**ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ**
(12)

РЕСПУБЛИКА БЕЛАРУСЬ

НАЦИОНАЛЬНЫЙ ЦЕНТР ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

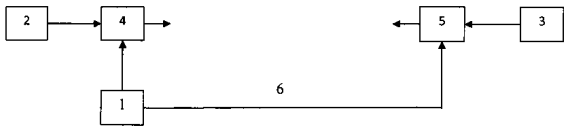
(19) **BY** (11) **17856**
(13) **C1**
(46) **2013.12.30**
(51) МПК
***H 04L 9/08*** (2006.01)

# (54) СПОСОБ РАСПРЕДЕЛЕНИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА МЕЖДУ АБОНЕНТАМИ

(21) Номер заявки: a 20111018
(22) 2011.07.19
(43) 2013.02.28
(71) Заявитель: Белорусский национальный технический университет (BY)
(72) Автор: Голиков Владимир Федорович (BY)
(73) Патентообладатель: Белорусский национальный технический университет (BY)
(56) БРАССАР Ж. Современная криптология. - М.: Полимед, 1999. - С. 132-137.
BY 14139 C1, 2011.
RU 2171012 C1, 2001.
CN 101227270 A, 2008.
ГОЛИКОВ В.Ф. и др. Материалы XIV международной конференции. - Минск, 2009. - С. 77-79.

(57)

Способ распределения криптографического ключа между абонентами, при котором формируют бинарные последовательности у двух абонентов A, B с некоторым процентом несовпадения бит, устраняют несовпадения путем обмена информацией о них по открытому каналу связи для получения общего для абонентов ключа в виде итоговой бинарной последовательности и увеличивают ее конфиденциальность, **отличающийся** тем, что бинарные последовательности формируют путем передачи одним из абонентов другому общей для них несекретной бинарной последовательности $X^0$ длиной n по открытому каналу связи, генерирования абонентами A, B независимо друг от друга случайных секретных последовательностей чисел соответственно $S_A$ и $S_B$, причем $S_A = \{s_1^a, s_2^a, ..., s_{r_a}^a\}$, $S_B = \{s_1^b, s_2^b, ..., s_{r_b}^b\}$, где $0 \le r_a \le n$, $0 \le r_b \le n$, соответственно, $s_i^a \in \{1, 2, ..., n\}$, $s_i^b \in \{1, 2, ..., n\}$, причем $s_i^a \ne s_j^a$ для всех $i \ne j$, где $i, j = 1, 2\ldots, r_a$, для $S_A$; $s_i^b \ne s_j^b$ для всех $i \ne j$, где $i, j = 1, 2\ldots, r_b$, для $S_B$, инвертирования абонентами A, B независимо друг от друга некоторых случайно выбранных бит последовательности $X^0$ в соответствии с полученными номерами бит $s_i^a$ и $s_i^b$ в количестве, обеспечивающем допустимый процент несовпадения бит в сформированных абонентами A, B бинарных последовательностях $X^A$ и $X^B$ соответственно, еще позволяющем устранить несовпадения с соблюдением уровня конфиденциальности формируемых бинарных последовательностей, обеспечивающего требуемый уровень конфиденциальности итоговой бинарной последовательности после повышения ее конфиденциальности.




Фиг. 1

BY 17856 C1 2013.12.30

Изобретение относится к области криптографии, а более конкретно к способам распределения общего криптографического ключа между абонентами с использованием открытого канала связи, и может быть использовано для защиты информации в телекоммуникациях.

Известны способы распределения общего криптографического ключа на основе односторонних функций, например алгоритм Диффи-Хеллмана [1]. Недостатками этого способа являются высокая сложность используемого математического аппарата, его программной или технической реализации, а также наличие потенциальных угроз криптостойкости алгоритма по мере развития компьютерных технологий и математических методов решения обратных задач.

Наиболее близким к предлагаемому способу является способ распределения общего криптографического ключа, включающий этапы формирования у абонентов исходных бинарных последовательностей с некоторым процентом несовпадений, устранения несовпадений путем обмена информацией о них по открытому каналу связи, увеличения конфиденциальности сформированного общего ключа [2].

Существенными недостатками указанного способа являются сложность и высокая стоимость оборудования для организации квантового канала, используемого для формирования у абонентов исходных бинарных последовательностей с некоторым процентом несовпадений, ограниченная дальность передачи оптических сигналов, а также возможность его использования только в условиях отсутствия прослушивания квантового канала.

Задача, решаемая изобретением, заключается в устранении перечисленных недостатков.

Решение поставленной задачи достигается тем, что в способе распределения криптографического ключа между абонентами, при котором формируют бинарные последовательности у двух абонентов A, B с некоторым процентом несовпадения бит, устраняют несовпадения путем обмена информацией о них по открытому каналу связи для получения общего для абонентов ключа в виде итоговой бинарной последовательности и увеличивают ее конфиденциальность, бинарные последовательности формируют путем передачи одним из абонентов другому общей для них несекретной бинарной последовательности $X^0$ длиной n по открытому каналу связи, генерирования абонентами A, B независимо друг от друга случайных секретных последовательностей чисел соответственно $S_A$ и $S_B$, причем $S_A = \{s_1^a, s_2^a, ..., s_{r_a}^a\}$, $S_B = \{s_1^b, s_2^b, ..., s_{r_b}^b\}$, где $0 \le r_a \le n$, $0 \le r_b \le n$, соответственно, $s_i^a \in \{1, 2, ..., n\}$, $s_i^b \in \{1, 2, ..., n\}$, причем $s_i^a \neq s_j^a$ для всех $i \neq j$, где $i, j = 1, 2\ldots, r_a$, для $S_A$; $s_i^b \neq s_j^b$ для всех $i \neq j$, где $i, j = 1, 2\ldots, r_b$, для $S_B$, инвертирования абонентами A, B независимо друг от друга некоторых случайно выбранных бит последовательности $X^0$ в соответствии с полученными номерами бит $s_i^a$ и $s_i^b$ в количестве, обеспечивающем допустимый процент несовпадения бит в сформированных абонентами A, B бинарных последовательностях $X^A$ и $X^B$ соответственно, еще позволяющем устранить несовпадения с соблюдением уровня конфиденциальности формируемых бинарных последовательностей, обеспечивающего требуемый уровень конфиденциальности итоговой бинарной последовательности после повышения ее конфиденциальности.

Сущность изобретения поясняется фигурами, где на фиг. 1 - блок-схема формирования исходных бинарных последовательностей у абонентов A и B; на фиг. 2 - диаграмма, поясняющая расчетные соотношения; на фиг. 3 - график закона распределения вероятностей числа несовпадающих битов.

Блок-схема для осуществления способа формирования исходных бинарных последовательностей содержит генератор 1 общей несекретной последовательности битов $X^0$, генератор 2 случайной последовательности чисел $S_A$ абонента A, генератор 3 случайной последовательности чисел $S_B$ абонента B, инвертор 4 абонента A, инвертор 5 абонента B, открытый канал 6 связи.

Формирование исходных конфиденциальных индивидуальных последовательностей битов у обоих абонентов происходит следующим образом. Абонент А с помощью генератора 1 генерирует бинарную последовательность $X^0$ длиной n, подает ее на инвертор 4 и одновременно посылает ее по 6 абоненту В на инвертор 5. Затем абоненты А и В с помощью генераторов 2, 3 независимо друг от друга генерируют случайные секретные последовательности чисел соответственно $S_A$ и $S_B$, при этом $S_A = \{s_1^a, s_2^a, ..., s_{r_a}^a\}$, $S_B = \{s_1^b, s_2^b, ..., s_{r_b}^b\}$, где $0 \le r_a \le n$, $0 \le r_b \le n$, $s_i^a \in \{1, 2, ..., n\}$, $s_i^b \in \{1, 2, ..., n\}$, причем $s_i^a \ne s_j^a$ для всех $i \ne j$, где i, j=1, 2…, $r_a$, для $S_A$; $s_i^b \ne s_j^b$ для всех $i \ne j$, i, j=1, 2…, $r_b$, для $S_B$. Далее абоненты А и В инвертируют биты $X^0$ помощью инверторов 4, 5 в соответствии с полученными номерами бит $s_i^a$ и $s_i^b$ и получают последовательности $X^A$ и $X^B$, обладающие следующими свойствами:

в последовательностях $X^A$ и $X^B$ имеются совпадающие и несовпадающие биты в количестве $n_c$ и $n_н$, очевидно, что $n = n_c + n_н$;

наличие совпадающих бит обусловлено для части бит взаимным инвертированием, таких бит $n_{ис}$, для части - взаимным неинвертированием, таких бит $n_{нис}$, очевидно, что $n_c = n_{ис} + n_{нис}$;

наличие несовпадающих бит обусловлено для части бит инвертированием в $X^A$ и неинвертированием $X^B$ и наоборот.

На фиг. 2 изображена диаграмма, поясняющая следующие расчетные соотношения: общее число совпадающих бит равно $n_c = n–(r_a+r_b) + 2n_{ис}$, число несовпадающих бит равно $n_н = (r_a + r_b)–2n_{ис}$. Число $n_н$ является случайной величиной с законом распределения вероятностей, зависящим от $r_a$, $r_b$ (фиг. 3). Выбор $r_a$, $r_b$ влияет на процент несовпадающих бит и конфиденциальность формируемых последовательностей, причем, чем меньше процент несовпадающих бит, тем меньше и конфиденциальность формируемых последовательностей. Под конфиденциальностью бинарной последовательности понимается степень ее неопределенности для лица, прослушивающего открытый канал связи. Действительно, для того чтобы конфиденциальность каждой последовательности $X^A$ и $X^B$ была максимальной и равнялась бы конфиденциальности последовательности, сгенерированной секретным образом, необходимо, чтобы выполнялось $r_a = r_b = n/2$. В этом случае каждый бит в $X^A$ и $X^B$ с вероятностью 1/2 либо равен биту $X^0$, либо противоположен ему, что соответствует максимальной его неопределенности. При этом $n_c = 2n_{ис}$, $n_н = n–2n_{ис}$. Можно показать, что при $r_a = r_b = n/2$ математическое ожидание величины $n_{ис}$ равно n/4. Тогда математические ожидания величин $n_c$ и $n_н$ равны n/2, что означает, что в среднем процент несовпадающих бит равен 50. Известно, что при таком проценте ошибок не существует методов их устранения [3]. Для уменьшения процента несовпадающих бит выберем $r_a = r_b = \frac{n}{2} - \delta$, где $\delta$ - положительное число, причем $0 \le \delta \le n/2$. Тогда доля несовпадающих бит равна

$$\frac{n_н}{n} = \frac{(r_a + r_b) - 2n_{ис}}{n} = \frac{n - 2\delta - 2n_{ис}}{n}.$$

Моделирование показало, что при $n > 100$ для получения процента несовпадающих бит в пределах 44-47 % необходимо выбрать $\delta$ в пределах 7-9 %.

Оценим уровень конфиденциальности $X^A$ и $X^B$ при таком выборе $r_a$, $r_b$. Для этого найдем долю $n_{нс}$ и $n_{ис}$ в этих последовательностях, учитывая только совпадающие биты, т.к. несовпадающие биты будут удалены в дальнейшем:

$$\frac{n_{ис}}{n_c} = \frac{n_{ис}}{2\delta + 2n_{ис}} = 0{,}5\frac{n_{ис}}{\delta + n_{ис}} \le 0{,}5; \quad \frac{n_{нис}}{n_c} = \frac{2\delta + n_{ис}}{2\delta + 2n_{ис}} = 0{,}5\frac{2\delta + n_{ис}}{\delta + n_{ис}} \ge 0{,}5.$$

Моделирование показывает, что при $\frac{\delta}{n} = 0{,}08$ получаем $\frac{n_{ис}}{n_с} \approx 0{,}35$; $\frac{n_{нис}}{n_с} \approx 0{,}65$. Следовательно, вероятность попадания в итоговую последовательность инвертированных в исходной последовательности бит оказывается меньше, чем неинвертированных, что снижает ее конфиденциальность. Конфиденциальность была бы максимально возможной, если бы в итоговой последовательности каждый бит с вероятностью 1/2 равнялся биту $X^0$ или противоположному биту. Однако эффект снижения конфиденциальности компенсируется на этапе усиления секретности [3].

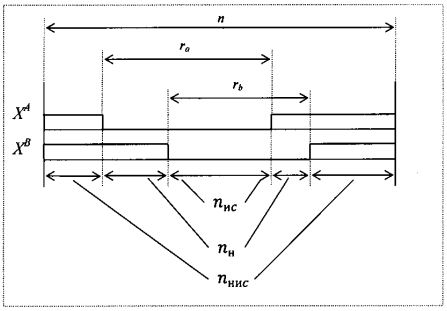
После реализации всех процедур длина итоговой последовательности оказывается существенно короче длины $X^0$, но легко наращивается до необходимой путем увеличения $X^0$.

Источники информации:

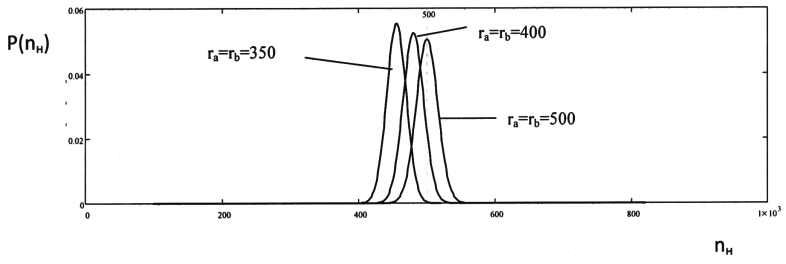
1. Diffie W. and Hellman M. Newdirections in cryptography. IEEE Trans. Inf. Theory. - 1976. -V. 22. -No. 11. - P. 644-654.

2. Брассар Ж. Современная криптология.- М.: Полимед, 1999. - С. 132-137.

3. Физика квантовой информации / Под ред. Д. Боумейстера, А. Экерта, А. Цайлингера.- М.: Постмаркет, 2002. - С. 60-61.




Фиг. 2




Фиг. 3

Национальный центр интеллектуальной собственности.
220034, г. Минск, ул. Козлова, 20.