Обзорная статья
УДК 004.056(075.58)
https://doi.org/10.31854/1813-324X-2024-10-6-79-98

Прогресс в теории прикладной криптографии: обзор и некоторые новые результаты. Часть 2. Бесключевая криптография

Валерий Иванович Коржик[1] ✉, val-korzhik@yandex.ru
Виктор Алексеевич Яковлев[1], yakovlev.va@sut.ru
Владимир Сергеевич Старостин[1], vm.ffp@sut.ru
Михаил Викторович Буйневич[2], bmv1958@yandex.ru

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, 196105, Российская Федерация

Аннотация

Настоящая работа является второй частью статьи «Прогресс в теории прикладной криптографии: обзор и некоторые новые результаты», опубликованной в четвертом номере журнала ТУЗС за 2024 год. Она посвящена специфическому разделу так называемой бесключевой криптографии (БК). Актуальность данной статьи состоит в том, что рассматриваемые в ней методы позволяют обеспечить конфиденциальность передачи информации по открытым каналам связи, либо вообще не выполняя никакого предварительного ее шифрования, а эксплуатируя лишь преобразования, естественно происходящие в каналах связи, либо, применяя обычную (ключевую) криптографию, ключи для которой передаются по открытым каналам связи с использованием методов БК.

Настоящая работа начинается с описания вайнеровской концепции подслушивающего канала и методов кодирования в нем, обеспечивающих надежную передачу по основному каналу с гарантированным малым количеством шенноновской информации, утекающей по каналу перехвата. Далее исследуются сценарий с коммутативной криптографией (CE) и протокол, обеспечивающий конфиденциальность передачи информации без всякого обмена ключами. Следующая модель относится к многолучевому каналу и применению MIMO-технологии по протоколу Дина и Голдсмит. Доказывается, что для него секретность передачи обеспечивается только при ограничении на количество приемных антенн перехватчика.

Следующий сценарий использует технологию антенн с управляемой диаграммой (VDA), причем устанавливаются условия на многолучевость и расположение корреспондентов радиосвязи, при которых может быть обеспечена конфиденциальность передачи информации.

Анализируется также недавно предложенная криптосистема EVESkey. Доказывается, что существует простая атака, которая может нарушить ее конфиденциальность.

Описывается ряд протоколов, выполняемых по бесшумному открытому каналу, которые, однако, не являются стойкими, поскольку они имеют нулевую секретную пропускную способность. Доказывается, что при матричном обмене в канале связи типа Интернет, конфиденциальность может быть обеспечена только по критерию ограничения сложности декодирования. В конце работы формулируются фундаментальные проблемы прикладной криптографии, решение которых могло бы значительно стимулировать дальнейшее развитие этой отрасли науки.

Ключевые слова: *бесключевая криптография, отводной канал, MIMO-технология, физический уровень секретности, усиление секретности, коммутативное шифрование.*

Ссылка для цитирования: Коржик В.И., Яковлев В.А., Старостин В.С., Буйневич М.В. Прогресс в теории прикладной криптографии: обзор и некоторые новые результаты. Часть 2. Бесключевая криптография // Труды учебных заведений связи. 2024. Т. 10. № 6. С. 79–98. DOI:10.31854/1813-324X-2024-10-6-79-98. EDN:HPBOWG

Review research
https://doi.org/10.31854/1813-324X-2024-10-6-79-98

Advance in Applied Cryptography Theory: Survey and Some New Results. Part 2. Keyless Cryptography

Valery I. Korzhik[1] ✉, val-korzhik@yandex.ru
Viktor A. Yakovlev [1], yakovlev.va@sut.ru
Vladimir S. Starostin[1], vm.ffp@sut.ru
Mikhail V. Buinevich[2], bmv1958@yandex.ru

[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]Saint Petersburg University of State Fire Service of Emercom of Russia,
St. Petersburg, 196105, Russian Federation

Annotation

Actuality. *The current paper is the second part of the paper "Advance in Applied Cryptography Theory: Survey and Some New Results. Part 1. Key Cryptography" published in the journal PTU, n.4, 2024. It is devoted to such specific area of applied cryptography as keyless one (KC\ Actuality of the current paper consists in the fact that considered in it methods allow to provide a confidentiality of information transmission over public communication channels, either without any its encryption in advance, executing a natural properties of communication channels or executing conventional key cryptography but with the keys which are elaborated before by means of KC.*
The natural properties of communication channels can be the following: additive noise, multiray wave propagation, MIMO technology and existence of feedback channel.
Our paper starts with a consideration of Wyner's concept of wire-tap channels and corresponding to it encoding and decoding methods providing very reliable information transmission over the main channels and negligible amount of information leaking over the wire-tap channels to eavesdroppers. Next it is investigated scenario with a commutative encryption (CE) and corresponding protocol of message exchange over ordinary noiseless public channel that provides security of encrypted information but without any key exchange between users in advance. It is proved which of well known symmetric and asymmetric ciphers are commutative or non-commutative ones. Next model concerns a fading channels under the application of Dean-Goldsmith protocol in frames of MIMO technology. We are proving that this protocol is secure if, and only if, the number of eavesdropper antennas is less than the number of antennas at legitimate users. Next scenario executes variable directional antennas (VDA) and it is proved for which conditions on a locations of legitimate users and eavesdroppers such approach occurs secure given the number of propagation rays is at least two.. We show in the next chapter that there is an attack compromising of recently proposed EVESkey cryptosystem and hence such one is not secure in spite of the statement of its authors.
Finally, we investigate several protocols intended for key sharing over noiseless constant public channels (like Internet) and established that they are mostly insecure because have all zero secret capacity. Only one protocol based on matrix channel exchange is able to provide security of key sharing but in terms of the required breaking complexity. Thus such approach can be used only for the case when legitimate users belong to low level of security requirements.
At the end of the paper we formulate several fundamental problems of applied cryptography which after of their solutions could be very useful for practice.

Keywords: *keyless cryptography, wire-tap channel concept, physical level security, MIMO technology, privacy amplification, commutative encryption*

For citation: Korzhik V.I., Yakovlev V.A., Starostin V.S., Buinevich M.V. Advance in Applied Cryptography Theory: Survey and Some New Results. Part 2. Keyless Cryptography. *Proceedings of Telecommunication Universities.* 2024;10(6):79–98. (in Russ.) DOI:10.31854/1813-324X-2024-10-6-79-98. EDN:HPBOWG

1. Введение

В части 1 настоящей статьи уже отмечалось, что термин «бесключевая криптография» (*от англ.* Keyless Cryptography) был предложен еще в 1983 г. в статье Б. Альперна и Ф. Шнайдера [1]. В последующие годы появилось множество работ, посвящен-

ных этой тематике, например [2–5] и другие. Попытаемся дать достаточно общее определение этому виду прикладной криптографии, хотя нужно признать, что термин «бесключевая криптография» не стал повседневно используемым, и иногда его заменяют частными случаями из данной области, например, «обеспечение секретности на физическом уровне» [5], сценарием с «отводным каналом» [6] и даже «квантовой криптографией» [7].

Само же общее понятие «бесключевой криптографии» можно определить следующим образом: это совокупность методов обеспечения секретности (конфиденциальности) передачи или хранения представленной в цифровом виде информации, в том числе и цифровых ключевых данных, без использования методов шифрования / дешифрования любого вида из арсенала методов современной криптографии или без предварительного обмена ключами для традиционной криптографии.

На первый взгляд, такое определение похоже на «оксюморон», поскольку криптография, казалось бы, основана именно на использовании различных преобразований открытой информации и секретных ключей, доступных только легитимным (то есть уполномоченным) пользователям. Даже несимметричная (или двухклассная криптография, или иначе – криптография с открытыми ключами (PKC, *аббр. от англ*. Public Key Cryptography), предложенная У. Диффи и М. Хеллманом, хотя и явившаяся подлинной революцией в криптографии, требует использования пары ключей, один из которых (шифрования), не должен быть секретным, но его необходимо передавать по каналам связи всем пользователям. Кажущееся противоречие в определении «бесключевая криптография» объясняется достаточно просто: секретность обеспечивается, прежде всего, преобразованиями, производимыми в каналах связи, между источниками информации и их получателями. В этом смысле так называемая квантовая криптография (QC, *аббр. от англ.* Quantum Cryptography) представляла бы собой частный случай бесключевой, поскольку ее секретность обеспечивается законами квантовой физики (принцип Гейзенберга, парадокс Эйнштейна – Подольского – Розена и т. д.). Однако, в настоящей статье мы не будем описывать направление QC и не столько потому, что авторы не являются специалистами в этой области. Так, один из них еще в конце прошлого века делал заказной доклад в лаборатории Calderonlab Оксфордского университета (Англия) на тему «Протоколы квантовой криптографии»; он же был научным руководителем кандидатской диссертации [8], посвященной именно исследованиям в области QC. Главная же причина того, что в данную статью не включена QC, состоит в том, что это специальная область знаний, где значительно большее внимание уделяется даже не прикладной математике, а физике (см. например, упомянутую выше диссертацию [8] и учебник «Основы криптографии», 3-е издание [9]). Кроме того, сейчас опубликовано много работ по QC (см., например [7, 10, 11] и др.), к которым мы не сможем добавить какие-либо свои новые результаты. Наконец, линии связи для передачи ключевых данных, протяженностью до 1000 км сейчас реализованы практически и достаточно хорошо описаны в [11]. Заметим также, что, если цель бесключевых криптосистем состоит в защите от перехвата самих ключевых данных, передаваемых по каналам связи, то на втором этапе ее выполнения могут использоваться общие (как симметричные, так и несимметричные) криптосистемы.

В работе [12] приводится обзор криптосистем, обеспечивающих секретность на физическом уровне, и также используется термин бесключевая криптография. Причем отмечается, что данные методы обеспечения конфиденциальности являются перспективными для технологии 6G.

Настоящая статья структурирована следующим образом. В разделе 2 описана бесключевая криптография, основанная на модели, когда в каналах связи, по которым предполагается передавать конфиденциальную информацию, присутствуют внешние шумы. Такой сценарий носит название Вайнеровской модели канала с отводом. Для данного сценария бесключевая криптография оказывается особенно эффективной в случае необходимости защиты от утечки информации по так называемым побочным каналам. В разделе 3 предлагается изучить сценарий передачи информации, когда между корреспондентами имеются бесшумные дуплексные каналы связи и используются так называемые коммутативные алгоритмы шифрования. В разделе 4 описываются сценарии, где имеются многолучевые (замирающие) каналы связи между корреспондентами, и по существу секретность обмена информацией обеспечивается различием некоторых характеристик таких каналов. В разделе 5 приведены новые результаты по предложенному японскими авторами методу распределения ключей при наличии смарт-антенны с управляемой диаграммой направленности и многолучевого канала связи между корреспондентами. Такой подход в дальнейшем был развит в работе авторов настоящей статьи. Раздел 6 иллюстрирует ситуацию, когда кажущаяся секретной бесключевая криптосистема на самом деле таковой не является. Это делается на примере EVESkey-схемы, сравнительно недавно предложенной китайскими учеными. Раздел 7 относится к методам передачи конфиденциальных ключевых данных по бесшумным дуплексным каналам с обратной связью типа Интернет. Раздел 8 подытоживает основные результаты настоящей работы.

2. Сценарий Вайнеровской концепции шумных каналов с отводом

Статья А. Вайнера [6] определила важное направление в теории, а, возможно, и на практике информационной безопасности. По нашему мнению, автора этой статьи А. Вайнера можно было бы смело назвать «Шенноном информационной безопасности». Действительно, К.Э. Шеннон в своей фундаментальной работе [13] впервые строго доказал, что существуют сколь угодно надежные методы передачи информации по каналам с помехами, причем достижимые не за счет тривиального уменьшения скорости передачи или увеличения отношения мощности сигнала к мощности шума, а за счет специальной обработки сигналов на передаче и приеме, т. е. кодирования и декодирования; к тому же существует максимальная скорость передачи, названная Шенноном *пропускной способностью канала связи.*

А. Вайнер доказал, что в каналах с отводом (т. е. с возможностью перехвата информации «оппонентами») существует такой метод кодирования / декодирования, который обеспечивает сколь угодную достоверность передачи информации по основному (легальному каналу) и сколь угодно малую утечку информации по отводному каналу. Им была также рассчитана максимально возможная при этом скорость передачи по основному каналу, названная им *секретной пропускной способностью.*

На рисунке 1 представлена блок-схема шумного канала связи с отводом и кодированием / декодированием по Вайнеру.

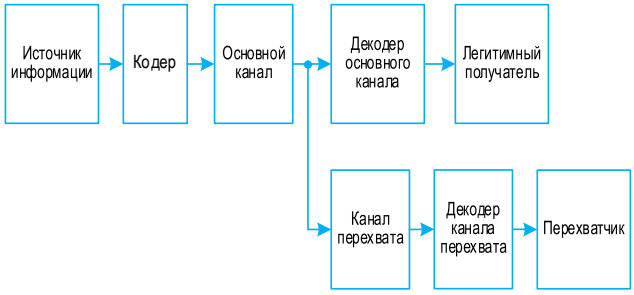

Рис. 1. Блок схема канала с отводом и кодированием / декодированием по Вайнеру

Fig. 1. Block-Scheme of Wire-Tap Channel with of Encoder / Decoder Due to Wyner

Основной особенностью канала, показанного на рисунке 1, является то, что канал перехвата всегда оказывается более шумным, чем основной канал. Поэтому его называют иногда *вырожденным каналом перехвата*.

На рисунке 2 представлена блок-схема Вайнеровской концепции с каналом перехвата, статистически независимым от основного канала, но с шумом, которая более приемлема для практики.

Не умаляя общности любых симметричных каналов без памяти в качестве основного и отводного каналов, рассмотрим далее двоичные симметрические каналы (ДСК), как из соображений большей простоты их рассмотрения, так и из-за частости их практического присутствия.

В работе [14], вскоре последовавшей после «пионерской» работы А. Вайнера [6], было доказано, что секретная пропускная способность C_s канала с отводом, показанном на рисунке 2, задается следующей формулой:

$$C_s = C_m - C_w, \qquad (1)$$

где C_m – шенноновская пропускная способность основного ДСК с вероятностью ошибки символа P_m: $C_m = 1 + P_m \log_2 P_m + (1 - P_m)\log_2 (1 - P_m)$; C_w – шенноновская пропускная способность отводного ДСК с вероятностью ошибок символа $P_w > P_m$: $C_w = 1 + P_w \log_2 P_w + (1 - P_w) \log_2 (1 - P_w)$.

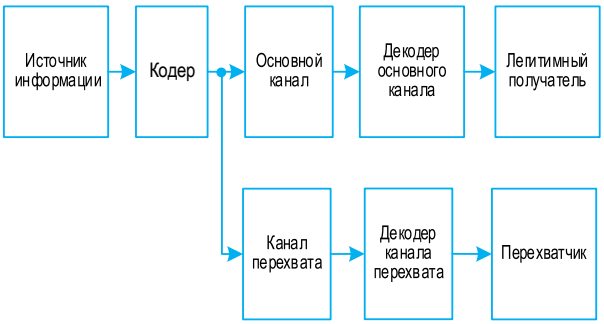

Рис. 2. Блок-схема с каналом перехвата, независимого по шумам от основного канала

Fig. 2. Block Scheme of Interception Channel Noisy Independent on the Main Channel

Если же отводной канал оказывается менее шумным, то есть $P_w < P_m$, то C_s нужно рассчитывать C_s по следующей формуле [14]:

$$C_s = h(P_m + P_w - 2P_m * P_w) - h(P_w), \qquad (2)$$

где $h(x) = x \log_2 x + (1 - x) \log_2 (1 - x)$.

При рассмотрении побочных каналов утечки информации (гальванических, оптических, вибрационных, электромагнитных) типичным является условие $P_w >> P_m$ и даже $P_m = 0$ (например, утечка по электромагнитным каналам от соединительных кабелей между выходом дешифратора и принтерами или мониторами). В этом случае формула (1) преобразуется к виду:

$$C_s = 1 - C_w. \qquad (3)$$

Важным отличием кодирования при помощи кодов с исправлением ошибок [16] от кодирования для концепции канала с отводом является то обстоятельство, что в последнем случае требуется рандомизация при помощи дополнительного шума. Такое кодирование в работе [15] было названо *кодовым зашумлением* (КЗ), которое может быть до-

статочно просто реализовано при помощи использования линейных блочных кодов и шумового генератора.

Пусть S – это двоичная информационная цепочка длиной k, подлежащая защите от перехвата при помощи технологии КЗ; γ – чисто случайная двоичная цепочка символов длиной $n-k$, получаемая от физического генератора шума; $V-(n,n-k)$ двоичный линейный код с длиной блока n и с числом информационных символов $n-k$; $c=f(\gamma)$ – проверочные символы кода V, полученные после кодирования цепочки γ. Тогда кодовый блок y для КЗ формируется следующим образом:

$$y=(x_1,x_2)=(\gamma, S \oplus c), \qquad (4)$$

где (x_1,x_2) – конкатенация цепочек x_1 и x_2; $\oplus$ – операция побитового сложения по mod2.

Легко видеть, что при отсутствии шума в основном канале $(P_m=0)$ сообщение $\check{S}$ восстанавливается без ошибок, т. е. $\check{S}=S$, как:

$$\check{S}= x_2 \oplus f(x_1). \qquad (5)$$

Основная теорема А. Вайнера утверждает, что в асимптотике, т. е. когда длина кодового блока $n\to\infty$ и выбран оптимальный код, максимальное количество информации, утекающее к перехватчику (т. е. пропускная способность канала утечки) $C_0=\max\limits_{s}(I(s;x)/k)$. На практике может интересовать и неасимптотика, когда $n<\infty$, и выбран какой-то конкретный линейный код V.

Точная формула для расчета этой величины C_0 была получена в работе [15]:

$$C_0=1+\frac{1}{k}\sum_{j=1}^{2^k}P(Vj)\log_2 P(Vj), \qquad (6)$$

где $P(V_j)=\sum_{i=1}^{n}N_{ij}P_w^i(1-P_w)^{n-i}$, N_{ij} – количество слов Хэммингова веса i в j-ом смежном классе стандартной расстановки V_n/V.

Расчет C_0 по формуле (6) осложняется тем обстоятельством, что коэффициенты N_{ij} (называемые обычно *спектром смежных классов кода V*) известны не для всех классов линейных кодов. Они известны для кодов: Хэмминга, БХЧ, исправляющих двухкратные ошибки, Голея, некоторых самодуальных, симплексных и кода Рида – Малера (см. подробности в работе [16]). К сожалению, расчет спектров для произвольных линейных кодов связан с экспоненциальными трудностями). Пример расчета C_0 по (6) для кода Голея – $(24,12)$, приведен в таблице 1 (см. также [17]). В последней строке этой таблицы показаны величины пропускной способности канала утечки $Co(P_w)$ без применения КЗ. Видно, что начиная с $P_w=5*10^{-2}$, использование КЗ демонстрирует его значительное преимущество.

ТАБЛИЦА 1. Результат расчета пропускной способности канала утечки C_0 при использовании в качестве КЗ линейного кода Голея – (24, 12) для различных вероятностей P_w

TABLE 1. Calculation of the Secrete Capacity C_0 for Goley Code – (24, 12) Given Different Probabliyties P_w

P_w	10^{-3}	10^{-2}	$5*10^{-2}$	10^{-1}	$2*10^{-1}$
C_0	0,977	0,838	0,458	0,156	$6{,}3*10^{-3}$
$C(P_w)$	≈ 1	0,91	0,72	0,53	0,28

Заметим, что использование КЗ для защиты от утечки по побочным каналам можно сочетать с такими традиционными средствами, как зашумление линий связи или окружающего аппаратуру пространства специальными шумовыми генераторами, экранировка кабелей и устройств, введение контролируемых зон и т. п. В этих случаях эффективность КЗ можно оценивать энергетическим выигрышем от его применения, который рассчитывается, как и для обычных систем связи:

$$\eta = 20\lg\frac{h_{\text{кз}}}{h}, \qquad (7)$$

где $h_{\text{кз}}$, h – отношение сигнал / шум с применением КЗ и без него, соответственно, для которых обеспечивается равная защищенность информации. В работе [17] показано, что для кодов с известными спектрами смежных классов, с защищенностью (в терминах пропускной способности) $C_0=10^{-3}$, энергетический выигрыш колеблется в пределах 20÷30 дБ, что даже превосходит энергетический выигрыш от применения некоторых кодов для обычного исправления ошибок в каналах связи.

Конечно, КЗ может использоваться не только для защиты от утечки по побочным каналам, но и – от перехвата информации по обычным каналам связи. Однако в этом случае зашумление основных каналов может оказаться даже больше, чем каналов перехвата. Для такого сценария У. Маурером был разработан специальный метод открытого обсуждения (PD, *аббр. от англ.* Public Discussion) [14]. Цель этой процедуры состоит в том, чтобы свести первоначальное условие $(P_m>P_w)$ к новому условию – $(P_m<P_w)$, но, конечно, без потери секретности передаваемой информации. Им же были предложены различные способы выполнения PD. Например, A передает к B каждый двоичный символ «S» раз, а B удерживает только такие S-блоки, в которых количество единиц (или нулей) оказывается больше некоторого заранее выбранного порога. Второй подход, также предложенный в [14], заключается в выполнении следующего интерактивного протокола между A и B.

Пусть E и D обозначают образцы ошибок в основном канале $(A\to B)$ и в канале перехвата $(A\to E)$, соответственно. Если A посылает B цепочку случайных бит X, то B принимает цепочку $Y=X+E$, а перехватчик – цепочку $Z=X+D$. Далее B посылает A

цепочку $W = Y + V$ по открытому каналу, где V – некоторая цепочка случайных бит, сгенерированных B. Наконец A вычисляет $W + X = V + E$, т. е. A принимает V с прежней битовой ошибкой P_m, тогда как E, приняв $Z = X + D$ и $W = X + E + V$, может лишь вычислить $Z + W = V + E + D$ с битовой ошибкой $P_m + P_w - 2\,P_m * P_w > P_w$.

Наконец, после выполнения процедуры PD, что обеспечивает выполнение условия $P_m < P_w$, легальные пользователи A и B могут исправить все ошибки в цепочке данных, которыми они, в конце концов, обменялись, а затем выполнить еще преобразование этих финальных данных, которое называется *усилением секретности* (PA, *аббр. от англ.* Privacy Amplification). PA представляет собой не что иное, как хеширование разделенной между A и B информации с использованием хеш-функции $h(..)$ из универсального класса, т. е.:

$$h(x) = [xxh]_k,$$

где x – умножение в конечном поле $GF(2^n)$, $x, h \in \in GF(2)^n)$; $[y]_k$ – удержание k наименьших значимых бит цепочки y.

В работе [18] доказана *обобщенная теорема усиления секретности*, которая дает верхнюю границу количества шенноновской информации, утекающей к перехватчику, после выполнения процедуры PA:

$$I_0 \leq \frac{2^{-(k-t_c-t-r)}}{\gamma \ln 2}, \qquad (8)$$

где k – полная длина цепочки, разделенная A и B после выполнения протокола PD; t_c – информация Реньи (или иначе – collision information), полученная E после перехвата цепочки x; t – финальная длина цепочки после выполнения протокола PA; r – количество проверочных символов, переданных от A к B для согласования их данных и переданных по открытому каналу; γ – коэффициент, приближающийся к 0,42, когда $k, k - t \to \infty$.

Для t_c справедлива следующая формула:

$$t_c = k(1 + \log_2(P_w{}^2 + (1 - P_w)^2)). \qquad (9)$$

Таким образом, если известна зашумленность основного (P_m) и отводного (P_w) каналов, то можно так выбрать параметры системы кодового зашумления, чтобы обеспечить утечку к перехватчику не более заданного наперед количества шенноновской информации и максимизировать, насколько это возможно, скорость передачи по основному каналу. Следует особо отметить, что перед выполнением протокола КЗ необходимо договориться между легитимными пользователями о надежном обеспечением их аутентификации. Более подробное описание протокола передачи информации в условиях активного перехвата (т. е. возможного навязывания перехватчиком ложной информации) можно найти в статье [19].

3. Коммутативное шифрование

Данный метод обеспечения информационной безопасности, при возможности дуплексного обмена информацией по каналам связи между пользователями, был впервые предложен А. Шамиром и описан в монографии [20]. Дальнейшее его исследование производилось в малодоступной для российских специалистов книге [21]. Поэтому приведем его в настоящем разделе с некоторыми «расширениями».

Пусть имеется шифр, обладающий свойством так называемого *коммутативного шифрования* (CE, *аббр. от англ.* Commutative Encryption). Заметим, что сам термин «коммутативное шифрование» не слишком укоренился в публикациях по тематике «криптография». Действительно, в почти 700-страничной книге [22] в разделе «Index» такой термин вообще отсутствует. Более того, в монографии [23] похожий термин «*некоммутативная криптография*» (non-commutative cryptography) означает совершенно другое, а именно использование некоммутативных (неабелевых) групп для построения несимметричных криптосистем.

Будем называть коммутативным шифрованием (КШ) любой алгоритм шифрования, если для него при любых ключах и любых сообщениях выполняется следующее условие:

$$f_{k_1}(f_{k2}(M)) = f_{k_2}(f_{k1}(M)), \qquad (10)$$

где $f_{k_1}(M)$ или $f_{k_2}(M)$ – алгоритм шифрования с использованием любых сообщений и любых ключей k_1, k_2.

На рисунке 3 показан протокол, который позволит пользователю A передать по бесшумному и открытому каналу связи другому пользователю B любое сообщение M, зашифрованное при помощи алгоритма КШ с выполнением следующих свойств:

– между корреспондентами A и B не требуется выполнения никакого предварительного протокола по обмену секретными ключами;

– стойкость данного протокола полностью эквивалентна стойкости исходной криптосистемы $f_k(M)$.

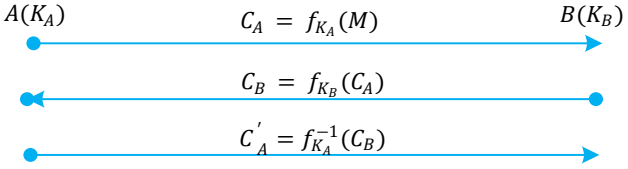

Рис. 3. Протокол передачи секретных сообщений при использовании КШ

Fig. 3. Protocol of Secret Message Transmission with the Use of CE

Действительно, первоначально A и B генерируют независимо свои ключи шифрования и дешифрования (они совпадают для симметричных криптосистем) и хранят их недоступными для посторонних пользователей. Далее они выполняют 3-шаговый протокол обмена по каналу, соединяющему A с B и B с A (т. е. такой канал должен между ними существовать). На первом шаге A передает B криптограмму, полученную им при использовании личного ключа K_A. Получив такую криптограмму C_A от A, пользователь B шифрует ее (как сообщение) своим личным ключом K_B и передает обратно пользователю A как криптограмму $C_B = f_{K_B}(C_A) = = f_{K_B}\left(f_{K_A}(M)\right)$.

Используя свойство коммутативности шифрования (10), получаем:

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

Тогда пользователь A может применять процедуру дешифрования на своем ключе дешифрования, соответствующему ключу шифрования, т. е. $f_{K_A}^{-1}(C_B)$.

После выполнения процедуры такого дешифрования A получает криптограмму C_A', которую и посылает B на третьем шаге протокола:

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

Тогда B тривиально применяет к полученной криптограмме C_A' процедуру дешифрования $f_{K_B}^{-1}(C_A')$ на ключе дешифрования, соответствующему своему ключу шифрования K_B, что дает окончательное выражение:

$$f_{K_B}^{-1}(C_A') = f_{K_B}^{-1}(f_{K_B}(M)) = M,$$

что и требовалось доказать.

Однако пока остается открытым вопрос – какие из известных симметричных (или несимметричных) шифров обладают свойством коммутативности (10)? Прежде всего заметим, что такие популярные симметричные блоковые шифры как DES, S-DES, 3-DES, ГОСТ-89, ГОСТ-2015, AES, (См. [9]), очевидно, не являются КШ. Докажем далее, что таким свойством обладает несимметричный шифр Райвеста – Шамира – Адлемана (РША).

Шифр РША задается следующими параметрами:
p, q – различные простые числа (генерируются случайно);
$n = p * q$ – модуль алгоритма;
$\varphi = (p-1)(q-1)$ – функция Эйлера.

Ключ шифрования e генерируется случайным образом, но он должен удовлетворять условию: $1 \le e < \varphi, gcd(e, \varphi) = 1$, где $gcd(a, b)$ означает *наибольший общий делитель* чисел a и b; ключ дешифрования $d = e^{-1} \bmod n$.

Сообщение M, подвергающееся шифрованию, должно быть целым положительным числом в диапазоне: $1 \le M \le n - 1$. Процедура шифрования РША имеет вид: $E = M^e \bmod n$.

Тогда условие (10) принадлежности РША к классу СЕ будет иметь вид:

$$(M^{e1} \bmod n)^{e2} \bmod n = (M^{e2} \bmod n)^{e1} \bmod n. \qquad (11)$$

Очевидно, предполагается, что все модули в (11) совпадают.

Используя в (11) коммутативность возведения целых чисел в степень по любому модулю и коммутативность их произведения, получим в левой части (11):

$$(M^{e1} \bmod n)^{e2} \bmod n = M_3^{e1*e2} \bmod n = M^{e2*e1} \bmod n.$$

Для правой части (11) аналогично будем иметь:

$$(M^{e2} \bmod n)^{e1} \bmod n = M^{e2*e1} \bmod n.$$

Видно, что левая и правая части (11) одинаковы, и, следовательно, шифр РША принадлежит к классу КШ. Проиллюстрируем выполнение условия (11) для шифра РША простейшим примером. Пусть параметры РША заданы как: $p = 3$, $q = 5$, $n = 15$, $M = 5$, $e_1 = 3$, $e_2 = 5$. Тогда легко убедиться, используя обычные операции по модулю, что обе части (11) оказываются равными 8, и, следовательно, условие (10) выполняется.

Рассмотрим теперь пример другой несимметричной криптосистемы – Рабина [9]. Она имеет следующие параметры: p, q – различные простые числа, которые играют роль секретного ключа дешифрования $n = p * q$ (открытый ключ шифрования). Сообщение M представляется целым положительным числом в диапазоне $0 \le M \le n - 1$. Алгоритм шифрования имеет вид: $E = M^2 \bmod n$. Данная криптосистема имеет следующую особенность по сравнению с РША – стойкость взлома этой криптосистемы строго эквивалентна задаче факторизации целых чисел, т. е. нахождению множителей p, q при заданном n; такие криптосистемы принято называть *доказуемо стойкими*. Таким образом, если найден алгоритм факторизации целых чисел с полиномиальной сложностью от длины ключа, это означает, что найден алгоритм взлома (нахождение секретного ключа) криптосистемы Рабина, и, наоборот (что особенно важно!) – если удается как-то взломать криптосистему Рабина с полиномиальной сложностью от длины ключа, то это означает, что найдется и алгоритм факторизации целых чисел с полиномиальной сложностью от их разрядности. (Заметим, что таким свойством не обладает криптосистема РША). Однако, к сожалению, шифр Рабина не принадлежит к классу КШ, что доказывается следующим простым примером.

Свойство СЕ для данной криптосистемы можно записать следующим образом:

$$(M^2 \bmod n_1)^2 \bmod n_2 = (M^2 \bmod n_2)^2 \bmod n_1 \quad (12)$$

Выберем следующие параметры криптосистемы Рабина: $p_1 = 3$, $q_1 = 5$, $n_1 = 15$, $p_2 = 11$, $q_2 = 7$, $n_2 = 77$, $M = 5$. Подставляя эти параметры в (12), получим, что левая часть (12) равна 23, а правая – 10. Это доказывает, что шифр Рабина не принадлежит к КШ.

В первой части настоящей статьи отмечалось, что появление квантовых компьютеров (КК) создает опасность как для симметричных, так и для несимметричных криптосистем, и, в частности, для шифров РША, стойкость которых зависела от возможности полиномиально-сложного решения задачи дискретного логарифмирования или факторизации чисел. Поэтому появился целый класс так называемых *постквантовых* криптосистем, т. е. таких, которые не могут быть взломаны даже при практическом появлении КК. Первым представителем такого класса явилась криптосистема Мак-Элиса [9].

Покажем далее, что криптосистема Мак-Элиса, к сожалению, не использует шифры, относящиеся к классу КШ.

Процедура шифрования для криптосистемы Мак-Элиса описывается следующим образом:

$$E = M\tilde{G} \oplus Z,$$

где M – столбец сообщений длиной «K»; $\tilde{G} = SGP$ – матрица размерности $K \times n$, которая является открытым ключом шифра Мак-Элиса; S – случайная, несингулярная $K \times K$ матрица; G – случайная порождающая матрица Гоппа кода [9]; P – случайная $n \times n$ перестановочная матрица; Z – случайный двоичный вектор длины n и заданного веса t.

Матрицы S, G, P являются секретным ключом дешифрования криптосистемы Мак-Элиса.

Заметим, что алгоритм шифрования этой криптосистемы является *рандомизационным*, поскольку вектор Z выбирается случайно и не входит в состав ключей криптосистемы Мак-Элиса.

Для того, чтобы шифр Мак-Элиса был бы коммутативным, он должен удовлетворять условию (10), которое для данной криптосистемы принимает следующий вид:

$$f_{k1}(f_{k2}(M)) = \left(M\tilde{G}_2 \oplus Z_2\right)\tilde{G}_1 \oplus Z_1 = \\ = M\tilde{G}_2\tilde{G}_1 \oplus Z_2\tilde{G}_1 \oplus Z_1, \quad (13)$$

$$f_{k2}(f_{k1}(M)) = \left(M\tilde{G}_1 \oplus Z_1\right)\tilde{G}_2 \oplus Z_2 = \\ M\tilde{G}_1\tilde{G}_2 \oplus Z_1\tilde{G}_2 \oplus Z_2. \quad (14)$$

Легко видеть, что правые числа в (13) и (14) не совпадают, поскольку $Z_1 \neq Z_2$. Ввиду этого шифр Мак-Элиса не принадлежит к классу коммутативных криптосистем.

Рассмотрим следующее несимметрическое шифрование на предмет его принадлежности к КШ – это шифр, построенный на *цифровых решетках*. Как известно [24], один из популярных вариантов такого шифра, с аббревиатурой LWE (*аббр. от англ.* Learning With Errors; *перев. на русск.* обучение с ошибками), имеет следующий алгоритм шифрования:

$$\bar{u} = A^{\mathrm{T}}\bar{a},\ \bar{c} = P^{\mathrm{T}}a + f(v) \in Z_q^n x Z_q^l,$$

т. е. криптограмма такой криптосистемы состоит из двух цепочек с целочисленными координатами общей длиной $n + l$, тогда как сообщение $v \in Z_q^n$ – таким образом, вообще невозможно с ее помощью производить повторное шифрование. Поэтому шифр LWE не принадлежит к классу КШ.

Сравнительно недавно был предложен такой новый класс криптосистем с открытым ключом, как *некоммутативная криптография* [23]. Однако решено было не менять заголовок настоящего раздела статьи, несмотря на его очевидную формальную схожесть с упомянутым выше термином, тем более, что у них имеется и очевидное различие. Действительно, КШ относится лишь к возможности перестановки ключей при двойном шифровании, тогда как термин «некоммутативная криптография» относится ко всей структуре криптосистем, базирующейся на некоммутативности определенных неабелевых групп, использующихся при построении всей криптосистемы.

Интересно отметить, что потоковые шифры являются коммутативными! Действительно, условие (10) для них тривиально выполняется:

$$M \oplus \gamma(K_1)) \oplus \gamma(K_2) = (M \oplus \gamma(K_2)) \oplus \gamma(K_1),$$

где $\oplus$ – операция побитового сложения по mod2; $\gamma(k)$ – двоичные гаммы, как функции секретных ключей.

Протокол передачи секретной информации без предварительного обмена секретными ключами, представленный на рисунке 3, для потоковых шифров имеет вид, показанный на рисунке 4.

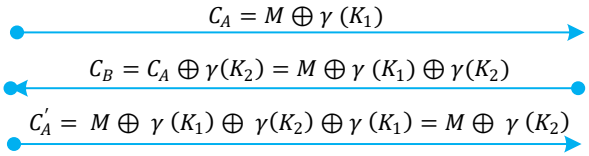

Рис. 4. Протокол, использующий КШ для потоковых шифров

Fig. 4. Protocol Using CE with Stream Ciphers

Однако из схемы (см. рисунок 4) видно, что перехватчик, побитно складывая по mod2 двоичные последовательности C_B и C_A', получает:

$$C_B \oplus C'_A = M \oplus \gamma(K_1) \oplus \gamma(K_2) \oplus M \oplus \gamma(K_2) = \gamma(K_1). \quad (15)$$

Затем перехватчик, складывая отдельно принятую им последовательность C_A и последовательность, которая была им вычислена по (15), дешифрует сообщение M:

$$M \oplus \gamma(K_1) \oplus \gamma(K_1) = M,$$

без всякого взлома гаммы потокового шифра...

Таким образом, для потокового шифра, даже при его коммутативности, протокол, представленный на рисунке 3, не работает, что объясняется линейностью для него процедуры шифрования.

Из всего вышеизложенного, можно сделать важное заключение, которое составляет одну приведенную далее проблему криптографии – доказать (или опровергнуть) утверждение, что существует постквантовый коммутативный шифр.

Поясним, однако, важно ли, вообще, заниматься решением этой проблемы? Это будет следовать из понимания того, имеет ли протокол, показанный на рисунке 3, существенное преимущество на практике. Для этого необходимо уточнить положительные и отрицательные свойства данного протокола. Поскольку пока не найдено ни одной симметричной криптосистемы, которая была бы также и коммутативной, т. е. удовлетворяла бы условию (10), то рассмотрим особенности использования КШ для несимметричных шифров.

Основное преимущество КШ состоит в том, что в этом случае не требуется никакой предварительной передачи ключей по каналам связи, в частности и открытых ключей, как, например, для КШ РША. Это может восприниматься, как дополнительный фактор повышения секретности. Важно подчеркнуть, что как КШ, так и не КШ, требуют защиты от *атак имперсонализации* активного злоумышленника, что, в свою очередь, нуждается в использовании методов аутентификации. Действительно, если такой злоумышленник выдаст себя за легитимного пользователя B и выполнит под видом B второй шаг протокола, показанного на рисунке 4, то ничего не подозревающий пользователь A , выполнит третий шаг протокола, предоставив злоумышленнику возможность просто расшифровать сообщение M , предназначенное A для легитимного пользователя B. Однако для КШ требуется *идентификация пользователей*, а для обычных несимметричных криптосистем шифрования сообщений требуется *аутентификация открытых ключей.* В этом и состоит преимущество КШ перед криптосистемами шифрования с открытыми ключами.(Собственно говоря, здесь атака имперсонизации ничем не отличается от подобной атаки при выполнении протокола распределения ключей Диффи – Хеллмана [9]).

4. Протокол Дина и Голдсмит передачи секретной информации по каналам с замираниями без предварительного обмена ключами

Криптосистема, предложенная Дином и Голдсмит [25], также принадлежит к классу *физически секретного уровня* (см. в [12] – «Physual layer security»), поскольку секретность передаваемых сообщений обеспечивается для нее естественными физическими свойствами канала связи без всякого использования шифрования / дешифрования и распределения ключей. Однако она может быть реализована не для любого канала связи, причем даже и с естественными шумами, но лишь для каналов связи с замираниями и с использованием технологии MIMO (*аббр. от англ.* Multiple-Input, Multiple-Output; *досл. перев. на русск.* множественный вход, множественный выход, по сути – это метод пространственного кодирования сигнала). Реально это соответствует использованию множества управляемых антенн на передаче и на приеме, а также при размещении легитимных пользователей и перехватчика в различных (и не совпадающих) точках пространства, что приводит к различным статистическим характеристикам каналов передачи, подвергающимся случайным изменениям.

Предположим сначала, что количество приемных антенн легитимных пользователей n_r и перехватчика n'_r одинаково (впоследствии это ограничение будет снято).

Пусть легитимный канал связи от корреспондента A к корреспонденту B описывается следующим выражением:

$$z = Ay + E, \quad (16)$$

где $A \in R^{n\times n}$ – матрица, описывающая канал связи $A \to B$; $z \in R^n$ – вектор сигнала, принимаемого B; $y \in R^n$ – вектор сигнала, переданного A; $E \in R^n$ – вектор аддитивного шума у B.

Предполагается также, что E – это гауссовские $i.i.d.$ векторы с параметрами $N(O, \sigma_E^2)$; элементы матрицы $A - (a_{ij})$, $i = (1, n)$, $j = (1, n)$ $i.i.d.$ – гауссовские $N(O, \sigma^2)$ величины.

Аналогичный (по структуре) канал перехвата $A \to E$ описывается выражением:

$$z' = By + E', \quad (17)$$

которое отличается от выражения (16) A лишь матрицей B и параметрами $\tilde{\sigma}_\varepsilon^2$ и $\tilde{\sigma}_w^2$.

Принятые для моделей каналов условия являются весьма важными и состоят в следующем:

– параметры каналов постоянны в течение выполнения процедур кодирования и декодирования;

– матрица A известна в точности легитимным пользователям;

– матрица A и B в точности известны перехватчику E.

В соответствии с [25] кодирование сообщения пользователем A выполняется следующим образом:

$$Y = Vx, \tag{18}$$

где $V \in R^{n\times n}$ – ортогональная матрица, взятая из SVD (*аббр. от англ.* Singular Value Decomposition; *перев. на русск.* сингулярное разложение), $A = USV^T$. Здесь $x \in R^n$ – вектор с двоичными координатами.

Декодирование легитимным пользователем B выполняется в два этапа. Первый этап – преддекодирование:

$$\begin{aligned} z' &= U^T z = U^T A y \\ +e' &= U^T U S V^T V x + U^T e = Sx + e', \end{aligned} \tag{19}$$

где $U \in R^{n\times n}$ – ортогональная матрица, взятая B из SVD-разложения матрицы A.

Поскольку S – диагональная матрица (по определению SVD), то на втором этапе декодирование B выполняет процедуру:

$$x' = \underset{x_i}{\operatorname{argmin}} |z_i - x_i\, S_i|,\ i = (1, n). \tag{20}$$

Из выражения (20) видно, что декодирование для легитимного пользователя B имеет линейную сложность в зависимости от параметра n.

По предположению авторов статьи [25], перехватчик E может повторить стратегию декодирования легитимного пользователя B, т. е.:

$$z'' = U^T Z'. \tag{21}$$

Тогда

$$z'' = U^T B y + E'' = U^T S' V'^T V x + e''. \tag{22}$$

где U', V', S' – матрица из SVD-разложения матрицы B.

Наконец, запишем (22) следующим образом:

$$z'' = Cx + e'', \tag{23}$$

где $C = S'V'^T V$.

Однако, поскольку матрица C не диагональна, то в этом случае оптимальное декодирование принимает вид:

$$x' = \underset{x_i}{\operatorname{argmin}} \|z'' - Cx_i\|, \tag{24}$$

где $||*||$ – евклидова норма в R^n.

Решение задачи (24) известно, как трудная CVP-проблема, и в [25] доказано, что она имеет экспоненциальную сложность от параметра n, если выполняется следующее (довольно очевидное) условие:

$$\sigma_w^2 * \tilde{\sigma}_e^2 > n^{\frac{1}{2}}.$$

Поэтому авторы статьи [25] сделали вывод, что предложенная ими криптосистема является стойкой, по крайней мере, если элементы матриц A и B являются взаимно независимыми случайными величинами. Это же условие обеспечивается, в свою очередь, при выполнении другого условия, когда расстояние от расположения легитимных пользователей A и B до перехватчика оказывается не меньше, чем несколько длин волн радиоканала $A \to B$.

Однако авторы статьи [25] не учли того обстоятельства, что перехватчик не обязательно должен следовать протоколу декодирования легитимных пользователей.

В работе [21] было предложено использовать следующий субоптимальный алгоритм декодирования при довольно вероятном условии, что матрица C из (24) окажется несингулярной:

$$C^{-1} z'' = x + C^{-1}\tilde{e}. \tag{25}$$

Из выражения (25) видно, что тогда процедура декодирования перехватчиком E принимает следующий вид:

$$x' = \underset{x_i}{\operatorname{argmin}} |\tilde{z}_i - x_i|, i = (z, n). \tag{26}$$

где $\tilde{z}_i$ – это i-я координата вектора $C^{-1}z''$.

Очевидно, что алгоритм декодирования по (26) имеет линейную сложность от параметра n, и тогда эффективность субоптимального декодирования можно будет оценить сравнением вероятности ошибки бита при оптимальном декодировании по (24) и субоптимального декодирования по (26).

В таблице 2 представлены результаты расчетов полученные в [21] для вероятностей ошибки P при оптимальном декодировании по (24) и при субоптимальном декодировании P' по (26) при «типичных» параметрах каналов связи $A \to B$ и $A \to E$.

ТАБЛИЦА 2. Результаты моделирования P и P' для типичных наборов параметров каналов $A \to B$ и $A \to E$

TABLE 2. Simulation Results of P and P 'for Typical Channel Parameters A → B and A → E

Наборы параметров	Для легитимных пользователей (P)	Для перехватчика (P')
$\sigma^2 = \sigma_w^2 = 2;\ \sigma_E^2 = \tilde{\sigma}_e^2 = 1;\ n = 100$	0,02	0,2
$\sigma^2 = \sigma_w^2 = 4;\ \sigma_E^2 = \tilde{\sigma}_e^2 = 8;\ n = 100$	0,037	0,3
$\sigma^2 = \sigma_w^2 = 1;\ \sigma_E^2 = \tilde{\sigma}_e^2 = 30;\ n = 100$	0,02	0,42
$\sigma^2 = 2; \sigma_w^2 = 1; \sigma_E^2 > \tilde{\sigma}_e^2 = 4;\ n = 1000$	$5{,}6 \cdot 10^{-3}$	0,3
$\sigma^2 = 4; \sigma_w^2 = 8; \sigma_E^2 = \tilde{\sigma}_e^2 = 12;\ n = 1000$	0,01	0,33

Таблица 2 показывает, что оптимальный алгоритм (24) дает вполне приемлемые результаты по вероятности ошибки символа, в то время как подоптимальный – приводит к недопустимо большим вероятностям ошибок. Более того, в работе

[21] строго доказано, что, даже используя избыточность сообщений (например, смысловой текст), его окажется невозможно восстановить с высокой надежностью.

Однако возникает очевидный вопрос – сохранится ли данное утверждение, если количество приемных антенн n_r' в MIMO-системе связи для перехватчика оказывается больше, чем количество приемных антенн n_r легитимной линии связи? Такое исследование было проведено в работе [21], и его результаты приведены в таблице 3, причем матрица C, получаемая при подоптимальном декодировании, теперь уже оказывается не квадратной, а прямоугольной, и поэтому для ее обращения (т. е. нахождения обратной матрицы C^{-1}) используется известный *алгоритм Мура – Пенроуза* [26].

ТАБЛИЦА 3. Результаты моделирования оптимального и подоптимального алгоритмов декодирования для параметров $n_r' > n_r$, $n_r = 100$

TABLE. 3 .Simulation Results of Optimal and Suboptimal Decoding Algorithms with Parameters: $n_r' > n_r$, $n_r = 100$

n_r'	100	101	102	103	105	107	108	109	110	120	150
P'	0,31	0,22	0,16	0,12	0,07	0,048	6,039	0,03	0,024	0,003	$7 \cdot 10^{-4}$

По результатам таблицы 3 можно сделать неожиданный вывод, что даже небольшое увеличение числа приемных антенн перехватчика создает возможность «взлома» данной криптосистемы.

В работе [27] было предложено изменить матрицу предкодирования V на матрицу A^{-1}, обратную матрице канала $A \to B$. Однако это приводит к требованию значительного увеличения мощности передаваемого сигнала для пользователя A (см. таблицу 5 в работе [21]). Кроме того, как отмечено в той же работе, неточность измерения матриц A и B легитимными пользователями приводит к значительному увеличению вероятностей ошибок в основном канале (см. таблицу 6 в работе [21]).

В заключение описания метода Дина и Голдсмит, можно высказать мнение, что, хотя дальнейшее теоретическое изучение этого метода представляет определенный интерес, особенно в направлении улучшения алгоритма преддекодирования, однако, с точки зрения практического применения, он представляется сомнительным. Тем более, что не всегда легитимным пользователям удается тщательно следить за изменениями характеристик канала связи $A \to E$.

5. Обеспечение секретности передачи ключевых данных в многолучевых каналах связи за счет использования антенн с управляемыми диаграммами направленности

Результаты по данному направлению были впервые получены японскими авторами и опубликованы в статье [28]. Значительное уточнение основных результатов и условий обеспечения секретности передачи ключевой информации (в терминах шенноновского количества информации) представлено в работе [29].

В настоящей статье будет описана модель, использованная для передачи ключевой информации, и сформулированы возможные направления исследований, поскольку, насколько нам известно, несмотря на многочисленные публикации по теории антенн с управляемой диаграммой направленности (VDA, *аббр. от англ.* Variable Directional Antenna), данная технология не развивалась российскими исследователями для обеспечения секретности передачи ключевых данных, а только лишь для повышения надежности радиосвязи в многолучевых каналах.

Схема передачи ключевых данных в условиях возможного их перехвата, на основе технологии VDA, приведена на рисунке 5.

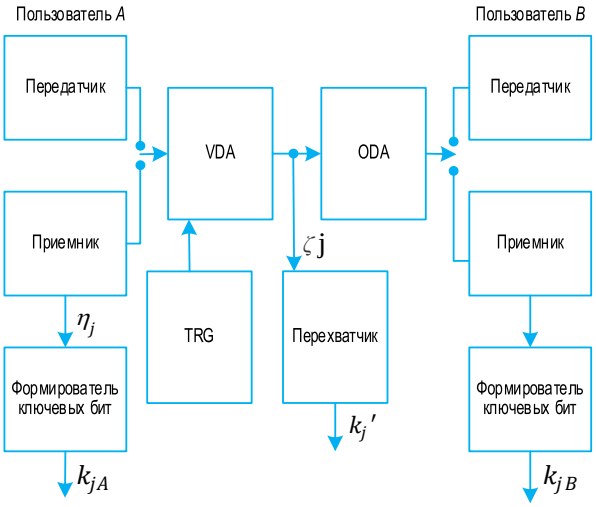

Рис. 5. Схема системы связи для передачи ключевых данных при использовании технологии VDA

Fig. 5. Block Scheme of Communication System for Key Transmission under the Use of VDA Technology

Протокол распределения ключевых данных описывается следующими шагами.

<u>*Шаг 1*</u>. Пользователь A формирует управляемую диаграмму направленности (VDA), используя чисто случайный генератор (TRG, *аббр. от англ.* Truly Random Generator) и фиксирует (запоминает) ее в течение временно́го интервала передачи (T) j-го ключевого бита.

<u>*Шаг 2*</u>. A передает B гармонический сигнал $S_j(\mathrm{t}) = \cos\omega_0 t$, $0 \le t \le T/2$ по многолучевому каналу.

<u>*Шаг 3*</u>. B принимает гармонический сигнал от всенаправленной антенны (ODA, *аббр. от англ.* Omni Directional Antenna) на интервале $(0, {}^{T}/_{2})$ и формирует ключевой бит, вычисляя выбранный функционал (амплитуду или фазу) сигнала.

Шаг 4. *B* также переключает свою ODA в режим передачи и передает тот же самый гармонический сигнал на интервале $T/2 \le t \le T$.

Шаг 5. Пользователь *A* подключает свою VDA (с сохраненной диаграммой направленности антенны) к приемнику и обрабатывает полученный сигнал также, как и *B*, выделяя *j*-й ключевой бит.

Шаг 6. *A* и *B* повторяют шаги 1–5 *n* раз с различными выходами генератора, чтобы создать желаемое число разделенных бит ключа между *A* и *B*.

Вследствие справедливости теоремы обратимости распространения радиоволн, ключевые последовательности пользователей *A* и *B* должны совпадать с точностью до шумов их приемников.

Поэтому сигналы, разделенные *A* и *B*, а также *A* и *E* будут иметь вид, соответственно:

$$y_j(t) = \sum_{i=1}^{m} v_{ij}\beta_{ij}\cos(\omega_{0t} + \theta_{ij}), \qquad (27)$$

$$z_j(t) = \sum_{i=1}^{m} v'_{ij}\,\beta'_{ij}\cos(\omega_{0t} + \theta'_{ij}), \qquad (28)$$

где *i* – *i*-й луч канала связи; *m* – общее количество лучей канала связи; β_{ij} – коэффициенты усиления каналов; v_{ij} – коэффициенты усиления VDA; θ_{ij} – фазовый сдвиг, включающий как фазу в антенной диаграмме, так и фазовый сдвиг в *i*-ом луче; штрихи над символами относятся к каналу перехвата.

В работе [29] было показано, что величины η_j и ζ_i могут быть достаточно хорошо аппроксимированы гауссовскими, а вероятность ошибки P_e между легитимными пользователями *A* и *B* и перехватчиком *E*, для функционалов выделения фаз сигналов, может быть представлена следующей формулой:

$$P_e = \frac{1}{\pi}\arctan\left(\frac{\sqrt{1-\rho^2}}{\rho}\right), \qquad (29)$$

где ρ – коэффициент корреляции между случайными величинами η_j и ζ_j.

На рисунке 6 представлена зависимость *Pe* от ρ. Интересно отметить, что вопреки нашей интуиции, вероятность расхождения бит ключа для легитимных пользователей и перехватчика, равная 0,1, может достигаться даже при коэффициенте корреляции $\rho \approx 0{,}95$!

Для существенного уменьшения утечки информации к перехватчику может быть использована процедура усиления секретности, подробно описанная в Разделе 2. Напомним, что формула для вычисления величины утечки информации к перехватчику в этом случае (т. е. для бесшумного основного канала) имеет вид:

$$I_0 \le \frac{-(k - t_c - t - r)}{\gamma_1 \ln 2}.$$

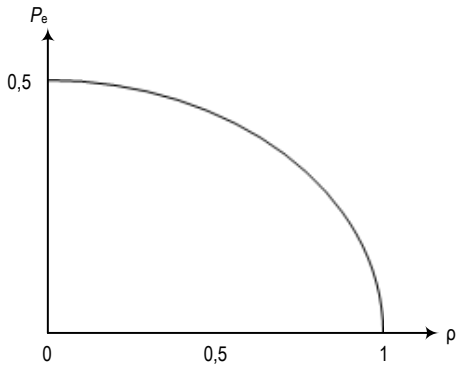

Рис. 6. Зависимость вероятности ошибки P_e от коэффициента корреляции ρ

Fig. 6. The Error Probability P_e versus Correlation Coefficient ρ

Параметры, входящие в формулу для I_0, описаны в формуле (8), где P_w, однако, вычисляется здесь по формуле (29).

При помощи теоретических расчетов и имитационного моделирования в работе [29] было показано, что метод, использующий VDA для распределения ключевых данных в многолучевом канале, при оптимизации параметров, позволяет обеспечить достаточно надежное распределение ключевых бит при малой утечке информации (по Шеннону) к перехватчику. Причем даже если канал перехвата является бесшумным, однако три следующих условия оказываются совершенно необходимыми для этого:

– хорошие свойства случайного генератора шума;

– наличие не менее двух лучей в канале с замираниями, как для основного, так и для канала перехвата;

– достаточная удаленность легитимных пользователей *A* и *B* от перехватчика *E*.

Заметим, однако, что эффективность рассмотренного метода зависит не только от расстояния между легитимными пользователями, но и от точного расположения последнего (*E*) относительно них.

6. Взлом криптосистемы EVESkey

В отличие от предыдущих, данный раздел поясняет необходимость тщательного анализа бесключевых систем современной криптографии с точки зрения их безопасности и невозможности присутствия различных побочных каналов, позволяющих обойти утверждение авторов об идеальной секретности предложенных ими бесключевых криптосистем. Типичным примером с таким пессимистичным сценарием является так называемая EVESkey-схема, предложенная в работе [30], которая характеризуется ее авторами, как абсолютно секретная. На рисунке 7 представлен сценарий, соответствующий данной схеме.

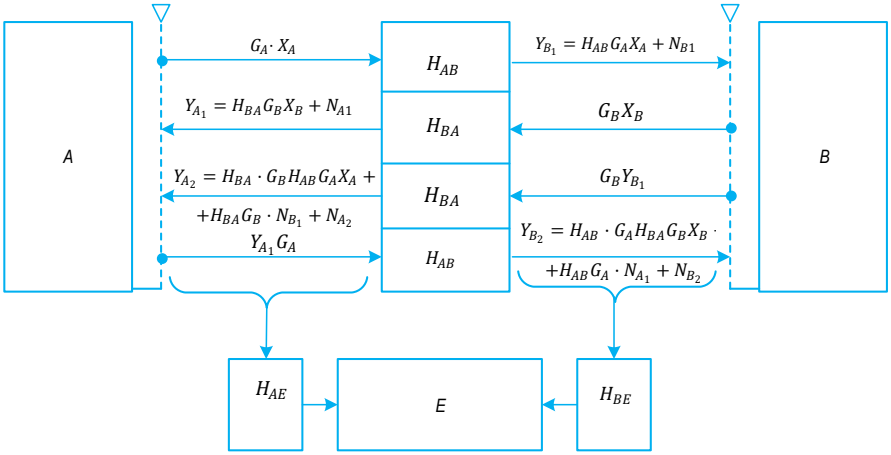

Fig. 7. Сценарий протокола для EVESkey-схемы

Fig. 7. Scenario of the Protocol for EVESkey-Scheme

Как видно из этой схемы, A и B генерируют случайные унитарные матрицы $X_A, X_B \in C^{n\times n}$, где n – количество антенн, использующихся этими пользователями), а также матрицы Дженибра [26] $G_A, G_B \in C^{n\times n}$. Матрицы H_{AB} и H_{BA} являются $n \times n$ передаточными матрицами каналов $A \to B$, $B \to A$, соответственно, а их элементы моделируются как взаимно независимые гауссовские величины $N(0,1)$.

Матрицы N_A, N_B положим $n \times n$ – матрицами аддитивного шума с элементами $N(0, \sigma^2)$.

Для упрощения доказательства введем вспомогательные матрицы $P = H_{BA}G_B$ и $Q = H_{AB}\,G_A$.

Тогда PQ и QP могут быть оценены легитимными пользователями как:

$$PQ = Y_{A2}(X_A)^{-1};\ QP = Y_{B2}(X_B)^{-1}. \qquad (30)$$

Из алгебры хорошо известно, что любые матрицы PQ и QP имеют одинаковые характеристические полиномы (CP, *аббр. от англ.* Characteristic Polynomials), т. е.:

$$CP(PQ) = CP(QP). \qquad (31)$$

Из равенства (31), очевидно, следует, что легитимные пользователи A и B, получая оценки матриц Y_{A2} и Y_{B2} и имея в своем распоряжении матрицы X_A и X_B, могут легко восстанавливать матрицы PQ и QP, соответственно, а затем, вычислив из CP собственные числа $EV(PQ)$ и $EV(QP)$ этих матриц и проквантовав их, получить с большой вероятностью совпадающие ключевые биты. В то же время перехватчик E не обладает знанием матриц X_A или X_B и поэтому не может воспользоваться одним из равенств (30), чтобы затем найти ключевые биты и после проквантовать $EV\,(QP)$ и $EV\,(PQ)$.

Покажем, однако, что протокол вычисления, описанный выше, может быть взломан, если не следовать строго протоколу, предписанному легитимным пользователям, а воспользоваться лишь теми данными, которые перехватчик сможет получить, наблюдая его выполнение легитимными пользователями, правда в предположении, что аддитивные шумы легитимных пользователей A, B и перехватчика E отсутствуют.

Тогда E (см. рисунок 7) сможет вычислить следующие матрицы:

$$\tilde{Y}_{A1} = H_{BE}G_BX_B, \tilde{Y}_{A2} = H_{BE}G_BH_{AB}G_AX_A,$$
$$\tilde{Y}_{B1} = H_{AE}G_AX_A, \tilde{Y}_{B2} = H_{AE}G_AH_{BA}G_BX_B. \qquad (32)$$

Докажем далее два утверждения.

Утверждение 1

Для всех стоящих в левых частях выражения (32) случайных матриц (в общем случае и для прямоугольных матриц) существует псевдообратная матрица Мура – Пенроуза $(\gamma_p)^{-1}$ с вероятностью единица.

Доказательство

Действительно, положим H – $n \times n$ матрица с комплексными элементами $N(0,1)$, которые взаимно независимы.

Тогда совместная плотность вероятности такой матрицы будет иметь вид:

$$f(H) = (2\pi)^{-n^2} \exp\left(-\frac{1}{2}Tr(H \times H^T)\right), \qquad (33)$$

где Tr (.) – след матрицы.

Вырожденные матрицы, у которых $detH = 0$ образуют $2n^2 - 2$ размерное многообразие, которое будучи несингулярным, обеспечивает нулевую вероятность для $detH = 0$. Таким образом, вероятность того, что $detH \neq 0$, будет равна единице. Подобные матрицы остаются обратимыми и будучи умноженными на унитарные матрицы G, X.

Утверждение 2

Обозначим через $EV(Y)$ множество собственных чисел матрицы Y. Тогда:

$$EV(Y) = EV(PQ) = EV(QP), \quad (34)$$

где

$$Y = \tilde{Y}_{A2}(\tilde{Y}_{B1})^{-1}\tilde{Y}_{B2}(\tilde{Y}_{A1})^{-1}. \quad (35)$$

Доказательство

Подставляя (32) в (35), получим:

$$Y = (H_{BE}G_B)QP(H_{BE}G_B)^{-1}.$$

Последнее выражение означает, что матрица Y подобна матрице QP, и тогда $EV(Y) = EV(QP)$ для любых матриц H_{BE}. Поэтому, вычислив $EV(Y)$, где Y находится по (35) и (32), перехватчик E находит ключевые биты, распределенные по данному протоколу A и B. Что и требовалось доказать.

Хотя ранее предполагалось, что все каналы передачи информации считаются бесшумными, но дополнительные расчеты показали, что и при не слишком больших мощностях шума вероятность битовых ключевых ошибок легитимных пользователей оказывается достаточно близкой к вероятности ошибки ключевых бит перехватчика E, выполняющего протокол, используя (34) и (35). Из этого следует, что схему распределения ключей EVESKey нельзя считать секретной. Интересно отметить, что авторы настоящего исследования посылали в журнал, где ранее опубликовали статью [30], материал, полностью компрометирующий EVESkey-схему, однако редакторы этого журнала, ссылаясь на дополнительные комментарии рецензентов, отказались опубликовать наше опровержение.

Подводя итоги различным методам бесключевой криптографии, описанным в разделах 2–6 настоящей работы, можно заметить, что все они требуют выполнения некоторых условий, относящихся к перехватчику.

Для удобства пояснения, все они сведены в таблицу 4, их которой видно, что требования зависят от возможностей перехватчика и сведений о его канале, что не всегда позволяет их выполнить. (Тем более, что они могут иногда скрытно изменяться). Поэтому возникает проблема – разработать протокол распределения ключей по постоянным, открытым и бесшумным каналам связи (типа Интернет). Попытка ее решения была предпринята в нескольких работах авторов настоящей статьи, и к обсуждению этих работ мы сейчас и переходим.

ТАБЛИЦА 4. Условия выполнимости секретных протоколов передачи данных по открытым каналам связи между легитимными пользователями методами бесключевой криптографии

TABLE 4. Conditions of Secret Data Transmission Availability over Communication Channels between Legitimate Users by the Means of Keyless Cryptography

Вайнеровская концепция отводного канала связи	Коммутативное шифрование	Протокол Дина и Голдсмит	Использование антенн с управляемой диаграммой
Необходимо знание, по крайней мере, мощности шума в канале перехвата, которая не должна быть менее определенного порога	Пока известна лишь одна такая криптосистема – РША, которая не является, однако, постквантовой	Необходимо выполнение условия, что количество антенн перехватчика в сценарии MIMO не превосходит количества антенн легитимных пользователей, использующих такой же сценарий MIMO	Необходимо использовать антенну с управляемой диаграммой направленности, а канал передачи должен иметь не менее 2-х лучей и случайное затухание сигналов

7. Протокол распределения крипто ключей, использующий постоянные, открытые и бесшумные каналы связи (типа Интернет)

В работе [31] был описан протокол распределения ключей, выполняемый по постоянному, открытому и бесшумному двоичному каналу связи при помощи передачи двоичных последовательностей. Схема такого протокола приведена на рисунке 8.

Как видно из рисунка 8, A и B предварительно генерируют чисто случайные двоичные последовательности δ_A, γ_A и δ_B, γ_B, соответственно, а затем обмениваются ими по каналам $A \to B, B \to A$ и генерируют предварительные ключи:

$$\tilde{K}_A = \delta_A \oplus \delta_B \oplus \gamma_B,\ \tilde{K}_B = \delta_B \oplus \delta_A \oplus \gamma_A,$$

где $\oplus$ – операция побитового сложения по mod2.

Перехватчик E вырабатывает подобный предварительный ключ:

$$\tilde{K}_E = \delta_A \oplus \delta_B \oplus \gamma_A \oplus \gamma_B.$$

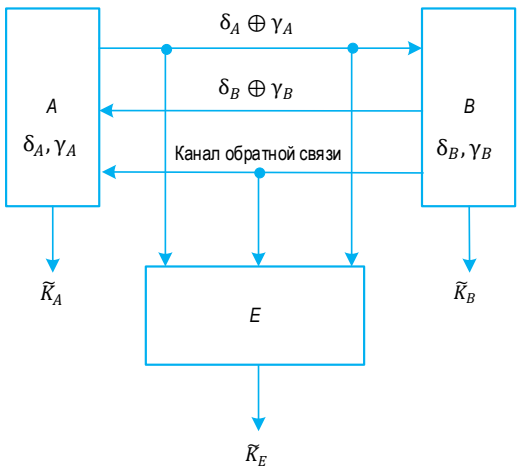

Рис. 8. Протокол распределения ключей с использованием обмена информации по двоичному бесшумному каналу

Fig. 8. Key Sharing Protocol with the Use of Information Exchange over Binary Noiseless Channel

Далее A и B используют для обеспечения хорошей статистики финального ключа γ дополнительную схему, приведенную на рисунке 9. Как видно из этой схемы, в качестве общего ключа между легитимными пользователями принимается последовательность γ, которая для B искажается шумом $\gamma_A \oplus \gamma_B$, а для E – шумом γ_B.

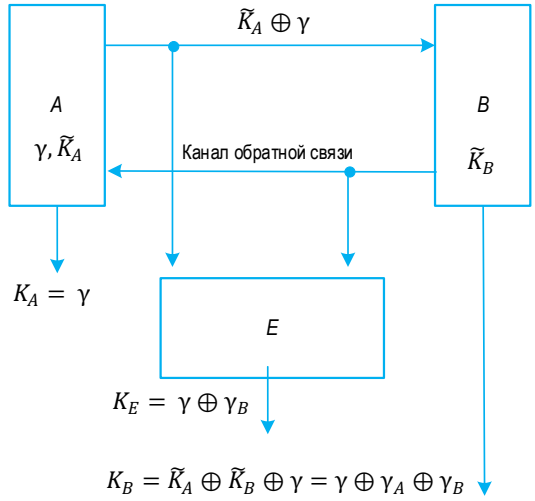

Рис. 9. Дополнительная схема для выработки финального ключа между *A* и *B*

Fig. 9. Additional Scheme for Elaboration of the Final Key between A and B

Схема на рисунке 9 эквивалентна схеме, приведенной на рисунке 10. В [32] схема, подобная приведенной на рисунке 10, названа *каналом с отводом при деградации основного канала.*

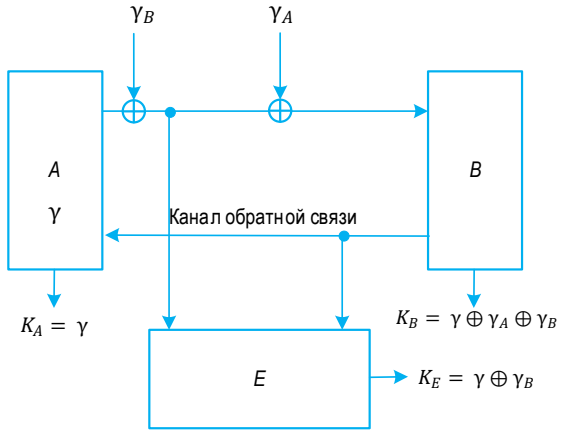

Рис. 10. Эквивалентная схема для схемы на рисунке 9

Fig. 10. Equivalent Scheme for the Scheme Shown in Fig,9

Более того, в той же работе [32] строго доказано, что для такой модели *секретная пропускная способность* $C_S = 0$. (Напомним, что по определению, данному в [14], секретной пропускной способностью, в терминах шенноновской информации, называется пропускная способность основного канала при обеспечении сколь угодно малой утечки по каналу с отводом). Это означает, что не существует никаких схем кодирования и декодирования, которые бы для данной модели обеспечили надежную передачу информации (в нашем случае ключевой) между легитимными пользователями при отсутствии утечки к перехватчику.

Рассмотрим другой протокол распределения ключей, который показан на рисунке 11, где обмен между легитимными пользователями осуществляется случайными вещественными числами.

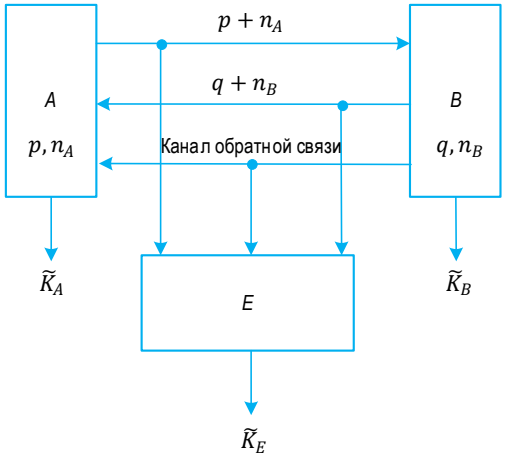

Рис. 11. Протокол распределения ключей при обмене по каналам связи вещественными числами

Fig. 11. Key Sharing Protocol for Communication Channel Exchange by Real Numbers

Предположим, что все случайные вещественные числа являются гауссовскими, взаимно независимыми, имеют нулевые матожидания, а дисперсии (вариации):

$$Var(p) = Var(q) = 1, Var(n_A) = Var(n_B) = \sigma^2.$$

После обмена по протоколу, показанному на рисунке 11, легитимные пользователи A и B формируют свои ключи по следующему правилу:

$$K_A = rect\big(p(q + n_B)\big),\ K_B = rect(q(p + n_A), \quad (36)$$

где «+» – обычное арифметическое сложение, а $rect(x) = \begin{cases} 0, \text{при } x \geq 0 \\ 1, \text{при } x < 0 \end{cases}$

Перехватчик E должен сформировать свой ключ, следуя выражению:

$$K_E = rect\big((p + n_A)(q + n_B)\big). \quad (37)$$

Используя легко доказываемое равенство:

$$rect(ab) = rect(a) \oplus rect(b),$$

где $\oplus$ – сложение по mod 2.

Схему, показанную на рисунке 11, можно заменить на схему, приведенную на рисунке 12, где все ключи вычисляются по правилам:

$$\begin{aligned} K_A &= rect(p) \oplus rect(q + n_B), \\ K_B &= rect(p + n_A) \oplus rect(q), \\ K_E &= rect(p + n_A) \oplus rect(q + n_B). \end{aligned} \quad (38)$$

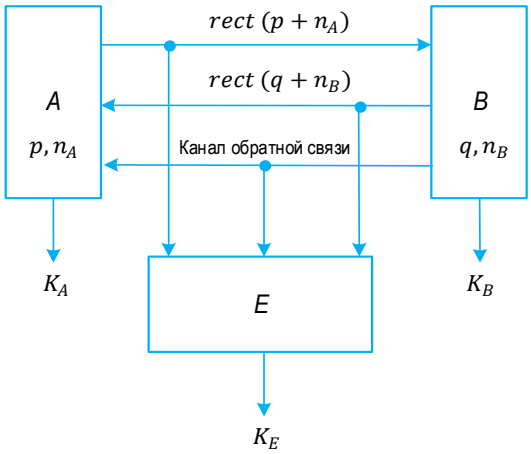

Рис. 12. Схема эквивалентная схеме на рисунке 11

Fig. 12. Scheme that is Equivalent to the Scheme in Fig.11

Найдем теперь аддитивные шумы между A и B (ε_{AB}) и между A и E (ε_{AE}):

$$\varepsilon_{AB} = K_A \oplus K_B = rect(p) \oplus rect(q + n_B) \oplus \oplus rect(p + n_A) \oplus rect(q),$$

$$\varepsilon_{AE} = K_A \oplus K_E = rect(p) \oplus rect(q) \oplus \oplus rect(p + n_A) \oplus rect(q + n_B) = = rect(p) \oplus rect(p + n_A). \quad (38)$$

Из (38) и (39) видно, что схема, приведенная на рисунке 12, будет эквивалентна схеме (см. рисунок 10), если в последней заменить γ_B и γ_A, соответственно, на:

$$rect(P) \oplus rect(P + n_A),\ rect(q) \oplus rect(q + n_B).$$

Но это означает, что схема на рисунке 12 согласуется со сценарием канала с отводом и деградацией основного канала. Тогда, как уже отмечалось при рассмотрении схемы на рисунке 8, в соответствии с результатами работы [32], мы получили и для схемы на рисунке 11 секретную пропускную способность $C_s = 0$, и, следовательно, выполнение по ней секретного протокола распределения ключей сказывается невозможным.

В работе [33] рассмотрен протокол при обмене между легитимными пользователями многомерными векторами с вещественными координатами. Однако мы не будем подробно рассматривать этот случай, поскольку для него не удалось строго доказать, что $C_s = 0$. Тем не менее, представляется, что это весьма вероятно, так как после применения этого протокола при моделировании не удалось получить необходимые условия для возможности применения теоремы усиления секретности, поскольку сохранилось прежнее неравенство: $P_m > P_w$, где P_m – вероятность битовой ошибки в основном канале; P_w – то же самое, но для канала перехвата.

Обратимся, наконец, к наиболее перспективному случаю, когда протокол выполняется при помощи обмена случайными матрицами, как это показано на рисунке 13. (Не умаляя общности, рассматриваем только квадратные матрицы, поскольку, по авторскому мнению, это не сможет существенно повлиять на фактор секретности протокола в терминах утечки к перехватчику определенного количества шенноновской информации).

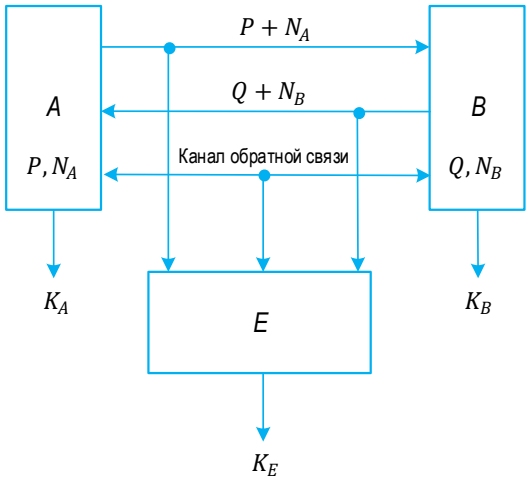

Рис. 13. KSP при обмене квадратными матрицами

Fig. 13. KSP under Square Matrices Exchange

Итак, пусть P, Q, N_A, N_B – $n \times n$ матрицы с гауссовскими взаимно независимыми элементами. Тогда, после выполнения протокола по схеме на рисунке 13 ключи легитимных пользователей A и B, а также перехватчика E вычисляются следующим образом:

$$K_A = rect(tr(P(Q + N_B))),$$
$$K_B = rect(tr(Q(P + N_A))),$$
$$K_E = rect\ (tr((P + N_A)(Q + N_b)),$$

где $tr(X)$ – след матрицы X (т. е. сумма ее диагональных элементов).

Заметим, что вместо функционала $tr(X)$ можно использовать и другие преобразования элементов матрицы. Так, в работе [31] были использованы $EV(X)$, т. е. собственные числа матриц (конечно, также с последующим их квантованием). В этой же работе было выполнено моделирование полного KSP и получены следующие обнадеживающие результаты: после применения LPDC-кодов и процедуры усиления секретности вероятность ошибочного приема хотя бы одного символа ключевого блока длиной 24039 бит оказалась равной $P_{ed} \approx \approx 2{,}5 \cdot 10^{-3}$, а утечка в этом блоке к перехватчику соответствовала $I_0 \approx 1{,}4 \cdot 10^{-3}$ бита. (Аналогичные по порядку результаты были получены и при выборе функционала tr вместо EV). Казалось бы, проблему распределения ключей по постоянному и бесшумному каналу можно считать полностью решенной, но это не так…

Дело в том, что до сих пор мы рассматривали обработку сигналов перехватчиком, как *жесткое декодирование*, т. е. при квантовании следов матриц

или их собственных чисел, на два уровня, которые сопоставляются двум битам – 0 и 1. Однако возможно и так называемое *мягкое декодирование* или квантование tr, EV или результатов применения других функционалов на $L > 2$ уровней! При этом перехватчик E может провести предобработку сигналов, т. е. составить специальную таблицу декодирования еще до получения результатов обмена данными между A и B. Пример такой таблицы представлен в работе [33]. Там же было произведено имитационное моделирование и всего соответствующего матричного протокола. Оно показало, что при оптимизации параметров квантования и декодирования перехватчик E получает преимущество перед легитимными пользователями, т. е. выполнение условия $P_w > P_m$, что не позволяет в дальнейшем, используя процедуру усиления секретности, обеспечить требуемую малую утечку информации при надежной передаче бит ключа от A к B. Конечно, составление таблицы предобработки требует значительно бóльшей сложности и / или бóльшего времени обработки, чем простое двоичное квантование. Поэтому подобный метод распределения ключей допустим лишь для легитимных пользователей не слишком высокого ранга, когда можно надеяться на жесткие ограничения сложности обработки сигнала перехватчиками. Более того, легитимные пользователи могут также заменить жесткое декодирование при обмене на мягкое, и тогда есть надежда, что в соревновании по сложности обработки, зависящем от числа уровней квантования, у них будет преимущество перед перехватчиком (см. также далее выводы, сформулированные в «Заключении»).

8. Заключение

В начале XX-го века Д. Гильберт сформулировал 23 математические проблемы, 16 из которых к настоящему времени уже решены в значительной степени, предопределив этим самым дальнейшее развитие математики. Заметим, что, в любой отрасли науки (физике, химии, биологии, а сейчас и в безопасности передачи цифровой информации), существуют свои, конечно, значительно меньшего масштаба проблемы, чем у «королевы наук» – математики. Однако их разрешение (или его невозможность его – см. труды К. Геделя) являются весьма важными для дальнейшего развития науки в данной отрасли – криптографии. Поэтому, отнюдь не претендуя по масштабу на «глобальность», по сравнению с проблемами Д. Гильберта, все же рискнем (по материалам обеих частей настоящей статьи) сформулировать весьма важные, по авторскому мнению, но, конечно, не единственные в области информационной безопасности, проблемы.

Во-первых, верхняя граница возможности использования одного и того же ключа шифрования без утечки информации к перехватчику для неидеального шифра (см. Часть 1).

Во-вторых, построение какой-либо постквантовой ассиметричной и коммутативной (в нашем смысле) криптосистемы (см. Раздел 3 Части 2);

В-третьих, вычисление секретной пропускной способности протокола распределения ключей при обмене информацией по постоянному, открытому и бесшумному каналу (см. Раздел 7 Части 2). Если окажется, что $C_S \neq 0$, – то остается проблема нахождения конструктивных методов кодирования и декодирования для такого сценария.

Список источников

1. 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

2. Korzhik V. Keyless cryptography // Proceedings of the 9th International Conference on System Administration, Networking and Security (Orlando, USA). 2000.

3. Korzhik V., Bakin M. Information-theoretical Secure Keyless intensification // Proceedings of the 2000 IEEE International Symposium on Information Theory (Sorrento, Italy, 25–30 June 2000). Piscataway: IEEE Press, 2000. DOI:10.1109/ISIT.2000.866310

4. Korzhik V. Keyless cryptography // Invited Talk at Security Seminar at CERIAS Purdue University. 2001.

5. Mukherjee A., Fakoorian S.A.A., Huang J., Swindlehurst A.L. Principles of Physical Layer Security in Multiuser Wireless Network A. Survey // IEEE Communications Surveys & Tutorials. 2014. Vol. 16. Iss. 3. PP. 1550–1573. DOI:10.1109/SURV.2014.012314.00178

6. Wyner A.D. The Wire-tap channel // Bell System Technical Journal. 1975. Vol. 54. Iss. 8. PP. 1355–1387. DOI:10.1002/j.1538-7305.1975.tb02040.x

7. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. Experimental quantum cryptography // Journal of Cryptology. 1992. Vol. 5. PP. 3–28. DOI:10.1007/BF00191318

8. Кушнир Д.В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам. Автореф. дис. канд. техн. наук. СПб.: СПбГУТ, 1996. 16 с. EDN:ZJDTTT

9. Коржик В.И., Яковлев В.А. Основы криптографии. СПб.: Интермедия, 2016. 296 с. EDN:WEQWMN

10. Korzhik V., Kushnir D. Key sharing based on the wire-tap channel type ii concept with noisy main channel // Proceedings of the International Conference on the Theory and Applications of Crypotology and Information Security (ASIACRYPT '96, Kyongju, Korea, 3–7 November 1996). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1996. Vol. 1163. PP. 210–217. DOI:10.1007/BFb0034848

11. Liu Y., Zhang W.J., Jiang C., Chen J.P., Zhang C., Pan W.X., et al. Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance // Physical Review Letters. 2023. Vol. 130. P. 210801. DOI:10.1103/PhysRevLett.130.210801

12. Milov M., Pham T.M., Chorti A., Barreto A.N., Fettweis G. Physical Layer Security – From Theory to Practice // IEEE BITS the Information Theory Magazine. 2023. Vol. 3. Iss. 2. PP. 67–79. DOI:10.1109/MBITS.2023.3338569

13. Шеннон К.Э. Работы по теории информации и кибернетике. М.: Издательство иностранной литературы, 1963. 829 с.

14. Maurer U.M. Secret key agreement by public discussion based on common information // IEEE Transactions on Information Theory. 1993. Vol. 39. Iss. 3. PP. 733–742. DOI:10.1109/18.256484

15. Коржик В.И., Яковлев В.А. Неасимптотическая оценка эффективности кодового зашумления в каналах с отводом // Проблемы передачи информации. 1991. № 4. С. 223–228.

16. Петерсон У., Уэлнод Э. Коды, исправленные ошибки. М.: Мир, 1976.

17. Коржик В.И., Яковлев В.А. Защита информации от утечки за счет побочных электромагнитных излучений и наводок на основе способа кодового зашумления // Информатика и вычислительная техника. 1993. Т. 8. № 1-2. С. 61–66.

18. Korzhik V., Morales-Luna G., Balakirsky V.B. Privacy amplification 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. Berlin, Heidelberg: Springer, 2001. Vol. 2200. PP. 18–26. DOI:10.1007/3-540-45439-X_2

19. Yakovlev V., Korzhik V., Morales Luna G. Key Distribution Protocol Based on Noisy Channels in Presence of Active Adversary // IEEE Transactions on Information Theory. 2008. Vol. 54. Iss. 6. PP. 2535–2550. DOI:10.1109/TIT.2008.921689

20. Шнайер Б. Прикладная криптография. М.: Триумф, 2002.

21. Korzhik V., Starostin V., Yakovlev V., Kabardov M., Krasov A., Adadurov S. Advance in Keyless Cryptography. Chapter 6 // In: Ramakrishnan S. (ed.) Lightweight Cryptographic Techniques and Cybersecurity Approaches. 2022. PP. 97–117. DOI:10.5772/intechopen.104429

22. Tilborg H.C.A. Encyclopedia of Cryptography and Security. Springer, 2005.

23. Myasnikov A.G., Shpilrain V., Ushakov A. Non-commutative Cryptography and Group-theoretic Problems. American Mathematical Society, 2011. 385 p.

24. Goldreich O., Goldwasser S., Halevi S. Public-key cryptosystems from Lattice reduction problems // Proceedings of the 17th Annual International Cryptology Conference (CRYPTO '97, Santa Barbara, USA, 17–21 August 1997). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1997. Vol. 1294. PP. 112–131. DOI:10.1007/BFb0052231

25. Dean T., Goldsmith Aj. Physical layer cryptography through massive MIMO // Proceedings of the 2013 IEEE Information Theory Workshop (ITW, 9–13 September 2013, Seville, Spain). Piscataway: IEEE, 2013. PP. 1–3. DOI:10.1109/ITW.2013.6691222

26. Ben-Israel A., Greville T.N.E. Generalized Inverses: Theory and Applications. Springer, 2003.

27. Steinfeld R., Sakzad A. On massive MIMO physical layer cryptosystems // Proceedings of IEEE Information Theory Workshop – Fall (ITW, Jeju, Korea (South), 11–15 October 2015). IEEE, 2015. PP. 292–296. DOI:10.1109/ITWF.2015.7360782

28. Aono T., Higuchi K., Ohira T., Komiyama B., Sasaoka H. Wireless secret key generation exploiting reactance-domain scalar response of multipath fadiny cannels // IEEE Transactions on Antennas and Propagation. 2005. Vol. 53. Iss. 11. PP. 3776–3784. DOI:10.1109/TAP.2005.858853

29. Korzhik V., Yakovlev V., Kovajkin Y. Secret Key Agreement Over Multipath Channels Exploiting a Variable-Directional Antenna // International Journal of Advanced Computer Science and Applications. 2012. Vol. 3. Iss. 1. PP. 172–178.

30. Qin D., Ding Z. Exploiting Multi Antenna Non-Reciprocal Channels for Share Secret Key Generation // IEEE Transactions on Information Forensics and Security. 2016. Vol. 11. Iss. 12. PP. 2691–2705. DOI:10.1109/TIFS.2016.2594143

31. Yakovlev V., Korzhik V., Starostin V., Lapshin A. Channel Traffic Minimizing Key Sharing Protocol Intended for the Use over the Internet and Secure without any Cryptographic Assumptions // Proceedings of the 32nd Conference of Open Innovations Association FRUCT (Tampere, Finland, 9–11 November 2022). FRUCT 32, 2022. PP. 300–307. DOI:10.23919/FRUCT56874.2022.9953895

32. Lai E., Gamal H.El., Poor H.V. The Wiretap Channel with Feedback Encryption over the Cannel // IEEE Transactions on Information Theory. 2008. Vol. 54. Iss. 11. PP. 5059–5067. DOI:10.1109/TIT.2008.929914

33. Korzhik V., Yakovlev V., Starostin V., Lapshin A. Vulnerability of the Key Sharing Protocol Executing over the Noiseless Public Cannels with Feedback // Proceedings of the 35th Conference of Open Innovations Association FRUCT-35 (Tampere, Finland, 24–26 April 2024). FRUCT-35, 2024. PP. 374–379 DOI:10.23919/FRUCT61870.2024.10516344

References

1. 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

2. Korzhik V. Keyless cryptography. *Proceedings of the 9th International Conference on System Administration, Networking and Security, Orlando, USA*. 2000

3. Korzhik V., Bakin M. Information-theoretical Secure Keyless intensification. *Proceedings of the 2000 IEEE International Symposium on Information Theory, 25–30 June 2000, Sorrento, Italy*. Piscataway: IEEE Press; 2000. DOI:10.1109/ISIT.2000.866310

4. Korzhik V. Keyless cryptography. *Invited Talk at Security Seminar at CERIAS Purdue University*. 2001

5. Mukherjee A., Fakoorian S.A.A., Huang J., Swindlehurst A.L. Principles of Physical Layer Security in Multiuser Wireless Network A. Survey. *IEEE Communications Surveys & Tutorials*. 2014;16(3):1550–1573. DOI:10.1109/SURV.2014.012314.00178

6. Wyner A.D. The Wire-tap channel. *Bell System Technical Journal*. 1975;54(8):1355–1387. DOI:10.1002/j.1538-7305.1975.tb02040.x

7. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. Experimental quantum cryptography. *Journal of Cryptology*. 1992;5:3–28. DOI:10.1007/BF00191318

8. Kushnir D.V. *Research and Development of Methods of Confidential Data Distribution on Quanto Channels*. PhD Thesis. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 1996. (in Russ.)

9. Korzhik V.I., Yakovlev V.A. Fundamentals of Cryptology St. Petersburg: Intermediia Publ.; 2016. 296 p. (in Russ.) EDN:WEQWMN

10. Korzhik V., Kushnir D. Key sharing based on the wire-tap channel type ii concept with noisy main channel // Proceedings of the International Conference on the Theory and Applications of Crypotology and Information Security, ASIACRYPT '96, 3–7 November 1996, Kyongju, Korea. Lecture Notes in Computer Science, vol.1163. Berlin, Heidelberg: Springer; 1996. p.210–217. DOI:10.1007/BFb0034848

11. Liu Y., Zhang W.J., Jiang C., Chen J.P., Zhang C., Pan W.X., et al. Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance. *Physical Review Letters*. 2023;130:210801. DOI:10.1103/PhysRevLett.130.210801

12. Milov M., Pham T.M., Chorti A., Barreto A.N., Fettweis G. Physical Layer Security – From Theory to Practice. *IEEE BITS the Information Theory Magazine*. 2023;3(2):67–79. DOI:10.1109/MBITS.2023.3338569

13. Shannon K.E. *Works on Information Theory and Cybernetics*. Moscow: Foreign Literature Publ.; 1963. 829 p. (in Russ.)

14. Maurer U.M. Secret key agreement by public discussion based on common information. *IEEE Transactions on Information Theory*. 1993;39(3):733–742. DOI:10.1109/18.256484

15. Korzhik V.I., Yakovlev V.A. Non-asymptotic estimation of the efficiency of coded noise cancellation in channels with diversion. *Problems of Information Transmission.* 1991;4:223–228. (in Russ.)

16. Peterson W., Welnod E. *Codes, Fixed Errors*. Moscow: Mir Publ.; 1976. (in Russ.)

17. Korzhik V.I., Yakovlev V.A. Information protection from leakage due to side electromagnetic radiation and interference based on the code noise method. *Informatika i vychislitelnaia tekhnika*. 1993;8(1-2):61–66. (in Russ.)

18. Korzhik V., Morales-Luna G., Balakirsky V.B. Privacy amplification 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, vol.2200*. Berlin, Heidelberg: Springer; 2001. p.18–26. DOI:10.1007/3-540-45439-X_2

19. Yakovlev V., Korzhik V. Key Distribution Protocol Based on Noisy Channels in Presence of Active Adversary. *IEEE Transactions on Information Theory*. 2008;54(6):2535–2550. DOI:10.1109/TIT.2008.921689

20. Schneier B. *Applied Cryptography*. Moscow: Triumf Publ.; 2002. (in Russ.)

21. Korzhik V., Starostin V., Yakovlev V., Kabardov M., Krasov A., Adadurov S. Advance in Keyless Cryptography. Chapter 6. *In: Ramakrishnan S. (ed.) Lightweight Cryptographic Techniques and Cybersecurity Approaches*. 2022. p.97–117. DOI:10.5772/intechopen.104429

22. Tilborg H.C.A. *Encyclopedia of Cryptography and Security*. Springer, 2005.

23. Myasnikov A.G., Shpilrain V., Ushakov A. *Non-commutative Cryptography and Group-theoretic Problems*. American Mathematical Society; 2011. 385 p.

24. Goldreich O., Goldwasser S., Halevi S. Public-key cryptosystems from Lattice reduction problems. *Proceedings of the 17th Annual International Cryptology Conference, CRYPTO '97, 17–21 August 1997, Santa Barbara, USA. Lecture Notes in Computer Science, vol.1294*. Berlin, Heidelberg: Springer; 1997. p.112–131. DOI:10.1007/BFb0052231

25. Dean T., Goldsmith Aj. Physical layer cryptography through massive MIMO. *Proceedings of the 2013 IEEE Information Theory Workshop, ITW, Seville, Spain, 9–13 September 2013*. Piscataway: IEEE; 2013. p.1–3. DOI:10.1109/ITW.2013.6691222

26. Ben-Israel A., Greville T.N.E. *Generalized Inverses: Theory and Applications*. Springer; 2003.

27. Steinfeld R., Sakzad A. On massive MIMO physical layer cryptosystems. *Proceedings of IEEE Information Theory Workshop – Fall, ITW, 11–15 October 2015, Jeju, Korea (South)*. IEEE; 2015. p.292–296. DOI:10.1109/ITWF.2015.7360782

28. Aono T., Higuchi K., Ohira T., Komiyama B., Sasaoka H. Wireless secret key generation exploiting reactance-domain scalar response of multipath fadiny cannels. *IEEE Transactions on Antennas and Propagation*. 2005;53(11):3776–3784. DOI:10.1109/TAP.2005.858853

29. Korzhik V., Yakovlev V., Kovajkin Y. Secret Key Agreement Over Multipath Channels Exploiting a Variable-Directional Antenna. *International Journal of Advanced Computer Science and Applications*. 2012;3(1):172–178.

30. Qin D., Ding Z. Exploiting Multi Antenna Non-Reciprocal Channels for Share Secret Key Generation. *IEEE Transactions on Information Forensics and Security*. 2016;11(12):2691–2705. DOI:10.1109/TIFS.2016.2594143

31. Yakovlev V., Korzhik V., Starostin V., Lapshin A. Channel Traffic Minimizing Key Sharing Protocol Intended for the Use over the Internet and Secure without any Cryptographic Assumptions. *Proceedings of the 32nd Conference of Open Innovations Association FRUCT, 9–11 November 2022, Tampere, Finland*. FRUCT-32; 2022. p.300–307. DOI:10.23919/FRUCT56874.2022.9953895

32. Lai E., Gamal H.El., Poor H.V. The Wiretap Channel with Feedback Encryption over the Cannel. *IEEE Transactions on Information Theory*. 2008;54(11):5059–5067. DOI:10.1109/TIT.2008.929914

33. Korzhik V., Yakovlev V., Starostin V., Lapshin A. Vulnerability of the Key Sharing Protocol Executing over the Noiseless Public Cannels with Feedback. *Proceedings of the 35th Conference of Open Innovations Association FRUCT-35, 24–26 April 2024, Tampere, Finland*. FRUCT Oy; 2024. p.374–379 DOI:10.23919/FRUCT61870.2024.10516344

Статья поступила в редакцию 29.10.2024; одобрена после рецензирования 21.11.2024; принята к публикации 09.12.2024.
The article was submitted 29.10.2024; approved after reviewing 21.11.2024; accepted for publication 09.12.2024.

Информация об авторах:

КОРЖИК Валерий Иванович
доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0002-8347-6527

ЯКОВЛЕВ Виктор Алексеевич
доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0009-0007-2861-9605

СТАРОСТИН Владимир Сергеевич
кандидат физико-математических наук, доцент, доцент кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0009-0000-2939-1971

БУЙНЕВИЧ Михаил Викторович
доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России
https://orcid.org/0000-0001-8146-0022

Коржик В.И. и Буйневич М.В. являются членами редакционного совета журнала «Труды учебных заведений связи» с 2016 г., но не имеют никакого отношения к решению опубликовать эту статью. Статья прошла принятую в журнале процедуру рецензирования. Об иных конфликтах интересов авторы не заявляли.

Korzhik V.I. and Buinevich M.V. have been a members of the journal "Proceedings of Telecommunication Universities" Editorial Council since 2016, but have nothing to do with the decision to publish this article. The article has passed the review procedure accepted in the journal. The authors have not declared any other conflicts of interest.