Научная статья
УДК 004.056(075.58)
https://doi.org/10.31854/1813-324X-2025-11-6-101-107
EDN:UPSBCH

Криптосистема и протокол передачи конфиденциальных данных без предварительного распределения закрытых и открытых ключей на основе использования процедуры коммутативного шифрования

Валерий Иванович Коржик ✉, korzhik.vi@ sut.ru
Виктор Алексеевич Яковлев, yakovlev.va@sut.ru
Владимир Сергеевич Старостин, starostin.vs@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация

Коммутативное шифрование, предложенное ранее А. Шамиром и опубликованное около 30 лет назад в монографии Б. Шнайера «Прикладная криптография», не нашло практического применения из-за отсутствия известных стойких шифров, обладающих свойством коммутативности. В настоящей работе подтверждается, что такие известные шифры, как AES, ГОСТ-2015, шифры Эль-Гамаля и Мак-Элиса, действительно таким свойством не обладают. Однако авторам удалось построить некоторую модификацию шифра РША, которая при использовании новой версии протокола позволяет обмениваться конфиденциальной информацией безо всякого предварительного распределения между легальными пользователями как открытых, так и секретных ключей шифрования. В этом заключается ***актуальность*** *настоящей работы, поскольку, как правило, необходимость предварительного распределения секретных ключей в симметричных или ключей шифрования в асимметричных криптосистемах и является узким местом при создании конфиденциальных систем цифровой связи. Хотя такие черты схожи со свойствами так называемых криптосистем с открытым ключом, однако, в отличие от них, предлагаемая криптосистема может использовать одинаковые открытые ключи для неограниченного количества пользователей. Такие ключи можно сделать общедоступными, поместив их, например, в облако. Именно это свойство предлагаемой криптосистемы отражает* ***новизну*** *подхода, так как до сих пор не описана ни одна криптосистема, где не требовалось бы предварительное распределение ключей. Данное свойство оказывается полезным для некоторых сценариев обмена конфиденциальными данными, например, такими, как передача паролей и широковещательной информации. В первом случае речь идет об аутентификации пользователей некоторым сервером. Если у него в базе данных хранятся секретные пароли всех пользователей, то аутентификация производится лишь при предъявлении соответствующих паролей. В то же время канал связи, используемый для этого, может быть перехвачен активным злоумышленником, однако предлагаемая схема предотвращает разглашение паролей. Другим* ***практическим результатом*** *новой криптосистемы является его применение в шировещательных каналах связи, если необходимо минимизировать количество используемых ключей шифрования.*

Ключевые слова: *коммутативное шифрование, криптосистемы с открытым ключом, шифр РША, вычислительно сложные задачи, широковещательная информация*

Ссылка для цитирования: Коржик В.И., Яковлев В.А., Старостин В.С. Криптосистема и протокол передачи конфиденциальных данных без предварительного распределения закрытых и открытых ключей на основе использования процедуры коммутативного шифрования // Труды учебных заведений связи. 2025. Т. 11. № 6. С. 101–107. DOI:10.31854/1813-324X-2025-11-6-101-107. EDN:UPSBCH

Original research
https://doi.org/10.31854/1813-324X-2025-11-6-101-107
EDN:UPSBCH

Cryptosystem and Protocol for Transmition of Confidential Data without Any Preliminary Distribution of Secret and Public Keys, Based on the Use of a Commutative Encryption Procedure

Valery I. Korzhik ✉, korzhik.vi@ sut.ru
Victor A. Yakovlev, yakovlev.va@sut.ru
Vladimir S. Starostrin, starostin.vs@sut.ru

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

Annotation

Commutative encryption, previously proposed by A. Shamir and published about 30 years ago in a monograph by B. Schneier "Applied Cryptography", has not found practical application due to the lack of known strong ciphers possessing the commutativity property. This paper confirms that such well-known ciphers as AES, GOST-2015, El-Gamal and Mc-Eliece ciphers, indeed, do not possess this property. However, the authors managed to construct a modification of the RSA cipher using a new version of the protocol, which allows the exchange of confidential information without any preliminary distribution of both public and secret encryption keys between legitimate users. This property is just the ***relevance*** *of the current paper, because, as a rule, a keys distribution problem is a bottleneck of Cryptosystem creation for their application to real confidential digital telecommunication system. Although such properties are close to the properties of so-called public-key cryptosystems, unlike them, the proposed cryptosystem can use the same public keys for an unlimited number of users. Such keys can be made publicly available, for example, by storing them in the cloud. It is this property of the proposed Cryptosystem that reflects the* ***novelty*** *of the approach, since, as the authors know, no key system has yet been described that does not require preliminary key distribution.*
This property can be useful for certain scenarios involving the exchange of confidential data, such as passwords and broadcast information. In the first case we have in mind that it is necessary to authenticate users by some server. If it has in data base user's passwords stored, then users are authenticated only upon presentation of the corresponding passwords. However, communication channel used for such authentication is vulnerable to adversary's interception, but our scheme prevents password's disclosing. Another ***practical outcome*** *of the proposed Cryptosystem consists in application to the broadband channels, if it is necessary to minimize the number of encryption keys used.*

Keywords: *commutative encryption, public-key cryptosystems, RSA cipher, computationally complexity problems, broadcast information*

For citation: Korzhik V.I., Yakovlev V.A., Starostin V.S. Cryptosystem and Protocol for Transmition of Confidential Data without Any Preliminary Distribution of Secret and Public Keys, Based on the Use of a Commutative Encryption Procedure. *Proceedings of Telecommunication Universities.* 2025;11(6):101–107. (in Russ.) DOI:10.31854/1813-324X-2025-11-6-101-107. EDN:UPSBCH

1. Введение

Понятие коммутативного шифрования (КШ) и протокол его использования были предложены А. Шамиром в его неопубликованной работе и затем представлены в монографии Б. Шнайера [1]. В этой статье КШ было определено для шифра, если ему присуще следующее свойство:

$$f_{K_1}\left(f_{K_2}(M)\right) = f_{K_2}\left(f_{K_1}(M)\right), \quad (1)$$

где $f_K(M)$ – функция шифрования сообщения M на ключе K, причем равенство (1) должно выполняться на любых ключах K_1, K_2 и для любых сообщений M.

Тогда, если для некоторого шифра всегда выполняется равенство (1), то при необходимости передачи конфиденциальной информации от пользователя A к пользователю B достаточно выполнить трех-шаговый протокол, показанный на рисунке 1.

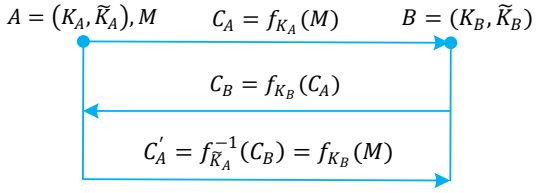

Рис. 1. Протокол А. Шамира для передачи конфиденциальной информации от пользователя *A* к пользователю *B*

Fig. 1. A. Shamir's Protocol for Transmitting of Confidential Information from user A to user B

На рисунке 1 $f_{\widetilde{K}}^{-1}(C)$ – функция, реализующая процедуру дешифрования криптограммы C на ключе дешифрования $\widetilde{K}$: $f_{\widetilde{K}}^{-1}(C) = M$.

Проверим, что пользователь B получит тогда сообщение M, отправленное пользователем A, и получим подтверждение:

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

Пользуясь коммутативностью (1) шифрования, находим, что на третьем шаге протокола пользователь B получит сообщение, зашифрованное его собственным ключом:

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

Чтобы восстановить M, ему остается лишь воспользоваться своим ключом дешифрования:

$$f_{\widetilde{K}_B}^{-1}\left(f_{K_B}(M)\right) = M.$$

Таким образом, пользователь A может передать конфиденциальное (секретное) сообщение M, используя протокол, показанный на рисунке 1, не обмениваясь никакими ключами, ни секретными, как в симметричных криптосистемах (КС), и даже ни открытыми, как в криптосистемах с открытым ключом (КОК). Такая «бесключевая» организация протокола при обмене конфиденциальными данными выглядит, казалось бы, весьма привлекательной при организации закрытых систем передачи информации. Однако проблема состоит в нахождении реально стойких КШ.

В работе [2] было показано, что такие известные симметричные шифры как ГОСТ-2015, DES, AES и несимметричные КОК, шифры Рабина, Эль-Гамаля, Мак-Элиса, не принадлежат к группе КШ.

В монографии [3] было также доказано, что, хотя потоковый шифр и является коммутативным, поскольку равенство (1) для него тривиально выполняется:

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

где $\gamma(K)$ – двоичная последовательность (гамма), которая генерируется в зависимости от ключа K; $\oplus$ – операция побитового сложения по модулю 2; легко убедиться, что, при выполнении с потоковым шифром протокола, показанного на рисунке 1, возможна тривиальная атака перехвата.

Действительно, для потокового шифра имеем $f_{\widetilde{K}}^{-1}(C) = C \oplus K$. Тогда побитовое сложение перехваченных криптограмм C_A, C_B, C_A' дает открытое сообщение M:

$$C_A \oplus C_B \oplus C_A' = (M \oplus K_A) \oplus (M \oplus K_A \oplus K_B) \oplus \\ \oplus (M \oplus K_A \oplus K_B \oplus K_A) = M.$$

Казалось бы, примером КШ является шифр РША. Равенство (1) для этого шифра принимает вид [4, 5]:

$$(M^{e_1} \bmod n)^{e_2} \bmod n = (M^{e_2} \bmod n)^{e_1} \bmod n, \qquad (2)$$

где e_1, e_2 – открытые ключи шифрования РША. Равенство (2), очевидно, выполняется.

Однако, это верно, только если пользователи A и B производят вычисления по одинаковому модулю n. Если же сравнение проводится по разным модулям, то равенство

$$(M^{e_1} \bmod n_1)^{e_2} \bmod n_2 = (M^{e_2} \bmod n_2)^{e_1} \bmod n_1$$

выполняться не будет.

С другой стороны, при использовании обоими легальными пользователями одинаковых модулей n в КС РША появляется, как показано в [4] и отмечено в [5], побочная атака, которая позволит одному пользователю вычислить с полиномиальной сложностью секретный ключ другого пользователя, что во многих случаях совершенно недопустимо. Поэтому применение РША в качестве КШ не может быть рекомендовано.

В следующем разделе настоящей статьи приводится описание предлагаемого нами шифра и протокола, которые позволяют избежать отмеченного выше недостатка.

2. Описание шифра и протокола, обеспечивающих передачу данных без предварительного обмена любыми ключами

Рассмотрим следующий протокол, который позволяет избежать отмеченного выше недостатка и полностью исключить атаку факторизации чисел, типичную для РША. Схема взаимодействия легальных пользователей A и B показана на рисунке 2. Пользователи A и B выбирают из общедоступной базы данных параметр p – *сильно простое число* (это число либо генерирует доверенный центр, либо один из пользователей и пересылает другому). Возможен и другой вариант – разместить это число *для всех пользователей*, например, в облаке (поэтому p даже не имеет смыла считать открытым ключом).

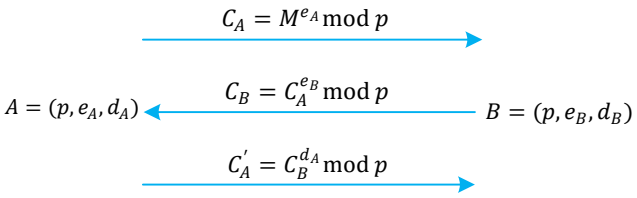

Рис. 2. Предлагаемый протокол передачи конфиденциальной информации от *A* к *B* с использованием коммутативного шифрования

Fig. 2. The Proposed Protocol for Transmitting of Confidential Information from A to B Using Commutative Encryption

Пользователи A и B вырабатывают случайно свои секретные ключи шифрования e_A и e_B, согласно условию $gcd(e_A, p-1) = 1, gcd(e_B, p-1) = 1$.

Затем они вычисляют секретные ключи:

$$d_A = e_A^{-1} \bmod (p-1), d_B = e_B^{-1} \bmod (p-1).$$

Важно отметить, что в данной схеме все ключи e_A, e_B и d_A, d_B *никому не передаются и сохраняются в секрете*. Именно этим предлагаемая КС отличается от КОК, известным в литературе по прикладной криптографии.

Передача сообщения M $(M < p)$ от A к B осуществляется в три этапа (см. рисунок 2).

Докажем, что после выполнения трехшагового протокола пользователь B получит криптограмму вида $C_A' = M^{e_B} \bmod p$ и, используя свой ключ дешифрования d_B, воспроизведет исходное сообщение M по правилу $(M^{e_B} \bmod p)^{d_B} \bmod p = M$. При этом нарушитель, перехватывающий криптограммы каждой передачи между пользователями, не сможет дешифровать криптограммы за полиномиальное время.

Доказательство

$$\begin{aligned} C_A' = C_B^{d_A} \bmod p = (C_A^{e_B} \bmod p)^{d_A} \bmod p = \\ = ((M^{e_A} \bmod p)^{e_B} \bmod p)^{d_A} \bmod p = \\ = ((M^{e_A} \bmod p)^{d_A} \bmod p)^{e_B} \bmod p. \end{aligned} \quad (3)$$

Покажем сначала, что $(M^{e_A} \bmod p)^{d_A} \bmod p = M$, для чего рассмотрим произведение $e_A d_A$. Так как $d_A = e_A^{-1}$ и $e_A e_A^{-1} = 1 \bmod (p-1)$, $e_A e_A^{-1} = k\varphi(p) + 1$, где $\varphi(p)$ – функция Эйлера, а k – некоторое целое число.

Тогда:

$$\begin{aligned} M^{e_A d_A} \bmod p = M^{k\varphi(p)+1} \bmod p = \\ = \left(M^{k\varphi(p)} \cdot M\right) \bmod p = \\ = ((M^{\varphi(p)} \bmod p)^k \cdot M) \bmod p = M. \end{aligned} \quad (4)$$

Последнее равенство следует из того факта, что по теореме Эйлера $M^{\varphi(p)} = 1 \bmod p$ и $M < p$. Подставляя последнее равенство в выражение (3), получим $C_A' = M^{e_B} \bmod p$, что и требовалось доказать.

Рассмотрим далее возможные атаки на данную КС. Подчеркнем еще раз, что в ней все ключи являются секретными, поскольку, зная ключи e_A, e_B, легко найти d_A, d_B, и наоборот.

Как видно из содержания обменов информацией в трех раундах протокола, вскрытие системы возможно на основе решения вычислительно трудной задачи *дискретного логарифмирования*. Действительно, пассивный нарушитель может перехватить криптограмму C_B на втором шаге протокола и C_A' на третьем шаге и попытаться выполнить дискретное логарифмирование $e_B = \log_{C_A} C_B \bmod p$, а затем – найти $d_B = e_B^{-1} \bmod (p-1)$. Наконец, зная d_B и перехватив $C_A' = C_B^{d_A} \bmod p$ на третьем шаге, он дешифрует сообщение, также как это делает легальный пользователь B.

Конечно, выполняя дискретное логарифмирование, нарушитель столкнется с непреодолимыми вычислительными трудностями, если параметры системы выбраны надлежащим образом. Однако, поскольку предлагаемая КС не является постквантовой, то при появлении квантовых компьютеров с достаточным числом кубит данная задача может быть решена за полиномиальное время. Активный нарушитель может на первом шаге заменить криптограмму C_A специально подобранным числом b и получить в ответ сообщение $C_B = b^{e_B} \bmod p$, затем – выполнить логарифмирование $e_B = \log_b C_B \bmod p$. Поскольку основанием логарифма является специально подобранное число, то эта задача может иметь меньшую сложность по сравнению с общей задачей дискретного логарифмирования.

Для блокирования этой атаки пользователь B должен провести маскировку своего ключа, используя ключ $e_B' = e_B \cdot x \bmod p$, где $x < p - 1$.

Тогда третий шаг протокола на основании (3) и (4) можно представить так:

$$\begin{aligned} C_A' = C_B^{d_A} \bmod p = (C_A^{e_B'} \bmod p)^{d_A} \bmod p = \\ = ((M^{e_A} \bmod p)^{e_B x} \bmod p)^{d_A} \bmod p = \\ = ((M^x)^{\cdot e_A d_A} \bmod p)^{e_B} \bmod p = (M^x \bmod p)^{e_B} \bmod p. \end{aligned}$$

Проведя дешифрование C_A', пользователь B получает $(M^{xe_B} \bmod \mathrm{p})^{d_B} \bmod p = M^x$. Затем он, зная x, снимает маскировку $(M^x \bmod p)^{-x} \bmod p = M$.

Нарушитель, проводя атаку логарифмирования с выбранным сообщением b, в случае ее успеха, получит ключ e_B', который не соответствует истинному ключу:

$$e_B' = \log_b C_B \bmod p = \log_b b^{xe_B} \bmod p = xe_B \bmod p$$

Активная атака с выбранным сообщением может быть осуществлена нарушителем и на первом шаге протокола, когда передается криптограмма $C_A = M^{e_A} \bmod p$. Нарушитель заменяет сообщение C_A на число b, которое он подбирает таким образом, чтобы осуществить атаку с малым порядком подгруппы. Для пояснения этой атаки отметим, что

числа $b^{e_B} \bmod p$ образуют группу, максимальный порядок которой $p-1$. Она содержит подгруппы, порядки которых есть множители порядка группы. Используя этот факт, нарушитель может получить некоторую информацию о ключе e_B. Так, например, если b – нечетное число, то четное $C_B = b^{e_B} \bmod p$ свидетельствует о том, что e_B четное число.

Важно отметить, что выполнение предлагаемого протокола принципиально требует шифра со свойством КШ, поскольку пользователи A и B ни на одном шаге протокола не обмениваются ключами. В отличие от конвенциональных КОК, предлагаемая схема требует двусторонних каналов обратной связи и выполнения трех-шагового протокола, что, безусловно, является ее недостатками. Однако в некоторых случаях она может иметь и преимущества перед традиционными КОК.

Так, во-первых, предлагаемая КС не требует никакой аутентификации ключей, а лишь идентификацию пользователей, что, как правило, оказывается более простой задачей.

Во-вторых, для передачи конфиденциальной информации различным пользователям A не должен перестраивать свой открытый ключ по ключам этих пользователей, как это требуется для КОК.

Одно из возможных применений данной криптосистемы состоит также в возможности надежной защиты парольной информации при взаимодействии пользователя с сервером. Например, при аутентификации пользователя в такой системе он, как известно, предъявляет свой пароль – уникальную последовательность символов достаточной длины. Если предъявляемый пароль совпадает с паролем, имеющимся у сервера, то пользователь проходит аутентификацию. Однако, поскольку пароль передается в открытом виде, он может быть перехвачен нарушителем. Для защиты от атаки перехвата пароля используются различные способы (запрос-ответ, одноразовый пароль и др. [5]).

Рассмотрим, как может быть решена задача аутентификации пользователя без раскрытия пароля на основе предложенной системы КШ (рисунок 3).

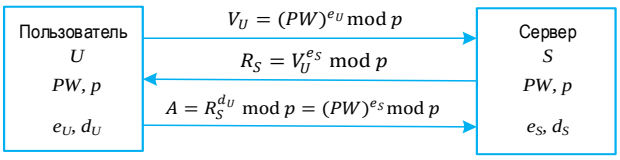

Рис. 3. Пример применения коммутативного шифрования для аутентификации пользователей без разглашения паролей

Fig. 3. An Example of Using the Commutative Encryption for Authentication of Users without Disclosing the Passwords

Для обеспечения такой аутентификации пользователь посылает вызов на сервер, в форме зашифрованного пароля $V_U = (PW)^{e_U} \bmod p$. Сервер формирует ответ, представляющий собой перешифрованный вызов пользователя $R_S = V_U^{e_S} \bmod p$, и пере-дает его обратно. Пользователь расшифровывает ответ своим ключом d_U и возвращает серверу подтверждение:

$$A = R_S^{d_U} \bmod p = V_U^{e_S d_U} \bmod p = \\ = ((PW)^{e_U d_U})^{e_S} = (PW)^{e_S}.$$

Сервер расшифровывает подтверждение и восстанавливает пароль $A^{d_S} = (PW)^{e_S d_S} \bmod p = PW$. Далее он сравнивает этот пароль с паролем пользователя, хранящемся в его базе и, если пароли совпадают, пользователь считается аутентифицированным.

Как следует из предложенной схемы, при обмене информацией между пользователем и сервером пароли не передаются в открытом виде, но лишь как криптограмма. Поэтому для компрометации пароля, то есть его вскрытия, нарушитель должен решить трудную вычислительную задачу нахождения дискретного логарифма $e_s = \log_{V_u} R_S \bmod p$.

Заметим, что предложенный алгоритм обеспечивает лишь одностороннюю аутентификацию.

Еще одним полезным применением предлагаемой КС является передача группе легитимных пользователей от сервера одного широковещательного сообщения, например, ключа для дешифрования приема платного ТВ. В этом случае телевизионный центр, управляющий доступом (ЦУД) к оплаченным программам, шифрует криптоключ доступа к критограммам программ, как показано на рисунке 2, на первом шаге, и помещает полученную криптограмму в некоторую базу данных, например, в облако. Любой пользователь данной системы платного ТВ может свободно считать эту криптограмму и перешифровать ее, используя свой секретный ключ, а затем послать полученную криптограмму с двойным шифрованием в ЦУД, где собираются для дальнейшей обработки только оплаченные криптограммы. Далее все такие, прошедшие контроль оплаченные криптограммы объединяются в один пакет и дешифруются на третьем шаге протокола, как показано на рисунке 2, ключом дешифрования ЦУД. Затем весь пакет направляется на свою, скажем, облачную базу данных. Теперь каждый пользователь системы, оплативший определенную криптограмму, может извлечь из базы данных оплаченную программу, а затем окончательно дешифровать ее своим секретным ключом (см. исход третьего шага на рисунке 2). Наконец, имея основной ключ дешифрования, пользователь может смотреть расшифрованное этим ключом ТВ-сообщение.

Очевидным преимуществом такой схемы является та ее особенность, что она не требует перестройки ключа сервера по всем ключам легитимных пользователей.

3. Заключение

В настоящей статье предложена и исследована новая «сверхнесимметричная» КС и соответствующий ей протокол, выполняющий передачу конфиденциальной информации безо всякого предварительного распределения ключей, причем, как ключей шифрования, так и дешифрования.

Стойкость предложенной КС соответствует решению вычислительной задачи дискретного логарифмирования. Этим данная схема отличается от информационно-теоретически секретной схемы [7], в которой, однако, были решены не все проблемы, связанные с ее безопасностью.

Поскольку рассмотренная КС не является постквантовой, то она будет уязвимой при появлении на практике достаточно мощных квантовых компьютеров [6].

Весьма перспективной представляется задача нахождения КС КШ, обладающих свойством постквантовости, подобных КС Мак-Элиса [4], которая основана на вычислительно трудных задачах теории корректирующих кодов. Другая пост-квантовая КС базируется на трудных задачах теории числовых решеток [8]. Наконец, в последнее время появились пост-квантовые КС, использующие некоммутативные группы [9], а также многовариантные КС [10, 11]. Однако предложенная авторами система превосходит перечисленные КС по оценке сложности реализации ими процедур шифрования и дешифрования. Поэтому она может найти практическое применение даже сейчас, пока еще не появились на практике квантовые компьютеры с достаточным объемом логических кубит, способные решать задачу дискретного логарифмирования за полиномиальное время.

Список источников

1. Шнайер Б. Прикладная криптография. М.: Триумф, 2002.
2. 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:10.31854/1813-32X-2024-10-6-79-98. EDN:HPBOWG
3. Korzhik V., Starostin V., Yakovlev V., Kabardov M., Krasov A., Adadurov S. Advance in Keyless Cryptography // In: Ramakrishnan S. (ed.) Lightweight Cryptographic Techniques and Cybersecurity Approaches. 2022. PP. 97–117. DOI:10.5772/intechopen.104429
4. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. Boca Raton, 1997. DOI:10.1201/9780429466335
5. Коржик В.И., Яковлев В.А. Основы криптографии. СПб.: Издательский центр "Интермедия", 2016. 296 с. EDN:WEQWMN
6. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. Vol. 26. Iss. 5. PP. 1484–1509. DOI:10.1137/S0097539795293172
7. Korzhik V.I., Starostin V.S., Kabardov M.M., Gerasimovich A.M., Yakovlev V.A., Zhuvikin A.G. Information-theoretically secure key sharing protocol with constant noiseless public channels // Математические вопросы криптографии. 2021. Т. 12. № 3. С. 125–141. DOI:https://doi.org/10.4213/mvk378
8. Mincciancio D., Regev O. Lattice-based Cryptography // In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Berlin, Heidelberg: Springer, 2009. PP. 147–191. DOI:10.1007/978-3-540-88702-7_5
9. Myasnikov A., Shpilrain V., Ushakov A. Non-Commutative Cryptography and Complexity of Groupe-Theoretical Problems. American Mathematical Society, 2011. 385 p. EDN:GPBUOR
10. Молдовян А.А., Молдовян Д.Н., Молдовян А.Н. Постквантовые двухключевые криптосхемы на конечных алгебрах // Информатика и автоматизация. 2024. Т. 3. № 4. С. 1246–1276. DOI:10.15622/ia.23.4.12. EDN:YZSVQH
11. Duong M.T., Moldovyan A.A., Moldovyan D.N., Nguyen M.H., Do B.T. Structure of quaternion-type algebras and post-quantum structure algorithm // International Journal of Electrical and Computer Engineering. 2025. Vol. 15. Iss. 3. PP. 2965–2976. DOI:10.11591/ijece.v15i3.pp2965-2976

References

1. Schneier B. *Applied Cryptography.* Moscow: Triumph Publ.; 2002. (in Russ.)
2. 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:10.31854/1813-32X-2024-10-6-79-98. EDN:HPBOWG
3. Korzhik V., Starostin V., Yakovlev V., Kabardov M., Krasov A., Adadurov S. Advance in Keyless Cryptography. *In: Ramakrishnan S. (ed.) Lightweight Cryptographic Techniques and Cybersecurity Approaches*. 2022. p.97–117. DOI:10.5772/intechopen.104429
4. Menezes A.J., van Oorschot P.C., Vanstone S.A. *Handbook of Applied Cryptography*. Boca Raton; 1997. DOI:10.1201/9780429466335
5. Korzhik V.I., Yakovlev V.A. *Fundamentals of Cryptography*. St. Petersburg: Intermedia Publ.; 2016. 216 p. (in Russ.) EDN:WEQWMN
6. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*. 1997;26(5):1484–1509. DOI:10.1137/S0097539795293172

7. Korzhik V.I., Starostin V.S., Kabardov M.M., Gerasimovich A.M., Yakovlev V.A., Zhuvikin A.G. Information-theoretically secure key sharing protocol with constant noiseless public channels. *Mathematical Aspects of Cryptography*. 2021;12(3):125–141. DOI:https://doi.org/10.4213/mvk378

8. Mincciancio D., Regev O. Lattice-based Cryptography. *In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography*. Berlin, Heidelberg: Springer; 2009. p.147–191. DOI:10.1007/978-3-540-88702-7_5

9. Myasnikov A., Shpilrain V., Ushakov A. *Non-Commutative Cryptography anComplexity of Groupe-Theoretical Problems*. American Mathematical Society, 2011. 385 p. EDN:GPBUOR

10. Moldovyan A., Moldovyan D., Moldovyan A. Post-Quantum Public-Key Cryptoschemes On Finite Algebras. *Informatics and Automation*. 2024:3(4):1246–1276. (in Russ.) DOI:10.15622/ia.23.4.12

11. Duong M.T., Moldovyan A.A., Moldovyan D.N., Nguyen M.H., Do B.T. Structure of quaternion-type algebras and post-quantum structure algorithm. *International Journal of Electrical and Computer Engineering*. 2025;15(3):2965–2976. DOI:10.11591/ijece.v15i3.pp2965-2976

Статья поступила в редакцию 19.11.2025; одобрена после рецензирования 03.12.2025; принята к публикации 10.12.2025.
The article was submitted 19.11.2025; approved after reviewing 03.12.2025; accepted for publication 10.12.2025.

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 защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0009-0000-2939-1971

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

Korzhik V.I. has been a member of the journal "Proceedings of Telecommunication Universities" Editorial Council since 2016, but has 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.