УДК 519.6

А. В. Александров

УСТОЙЧИВОСТЬ SMT-ПРОТОКОЛА К АТАКАМ ПРОТИВНИКА В МОДЕЛИ БЕЗОПАСНОСТИ ДОЛЕВА—ЯО

Устанавливаются свойства конфиденциальности SMT-протокола (Secure Message Transmission Protocols) с общей памятью. Конфиденциальность понимается как устойчивость протокола передачи к атакам активного или пассивного противника в обобщенном канале связи, подчиненного модели безопасности Долева—Яо.

Ключевые слова: *криптографические протоколы передачи, схема разделения секрета, модель безопасности Долева—Яо.*

Введение. Практическая стойкость, которая лежит в основе современных криптосистем и криптографических протоколов, обеспечивает противодействие взлому закрытого текста или протокола передачи данных на время, большее времени сохранения конфиденциальности и жизни самого передаваемого документа. Возрастание вычислительной мощности компьютеров, появление новых видов криптографических атак на ключи шифрования и криптографические протоколы [1, 2] могут резко снизить порог практической стойкости современных криптографических средств. При создании практически стойких криптографических схем используется теория сложности алгоритмов и, в частности, так называемые односторонние функции. Доказательство существования односторонних функций опирается на не доказанную гипотезу о несовпадении классов алгоритмически P-сложных и NP-сложных задач: $P \neq NP$.

В криптографии востребован конфиденциальный обмен, обладающий параметрами стойкости и надежности в абсолютном или почти абсолютном смысле. В работе К. Шеннона [3] решен вопрос о существовании абсолютно стойкого шифра, обеспечивающего противодействие пассивному противнику. Современные исследования по абсолютно или почти абсолютно секретной и надежной связи развиваются в рамках так называемых SMT-протоколов (Secure Message Transmissions Protocols) и обобщают результаты К. Шеннона по нескольким важным направлениям. На основе этого возникла современная модель безопасности Долева—Яо [4], в соответствии с которой возможность противостоять противнику в канале связи переносится на сетевой граф. Кроме того, противник помимо прослушивания трафика может производить быструю подмену сообщений в определенных ветвях графа. Последнее, в частности означает, что воздействие противника приравнивается к воздействию некоторого шума в обобщенном канале связи.

(n,n)-пороговые и (k,n)-пороговые схемы разделения секретного сообщения. Основным инструментом в SMT-протоколах выступают пороговые схемы разделения секретного сообщения (секрета), работающие в конечных полях. Схема предложенная А. Шамиром, представляет собой классическую (n,n)-пороговую схему разделения секрета, позволяющую вычислять доли секрета S для любых значений n. Схема разделения секрета Шамира использует многочлены степени n–1 над полем Галуа GF_p:

$$p_{n-1}(x) = a_n x^{n-1} + \ldots + a_1 x + S \,,\; a_{n-1}, \ldots, a_1 \in \text{rand}\, GF_p \,. \qquad (1)$$

Долей секрета $Share_i(S)$ является упорядоченная пара:

$$Share_i(S) = (i, p_{n-1}(i)),\; i \neq 0 \,.$$

Теорема о полиномиальной интерполяции для многочленов (1) над полем GF_p сохраняет свою силу, поэтому при наличии не менее n совокупностей попарно различных долей секрет S восстанавливается по интерполяционной формуле Лагранжа:

$$p_{n-1}(x) = \prod_{i=1, j\neq i}^{n-1} \frac{x - x_i}{x_j - x_i},\ p_{n-1}(0) = S.$$

Можно показать, что при количестве долей секрета мощностью менее n значение S не только неопределенно, но и с равной вероятностью распределено по всему полю, так что любой элемент поля может приобрести значение S. Аналогичным образом, на основе многочленов над полем строятся (k,n)-пороговые схемы разделения секрета $k>n$. В работе [5] отмечено, что (k,n)-пороговые схемы разделения для $k=3n+1$ эквивалентны кодам Рида—Соломона, исправляющим ошибки в канале связи.

SMT-протоколы. Современные работы по SMT-протоколам обширны (см. обзоры [3, 4]). Свойства конфиденциальности SMT-протоколов с нулевой общей памятью и некоторыми дополнительными условиями на пути в канале связи, а также их криптоанализ приведены в [4].

В настоящей статье рассматривается протокол конфиденциального обмена с общей памятью между абонентами A и B. Абоненты расположены в вершинах ориентированного графа и связаны между собой, по крайней мере, $n>1$ непересекающимися путями. Такие графы называются графами высокого порядка связности. Степень активности противника в рамках модели Долева—Яо предполагается такой, что он может контролировать почти все каналы связи в режиме прослушивания и некоторую часть каналов — в режиме перехвата и быстрой замены проходящего трафика. Эти случаи различаем терминами „пассивный противник“ и „активный противник“ соответственно.

Основные определения. Пусть $G(V, R)$ — ориентированный граф, с множеством вершин V, включающим в себя элементы $\{A, B\}$ и ребра $R = \{\Gamma_1, ..., \Gamma_n, q\}$, $n>1$ такие, что:

$\Gamma_1, ..., \Gamma_n$ — ориентированы от A к B,

q — ориентирован от B к A.

Все ребра попарно не пересекаются, за исключением своих концов в A и B, и их ориентация задает в графе направление передачи трафика в сети.

Передаваемый секрет S считаем элементом числового поля GF_p (p — простое, достаточно большое число), S находится в A. Множество пересылки сообщений $D = \{d_1 ...., d_k\}$ назовем историей переписки между A и B. Это множество всех сообщений, которыми обмениваются A и B в рамках действия протокола. Случай пустого множества D не исключается.

Обозначим $\Pi(A,B,D,S)$ — протокол обмена сообщениями между A и B, в результате которого в точке B должно быть получено числовое значение $S \in GF_p$. Во время работы всего протокола Π в графе $G(V, R)$ действует k-активный противник P ($k<n$). Это означает, что P прослушивает, вообще говоря, трафик протокола в графе $G \setminus \{A, B\}$ в k каналах связи. Более точно — противник контролирует в режиме подмены сообщений не более k каналов, и это множество противник не может изменять на протяжении выполнения всего протокола.

Определение 1. Пусть $0 \le \delta < \frac{1}{2}$. Назовем протокол Π δ-надежным, если в точке B в результате выполнения протокола с вероятностью не менее $1 - \delta \left(0 \le \delta < \frac{1}{2} \right)$ появляется сообщение $S^B = S^A$.

Определение 2. Протокол П называется абсолютно надежным, если $\delta = 0$.

Следуя работе [5], введем вероятностную функцию adv, отражающую активность соперника. Более точно — функция adv(S,r) отражает количество наблюдений r противника P за выполнением протокола, необходимых для получения S=S^A вне точки B с вероятностью c.

Определение 3 (см. [5]). Пусть $0 \le \varepsilon < 1$. Назовем протокол П ε-секретным, если для любых двух сообщений S_0, S_1 и для любого r:

$$\sum_c \left| \left[\text{adv}(S_0, r) = c\right] - \left[\text{adv}(S_1, r) = c\right] \right| \le 2\varepsilon .$$

Определение 4. Протокол П назовем абсолютно секретным, если он 0-секретен в смысле определения 3.

Определение 5. Назовем протокол $\Pi(\delta, \varepsilon)$-безопасным, если он δ-надежен и ε-секретен. Протокол П(0,0) называем совершенным.

В протоколе П(A,B,S,D,P) выделим три этапа. Первый предназначен для создания проверяемого и согласованного непустого множества D в точках A и B, а также определения тех элементов сети, которые контролируются противником P. Основным инструментом первого элемента для создания D является проверяемая схема разделения секрета Шамира [6].

В результате выполнения второго этапа на основе множества D в точке A решается задача „укладка рюкзака“ с некоторым модулярным слагаемым в поле GF_p, и необходимый набор битов (обозначим его E) для сборки решения пересылается в точку B.

На завершающем протокол третьем этапе модулярное слагаемое Δ передается в точку B. В силу того что величины Δ и S независимы, справедливо следующие равенство:

$$H(\Delta \mid S) = H(S), \qquad (2)$$

где $H(x \mid y)$ — условная энтропия по Шеннону.

Описание SMT-протокола с общей памятью

Этап I. Формирование истории переписки D и передача ее абоненту B.

В начале выполнения протокола у абонентов A и B множество переписки — пустое. Абонент A формирует случайным образом множество $D = \{d_1, ..., d_k\}$, где $d_i \in GF_p$. Для передачи $d_i \in GF_p$, $i = 1, ..., k$, используем проверяемое разделение секрета Шамира [6] порядка $(k+1, n)$ на доли d_{ij}, где $j = 1, ..., n$ — номер провода, по которому отправлена доля d_{ij} из Γ. Абонент B получает доли d_{ij} и при помощи проверяемой интерполяции пытается вычислить $d'_i = d_i$. Провода с номерами j, для которых интерполяция проведена неуспешно, признаются ошибочными или контролируемыми активным противником и в дальнейшей работе протокола не участвуют. Список ошибочных проводов абонент B отправляет по каналу обратной связи q абоненту A. Этот этап соответствует первому этапу SMT(0,0)-протокола, описанному и изученному в работе [6], за тем исключением, что в [6] история переписки D после выполнения этапа I отбрасывается.

Этап II. Выбор абонентом A коэффициентов „рюкзачной схемы“ и передача их абоненту B. Отправитель A выбирает коэффициенты $e_1, ..., e_k$, где $e_i = \{0,1\}$, такие что:

$$\sum_{i=1}^{k} d_i e_i = S + \Delta . \qquad (3).$$

Здесь операция сложения по mod p, Δ — некоторый элемент из GF_p, подчиненный свойству (2). Набор битов $e_1, ..., e_k$ передается абоненту B.

Этап III. Сборка секрета абонентом B. Абонент B получает коэффициенты $e_1,...,e_k$, вычисляет значение $S+\Delta$ и передает его абоненту A по обратному каналу q. После получения сообщения от B абонент A отправляет Δ любым способом по достоверным каналам. Абонент B получает Δ и вычисляет секретное сообщение S. На этом заканчивается выполнение протокола П.

Теорема: Пусть противник P является k-активным ($k<n$), при этом не имеет доступа к обратному каналу связи q. Тогда условие

$$k < 2n+1 \tag{4}$$

необходимо для того, чтобы протокол $\Pi(A,B,D,S,P)$ был (0,0)-безопасным.

Доказательство: Представим действие протокола $\Pi(A,B,D,S,P)$ в виде композиций протоколов $\Pi(A,B,D,S,P)=\Pi_1\circ\Pi_2\circ\Pi_3(A,B,D,S,P)$, где i=1,..,3 соответствует этапу протокола П. Свойство идеальности протокола Π_1 хорошо известно [7]. Отсюда следует, что противник P может восстановить или угадать элементы множества D с вероятностью $1/|GF_p|$, где $|GF_p|$ — мощность числового поля. Если трафик прослушивается $E=\{e_1,...,e_k\}$, то $H(E\mid D)=H(D)$. Последнее равенство доказывает совершенность протокола Π_2. Свойство совершенности протокола Π_3 вытекает из (3), что завершает доказательство теоремы.

Нетрудно показать, что однократное применение схемы разделения секрета Шамира эквивалентно применению n шифров Вернама по каждому из путей $R=\{\Gamma_1,...,\Gamma_n\}$ с попарно различными ключами, определяемыми по значениям многочлена $p_n(x_j)-S$ в схеме разделения секрета. Из этого, с учетом абсолютной стойкости однократного шифрования Вернама [3], следует 0-секретность по Шеннону протокола Π_1, его композиций, а следовательно, и всего протокола $\Pi(A,B,D,S,P)=\Pi_1\circ\Pi_2\circ\Pi_3(A,B,D,S,P)$.

Ограничение на доступ противника P к обратному каналу q в теореме является необходимым. Криптоанализ протокола Π_1 [8] показывает, что в случае активного доступа противника к обратному каналу q успешно проводится криптографическая атака „человек посередине“ (“Man in the middle”). Этот факт, вообще говоря, приводит к понижению стойкости протокола Π_1, а следовательно и $\Pi(A,B,D,S,P)$, до $(0,\varepsilon)$-безопасного, где ε удовлетворяет неравенству $\frac{1}{p}<\varepsilon<\frac{5}{p}$.

СПИСОК ЛИТЕРАТУРЫ

1. *Панасенко С.* Алгоритмы шифрования. СПб: БХВ, 2008. 563 с.
2. *Черемушкин А. В.* Криптографические протоколы: основные свойства и уязвимости. М.: Изд. центр Академия, 2009. 272 с.
3. *Shannon C.* Communication theory of secrecy systems // Bell System Techn. J. 1949. Vol. 28, N 4. P. 656—715.
4. *Dolev D. D., Yao A.* // IEEE Transact. on Inform. Theory. 1983. Vol. IT-29, N 2. P. 198—208.
5. *Franklin M., Wright R.* Secure communication in minimal connectivity models // J. Cryptology. 2000. Vol. 13, N 1. P. 9—30.
6. *Shamir A.* How to share a secret // Communication of ACM. 1979. Vol. 22, N 11. P. 612—613.
7. *Dolev D., Dwork C.* Perfectly Secure Message Transmission // Proc. 31st Annu. Symp. on Found. of Comput. Sci. 1990. P. 36—45.
8. *Yang Q., Desmedt Y.* Cryptanalysis of Secure Message Transmission Protocols with Feedback // ICITS. 2009. P. 159—176.

Сведения об авторе

Алексей Викторович Александров — канд. физ.-мат. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: alex_izi@mail.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.