значения 0 и 1 логических переменных и выражений интерпретируются как целые числа. Доказывающий посылает проверяющему m из n сообщений посредством NIOT_{n}^{m}.

Верификация: Проверяющий получает *m-из-n* сообщений $m_{(e_{i1},\ldots,e_{it})}$, i=1,…, t+1, соответствующих t+1 произвольно выбранным бинарным наборам $(e_1,\ldots,e_t)$, неизвестным доказывающему и проверяет m=t+1 значений предиката

Verify($c,c_1,\ldots,c_i,\ldots, c_t, r_{(e_{i1},\ldots,e_{it})},z$):

$$f(r(e_{i1},\ldots,e_{it}) = cc_1^{e_{i1}}\cdots c_t^{e_{it}} z^{(e_{i1}\vee\cdots\vee e_{it})},$$

i=1,…, …, t+1. .

Если все эти значения суть *true*, аргументация принимается, в противном случае отклоняется.

При этом параметр полноты σ=1, поскольку если сообщения вычислены честным доказывающими, то все они будут соответствовать предикату проверки.

Чтобы оценить границу неустойчивости, заметим, что нечестный доказывающий $\tilde{P}$, который знает z, но не имеет информации об s, может вычислить не более t+1 сообщений, удовлетворяющих предикат (7).

Он не может выбрать l и вычислить $l_1,\ldots,l_t$ так, что t+2 ответов $r_{(e_1,\ldots,e_t)}$ будут удовлетворять предикат. Если это случится, то из t+2 уравнений

l+$e_{i1}l$1+…+ $e_{it}l_t$ +s, i=1,…,t+2

можно будет найти значение $s=f^{-1}(z)$, то есть прообраз значения односторонней функции,

С другой стороны, нечестный доказывающий $\tilde{P}$ может вычислить t+1 сообщений, имеющих индексы ($e_1,\ldots,e_t$) веса 0 или 1, соответствующих значениям $c,c_1,\ldots,c_i,\ldots, c_t$, и удовлетворяющих предикат, следующим образом: выбрать случайное значение l=$r_{(0,\ldots,0)}$ и определить значение c=$f(l)$. Затем случайно выбрать t различных значений $r_{(e_1,\ldots,e_t)}$ с индексами веса 1 и вычислить значения c_i=$f(r_i$–$r)z^{-1}$, где r_i= $r_{(e\_1,\ldots,e\_\{t\})}$ при e_i=1,i=q,…,t, r=l. теперь, чтобы определить недостающее сообщение $r_{(e\_1,\ldots,e\_\{t\})}$, надо знать секрет s. Нечестный доказывающий при ограниченных вычислительных ресурсах вынужден выбирать его случайно. Вероятность, что в итоге будет удовлетворен предикат проверки ничтожна. Отсюда следует, что ложное принятие t+1 из 2^t сообщений не превышает $\frac{1}{C_{2^t}^{t+1}}$.

Для доказательства совершенства заметим, что проверяющий получает t+1 сообщений, что позволяет ему иметь систему t+1 уравнений от t+2 переменных, имеющую решение при любом значении s, то есть секретность является безусловной.

Теперь можно оценить границу неустойчивости в сравнении с NIZKOT_{2}^{1} [1]. Транзакции протокола $\mathrm{NIZKOT}_{2^t}^{t+1}$ argument имеют вид :

$$c,c_1,\ldots,c_t\, z\ \mathrm{OT}(m_1,\ \ldots,\ m_{2^t})$$

где OT транзакция состоит их 2^t криптограмм Эль Гамаля, т.е. содержит 2^{t+1} элементов группы G' и t+1 элементов алгебраической структуры, соответствующей функции f. Граница неустойчивости оценивается как $\frac{1}{C_{2^t}^{t+1}}$.

Если применяется эффективная (с повторным использованием рандомизатора) забывающая передача, то OT транзакция содержит один элемент (экспонента рандомизатора) и 2^t вторых элементов криптограмм Эль Гамаля, т.е. транзакция состоит из 2^t +1 элементов группы G' и t+1 элементов алгебраической структуры. соответствующей функции f. Граница неустойчивости не изменяется.

По протоколу $\mathrm{NIZKEOT}_{2}^{1}(2^t)$ [1] пересылаются 3x2^{t}+1 элементов, его граница неустойчивости есть $\left(\frac{1}{2}\right)^{-2^t}$.

При сравнении границ неустойчивости слагаемыми t+1 и 1 можно пренебречь.

Отсюда

$$\delta_{\mathrm{NIZK\,E\,OT}_{2^t}^{t+1}} \approx \delta_{\mathrm{NIZK\,OT}_{2^t}^{t+1}(2)} = \left(\delta_{\mathrm{NIZK\,OT}_{2^t}^{t+1}}\right)^2. \quad (1)$$

За время исполнения $\mathrm{NIZKOT}_{2^t}^{t+1}(3)$ с границей устойчивости $\delta_{\mathrm{NIZKOT}_{2^t}^{t+1}(3)} = \left(\frac{1}{C_{2^t}^{t+1}}\right)^3$ можно дважды исполнить $\mathrm{NIZKEOT}_{2}^{1}(2^t)$ обеспечивая границу

неустойчивости $\delta_{\mathrm{NIZKEOT}_2^1(2\times 2^t)}=\left(\frac{1}{2}\right)^{-2^{t+1}}$.

За время исполнения $\mathrm{NIZKEOT}_{2^t}^{t+1}(3)$ с такой же границей неустойчивости $\delta_{\mathrm{NIZKEOT}_{2^t}^{t+1}(3)}=\left(\frac{1}{C_{2^t}^{t+1}}\right)^3$ можно исполнить $\mathrm{NIZKEOT}_2^1(2^t)$ только один раз, что соответствует границе неустойчивости $\delta_{\mathrm{NIZKEOT}_2^1(2^t)}=\left(\frac{1}{2}\right)^{-2^t}$.

В таблице 1 представлены некоторые значения этих границ и данные об их сравнении.

Таблица 1. Сравнение границ неустойчивости

t	3	4	5	6	7
$\frac{\delta_{\mathrm{NIZKOT}_2^1(2^t\times 5)}}{\delta_{\mathrm{NIZKOT}_{2^t}^{t+1}(3)}}$	≈ 100	≈ 5649	<1	$<<1$	$<<1$
$\frac{\delta_{\mathrm{NIZKEOT}_2^1(2^t\times 2)}}{\delta_{\mathrm{NIZKOT}_{2^t}^{t+1}(3)}}$	$\approx 5{,}5$	$\approx 19{,}5$	<1	$<<1$	$<<1$
$\frac{\delta_{\mathrm{NIZKEOT}_2^1(2^t)}}{\delta_{\mathrm{NIZKEOT}_{2^t}^{t+1}(3)}}$	≈ 1339	$\approx 655\times 10^3$	$\approx 733\times 10^5$	$\approx 130\times 10^5$	$<<1$
$\delta_{\mathrm{NIZKEOT}_{2^t}^{t+1}(3)}{}^{-1}$	$\approx 343\times 10^3$	$\approx 833\times 10^8$	$\approx 744\times 10^{15}$	$\approx 240\times 10^{24}$	$\approx 292\times 10^{35}$
$\delta_{\mathrm{NIZKEOT}_2^1(2^t)}{}^{-1}$	256	65536	$\approx 429\times 10^7$	$\approx 184\times 10^{15}$	$\approx 340\times 10^{36}$

Из описаний протоколов следует, что эффективность протокола $\mathrm{NIZKEOT}_{2^t}^{t+1}$ (относительно протокола $\mathrm{NIZKOT}_{2^t}^{t+1}$) оценивается как:

$$\rho_{\mathrm{NIZKEOT}_{2^t}^{t+1}}=\frac{t+1+2^{t+1}}{t+2+2^t}\approx 2. \qquad (2)$$

Из аппроксимаций (1,2) и таблицы 1 можно видеть, что повторное использование рандомизатора влечет существенное понижение границ неустойчивости, что делает $\mathrm{NIZKEOT}_{2^t}^{t+1}$ более эффективным по сравнению с $\mathrm{NIZKOT}_{2^t}^{t+1}$ и при $t\le 6$, гораздо более привлекательными, чем $\mathrm{NIZKEOT}_2^1(2^t)$, с обеспечением малой границы неустойчивости.

Как видим, эффективность протокола $\mathrm{NIZKEOT}_{2^t}^{t+1}$ (относительно $\mathrm{NIZKOT}_{2^t}^{t+1}$) оценивается как $\rho_{\mathrm{NIZKEOT}_{2^t}^{t+1}}=\frac{t+1+2^{t+1}}{t+2+2^t}\approx 2$.

В работе [4] доказано

Утверждение 1. *Многократное использование одного и того же рандомизатора в протоколе* NIEOT_n^m *безопасно.*

Поэтому справедливо

Следствие 1. *Повторное использование рандомизатора в пределах одной итерации* $\mathrm{NIZKEOT}_n^m$ *безопасно.*

Повторное использование рандомизатора y в различных итерациях $\mathrm{NIZKEOT}_n^m(p)$ тем более безопасно, поскольку в отличие от ключей, используемых в пределах одной итерации, ключи, используемые в различных итерациях алгебраически не связаны.

Следствие 2. *Повторное использование рандомизатора* y *во всех итерациях* $\mathrm{NIZKEOT}_n^m(p)$ *безопасно.*

Следствие 3. Аппроксимации (1,2) справедливы.

Остается открытым следующий вопрос: можно ли решить проблему Диффи − Хеллмана с использованием алгоритма для вычисления m_i, i вне области определения π, при условии, что V знает элементы $x_{\pi(i)}$, U, $m_{\pi(i)}(\beta_{\pi(i)}{}^y)$, $\beta_{\pi(i)}=b^{x_{\pi(i)}}$ при i=1,..., m, и c=b^y.

Особенности протоколов для языков

Как отмечено во введении, применение забывающей передачи возможно лишь при ограничении вычислительных возможностей нечестного доказывающего. Поэтому интерактивные протоколы доказательства с нулевым разглашением для языков трансформируются в неинтерактивные протоколы аргументации с нулевым разглашением. Такие протоколы могут быть реализованы на основе подходов к аргументации знания прообраза односторонней функции, рассмотренных в работе [1] и в предыдущем разделе настоящей работы.

Пример. Для языка $L=Q_n$, состоящего из квадратичных вычетов (QR) по модулю составного числа n со свидетелем w, являющимся факторизацией числа n, известен сле-

дующий интерактивный протокол [6]. Доказывающий убеждает проверяющего, что элемент z есть квадратичный вычет по модулю n.

1. Проверяющий P выбирает случайный вычет l (*committal*), вычисляет и посылает проверяющему *commit* $c=l^2$.

2. Проверяющий выбирает случайный запрос $e\in\{0,1\}$ и посылает его доказывающему.

3. Доказывающий вычисляет ответ $r=ls^e$, где s есть квадратный корень из z по модулю n и посылает его проверяющему.

4. Последний вычисляет предикат $r^2=cz^e$. Если он получает *true*, то принимает доказательство, иначе отклоняет.

Из таблицы 2 видно, что нечестный доказывающий успешно докажет, что квадратичный невычет $\tilde{z}$ является квадратичным вычетом только если он угадает запрос проверяющего, даже если он знает свидетеля языка (разложение n). Таким образом, вычислительные возможности нечестного доказывающего могут быть неограниченными.

Таблица 2. Ситуации для нечестного доказывающего

Ожидаемый запрос	Commit	Ответ	Неожиданный запрос	Нереализуемый ответ
e=1	$c=l^2/\tilde{z}$ mod n	$r=l$	$e=0$	$r=\sqrt{l^2/\tilde{z}} \bmod n$
$e=0$	$c=l^2$ mod n	$r=l$	$e=1$	$r=\sqrt{l^2\tilde{z}} \bmod n$

Рассмотрим неинтерактивную версию протокола .

1. Доказывающий P выбирает случайно вычет l (*committal*) и вычисляет *commit* $c=l^2$.

2. Доказывающий вычисляет ответы $r_0=l$ и $r_1=ls$ где s есть квадратный корень из z по модулю n.

3. Доказывающий посылает проверяющему транзакцию (c, OT(r_0,r_1))

4. Проверяющий вычисляет значение предиката $r^2=c$, если в соответствии с его секретным ключом выбрано первое сообщение, или значение предиката $r^2=cz$, если выбрано второе сообщение. Если получено значение *true*, доказательство принимается, иначе отклоняется.

Нечестный доказывающий, имеющий неограниченные вычислительные возможности, из открытых ключей проверяющего может найти его секретные ключи и узнать выбор проверяющего. Если он соответствует первому сообщению, нечестный доказывающий посылает транзакцию с *commit* $c=l^2$ mod n, $r_0=l$ и произвольным r_1, иначе он посылает транзакцию, где $c=l^2\tilde{z}$ mod n, $r_1=l$ и произвольное r_0. Следовательно, вычислительные возможности нечестного доказывающего должны быть полиномиально ограничены. Тогда он будет иметь успех только тогда, если угадает выбор проверяющего, даже при знании разложения модуля.

Заключение

В статье представлены новые эффективные неинтерактивные протоколы идентификации, являющиеся аналогами интерактивных протоколов с множественными запросами, оценена их эффективность и доказана безопасность при условии полиномиального ограничения вычислительных возможностей нечестного доказывающего.

Работа выполнена при финансовой поддержке РФФИ, проект № 11-01-00792а.

СПИСОК ЛИТЕРАТУРЫ

1. Фролов, А.Б. Повышение устойчивости неинтерактивных аналогов Σ-протоколов с бинарными запросами/ А.Б. Фролов// Ползуновский вестник, 2013, № 2.. — С. 247 -252 .
2. Введение к криптографию.\Под ред. В.В.Ященко. Санкт-Петербург: МЦНМО.2001.
3. Коблиц, Н. Курс теории чисел и криптография/ Н. Коблиц − М. : ТВП, 2001 − 260 с.
4. Фролов, А.Б. Эффективные протоколы передачи комбинации сообщений с забыванием/А.Б. Фролов // Ползуновский вестник. 2012.№ 2/1.. 2012 — С. 129-133.
5. Frolov, A. Effective Oblivious Transfer Using Probabilistic Encryption/ A. Frolov// In AISC-170. Complex Systems and Dependability. Springer Verlag, 2012 — P. 131-147.
6. Венбо, Мао. Современная криптография. Теория и практика. / Мао Венбо.- М.: − Триумф. 2005. – 768 с.

Профессор кафедры математического моделирования Национального исследовательского университета «МЭИ» д.т.н., проф. ***Фролов А.Б.*** *– abfrolov@mail.ru*