5. Kumamoto H., Henley E. Probabilistic risk assessment and management for engineers and scientists/ H.Kumamoto,E. Henley//2-nd edition. Institute of Electrical and Electronics Engineers. Inc. New York, 1996.
6. Chi-Chun Lo, Wan-Jia Chen. A hyd information security risk assessment procedure considering interdependences between controls // Expert Systems with Applications. 2011. V. 39. P. 248-257.
7. Заркумова-Райхель, Р.Н. Прогнозирование количества инцидентов в системе информационной безопасности предприятия при помощи динамической модели /Р. Н. Заркумова-Райхель, А.Ж. Абденов// Фундаментальные исследова-ния, No.6 (2). 2012.С. 429-434.
8. Абденова, Г.А. Прогнозирование значений уровня временного ряда на основе уравнений фильтра Калмана/Г.А. Абденова. // Ползуновский вестник. Барнаул: АлтГТУ, 2010. № 2. С. 4–6.

Профессор кафедры защита информации, ***Абденов А.Ж,.*** *д.т.н., профессор, тел. 8-923-151-77-21 amirlan21@gmail.ru; соискатель кафедры защита информации* ***Заркумова-Райхель Р.Н.*** *zarkumova@gmail.com - Новосибирский государственный технический университет.*

УДК: 519.24

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ НЕИНТЕРАКТИВНЫХ АНАЛОГОВ Σ-ПРОТОКОЛОВ С БИНАРНЫМИ ЗАПРОСАМИ

А.Б. Фролов

В статье рассматриваются неинтерактивные аналоги протоколов идентификации (Σ-протоколов) с бинарными запросами. Показано, что для повышения их устойчивости число проверок может быть увеличено при сохранении информационной скорости за счет применения эффективной забывающей передачи при многократном использовании единого рандомизатора.

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

Введение

Интерактивные и неинтерактивные протоколы с нулевым разглашением секрета являются весьма важными криптографическими примитивами современных криптосистем таких как электронные платежные системы, электронные системы голосования, сохраняющие приватность интеллектуальные измерительные системы и др. [1]. Они обеспечивают идентификацию участников протокола. Протокол доказательства с нулевым разглашением $(P,V)(x)$ исполняется двумя участниками — доказывающим P и проверяющим V, владеющими общей информацией x [2]. Эта общая информация может быть значением $z=f(s)$ односторонней функции $f(s)$, прообраз s которого является секретом P. Исполняя протокол, P убеждает проверяющего V, что он владеет секретом s, не разглашая никакой информации о секрете. 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 $\widetilde{P}$, не владеющим секретом, — граница неустойчивости). Понижение этого порога означает повышение устойчивости протокола. В этой статье мы рассматриваем протоколы, для которых $\sigma=1$, $\delta\leq 1/2$. Третьей характеристикой является *совершенство* — полное скрытие секрета в процессе исполнения протокола. Информационная скорость зависит от длины транзакции, пересылаемой от P проверяющему, она тем больше, чем короче транзакция.

Имеются два типа протоколов с нулевым разглашением секрета: интерактивные и неинтерактивные. Интерактивный протокол (т.н. Σ-протокол) обычно исполняется в три раунда [3]:

1) Сообщение *commit*, являющееся значением *c* односторонней функции, соответствующим текущему случайно выбранному секретному значению *committal*, пересылается доказывающим P проверяющему V.

2) Сообщение *challenger*, являющееся случайно выбранной бинарной строкой e длины t, $t\geq 1$, пересылается от V к P.

3) Сообщение *r response*, зависящее от *committal*, *challenger* и от секрета s пересылается от P к V. (s скрывается случайным сообщением *committal*).

После этих обменов V проверяет ответ *response* по значению предиката *Verify*(c,e,r,z). Если это значение *true*, то принимает доказательство, иначе отклоняет. При t=1 мы называем такие протоколы Σ-протоколами с бинарными запросами, при t>1 — Σ-протоколами с множественными запросами. В настоящей статье мы рассматриваем неинтерактивные аналоги Σ-протоколов с бинарными запросами, неинтерактивным аналогам Σ-протоколов с множественными запросами посвящена статья [4].

Такие протоколы с вероятностной характеристикой неустойчивости δ могут исполняться p раз. Если каждый раз результат проверки — *true*, то V принимает доказательство с вероятностью ошибки не более δ^p, иначе доказательство отклоняется.

Интерактивность является нежелательным свойством таких протоколов, поскольку требуются непосредственный контакт участников и соответствующие затраты времени на коммуникации.

В отличие от интерактивных протоколов, неинтерактивные протоколы используют предварительно подготавливаемую информацию и исполняются без запросов проверяющего. Такими являются протоколы с общей случайной строкой [5].

Имеются два подхода к трансформации интерактивных протоколов в неинтерактивные протоколы:

- трансформация с использованием эвристики Фиата — Шамира [6];
- трансформация с использованием забывающей (скрытой) передачи [7].

В настоящей работе изучаются трансформации последнего типа. В таких протоколах неинтерактивной коммуникационной фазе предшествует интерактивная фаза инициализации параметров забывающей передачи. Использование забывающей передачи требует ограничения вычислительных возможностей доказывающего. В связи с этим неинтерактивный 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 языков или односторонних функций.

Будем использовать следующие обозначения:

- NIOT_2^1 - неинтерактивная 1-из-2 забывающая передача (Oblivious Transfer – OT) [8];

- NIZKOT_2^1 - неинтерактивная аргументация с нулевым разглашением с использованием NIOT_2^1;

- NIEOT_2^1 - эффективная неинтерактивная 1-из-2 забывающая передача [8,9];

- $\mathrm{NIZKEOT}_2^1$ - неинтерактивная аргументация с использованием NIEOT_2^1;

- $e_{\mathrm{NIZKOT}_2^1}$ ($e_{\mathrm{NIZKEOT}_2^1}$) - длина транзакции NIZKOT_2^1 ($\mathrm{NIZKEOT}_2^1$);

- $\rho_{\mathrm{NIZKEOT}_2^1} = \dfrac{e_{\mathrm{NIZKOT}_2^1}}{e_{\mathrm{NIZKEOT}_2^1}}$ - коэффициент возрастания информационной скорости протокола $\mathrm{NIZKEOT}_2^1$ относительно протокола NIZKOT_2^1 при одинаковой устойчивости (эффективность).

Вероятностные характеристики неустойчивости таких протоколов обозначаются $\delta_{\mathrm{NIZKOT}_2^1}$ и $\delta_{\mathrm{NIZKEOT}_2^1}$ соответственно.

$\mathrm{NIZKEOT}_2^1(p)$ обозначает p итераций протокола $\mathrm{NIZKEOT}_2^1$.

В этой статье мы сравниваем границы неустойчивости протоколов, исполняемых за одно и то же время, то есть имеющих примерно одинаковые информационные скорости и сравниваем информационные скорости протоколов, имеющих примерно одинаковые границы неустойчивости. Обсуждаются традиционные протоколы $\mathrm{NIZKOT}_2^1(p)$ и их усовершенствованные варианты $\mathrm{NIZKEOT}_2^1(p)$. Доказывается безопасность повторного использования рандомизаторов, позволяющего существенно понизить границы неустойчивости при сохранении информационной скорости. Последнее демонстрируется сравнением границ неустойчивости и оценкой эффективности.

Сравнение NIZKOT $\frac{1}{2}$ и NIZKEOT $\frac{1}{2}$

В этом разделе мы представляем протоколы NIZKOT$_2^1$, соответствующие интерактивным протоколам доказательства или аргументации с бинарными запросами. В таких протоколах общая информация доказывающего P и проверяющего V является значением $z=f(s)$ односторонней функции $f(x)$. P владеет прообразом s значения z. Исполняя неинтерактивный протокол с нулевым разглашением, честный *P* убеждает *V* в том, что он владеет упомянутым элементом *s*. Нечестный доказывающий $\widetilde{P}$, не владеющий этой информацией, способен убедить проверяющего в противном с вероятностью не более 2^{-1} (или не более 2^{-p} в *p* последовательных итерациях).

По идее Н. Коблица [7] предполагается, что *P* в фазе инициализации получил длинную последовательность открытых ключей проверяющего (β_{1i},β_{2i}), i=1,…,*p* для *p* итераций 1-из-2 забывающей передачи. Эта последовательность может использоваться *P* во многих аргументациях с нулевым разглашением. *P*, имитируя логику интерактивного протокола с бинарным запросом, посылает проверяющему в каждой из *p* итераций в неинтерактивном режиме вызов (*commit*) *c* и затем посылает с забыванием два ответа (*responses*) (r_0, r_1) на оба возможные бинарные запросы (challengers) 0 и 1 соответственно. Проверяющий *V* читает по своему выбору один из них. Доказывающий *P* выбор проверяющего *V* не знает. Затем *V* вычисляет значение предиката точно так же, как в интерактивном протоколе. Граница неустойчивости протокола равна 2^{-p}. В результате эффект интерактивного протокола достигается в неинтерактивном режиме. Для реализации этой идеи используется вероятностное шифрование, например, по криптосистеме Эль Гамаля. В [6] предложено применять аддитивное маскирование вместо мультипликативного: второе сообщение $C_2=m\beta^y$ криптограммы Эль Гамаля, где *m* есть скрываемое сообщение, β есть открытый ключ криптосистемы Эль Гамаля, а *y* — рандомизатор, заменяется сообщением $C_2=m\oplus\psi(\beta^y)$. Здесь ψ: $G\to\{0,1\}^n$ есть обратимое отображение (*G* это базовая группа криптосистемы Эль Гамаля). С использованием генератора α и секретного ключа *x* расшифрование выполняется как $C_2\oplus\psi(\alpha^{xy})=C_2\oplus\psi(\beta^y)=m$. В [8,9] показано, что вследствие использования различных секретных ключей в двух или более шифрованиях повторное использование рандомизатора безопасно. В этом случае информационная скорость в коммутационной фазе ОТ протокола возрастает. В этой статье идея повторного использования рандомизатора распространяется на последовательно исполняемые сессии неинтерактивного протокола аргументации с нулевым разглашением. В результате существенно понижается граница неустойчивости. В данном разделе оценивается степень этого понижения.

Пусть NIZKOT$\frac{1}{2}$ исполняется *p* раз с различными вызовами *commit* и различными ключами вероятностного шифрования. Протокол использует NIOT$\frac{1}{2}$ на основе группы *G* высокого простого порядка с генератором α, элементом *U* с неизвестным ни доказывающему, ни проверяющему дискретным логарифмом. Допустим, что эти параметры установлены в фазе инициализации. Дополнительно в этой фазе *V* выбирает последовательность секретных ключей (i_j,x_j), j=1,…,*t*, где $i_j=e_j+1\in\{1,2\}$ соответствуют бинарным запросам $e_j\in(0,1)$, $x_j\in\{2,\ldots,\ \mathrm{ord}\ \alpha-1\}$ — секретные ключи последовательных сессий, вычисляет и посылает в доверенный сертификационный центр последовательность соответствующих открытых ключей:

$$((\beta_{11},\beta_{21}),\ldots,(\beta_{1j},\beta_{2j}),\ldots,(\beta_{1t},\beta_{2t})),\ \beta_{ij}=\alpha^{x_j},$$

$$\beta_{3-i_j}=U\alpha^{-x_j},\ j=1,\ldots,p. \qquad (1)$$

Доверенный центр публикует их после проверки: для всех *j* должны выполняться равенства $\beta_{1i}\beta_{2i}=U$. *P* получает эту последовательность от доверенного центра.

Теперь можно рассмотреть основную коммуникационную неинтерактивную фазу в двух вариантах: традиционном и ускоренном. Мы желаем получить неинтерактивную версию известного интерактивного протокола, исполнение которого включает вызов *commit* $c_j=f(l_j)$ от случайно выбираемого элемента committal l_j (c_j пересылается от *P* к *V*), случайно выбираемый бинарный запрос *challenger* $e_j\in\{0,1\}$ (от *V* к *P*), ответ *response* $r_j\in\{r_{0j},r_{1j}\}$, $r_{ij}=l_j\circ(s\bullet i)$ (от *P* к *V*) и проверку Verify(c_j,e_j,r_j,z), исполняемую *V*. Выше ∘ есть умножение или сложение, • есть возведение в степень или умножение в зависимости от типа функции *f*.

Начнем с традиционного варианта — протокола NIZKOT$\frac{1}{2}$(*p*).

P случайно выбирает *p* элементов *committal* l_j и вычисляет последовательность *c* из *p* значений *commit* $c_j=f(l_j)$, *j*=1,…,*p*. Затем он вычисляет текущие параметры забывающей передачи — последовательность

$$\mathbf{y}=\Big((y_{11},y_{21}),\ldots,\ (y_{1j},y_{2j}),\ldots,\ (y_{1p},y_{2p})\Big)$$

секретных случайно выбираемых пар различных рандомизаторов. Используя эти рандомизаторы и открытые ключи проверяющего *V*, *P* вычисляет пары возможных ответов (m_{1j}, m_{2j}), $m_{ij} = r_{i-1,j}, i = 1,2, j = 1,...,p$ и последовательность OT транзакций

$$\mathrm{OT}(m_{11}, m_{21}), \ldots, \mathrm{OT}(m_{1j}, m_{2j}), \ldots, \mathrm{OT}(m_{1p}, m_{2p}),$$

где

$$\mathrm{OT}\left(m_{1j}, m_{2j}\right) = ((\alpha^{y_{1j}}, m_{1j} \oplus \psi(\beta_{1j}{}^{y_{1j}})),$$

$$(\alpha^{y_{2j}}, m_{2j} \oplus \psi(\beta_{2j}{}^{y_{2j}}))). \quad (2)$$

Наконец, *P* посылает к *V* последовательность *c* и последовательность (2).

Из троек (c_j, $\left(\alpha^{y_{1j}}, \alpha^{y_{2j}}\right)$, $((m_{1j} \oplus \psi(\beta_{1j}{}^{y_{1j}})), (m_{2j} \oplus \psi(\beta_{2j}{}^{y_{2j}})))$), проверяющий *V*, используя свои секретные ключи, получает множество сообщений, вычисляя m_{i_j} следующим образом:

$$\left(m_{ij} \oplus \psi(\beta_{ij}{}^{y_{ij}})\right) \oplus \psi(\alpha_{ij}{}^{y_{ij} x_j}) = m_{ij} \oplus \psi(\beta_{ij}{}^{y_{ij}}) \oplus \psi(\beta_{ij}{}^{y_{ij}}) =$$

$$= m_{ij} = r_{i-1,j} = r_{e_j} = r_j.$$

Он проверяет эти p сообщений, вычисляя Verify(c_j,e_j,r_j,z), j=1,…p.

Если хотя бы в одном случае получается *false*, он отказывает, иначе принимает аргументацию.

Пример 3.1. Аргументация с нулевым разглашением знания дискретного логарифма элемента $z=b^s$ по снованию *b*. здесь $f(x)=b^x$;

$$c_j = b^{l_j}; r_{0j} = l_j; r_{1j} = l_j + s; \mathrm{Verify}(c_j, e_j, r_j, z): b^{r_j} = c_j z^{e_j}.$$

Пример 3.2. Аргументация с нулевым разглашением секрета знания квадратного корня по модулю составного числа *n*. здесь $f(x)=x^2$ mod *n*.

$$c_j = l_j{}^2; r_{0j} = l_j s^0; r_{1j} = l_j s^1;$$

$$\mathrm{Verify}(c_j, e_j, r_j, z): r_j{}^2 = c_j z^{e_j}.$$

Подчеркнем, что оба примера могут быть реализованы с использованием параметров забывающей передачи, инициализированных однократно.

Ускоренный вариант протокола аргументации с нулевым разглашением секрета NIZKEOT$\frac{1}{2}$(*p*) отличается от протокола NIZKOT$\frac{1}{2}$(*p*) тем, что вместо последовательности ***y*** случайно выбирается единственный рандомизатор *y*. Вместо транзакций (2) вычисляются и пересылаются *V* элемент α^y и транзакции

$$\mathrm{OT}\left(m_{1j}, m_{2j}\right) =$$

$$(m_{1j} \oplus \psi(\beta_{1j}{}^{y}), m_{2j} \oplus \psi(\beta_{2j}{}^{y})), j=1,\ldots,p.$$

Использованием элемента α^y эти транзакции могут быть представлены как последовательность пар криптограмм

$$(\alpha^y, m_{1j} \oplus \psi(\beta_{1j}{}^{y})), (\alpha^y, m_{2j} \oplus \psi(\beta_{2j}{}^{y})),$$

j=1,…,*p*.

В итоге *P* посылает к *V* последовательность *c* и эту последовательность транзакций.

V получает множество сообщений $(m_{i_1},...,m_{i_j},...,m_{i_t})$, используя соответствующие открытые ключи, вычисляя m_{i_j} из троек

(c_j, α^y, $(m_{1j} \oplus \psi(\beta_{1j}{}^{y}), m_{2j} \oplus \psi(\beta_{2j}{}^{y}))$)

следующим образом:

$$(m_{ij} \oplus \psi(\beta_{ij}^{y})) \oplus \psi(\alpha^{yx_j}) = (m_{ij} \oplus \psi(\beta_{ij}^{y})) \oplus \psi(\beta_{ij}^{y}) =$$

$$= m_{ij} = r_{i-1,j} = e_{e_j} = r_j.$$

Сравним границы неустойчивости, протоколов, исполняемых за примерно одно и то же время. В течение *p* исполнений традиционного протокола в коммуникационной фазе передаются 5*p* элементов группы *G*. Для их вычисления доказывающий *P* осуществляет такое же число возведений в степень. В ускоренном протоколе это число уменьшается до 3*p*+1.

Таким образом, протоколы NIZKOT$\frac{1}{2}$(3) и NIZKEOT$\frac{1}{2}$ (5) исполняются примерно за одно и то же время (с одинаковой информационной скоростью), обеспечивая границы неустойчивости

$$\delta_{\mathrm{NIZKOT}\frac{1}{2}(3)} = \left(\delta_{NIZKOT\frac{1}{2}}\right)^3 \text{ и}$$

$$\delta_{\mathrm{NIZKEOT}\frac{1}{2}(5)} = \left(\delta_{\mathrm{NIZKEOT}\frac{1}{2}}\right)^5.$$

Принимая во внимание, что $\delta_{\mathrm{NIZKOT}\frac{1}{2}} = \delta_{\mathrm{NIZKEOT}\frac{1}{2}} = \frac{1}{2}$, можно видеть, что

$$\left(\delta_{\mathrm{NIZKOT}\frac{1}{2}(3p)}\right)^5 = \left(\delta_{\mathrm{NIZKOT}\frac{1}{2}}\right)^{15p} \approx \left(\delta_{\mathrm{NIZKEOT}\frac{1}{2}(5p)}\right)^3 = \left(\delta_{\mathrm{NIZKEOT}\frac{1}{2}}\right)^{15p}$$

Отсюда

$$\delta_{\mathrm{NIZKEOT}\frac{1}{2}(5p)} \approx \left(\delta_{\mathrm{NIZKOT}\frac{1}{2}(3p)}\right)^{\frac{5}{3}}. \quad (3)$$

Таким образом, при одной и той же информационной скорости применение

NIZKEOT вместо NIZKOT влечет существенное снижение неустойчивости.

С другой стороны, $e_{\mathrm{NIZKEOT}_2^1(5p)} \approx 45p$ и $e_{\mathrm{NIZKOT}_2^1(15p)} \approx 75p$ и при тех же границах неустойчивости применение NIZKEOT$^1_2$ вместо NIZKOT$^1_2$ влечет существенное повышение информационной скорости:

$$\rho_{\mathrm{NIZKEOT}_2^1(5p)} \approx \frac{5}{3}. \qquad (4)$$

В заключение напомним доказательство безопасности повторного использования рандомизатора в протоколе NIEOT$^1_2$ [9,10], применяемом в NIZKEOT$^1_2$, учитывая аддитивный способ скрытия.

Утверждение 1. *Проблема извлечения второго сообщения при повторном использовании рандомизатора в транзакциях протокола* NIEOT *и проблема Диффи — Хеллмана полиномиально эквивалентны.*

Доказательство. Допустим, что по тройке (c_j, α^y, ($m_{1j} \oplus \psi(\beta_{1j}{}^y)$, $m_{2j} \oplus \psi(\beta_{2j}{}^y)$))=(c_j, α^y, (C_{1j}, C_{2j})) с использованием секретного ключа (ij, βij) проверяющего вычислено сообщение $m_{i_j} = C_1 \oplus \psi(\beta_{i_j}^y)$. Для вычисления второго сообщения надо найти $\beta_{3-i_j}^y$ то есть необходимо решить проблему Диффи — Хеллмана: при известных значениях α, α^y, $\beta_{3-i_j} = \alpha^{x'}$ найти $\beta_{3-i_j}^y = \alpha^{yx'}$. Знание $\beta_{i_j}^y$, позволяющее вычислить значение m_{i_j} бесполезно для вычисления значения $\beta_{3-i_j}^y$, требуемого для вычисления второго сообщения m_{3-i_j}:

$$\beta_{3-i_j}^y = U^y (\beta_{i_j}^y)^{-1}, \qquad (6)$$

так как проверяющий для этого должен знать секретный текущий ключ *y* доказывающего, известный только ему. Допустим, что при известных значениях α и α^y с использованием эффективного алгоритма вычислено сообщение $\beta_{3-i_j} = \psi^{-1}(C_2 \oplus m_{3-i_j})$. Положим $U = \alpha^z$. Тогда из уравнения (6) вычислим $U^y = (\beta_{i_j}^y)(\beta_{3-i_j}^y)^{-1}$. Значит, если мы можем вычислить m_{3-i_j}, мы можем решить проблему Диффи — Хеллмана: используя известные значения $\alpha, \alpha^z, \alpha^y$ вычислить α^{zy}. Таким образом, доказано

Следствие 1. *Повторное использование рандомизатора в пределах одной итерации протокола NIZKEOT*$^1_2$ *безопасно*.

Повторное использование рандомизатора *y* в различных *p* итерациях протокола NIZKEOT$^1_2$(p) тем более безопасно, поскольку ключи, используемые в различных итерациях, не связаны между собой алгебраически.

Следствие 2. *Протокол NIZKEOT*$^1_2$ *является секретным в стандартной модели*.

Следствие 3. *Повторное использование рандомизатора y во всех итерациях протокола NIZKEOT* $^1_2$ *(p) безопасно*.

Следствие 4. *Аппроксимации и оценки* (3,4) *справедливы*.

Результаты данной работы и работы [4] отражены также в работе [11].

Заключение

Представлены новые эффективные неинтерактивные протоколы идентификации, являющиеся аналогами интерактивных протоколов с бинарными запросами, оценена их эффективность и доказана безопасность.

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

СПИСОК ЛИТЕРАТУРЫ

1. Введение к криптографию./ Под ред. В.В.Ященко. Санкт-Петербург: МЦНМО.2001. 260 с.
2. Венбо Мао. Современная криптография. Теория и практика. М.:Триумф. 2005. — 768 с.
3. Goldwasser S., Micali S., and Rakoff C. Knowledge Complexity of Interactive Proof Systeams/ Advances in Computing Research: Vol.5 (Randomness and computation, S. Micali ed.), 1986 – P.73-90.
4. Фролов А.Б. Повышение устойчивости неинтерактивных аналогов Σ-протоколов с множественными запросами./ А.Б. Фролов // Ползуновский вестник, 2013. № 2. – С. 252-256.
5. Blum M., Feldman P., and Micali S. Non-interactive zero-knowledge and its applications (extended abstract). In 20th Annual ACM STOC, 1988 – P. 103–112.
6. Fiat A., Shamir A. How to prove yourself: practical solutions of identification and signature problems. In A.M. Odlyzko, editor, Advances in Cryptology – Proceedings of CRYPTO'86, LNCS 263, Springer Verlag, 1986 – P. 186-194.

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-