УДК 519.872 DOI:10.31854/1813-324X-2021-7-4-119-127

Безопасная передача информации при помощи двух методов бесключевой криптографии

А.С. Герасимович[1]*

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: Alexgera93@gmail.com

Информация о статье
Поступила в редакцию 06.12.2021
Поступила после рецензирования 21.12.2021
Принята к публикации 22.12.2021

Ссылка для цитирования: Герасимович А.С. Безопасная передача информации при помощи двух методов бесключевой криптографии // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 119–127. DOI:10.31854/1813-324X-2021-7-4-119-127

Аннотация: *В статье рассматриваются два протокола обеспечения информационной безопасности, использующие свойства каналов связи между пользователями. Первый из них основан на известном протоколе передачи конфиденциальных сообщений Шамира. Доказывается, что в нем может быть реализована криптосистема РША, но неприменимы такие криптосистемы, как Рабина, Мак-Элис, на решетках и потоковые шифры. Основное содержание статьи посвящено описанию второго протокола распределения ключей по постоянному и бесшумному каналу связи (типа Интернет). Доказано, что он может обеспечить высокую надежность распределения ключей и требуемый уровень их секретности в терминах Шенноновской информации, причем при отсутствии каких-либо дополнительных требований к каналам связи и безо всяких криптографических предположений.*

Ключевые слова: *криптосистемы с открытым ключом, распределение ключей, безопасность на физическом уровне, усиление секретности, квантовые компьютеры, протоколы.*

1. Введение

Общеизвестно, что основным методом обеспечения информационной безопасности является стойкое шифрование сообщений. Это тем более верно сейчас, поскольку появились открытые стандарты шифрования [1, 2]: 3DES, AES, GOST, RSA и другие, которые, насколько можно судить по доступным литературным источникам, обеспечивают невозможность выделения зашифрованной информации без знания ключей дешифрования и в обозримом будущем. Однако, именно такие ключи, а также их распределение между пользователями, нуждаются в обмене конфиденциальной информацией, и оказываются «узким местом» современной криптографии.

Действительно, в современном «Цифровом Мире» такие ключи должны передаваться каким-то цифровым способом между пользователями по каналам связи, что требует их защиты от перехвата злоумышленниками. Казалось бы, такая проблема была уже решена ранее благодаря изобретению У. Диффи и М. Хеллмана [2], так называемых криптосистем с открытым ключом (КОК). Хотя более точно их можно было бы назвать криптосистемами с открытыми ключами шифрования. В случае КОК, шифрование сообщений производится на общедоступных ключах, тогда как дешифрование выполняется на закрытых ключах; и их имеют только пользователи, которым принадлежит передаваемая конфиденциальная информация. Причем знание открытых ключей не облегчает нахождение закрытых ключей. Подобные условия обеспечиваются сложностью решения (в обозримое время) так называемых трудных математических задач. Например, таких, как факторизация целых чисел, вычисление дискретных логарифмов и так далее. Это условие называют обычно «криптографическими предположениями» (*от англ.* Cryptographic Assumptions).

Хотя изобретение КОК и явилось в свое время подлинной революцией в криптографии, но со временем выяснились его некоторые слабости, такие как:

– возможность простого полиномиального решения трудных задач при помощи квантовых компьютеров, которые в будущем времени возможно будут реализованы [3];

– необходимость иметь сертифицированный центр для накопления и передачи открытых ключей пользователям;

– достаточная сложность теоретико-числовых вычислений для выполнения процедур шифрования или дешифрования в системах КОК.

Для решения первой проблемы были предложены так называемые постквантовые криптосистемы, то есть такие, которые не могут быть взломаны даже при практическом появлении квантовых компьютеров. Такова, например, криптосистема Мак-Элис [1], которая, однако, требует большой длины ключа и высокой вычислительной сложности шифрования/дешифрования. Еще одним направлением возможного распределения ключей является использование квантовой криптографии [4], однако ее использование не всегда возможно, так как требует наличия специального квантового оборудования.

В последнее время развивается так же такое направление распределения ключей, или точнее обеспечения безопасности шифрования, как Keyless Cryptography, основанное на присутствии некоторых, обладающих определенными физическими свойствами, физических каналов связи (*от англ.* Physical Layer Security) [5]. Именно развитию этого направления и посвящена настоящая статья.

В разделе 2 исследуются алгоритмы, позволяющие обеспечить безопасность шифрования за счет использования каналов с обратной связью и, так называемых криптосистем коммутативного шифрования (КШ). В разделе 3 описывается метод распределения ключей, основанный на использовании постоянных бесшумных открытых каналов связи (типа Интернет) и концепции усиления секретности. Заключение подводит итог данной работе, и представляет возможные перспективы проведения исследований в данных направлениях в будущем.

2. Использование коммутативного шифрования

В [6] был описан предложенный ранее Шамиром метод шифрования/дешифрования безо всякого предварительного распределения ключевых данных. Для его использования необходимо выполнение следующего требования для алгоритмов шифрования, которое можно условно назвать коммутативным шифрованием (КШ):

$$f_{K_A}\left(f_{K_B}(M)\right) = f_{K_B}\left(f_{K_A}(M)\right), \qquad (1)$$

где $f_{K_A}(M)$, $f_{K_B}(M)$ – алгоритмы (функции) шифрования сообщения M на ключах K_A, K_B, соответственно. В словесной формулировке требование (1) означает, что результат шифрования любого сообщения M не зависит от того, в каком порядке будут использованы ключи: сначала K_B, а потом K_A, или наоборот, сначала K_A, а потом K_B.

Действительно, при выполнении условия (1) передача зашифрованного сообщения M от корреспондента A к корреспонденту B с возможностью его расшифровки последним, причем при отсутствии всякого предварительного распределения общих ключей между A и B, доказывается представленным на рисунке 1 протоколом (при наличии у A и B каналов обратной связи).

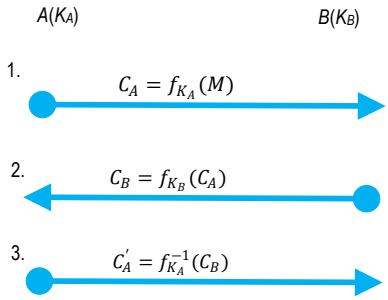

Рис. 1. Протокол секретной передачи сообщений

Fig. 1. Secret Message Transfer Protocol

Так, $C_B = f_{K_B}(C_A) = f_{K_B}(f_{K_A}(M))$, и тогда:

$$C_A' = f_{K_A}^{-1}(C_B) = f_{K_A}^{-1}\left(f_{K_B}(f_{K_A}(M))\right). \qquad (2)$$

При выполнении условия (1), получаем из (2):

$$C_A' = f_{K_A}^{-1}\left(f_{K_B}(f_{K_A}(M))\right) = \\ = f_{K_A}^{-1}\left(f_{K_A}(f_{K_B}(M))\right) = f_{K_B}(M). \qquad (3)$$

Поскольку по определению преобразований шифрования $f_{K_A}(M)$ и дешифрования $f_{K_A}^{-1}(M)$ на одном и том же ключе они дают исходное M', получаем в (3) действительно $f_{K_B}(M)$. Наконец, B восстанавливает M, выполняя преобразование дешифрования $f_{K_B}^{-1}\left(f_{K_B}(M)\right) = M$. Заметим, что условие (1) требуется только для преобразования шифрования, но не для обоих преобразований – шифрования и дешифрования!

Однако возникает вопрос, существуют ли какие-то преобразования шифрования, удовлетворяющие (1)? Докажем далее, что примером алгоритма, соответствующего условию (1), может служить широко известная криптосистема Райвеста – Шамира – Адлемана (РША), описанная в [1, 7], а также в других источниках.

Как известно, для шифра РША выполняются следующие условия:

– $n = p \cdot q$, где $p \neq q$ простые числа; n – модуль;

– $\varphi = (p-1)(q-1)$;

– $1 \le e_A \le \varphi$, $1 \le e_B \le \varphi$, где e_A, e_B – целые положительные числа, причем $gcd(e_A,\varphi) = 1$, $gcd(e_B,\varphi) = 1$, $1 \le M \le n-1$ целые числа.

Тогда, если A и B имеют одинаковые модули n, то условие (1) может быть представлено следующим образом:

$$(M^{e_A} \bmod n)^{e_B} \bmod n = (M^{e_B} \bmod n)^{e_A} \bmod n. \qquad (4)$$

Справедливость (4) следует из хорошо известных свойств модульных операций, однако поскольку в источниках [2] и [6] явно это равенство отсутствует, то имеет смысл доказать его ниже еще раз для убедительности.

Очевидно, что по определению модульных операций

$$M^{e_A} \bmod n = M^{e_A} - nl, \quad (5)$$

где l – некоторое целое положительное число.

Подставляя (5) в левую часть (4), получим:

$$(M^{e_A} \bmod n)^{e_B} \bmod n = (M^{e_A} - nl)^{e_B} \bmod n = \\ = (M^{e_A * e_B} - n * \text{БН})^{l_B} \bmod n, \quad (6)$$

где БН – бином Ньютона без первого члена из с вынесенным общим множителем n.

Далее по свойству модульных операций, получим из (6):

$$n * \text{БН} \bmod n = 0, \quad (7)$$

тогда из (6) и (7) получим:

$$(M^{e_A} \bmod n)^{e_B} \bmod n = M^{e_A * e_B} \bmod n. \quad (8)$$

Аналогично (8), легко показать, что для правой части (4) будет справедливо аналогичное равенство:

$$(M^{e_B} \bmod n)^{e_A} \bmod n = M^{e_B * e_A} \bmod n. \quad (9)$$

Совпадение (8) и (9) доказывает справедливость равенства (4).

Пример. Пусть $p = 3$, $q = 5$, $M = 2$, $e_A = 3$, $e_B = 5$. Тогда можно проверить, что обе части (4) равны 8.

Поскольку, как уже было сказано выше, данный алгоритм соответствует системе РША, то очевидно, что в этом случае алгоритм шифрования в (1) будет иметь вид:

$$E = f_{K_{A(B)}}(M) = M^{e_{A(B)}} \bmod n, \quad (10)$$

а алгоритм дешифрования:

$$f^{-1}_{K_{A(B)}}(E) = E^{d_{A(B)}} \bmod n, \quad (11)$$

где $d = e^{-1} \bmod \varphi$.

Стойкость данной криптосистемы будет определяться криптографическим предположением о невозможности факторизации модуля n для допустимого времени криптоанализа и допустимого объема оборудования; другим требованием для обеспечения защищенности такой криптосистемы является предположение о сложности вычисления дискретных логарифмов, поскольку иначе на втором шаге протокола криптоаналитик, зная C_B, сможет вычислить ключ дешифрования d [1]. Поскольку система РША является «самодостаточной», то, казалось бы, описанный выше протокол и не потребуется, если конечно, на стадии шифрования известен открытый ключ $e_{A(B)}$ противоположного корреспондента. Это может быть достигнуто или при помощи открытой передачи такого ключа по каналу связи от A к B или наоборот, или же от сертифицированного центра, который предварительно получает такие ключи и гарантируют их подлинность.

Некоторым преимуществом описанного выше протокола может служить факт, что корреспондент, шифрующий сообщение, может даже и не знать открытого корреспондента, которому оно предназначается, что не отменяет, конечно, необходимости аутентификации пользователей для исключения атаки имперсонализации.

В качестве еще одного претендента на выполнение условия (1), рассмотрим криптосистему Рабина [1]. В этом случае, в качестве открытого ключа выступает целое число $n = p \cdot q$, где p и q – простые неизвестные числа, а в качестве секретного ключа используются именно эти числа. Шифрование выполняется по правилу:

$$C = M^2 \bmod n, \quad (12)$$

где сообщение M – любое целое число в интервале $0 \le M \le n - 1$.

Применительно к данному случаю условие (1) принимает следующий вид:

$$(M^2 \bmod n_A)^2 \bmod n_B = (M^2 \bmod n_B)^2 \bmod n_A. \quad (13)$$

Легко проверить, что, по крайней мере, при некотором выборе параметров равенство (13) не выполняется. Действительно, если взять $p = 3$, $q = 5$, что дает $n_A = 15$ и $p = 11$, $q = 7$, а $n_B = 77$, то при выборе сообщения $M = 5$ левая часть (13) оказывается равной 23, а правая – 10 и, следовательно, равенство (13) не выполняется. То есть криптосистема Рабина не годится для использования в протоколе, описанном на рисунке 1. Заметим, что доказательство равенства (4) «не проходит» из-за невозможности доказать равенство аналогичное (7).

В ряде работ последнего десятилетия, в частности в работе Shor [8], было показано, что некоторые трудные задачи (такие, например, как задача факторизации и дискретного логарифмирования) могут быть решены в полиноминальное время при использовании так называемых квантовых компьютеров. Хотя практическая реализация таких компьютеров все еще остается нерешенной проблемой [3], но не учитывать такой возможности, пусть и в далеком будущем, было бы недальновидным решением. Поэтому появились целые направления разработки так называемых постквантовых криптосистем. Такие алгоритмы гарантируют невозможность полиномиального решения трудных задач, на которых основаны эти криптосистемы, даже при практической реализации квантовых компьютеров.

К постквантовым относится, например, криптосистема Мак-Элис [1, 7]. Как следует из ее описания, ключом шифрования классической криптосистемы

Мак-Элис является матрица $\hat{G} = SGP$, где S – несингулярная квадратная матрица kxk; G – порождающая матрица некоторого линейного двоичного кода; P – перестановочная nxn матрица. Тогда преобразования шифрования сообщения M для пользователя A и B будут иметь вид, соответственно:

$$f_{KA}(M) = M\hat{G}_A \oplus Z_A; \quad f_{KB}(M) = M\hat{G}_B \oplus Z_B, \tag{14}$$

где Z_A, Z_B – случайные двоичные векторы длиной n и заданного веса t; M – двоичная последовательность длиной k; $\oplus$ – операция побитового сложения по mod2.

Поскольку процедура шифрования изменяет длину сообщения от k к n, то повторное шифрование с различными ключами вообще не имеет смысла. Однако даже, если пользователи предварительно согласуют свои открытые ключи так, чтобы у одного из них параметр k был бы заменен на n, а n – на $n' > n$, то левая и правая части выражения (1) примут вид:

$$f_{KA}\left(f_{KB}(M)\right) = \left(M\hat{G}_B \oplus Z_B\right)\hat{G}_A \oplus Z_A = M\hat{G}_B\hat{G}_A \oplus Z_B\hat{G}_A \oplus Z_A, \tag{15}$$

$$f_{KB}\left(f_{KA}(M)\right) = \left(M\hat{G}_A \oplus Z_A\right)\hat{G}_B \oplus Z_B = M\hat{G}_A\hat{G}_B \oplus Z_A\hat{G}_B \oplus Z_B. \tag{16}$$

Видно, что (15) и (16) не будут совпадать, хотя бы из-за несовпадения векторов Z_A и Z_B. Поэтому использование криптосистемы Мак-Элис в представленном виде оказывается невозможным.

Еще одним примером постквантовых криптосистем является криптосистема на решетках [9]. Можно также проверить, что и для таких криптосистем условие (1) не выполняется. Очевидно, что такое условие не выполняется и для симметричных блоковых криптосистем, таких, например, как 3DES, GOST или AES.

На первый взгляд кажется, что условие (1) может быть тривиально выполнено при использовании потоковых шифров [1, 7]. Действительно, пусть используется потоковый шифр с гаммированием, когда формирование криптограммы $E(M,K)$ задается следующим соотношением:

$$E(M,K) = M \oplus \gamma(K), \tag{17}$$

где M – произвольная двоичная последовательность; $\gamma(K)$ – двоичная последовательность (гамма), которая формируется как функция секретного ключа K при помощи его линейных и нелинейных преобразований; $\oplus$ – поэлементное сложение по mod2.

Тогда для двух пользователей A и B, использующих ключи K_A и K_B, соответственно, выполнение условия (1) оказывается очевидным:

$$f_{K_A}\left(f_{K_B}(M)\right) = M \oplus \gamma(K_B) \oplus \gamma(K_A), \tag{18}$$

$$f_{K_B}\left(f_{K_A}(M)\right) = M \oplus \gamma(K_A) \oplus \gamma(K_B).$$

Однако использование в данном случае приведенного выше уравнения дает следующий протокол, показанный на рисунке 2.

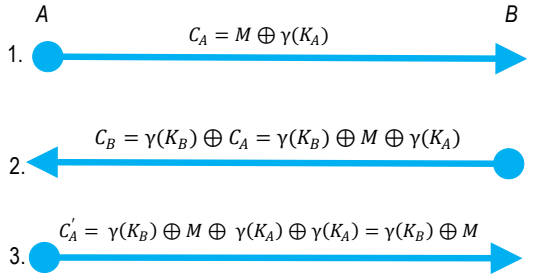

Рис. 2. Протокол секретной передачи сообщений для потокового шифра

Fig. 2. Secret Message Transfer Protocol for a Stream Cipher

Из рисунка 2 видно, что перехватчик, получая последовательности на третьем и втором этапах $\gamma(KB) \oplus M$ и $\gamma(KB) \oplus M \oplus \gamma(K_A)$, может поэлементно сложить их по mod2, что дает $\gamma(K_A)$, а далее – найти сообщения M после сложения по mod2 последовательности $\gamma(K_A)$ и последовательности, найденной им на первом этапе. Таким образом, использование потокового шифра для секретной передачи сообщений M при помощи приведенного ранее протокола также оказывается невозможным, что очевидно является следствием линейного сложения сообщения с гаммами. Заметим, что факт невозможности использования потоковых шифров в протоколе, показанном в рисунке 2, был установлен ранее в [6].

Наличие каналов обратной связи между пользователями позволяет выполнить секретное распределение между ними ключевых данных при дополнительных ограничениях на эти каналы. Так, в работе [10] предполагается, что, хотя данные каналы могут иметь или не иметь шума и быть доступными для перехвата, но они должны быть анонимными по отношению к обоим пользователям, то есть не позволять перехватчикам определить, кому принадлежат биты, наблюдаемые в каналах обмена от A к B, или наоборот. Такой сценарий рассмотрен в работе [10], где каждый из пользователей A и B генерирует случайные цепочки $K_A[1]$, ..., $K_A[2n]$, $K_B[1]$, ..., $K_B[2n]$, которые открыто публикуются с сопровождением номера битов $i = 1, 2, ..., 2n$, но без описания принадлежности их к авторам A или B. По предварительному согласованию, пользователи A и B изымают из обращения совпадающие биты для каждого индекса $i = 1, 2, ..., 2n$, тогда как A выбирает в качестве совместного ключа K_{AB} свои оставшиеся, упорядоченные по возрастанию i биты, причем B выбирает в качестве общего ключа K'_{AB} его оставшиеся, но инвертированные биты, что обеспечивает равенство ключей $K_{AB} = K'_{AB}$. Основная проблема заключается именно в возможности обеспечения анонимности источника (A или B) для каждого бита. В той же работе [10] проводится несколько примеров создания

таких анонимных каналов. Одним из них оказывается использование «третьего лица», которое ретранслирует в широковещательную сеть биты ключей A и B, без указания пользователя, от которого был получен каждый бит.

3. Обмен ключами по постоянному, открытому и бесшумному каналу связи (типа Интернет)

В фундаментальном обзоре [5] приводятся различные сценарии распределения ключей в рамках использования общего подхода к обеспечению информационной безопасности, названного авторами Physical Layer Security. Данный подход не отказывается полностью от использования криптографических методов, например, криптосистем с открытым ключом, хэш-функций, Вайнеровской концепции подслушивающего канала, открытого обсуждения [11] и т. п., но использует данные методы только в условиях естественной или даже искусственной рандомизации каналов связи.

Однако недостатком практических всех методов, представленных в настоящем обзоре, является не реализуемые на практике требования к каналам связи. Примерами таких нереальных ограничений могут служить ограничения на мощность шума в каналах перехвата или количества антенн у перехватчика при использовании технологии MIMO и т. п.

В последнее время появилось несколько публикаций [12, 13], в которых такие недоказуемые на практике требования отсутствуют. Эти методы предполагают достаточно сложную обработку сигналов. Цель же настоящей статьи состоит в том, что она показывает возможность решения задачи распределения ключей между двумя пользователями, опирающейся на «ключевую идею», что каждый пользователь обладает хотя бы частью секретов, недоступных перехватчику, но в то же время не использует какие-либо криптографические предположения.

Опишем далее протокол, предложенный недавно в работе [14], поскольку он пока не был опубликован в русскоязычных статьях. В отличие от протокола, описанного в [15], он реализуется при помощи двухшаговой процедуры обмена информацией по каналу связи, в то время как в [15] выполняется четырехшаговая процедура, требующая больших временных затрат. На рисунке 3 представлен такой протокол, где G и P – это nxn матрицы, генерируемые легальными пользователями A и B, также, как и матрицы N_A, N_B искусственного шума. Элементы этих матриц представляют собой независимые гауссовские величины с нулевыми средними и заданными дисперсиями. Из рисунка 3 видно, что после взаимной передачи матриц по каналам связи, A и B вычисляют матрицы $\widetilde{K}_A$, $\widetilde{K}_B$, соответственно, и затем находят «сырые ключи» $\widetilde{\widetilde{K}}_A$, $\widetilde{\widetilde{K}}_B$, квантуя собственные числа соответствующих матриц, как $EV(\widetilde{K}_A)$, $EV(\widetilde{K}_B)$. В то же время, перехватчик E оптимально находит после квантования зашумленные биты ключа между A и B, как и показано на рисунке 3: $EV(\widetilde{K}_E)$, где $\widetilde{K}_E = (G + N_A)(P + N_B)$.

Моделирование протокола, представленного на рисунке 3, показывает, что расхождение бит ключей $\widetilde{\widetilde{K}}_A, \widetilde{\widetilde{K}}_B$ между легитимными пользователями оказывается даже больше, чем расхождение бит ключа между легитимными пользователями и перехватчиком E. Для того, чтобы исправить такую ситуацию, был использован специальный протокол (PIMC, называемый протоколом преимущественного улучшения основного канала). Суть протокола PIMC состоит в том, что пользователь B повторяет каждый бит ключа S-раз и посылает эти биты по каналу связи к A, в то время как A принимает S-блоки тогда и только тогда, когда все они состоят из одинаковых бит (нулей или единиц). В противном случае A посылает B сигнал стирания этого блока.

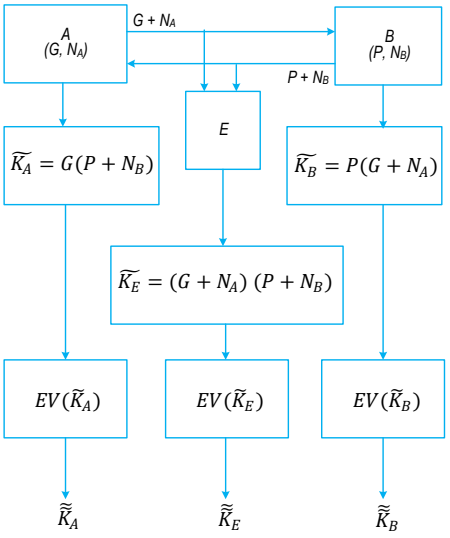

Рис. 3. Двухшаговый протокол, выполняемый по открытому и бесшумному каналу связи (типа Интернет)

Fig. 3. Two-Step Protocol Performedthrough an Open and Silent Communication Channel (Such as the Internet)

Для получения хорошей статистики бит ключа используется схема, показанная на рисунке 4, из которого видно, что B генерирует шумовые биты γ, как биты ключа между A и B, используя физический генератор шума. Биты γ складываются с битами ключа $\widetilde{\widetilde{K}}_B$, выделенными по правилу, показанному на рисунке 3.

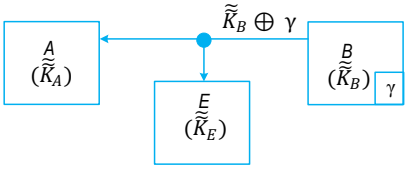

Рис. 4. Схема генерирования и пересылки бит ключа от пользователя *B* к пользователю *A*

Fig. 4. Scheme for Generating and Sending Key Bits from User B to User A.

Далее A формирует свой ключ K_A по правилу:

$$K_A = \widetilde{K_B} \oplus \gamma \oplus \widetilde{\widetilde{K_A}} = \\ = \widetilde{\widetilde{K_A}} \oplus \varepsilon_{AB} \oplus \widetilde{\widetilde{K_A}} \oplus \gamma = \gamma \oplus \varepsilon_{AB}, \quad (20)$$

где ε_{AB} – битовый шум между $\widetilde{\widetilde{K_A}}, \widetilde{\widetilde{K_B}}$.

В то же время перехватчик E, зная схему, показанную на рисунке 4, формирует свои ключи по правилу:

$$K_E = \widetilde{\widetilde{K_E}} \oplus \gamma \oplus \widetilde{\widetilde{K_B}} = \\ = \widetilde{\widetilde{K_B}} \oplus \varepsilon_{BE} \oplus \gamma \oplus \widetilde{\widetilde{K_B}} = \gamma \oplus \varepsilon_{BE}. \quad (21)$$

В работе [14] показано, что после применения протокола PIMC вероятность ошибок $\widetilde{P_l}$ между ключами A и B, будет определяться соотношением:

$$\widetilde{P_l} = \frac{P_l^S}{P_l{}^S + (1 - P_l)^S}, \quad (22)$$

где P_l – вероятность ошибок (вероятность появления единицы) в образце шума ε_{AB}.

Перехватчик E принимает K_E по (21) и контролирует сообщения от A к B о стирании бит. Тогда, как показано в [14], вероятность ошибок у E относительно бит ключа γ будет определяться соотношением:

$$\widetilde{P_e} = \sum_{i=\frac{S+1}{2}}^{S} \binom{S}{i} P_e^i (1 - P_e)^{S-i}, \quad (23)$$

где P_e – вероятность ошибок в векторе ε_{BE}.

Поскольку в действительности ключевые потоки K_A и K_E имеют зависимые ошибки, то для уточнения дальнейших расчетов необходимо было провести их моделирование. В работе [14] было произведено моделирование протокола, показанного на рисунке 3, и PIMC для различных параметров S и величин дисперсии σ^2 искусственного шума, с целью вычисления вероятности ошибок $\widetilde{P_l}$ и $\widetilde{P_e}$. Наиболее предпочтительным оказался выбор размеров матриц 64×64. В таблице 1 приведены результаты такого моделирования.

Из таблицы 1 видно, что при некотором выборе параметров S и σ^2 вероятности ошибок в битах ключей для основного канала ($\widetilde{P_l}$) и канала перехвата ($\widetilde{P_e}$) значительно расходятся между собой после использования PIMC протокола. Однако такое расхождение оказывается недостаточным, как для обеспечения надежного совпадения ключей в основном канале, так и для пренебрежимой утечки в канале перехвата. Поэтому целесообразно повысить надежность совпадения ключей K_A и K_B при помощи использования корректирующего кода, передавая проверочные биты такого кода по открытому каналу связи.

В качестве такого кода целесообразным оказалось выбрать линейный код с малой плотностью проверок (LDPC-код), поскольку он, с одной стороны, приближается к «пределу Шеннона», а с другой стороны, обеспечивает реализуемый по сложности метод исправления ошибок [16, 17].

ТАБЛИЦА 1. Результаты моделирования вероятности ошибок $\widetilde{P_l}$ и $\widetilde{P_e}$ для различных параметров S и σ^2

TABLE 1. Simulation Results for Error Probabilities $\widetilde{P_l}$ and $\widetilde{P_e}$ with Various Parameters S и σ^2

S \ σ^2	0,1	0,2	0,3	0,4	$\widetilde{P_l}, \widetilde{P_e}$
1	0,0816	0,0851	0,0859	0,0963	$\widetilde{P_l}$
	0,0922	0,117	0,140	0,154	$\widetilde{P_e}$
3	0,00362	0,00402	0,00407	0,00396	$\widetilde{P_l}$
	0,0185	0,0439	0,0673	0,0822	$\widetilde{P_e}$
5	0,000193	0,000294	0,000258	0,000226	$\widetilde{P_l}$
	0,00875	0,0314	0,053	0,0699	$\widetilde{P_e}$
7	$1{,}44 \cdot 10^{-5}$	$3 \cdot 10^{-5}$	$1{,}79 \cdot 10^{-5}$	$1{,}68 \cdot 10^{-5}$	$\widetilde{P_l}$
	0,00529	0,0256	0,0455	0,059	$\widetilde{P_e}$

Что же касается требования уменьшения утечки информации по каналу перехвата, то для этого целесообразно использовать процедуру, называемую *усилением секретности*. Она подробно описана в работе [18] и заключается в применении хэширования при помощи хэш-функций, выбранных из универсального$_2$ класса и последующего «выкалывания» некоторых элементов. В работе [18] была выведена граница для количества Шенноновской информации, утекающей к перехватчику после такой процедуры (с учетом передачи проверочных бит по каналу связи). Эта граница имеет следующий вид:

$$I \leq \frac{2^{-(k - t_c - l_0 - r)}}{\alpha \ln 2}, \quad (24)$$

где k – длина цепочки бит ключа, разделенного между пользователями A и B после выполнения протокола PIMC; l_o – фактическая длина ключа после выполнения процедуры усиления секретности; t_c – информация Реньи (или *коллизионная* информация), полученная по каналу перехватчика с вероятностью ошибки $\widetilde{P_e}$; r – количество проверочных бит LDPC кода, передаваемых между легальными пользователями по открытому каналу связи; α – коэффициент, приближающиеся к 0,42 при больших k, $k - r$.

В работе [14] были выбраны следующие первичные параметры протокола, обеспечивающие его требуемые свойства $n = 64$, $\sigma^2 = 0{,}4$, $S = 5$, что позволило получить следующие вероятности ошибок для основного канала и для канала перехвата $\widetilde{P_l} = 0{,}0002$, $\widetilde{P_e} = 0{,}0699$. (см. таблицу 1). В этой же работе, путем расчетов и моделирования был выбран LDPC код с параметрами: $k = 24039$, $r = 961$, который обеспечивает основную длину ключа $l_o = 3659$ бит, а также вероятность блоковой ошибки после декодирования $P_{ed} = 2{,}5 \cdot 10^{-3}$ и утечку информации к перехватчику $I = 9 \cdot 10^{-4}$ бита.

При выборе других параметров LDPC кода k = 50001, r = 1999 можно получить финальную длину ключа l_o = 7624, $P_{ed} = 8 \cdot 10^{-4}$ и $I = 1{,}4 \cdot 10^{-3}$ бита.

В работе [14] была выведена формула для объема трафика (Tr), требуемого для данного протокола выработки совместного ключа и представленного на рисунке 1 с учетом дополнительного выполнения протокола PIMC:

$$Tr = 2{,}66 \cdot 10^{-6} \frac{\mathrm{Sk}\, n}{\left((1-P_l)^S + P_l{}^S\right)^2}. \qquad (25)$$

Расчет объема трафика по этой формуле при выборе LDPC кода с параметрами k = 24039, r = 961 дает величину 32 МБ, что является приемлемым для практики.

Как уже отмечалось ранее, для выработки чисто случайной двоичной последовательности γ, показанной на рисунке 4, рекомендуется использовать аппаратно реализованный генератор. В качестве такого генератора предложено использовать генератор Crypton USB-DRN, производимый фирмой «Анкад» [19]. На рисунке 5 показан внешний вид этого генератора, выполненного в размерах flash-памяти.

Рис. 5. Вид генератора Crypton USB-DRN фирмы «Анкад»

Fig. 5. View of the Crypton USB-DRN Generator by "Ankad"

В работе [14] было произведено дополнительное тестирование статистических свойств этого генератора при помощи NIST тестов, которые показали его близость к чисто случайный (и непредсказуемой) двоичной последовательности.

Представленный выше протокол распределения ключевых данных между пользователями требует, как и любой другой протокол распределения ключей, обеспечения аутентификации легитимных пользователей. В противном случае активный перехватчик E может, используя такой же протокол, навязать легитимным пользователям общие с ними ключи. Для воспрепятствования таким возможным действиям перехватчика, можно использовать различные методы аутентификации, начиная с простых, когда подлинность пользователя, выполняющего протокол, подтверждается его известным голосовым сообщением, переданным по дополнительному телефонному каналу [6] или такими более надежными методами, как протокол Нидхама – Шредера [20] или при помощи процедуры «спаривания» устройств, когда возможно их предварительное физическое взаимодействие [21].

4. Заключение

В настоящей работе были исследованы некоторые методы обеспечения информационной безопасности при помощи такого, появившегося сравнительно недавно, направления, как бесключевая криптография. Доказано, что один из таких методов обеспечивает возможность передачи зашифрованных криптосистем РША информации без предварительного распределения как закрытых, так и открытых ключей. С другой стороны, показано, что при использовании таких криптосистем с открытым ключом как Рабина, Мак-Элис, а также потокового шифра, получить такой же результат оказывается невозможным. Подробно описан и исследован протокол распределения ключей для его выполнения в общедоступных и бесшумных каналах с постоянными параметрами (типа Интернет). В отличие от похожего протокола, описанного в [15], он требует меньшего объем трафика, выполняемого по каналам связи. Для обеспечения хорошей статистики ключевых данных было предложено использовать аппаратный датчик случайных чисел и схему выработки сырого ключа, показанную на рисунке 4.

В дальнейшем перспективным может оказаться переход от передачи матриц по каналам связи к обмену обычными случайными числами, что обеспечит значительное уменьшение объема трафика для такого обмена. Однако такая модернизация требует проведения дальнейших углубленных исследований.

БЛАГОДАРНОСТЬ

Автор выражает благодарность профессору Коржику В.И. за помощь при подготовке и обсуждении работы.

Список используемых источников

1. Коржик В.И., Яковлев В.А. Основы криптографии. СПб: Интермедия, 2016. 312 с.
2. Diffie W., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22. Iss. 6. PP. 644–654. DOI:10.1109/TIT.1976.1055638
3. Dyakonov M.I. Is Fault-Tolerant Quantum Computation Really Possible? // In Luryi S., Xu J., Zaslavsky A. Future Trends in Microelectronics. John Wiley & Sons, 2007. PP. 4–18.
4. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography // Journal of Cryptology. 1992. Vol. 5. PP. 3–28.
5. Mukherjee A., Fakoorian S.A.A., Huang J., Swindlehurst A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey // IEEE Communications Surveys & Tutorials. 2014. Vol. 16. Iss. 3. PP. 1550–1573. DOI:10.1109/SURV.2014.012314.00178

6. Schneier B. Applied Cryptography. Montreal: JW Publ. Inc., 1994.
7. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997. DOI:10.1201/9780429466335
8. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Santa Fe, USA, 20–22 November 1994). IEEE Computer Society Press, 1994. PP. 124–134.
9. Goldreich O., Goldwasser S., Halevi S. Public–key cryptography from lattice reduction problems // Proceedings of the 17th Annual International Cryptology Conference (Santa Barbara, USA, 17–21 August 1997). Lecture Notes in Computer Science. Vol. 1291. Berlin, Heidelberg: Springer, 1997. PP. 112–131. DOI:10.1007/BFb0052231
10. Alpern B., Schneider F.B. Key exchange using 'keyless cryptography' // Information Processing Letters. 1983. Vol. 16. Iss. 2. PP. 79–81. DOI:10.1016/0020-0190(83)90029-7
11. Maurer U.M. Secrete key agreement by public discussion from common information // IEEE Transactions on Information Theory. 1993. Vol. 39. Iss. 3. PP. 733–742. DOI:10.1109/18.256484
12. Yakovlev V., Korzhik V., Morales-Luna G. Key Distribution Protocols Based on Noisy Channels in Presence of an Active Adversary: Conventional and New Versions with Parameter Optimization // IEEE Transactions on Information Theory. 2008. Vol. 54. Iss. 6. PP. 2535–2549. DOI:10.1109/TIT.2008.921689
13. Korzhik V., Starostin V., Kabardov M., Gerasimovich A., Yakovlev V., Zhuvikin A. Protocol of key distribution over public noiseless channels executing without cryptographic assumptions // International Journal of Computer Science and Application. 2020. Vol. 17. Iss. 1. PP. 1–14.
14. Korzhik V., Starostin V., Kabardov M., Gerasimovich A., Yakovlev V., Zhuvikin A. Optimization of the Key Sharing Protocol for Noiseless Public Channels without the Use of Cryptographic Assumptions // Proceedings of the 44th International Convention on Information, Communication and Electronic Technology (MIPRO, Opatija, Croatia, 27 September–1 October 2021). IEEE, 2021. PP. 1202–1207. DOI:10.23919/MIPRO52101.2021.9596703
15. Korzhik V.I., Starostin V.S., Kabardov M.M., Gerasimovich A.M., Yakovlev V.A., Zhuvikin A.G. Information theoretically secure key sharing protocol executing with constant noiseless public channels // Matematicheskie Voprosy Kriptografii. 2021. Vol. 12. Iss. 3. PP. 125–141. DOI:10.4213/mvk378
16. MacKay D.J.C., Neal R.M. Near Shannon Limit Performance of Low Density Parity Check Codes // Electronics Letters. 1997. Vol. 33. Iss. 18. PP. 457–458.
17. Fossorier M. P.C., Mihaljevic M., Imai H. Reduced complexity iterative decoding of low density parity check codes based on belief propagation // IEEE Transactions on Communications 1999. Vol. 47. Iss. 5. PP. 673–680. DOI:10.1109/26.768759
18. Korjik V., Morales-Luna G., Balakirsky V.B. Privacy Amplfication Theorem for Noisy Main Channel // Proceedings of the 4th International Conference on Information Security (ISC 2001, Malaga, Spain, 1–3 October 2001). Lecture Notes in Computer Science. Vol. 2200. Berlin, Heidelberg: Springer, 2001. PP. 18–26. DOI:10.1007/3-540-45439-X_2
19. Подорожный И.В. Обзор аппаратных генераторов случайных чисел // Молодой ученый. 2015. № 1(105). URL: http://moluch.ru/archive/105/24688 (дата обращения 24.06.2020)
20. Needham R.M., Schroeder M.D. Using encryption for authentication in large network of computers // Communications of the ACM. 1978. Vol. 21. Iss. 12. PP. 993–999. DOI:10.1145/359657.359659
21. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. Vol. 11. Iss. 6. PP. 1306–1320. DOI:10.1109/TIFS.2015.2505626

* * *

Secure Information Transfer Using Two Keyless Cryptography Methods

A. Gerasimovich[1]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-4-119-127
Received 6th December 2021
Revised 21st December 2021
Accepted 22th December 2021

For citation: Gerasimovich A. Secure Information Transfer Using Two Keyless Cryptography Methods. *Proc. of Telecom. Universities.* 2021;7(4):119–127. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-119-127

Abstract: *In the current paper, some methods of information security protocols based on physical layer security are considered. It is proved that well known Shamir's protocol can be applied to RSA cryptosystem but not to Rabin, MacEllice and trellis based cryptosystems.*

The main stream of this paper is a description of key sharing protocol on constant public and noiseless channels (like Internet). It is shown that it is able to provide a high reliability and control of security in terms of Shannon's information providing nothing-additional requirements to communication channels and without any cryptographic assumptions.

Keywords: *public key cryptosystem, key distribution, Shannon's information, privacy amplification, physical layer security quantum computers.*

References

1. Korzhik V.I., Yakovlev V.A. *Fundamentals of Cryptography*. St. Petersburg: Intermediia Publ.; 2016. 312 p. (in Russ.)
2. Diffie W., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976;22(6):644–654. DOI:10.1109/TIT.1976.1055638
3. Dyakonov M.I. Is Fault-Tolerant Quantum Computation Really Possible? *In Luryi S., Xu J., Zaslavsky A. Future Trends in Microelectronics*. John Wiley & Sons; 2007. p.4–18.
4. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography. *Journal of Cryptology*. 1992;5:3–28
5. Mukherjee A., Fakoorian S.A.A., Huang J., Swindlehurst A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Communications Surveys & Tutorials*. 2014;16(3):1550–1573. DOI:10.1109/SURV.2014.012314.00178
6. Schneier B. *Applied Cryptography*. Montreal: JW Publ. Inc.; 1994
7. Menezes A.J., van Oorschot P.C., Vanstone S.A. *Handbook of Applied Cryptography*. Boca Raton: CRC Press; 1997. DOI:10.1201/9780429466335
8. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 20–22 November 1994, Santa Fe, USA*. IEEE Computer Society Press; 1994. p.124–134.
9. Goldreich O., Goldwasser S., Halevi S. Public–key cryptography from lattice reduction problems. *Proceedings of the 17th Annual International Cryptology Conference, 17–21 August 1997, Santa Barbara, USA. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer, 1997. vol.1291. p.112–131. DOI:10.1007/BFb0052231
10. Alpern B., Schneider F.B. Key exchange using 'keyless cryptography'. *Information Processing Letters*. 1983;16(2):79–81. DOI:10.1016/0020-0190(83)90029-7
11. Maurer U.M. Secrete key agreement by public discussion from common information. *IEEE Transactions on Information Theory*. 1993;39(3):733–742. DOI:10.1109/18.256484
12. Yakovlev V., Korzhik V., Morales-Luna G. Key Distribution Protocols Based on Noisy Channels in Presence of an Active Adversary: Conventional and New Versions with Parameter Optimization. *IEEE Transactions on Information Theory*. 2008;54(6):2535–2549. DOI:10.1109/TIT.2008.921689
13. Korzhik V., Starostin V., Kabardov M., Gerasimovich A., Yakovlev V., Zhuvikin A. Protocol of key distribution over public noiseless channels executing without cryptographic assumptions. *International Journal of Computer Science and Application*. 2020;17(1):1–14.
14. Korzhik V., Starostin V., Kabardov M., Gerasimovich A., Yakovlev V., Zhuvikin A. Optimization of the Key Sharing Protocol for Noiseless Public Channels without the Use of Cryptographic Assumptions. *Proceedings of the 44th International Convention on Information, Communication and Electronic Technology, MIPRO, 27 September–1 October 2021, Opatija, Croatia*. IEEE; 2021. p.1202–1207. DOI:10.23919/MIPRO52101.2021.9596703
15. Korzhik V.I., Starostin V.S., Kabardov M.M., Gerasimovich A.M., Yakovlev V.A., Zhuvikin A.G. Information theoretically secure key sharing protocol executing with constant noiseless public channels. *Matematicheskie Voprosy Kriptografii*. 2021;12(3):125–141. DOI:10.4213/mvk378
16. MacKay D.J.C., Neal R.M. Near Shannon Limit Performance of Low Density Parity Check Codes. *Electronics Letters*. 1997;33(18):457–458.
17. Fossorier M. P.C., Mihaljevic M., Imai H. Reduced complexity iterative decoding of low density parity check codes based on belief propagation. *IEEE Transactions on Communications.* 1999;47(5):673–680. DOI:10.1109/26.768759
18. Korjik V., Morales-Luna G., Balakirsky V.B. Privacy Amplfication Theorem for Noisy Main Channel. *Proceedings of the 4th International Conference on Information Security, ISC 2001, 1–3 October 2001, Malaga, Spain. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer; 2001. vol.2200. p.18–26. DOI:10.1007/3-540-45439-X_2
19. Podorozhnyi I. V. Overview of Hardware Random Number Generators. *Molodoy uchenyi*. 2015;1(105). Available from: http://moluch.ru/archive/105/24688 [Accessed 24th June 2020] (In Rus.)
20. Needham R.M., Schroeder M.D. Using encryption for authentication in large network of computers. *Communications of the ACM*. 1978;21(12):993–999. DOI:10.1145/359657.359659
21. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. Vol. 11. Iss. 6. PP. 1306–1320. DOI:10.1109/TIFS.2015.2505626

Сведения об авторе:

ГЕРАСИМОВИЧ Александр Сергеевич

аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
Alexgera93@gmail.com
https://orcid.org/0000-0002-9174-531X