Обзорная статья
УДК 004.056(075.58)
https://doi.org/10.31854/1813-324X-2024-10-4-126-141

Прогресс в теории прикладной криптографии: обзор и некоторые новые результаты. Часть 1. Ключевая криптография

Валерий Иванович Коржик[1] ✉, val-korzhik@yandex.ru
Виктор Алексеевич Яковлев[1], yakovlev.va@sut.ru
Борис Викторович Изотов[2], izotov.b@yandex.ru
Владимир Сергеевич Старостин[1], vm.ffp@sut.ru
Михаил Викторович Буйневич[3], bmv1958@yandex.ru

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]ЗАО «Научные приборы», Санкт-Петербург, 198095, Российская Федерация
[3]Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, 196105, Российская Федерация

Аннотация

В настоящей работе, состоящей из двух частей, представлены как уже опубликованные ранее (но труднодоступные) результаты, так и новые. ***Актуальность*** *данной работы заключается, во-первых, в том, что в последнее время получен ряд новых результатов в области прикладной криптографии, которые нуждаются как в разъяснении, так и в практическом применении. Именно это и является основной* ***целью*** *настоящей работы.* ***Постановка проблемы*** *в первой части статьи касается сложности взлома симметричных шифров, в то время как во второй части статьи обсуждается так называемая бесключевая криптография, а именно: концепция канала прослушивания, реализация каналов связи, позволяющих обеспечить информационную безопасность без процедуры обмена ключами между легитимными корреспонденциями. В работе широко используются* ***методы*** *прикладной математики, а именно: алгебры, чисел, вероятностей и теории информации. Также используется компьютерное моделирование.* ***Новизна*** *первой части работы заключается в следующем: во-первых, проясняется смысл ограничения времени жизни ключа для различных режимов симметричного шифрования, во-вторых, поясняется подход взлома шифра с использованием квантовых компьютеров, в-третьих, подробно исследуется аутентификация ключа для протокола Диффи – Хеллмана на основе технологии «спаривания» мобильных устройств. Во второй части статьи представлена уязвимость криптосистемы Дина – Голдсмита при некотором расширении атак.* ***Основными результатами*** *данной статьи являются: оценка времени жизни ключа для симметричного шифрования в режиме CBC, прояснение алгоритма Гровера взлома симметричных шифров методом грубой силы, разработка метода аутентификации значений Диффи – Хеллмана на основе предварительно распределенных последовательностей, выбор шифров, позволяющих работать с протоколом Шамира без предварительного разделения ключа, взлом протокола Дина – Голдсмита при некоторых условиях, доказательство факта о возможной взламываемости протокола разделения ключа по бесшумным каналам связи.* ***Практическое применение*** *результатов статьи заключается в стимулировании правильного выбора шифров и их параметров с целью обеспечения их устойчивости к различным атакам и большего внимания к алгоритмам бесключевой криптографии.*

Ключевые слова: *срок действия ключей, алгоритмы Гровера и Шора, аутентификация ключей, квантовые компьютеры, кодовое зашумление, коммутативная криптография, бесключевая криптография*

Ссылка для цитирования: Коржик В.И., Яковлев В.А., Изотов Б.В., Старостин В.С., Буйневич М.В. Прогресс в теории прикладной криптографии: обзор и некоторые новые результаты. Часть 1. Ключевая криптография // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 126–141. DOI:10.31854/1813-324X-2024-10-4-126-141. EDN:NNNFBU

Review research
https://doi.org/10.31854/1813-324X-2024-10-4-126-141

Advance in Applied Cryptography Theory: Survey and New Results. Part 1. Key Cryptography

Valery I. Korzhik[1] ✉, val-korzhik@yandex.ru
Viktor A. Yakovlev [1], yakovlev.va@sut.ru
Boris V. Izotov [2], izotov.b@yandex.ru
Vladimir S. Starostin[1], vm.ffp@sut.ru
Mikhail V. Buinevich[3], bmv1958@yandex.ru

[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]JSC Scientific Instruments,
St. Petersburg, 198095, Russian Federation
[3]Saint Petersburg University of State Fire Service of Emercom of Russia,
St. Petersburg, 196105, Russian Federation

Annotation

In the current paper, consisting from two parts, are presented both results already published before (but hard for access) and new once. ***Actuality*** *of this work is firstly in a fact that recently has been obtained a number of new results in area of applied cryptography that are needed both in a clarification and be put into practice. This is namely the main goal of the current paper. The* ***setting problem*** *in the first paper part concerns to a complexity of symmetric cipher breaking while in the second part of the paper is discussed, so called, keyless cryptography, namely: wiretap channel concept, execution of communication channels which allow to provide information security without of key exchange procedure between legal correspondences. In the part widely used* ***methods*** *of applied mathematics, namely: algebra, number, probability and information theories. Computer simulation also used there. A* ***novelty*** *of the first part of work consists in the following: first of all it is clarified the sense of a key lifetime limitation for different symmetric cipher modes, secondly, it is explained an approach of cipher breaking by the use of quantum computers, finely, the key authentication for the Diffie – Hellman protocol based on the mobile device pairing technology is investigated in detail. In the second part of the current paper has been presented a vulnerability of Dean – Goldsmith cryptosystem under some extension of attacks. The* ***main results*** *of this paper are: estimation of the key lifetime of single key for symmetric cipher in CBC mode, clarifying of Grover's algorithm breaking of symmetric ciphers by brute force attack, development of a method for authentication of Diffie – Hellman values based on pre-distributed sequences, selection of ciphers which allow to execute with Shamir's protocol without any key sharing in advance, breaking of Dean – Goldsmith protocol under some conclusions, proof the fact regarding of a possible breakability of the key sharing protocol over noiseless communication channels.* ***Practical application*** *of paper results consists in the fact of stimulation the correct choice of ciphers and their parameters in order to provide their resistance to different attacks and more attention to algorithms of keyless cryptography.*

Keywords: *key expiration, Grover and Shor algorithms, Diffie – Hellman key authentication, quantum computers, code noising, commutative cryptography, keyless cryptography*

For citation: Korzhik V.I., Yakovlev V.A., Izotov B.V., Starostin V.S., Buinevich M.V. Advance in Applied Cryptography Theory: Survey and New Results. Part 1. Key Cryptography. *Proceedings of Telecommunication Universities.* 2024;10(4):126–141. (in Russ.) DOI:10.31854/1813-324X-2024-10-4-126-141. EDN:NNNFBU

ВВЕДЕНИЕ

Нет сомнения, что вопросы теории в прикладной криптографии имеют большое значение для изучения проблем информационной безопасности. Причем это распространяется как на обучение в ВУЗах, так и на поисковые исследования в данной области. Настоящим прорывом здесь явилось создание ГОСТа (и последующая реализация отече-

ственных алгоритмов шифрования/дешифрования), впервые представленного в 1989 г. [1] и затем усовершенствованного в 2015 г. [2], а также появление стандартов на электронные (цифровые) подписи [3] и хэш-функции [4].

Значимость этих «государственных» документов состоит в том, что методы шифрования, наверное, впервые в СССР, а затем и в РФ, разрешались для использования не только специальным ведомствам в определенных областях, но и гражданским организациям и бизнес-сообществу, легитимизовав их права на конфиденциальную информацию. Что, конечно, не отрицает возможность и существование «закрытых» стандартов в этой области.

Весьма важным в этой связи является то обстоятельство, что появление «открытых» стандартов шифрования стимулировало издание целого ряда зарубежных и отечественных монографий по данному направлению науки, а также проведение исследований «гражданскими» специалистами [5–7]. Более того, в ряде университетов были созданы и начали читаться курсы по основам криптографии, обеспеченные соответствующими учебниками и учебными пособиями [8–9].

Однако некоторые теоретические достижения в области прикладной криптографии еще не заняли должного места в вузовской научно-педагогической деятельности и, тем более, не стали широким достоянием ученых и специалистов в области информационной безопасности; что, по мнению авторов, является серьезным упущением. Поэтому целью данной статьи является попытка представить в систематизированном виде как малоизвестные или редко применяемые на практике, так и отдельные авторские научные результаты, частично опубликованные в отечественных и зарубежных высокорейтинговых изданиях; некоторые из них являются впервые представленным на апробацию обобщением ранее известных результатов.

Статья состоит их двух частей, описывающих прогресс в области ключевой и бесключевой криптографии. Последний термин не придуман авторами настоящей статьи, а был предложен еще в 1983 г. Б. Алперном и Ф. Шнайдером [10]. В последующем по этой тематике проф. В.И. Коржиком вместе с соавторами было опубликовано свыше десятка статей в зарубежных журналах и трудах международных конференций, которые, к сожалению, не все легко доступны для отечественного читателя. Особого внимания, на наш взгляд, заслуживает глава с аутентичным названием «Advance in Keyless Cryptography» (*перев. на русск.* «Прогресс в бесключевой криптографии») в монографии [11], изданной InterTech в 2022 г.

В первой части уточняются понятие стойкости для блоковых шифров, описываются пути использования квантовых компьютеров для взлома симметричных и асимметричных криптосистем и представляются усовершенствованные протоколы аутентификации пользователей компьютерных сетей.

Во второй части рассматриваются так называемые методы обеспечения секретности информации на физическом уровне, то есть с использованием физических свойств каналов связи. К таким свойствам относятся: присутствие обратной связи, наличие шума, квантовые эффекты, многолучевость и использование смарт-антенн.

Авторы надеются, что предлагаемая вниманию читателей статья послужит важным стимулом для развития исследований в данных направлениях, причем как теории, так и в продвижении для практического использования содержащихся в ней основных научных результатов.

1. СТОЙКОСТЬ БЛОКОВЫХ ШИФРОВ ПРИ ИСПОЛЬЗОВАНИИ РАЗЛИЧНЫХ МОД ШИФРОВАНИЯ

Как уже упоминалось во введении, в настоящее время доступен для практического использования целый ряд «открытых» стандартов шифрования для симметричных блоковых шифров. Напомним, что блоковыми называются такие шифры, которые однозначно отображают двоичные последовательности криптограмм такой же длины и используют во время шифрования определенное количество блоков открытого текста одного и того же секретного ключа; причем тот же самый ключ используется и для дешифрования криптограмм обратно в блок открытых сообщений. Отсюда и термин «симметричные шифры», что относится именно к ключам.

Очевидно, что основным требованием к таким, как, впрочем, и к другим шифрам, является их стойкость, то есть устойчивость к возможности дешифрования криптограмм без знания ключа. Зачастую такое воздействие называют «взломом шифра». В современной постановке этой задачи обычно предполагается, что при поиске ключа возможно знание не только блоков криптограммы, но и некоторого количества соответствующих им блоков открытых сообщений (так называемая, «атака с частично известным открытым сообщением»). Более того, иногда возможно навязывание «противником» при шифровании заранее выбранных блоков открытого сообщения («атака с частично выбранным открытым сообщением»). Есть версия, что именно такой атакой США взломали «Пурпурный шифр», использовавшийся японцами

во время морских сражений на Тихом океане во время Второй Мировой войны.

Что касается атаки, упомянутой первой, то одному из авторов настоящей статьи от криптографа, занимавшегося вскрытием немецких шифров периода ВОВ, стало известно, что это ему достаточно легко удавалось, поскольку почти любая военная криптограмма в Третьем Рейхе заканчивалась фразой «Heil Hitler!».

Попытка создания идеального секретного шифра официально датируется 1948 г., когда «вышла в свет» и была рассекречена работа К. Шеннона Communication Theory of Secrecy Systems [12], хотя такой алгоритм был запатентован еще раньше Г. Вернамом [13]; справедливости ради надо отметить, что шифр носит его имя – «шифр Вернама». Однако заслуга К.Э. Шеннона состояла в том, что он рассчитал минимально известную длину криптограммы (измеряемую, например, числом символов), для которой существует единственно возможное открытое сообщение. Эта величина была названа им «расстоянием единственности» (РЕ).

Заметим, что это единственное открытое сообщение, тогда может быть найдено при помощи полного перебора всех возможных ключей, называемой обычно «грубой лобовой атакой». Несколько неожиданным оказался тот факт, что для достаточно избыточных сообщений (таких, например, как текст на каком-либо естественном языке) РЕ удивительно мало – см. например, формулу Шеннона для РЕ в зависимости от величины энтропии источника и длины ключа в [8]. Поэтому, если необходимо зашифровать «длинные сообщения коротким ключом», следует выбирать такой ключ, который безусловно является неперебoрным, то есть все его варианты невозможно опробовать ни при каком разумном времени и/или реалистичном объеме вычислительного оборудования.

Однако «атака перебором» не является единственно возможной. Существует еще множество других атак (не экспоненциальной сложности), к которым относятся, например: линейный и дифференциальный криптоанализ, решение нелинейных уравнений, атака на основе принципа максимального правдоподобия, атака со связкой ключей и т. д.; см. некоторые примеры в [8]. Поэтому возникает естественный вопрос – можно ли вывести нижнюю границу для числа элементарных вычислений при наилучшей (пусть даже и неизвестной) атаке по взлому блокового шифра с известными алгоритмами шифрования/дешифрования и заданными параметрами (длиной блока шифра и его ключа)?

Более того, как известно, блоковые шифры могут использоваться в различных модах, то есть, формировать каждый блок криптограмм с использованием нескольких блоков открытого текста. Так, мода с зацеплением блоков (CBC-мода, *аббр. от англ.* Cipher Block Chaining) реализуется в виде:

$$\begin{aligned} E_i &= f_k(E_{i-1} \oplus M_i), i = 1, 2, \ldots, \\ M_i &= E_{i-1} \oplus g_k(E_i), i = 1, 2, \ldots, \end{aligned} \quad (1)$$

где E_i, E_{i-1} – i-й и i–1-й блоки криптограмм; M_i – i-й блок сообщения; $f_k(\cdot)$ – функция шифрования на ключе K; $g_k(\cdot)$ – функция дешифрования на ключе K; $\oplus$ – операция побитового сложения по mod2.

В [8] описаны также моды с обратной связью по криптограмме и по сообщению.

Поэтому возникает следующий естественный вопрос – как выбор моды влияет на стойкость блокового шифра? Интуитивно ясно, что чем больше блоков будет зашифровано без смены ключа, тем менее стойким может оказаться шифр, поскольку атакующим доступна возможность анализировать больший объем статистики. Отсюда логично возникает уточнение вопроса о стойкости шифра – сколько (максимум) блоков можно зашифровать без смены ключа, чтобы шифр оставался стойким?

В точной формулировке, при «атаке с частично известными сообщениями», эта задача может быть сформулирована следующим образом. Пусть $N = U + V$ блоков открытого текста были зашифрованы с использованием одного ключа. Обозначим эти блоки как $P_1, P_2, \ldots P_U, P_1', P_2', \ldots P_V'$ и соответствующие блоки криптограммы как $C_1, C_2, \ldots C_U, C_1', C_2', \ldots C_V'$, причем первые «$U$» блоков полагаются известными, а последние «V» блоков – неизвестными.

Обозначим через $\boldsymbol{\pi}$ максимальную приемлемую для легального собственника шифра величину вероятности получения дополнительной информации о неизвестной части открытого текста $P_1', P_2', \ldots P_V'$, то есть вероятность его риска. Максимальное количество блоков, которое нужно зашифровать на одном ключе без потери информации о блоках сообщений, обозначим через $N_{\text{макс}}$. Основная проблема состоит в том, чтобы найти функциональную зависимость между $N_{\text{макс}}$ и $\boldsymbol{\pi}$, причем для различных мод шифрования.

В работе [14] доказано, что если блоковый шифр является идеальным (то есть представляет собой случайные подстановки сообщений в криптограммы), то для максимального количества блоков, зашифрованных на одном ключе и при использовании, например, CBC-моды, будет справедливо следующее неравенство:

$$N_{\text{макс}} \leq 2^{\frac{n}{2}+1} \sqrt{\ln\left(\frac{1}{1-\pi}\right)}. \quad (2)$$

Для получения оценочных формул подобных (2), связывающих основные параметры мод шифрования $N_{\text{макс}}$ и $\boldsymbol{\pi}$, использовались различные ва-

рианты метода, основанного на так называемом «парадоксе дня рождения» (в основе этого метода при использовании двоичного блокового шифра лежит тот факт, что при последовательном случайном и равномерном выборе блоков открытых сообщений длиной n произойдет совпадение (коллизия) двух таких блоков с вероятностью ½ при проведении примерно $2^{n/2}$ испытаний).

Приведем пример расчета границы для $N_{макс}$. Пусть **π** задана как вероятность утечки любого количества информации о неизвестной части блоков открытого текста $P'_1, P'_2, \ldots P'_V$, то есть практически вероятность риска частичной компрометации. Тогда, если выбрать достаточно малую вероятность, допустим 10^{-6}, а длину блока n = 64, то по формуле (2) получим: $N_{макс} \leq 8 \cdot 10^6$ блоков. При задании же бóльшей вероятности риска, например **π** = 0,1, по (2) получим: $N_{макс} \leq 2{,}6 \cdot 10^9$ блоков, – что значительно больше, чем в предыдущем примере.

Если же шифр не идеальный (то есть не является случайной подстановкой) и обладает лишь свойством биективности (то есть, однозначности шифрования/дешифрования, что обычно имеет место для таких известных стандартов, как ГОСТ, DES, AES), то при вычислении максимально возможного числа блоков при шифровании на одном ключе с отсутствием утечки информации необходимо, как отмечено в работе [14], учесть эту «неидеальность», что по мнению авторов этой статьи требует проведения дополнительных исследований.

Неравенства, аналогичные (2), были получены авторами [14] и для таких мод шифрования, как OFB (*аббр. от англ*. Output Feed Back, обратная связь по выходу внутреннего блокового шифра) и CFB (*аббр. от англ*. Cipher Feedback, обратная связь по криптограмме). Что же касается моды ECB (*аббр. от англ*. Electronic CodeBook, электронная шифровальная книга), то для нее тривиально $N_{макс}$ = 1, так как даже при использовании одного и того же ключа только для двух блоков, при повторении блоков открытого текста получаем одинаковые блоки криптограмм, то есть утечку дополнительной информации.

Итак, вопрос о нахождении строгой границы для $N_{макс}$ при неидеальном шифре, насколько известно авторам настоящей статьи, остается открытым.

2. ВОЗМОЖНОСТИ УПРОЩЕНИЯ КРИПТОАНАЛИЗА ПРИ ИСПОЛЬЗОВАНИИ КВАНТОВЫХ КОМПЬЮТЕРОВ

Прежде всего необходимо подчеркнуть, что, по крайней мере, по своему целевому предназначению квантовый компьютер (КК) коренным образом отличается от квантовой криптографии (ККР); можно метафорически заметить это отличие на примере понятий «Государь» и «Милостивый государь»). Сформулируем эти различные цели: КК, применяемый для решения проблем криптоанализа, предназначен для отыскания секретных ключей, как для симметричных, так и для несимметричных криптосистем, в то время как ККР – для построения метода защиты от перехвата конфиденциальной информации (прежде всего ключевой) при ее передаче по незащищенному от перехвата каналу связи.

Говоря о принципах построения КК, следует отметить среди их основных задач сокращение вычислительной сложности при выполнении криптоанализа. Здесь обычно рассматривают две ее разновидности: умеренное (квадратичное) уменьшение сложности вычислений – или алгоритм Гровера (АГ), и переход от экспоненциальной зависимости количества вычислений от размеров криптоключа к полиномиальной – или алгоритм Шора (АШ). Причем АГ рассмотрим более подробно, а для АШ представим лишь оценки для количества вычислений ввиду достаточной полноты его описания в доступных источниках.

Вообще говоря, АГ может использоваться далеко не только для криптоанализа, а например, для упрощенного решения задач поиска в любой неструктурированной базе данных. Постановка такой задачи имеет следующий вид: пусть имеется некоторое множество M элементов, снабженных нумерацией и, возможно еще, уникальными идентификаторами (ID), состоящими из N «неструктурированных» (то есть, которые нельзя как-то упорядочить) элементов; требуется определить номер (или ID) одного их элементов этого множества, который известен решающему задачу.

Математическая модель этой проблемы описывается следующим образом: пусть задана некоторая булева функция $f(x), x \in M$, причем $f(x) = 1$ тогда и только тогда, когда элементы x удовлетворяют критерию поиска, и $f(x) = 0$ для всех остальных элементов. Пусть, не умаляя общности, $N = 2^n, n \geq 0$. Очевидно, что при «лобовом» переборе потребуется не более, чем 2^n операций для достоверного решения задачи или 2^{n-1} операций нахождения решения с вероятностью ½. АГ позволяет, при использовании ККР, сократить этот перебор до $2^{n/2}$ операций, что в некоторых случаях является весьма существенным.

Обычно в качестве простейшего примера постановки такой задачи предлагается по номеру телефона найти фамилию абонента или в огромной базе неупорядоченных фотографий найти по заданной фотографии фамилию, и дополнительно ID, искомого лица.

В случае *криптоанализа* задача формулируется так: пусть имеется пара – сообщение x и криптограмма y, полученная с использованием неизвестного ключа K – то есть $y = f(x, K)$, где $f(\cdot)$ – алгоритм (функция) шифрования; требуется найти секретный ключ K, используя АГ. Полагается, что такой ключ должен быть единственным, что, в свою очередь, обеспечивается, если длина криптограммы оказывается не менее чем так называемое *расстояние единственности*.

Заметим, что АГ, открытый его автором в 1996 г., описан на сегодня, наверно, в нескольких десятках превосходных монографий, статей и лекций, которые можно свободно найти в интернете [15–19].

Однако для специалистов в области IT (включая и информационную безопасность), которые не знакомы профессионально с квантовой физикой, достаточно трудно сознательно воспринять факт возможности существенного сокращения количества вычислений в рассмотренной выше задаче «лобового» поиска ключа до $2^{n/2}$ по сравнению с традиционным методом тотального опробования всех ключей, требующим 2^n вычислений. Поэтому поясним это замечательное свойство ККР, проявляющееся при использовании АГ.

Главное, что требуется для выполнения АГ при решении рассматриваемой задачи – это задание функции шифрования $f(\cdot)$ в виде квантовой схемы. В этом случае схема криптоанализа может быть представлена, как показано на рисунке 1.

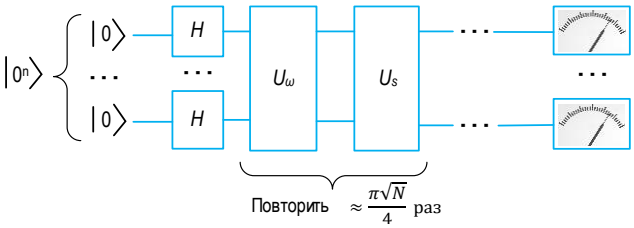

Рис. 1. Квантовая схема отыскания действующих ключей для симметричной криптосистемы при помощи АГ

Fig. 1. Quantum Scheme for Finding Valid Keys for a Symmetric Cryptosystem Using AG

Левый столбец схемы представляет собой так называемый квантовый регистр, состоящий из n кубитов, находящихся в нулевых состояниях. Напомним, что согласно [20], кубит представляет собой квантовое физическое устройство, например, электрон в квантовой точке или в ионной ловушке, которое может находиться в одном из двух базисных состояний. С физической точки зрения – это те и только те состояния системы, в одном из которых она будет обнаружена в результате измерения. В нотациях Дирака – это состояния обозначаются $|0\rangle, |1\rangle$. Первоначально все кубиты устанавливаются в состояние $|0\rangle$. Под действием оператора Адамара H на каждый кубит регистра состояние всего регистра a превращается в «равномерную» линейную комбинацию всех его возможных состояний:

$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \times$$
$$\times (|00\cdots0\rangle + |00\cdots1\rangle + \cdots + |01\cdots1\rangle + |11\cdots1\rangle) = |s\rangle.$$

При решении задач криптоанализа эти базисные состояния описывают все возможные ключи шифрования длины n. Это начальное состояние регистра перед запуском итераций Гровера. При измерении системы, находящейся в таком состоянии, она редуцируется в одно из всех возможных базисных состояний с одной и той же вероятностью $\frac{1}{2^n}$. Такое состояние регистра в точности соответствует состоянию неструктурированной базы данных из $N = 2^n$ элементов.

Оператор U_ω сохраняет без изменения все векторы состояний n-мерного квантового регистра x, кроме состояния $x = \omega$, при котором обеспечивается выполнение равенства $f(x, \omega) = y$, где $f(\cdot,\cdot)$ – функция шифрования, x – сообщение, а y – криптограмма, получаемая при данном сообщении x и ключе ω; очевидно, что x и ω должны быть предварительно введены в квантовый шифратор.

Для выделенного состояния ω преобразование U_ω изменяет состояние квантового регистра на противоположное, то есть $U_\omega(|x\rangle) = -|x\rangle$.

Итак, на первом шаге итерации Гровера выполняется преобразование $U_\omega|s\rangle$. На втором шаге это состояние преобразуется с помощью так называемого оператора диффузии $U_S = 2|s\rangle\langle s| - I$: $U_s U_\omega|s\rangle$. Здесь I – тождественное преобразование.

Совместное применение операторов U_ω и U_s, называемое *оператором Гровера* $U_G = U_s U_\omega$, повторяется примерно $\frac{\pi}{4}2^{n/2}$ раз (слово «примерно» означает, что оптимальное значение количества повторений колеблется вокруг данной величины, и оно подбирается экспериментально вокруг указанного значения).

После выполнения требуемого числа итераций производится измерение состояния кубитового регистра и, согласно доказательству, приведенному в работе самого Гровера [21], оно должно с вероятностью, близкой к 1, совпадать с искомым ключом ω. При прочтении описания АГ возникает естественный вопрос – зачем вообще нужны итерации оператора Гровера, если преобразование U_ω, казалось бы, находит ключ ω уже на первой итерации, поскольку выполняется равенство $f(x, \omega) = y$?

Ответ на этот вопрос заключается в том, что правильность измерения ключа после первых итераций имеет почти такую же вероятность, как и для неправильных решений; ситуация сходится к пра-

вильному решению с вероятностью, близкой к 1, лишь после проведения примерно $\frac{\pi}{4}2^{n/2}$ итераций.

Для того, чтобы пояснить этот «трюк» со сходимостью по вероятности к истинному ключу, рассмотрим упрощенную схему, никак не связанную с КК и называемую *усилением амплитуды*.

Пусть имеется набор из N, например, вещественных чисел $a_1, a_2, \dots, a_N$, аналогов амплитуд квантовых состояний. Для полного сходства положим их равными и нормируем:

$$a_1 = a_2 = \cdots = a_N = \frac{1}{\sqrt{N}}.$$

Такой набор чисел соответствует неструктурированной базе данных. Задача состоит в усилении некоторой выделенной амплитуды a_ω. Для этого введем операцию $\hat{U}_\omega$ преобразования числового набора по правилу $\hat{U}_\omega a_x = a_x \; \forall x \neq \omega$ и $\hat{U}_\omega a_\omega = -a_\omega$. Очевидно, что это преобразование – аналог оператора U_ω. Аналогом оператора диффузии U_S является преобразование числового набора по формуле $\hat{U}_S a_x = \frac{2}{N}\sum_y a_y - a_x$. Нетрудно сообразить, что это отражение значений a_x относительно их среднего $\overline{a} = \frac{1}{N}\sum_y a_y$. Последовательное применение операций $\hat{U}_S\hat{U}_\omega = \hat{U}_G$ действует на числовой набор также, как и оператор Гровера $U_G = U_S U_\omega$. В лекции [22] наглядно продемонстрировано, как происходит усиление выделенной амплитуды, соответствующей вероятности выделенного состояния и уменьшение всех остальных вероятностей.

Для примера выполним на классическом компьютере процедуру усиления «пяти-кубитного» набора чисел (N = 32). В качестве выделенной амплитуды возьмем a_2. Результаты выполнения девяти итераций $\hat{U}_G$ приведены в таблице 1. Первый столбец содержит номер итерации k, второй – среднее значение амплитуд $\overline{a}$ на каждом шаге, третий – вторую амплитуду a_2.

ТАБЛИЦА 1. Процедура усиления амплитуды (N = 32)

TABLE 1. Amplitude Enhancement Procedure (N = 32)

k	$\overline{a}$	a_2
0	0,17677	0,17677
1	0,16572	0,50823
2	0,13396	0,77616
3	0,08545	0,94707
4	0,02626	0,99959
5	0,03621	0,92716
6	0,09416	073884
7	0,14034	0,45817
8	0,16897	0,12022
9	0,17649	0,23275

Хорошо видно, как вторая амплитуда сходится по модулю к единице при $k \to 4$ и как деградируют все остальные амплитуды.

Так как с геометрической точки зрения оператор Гровера U_G, как и преобразование $\hat{U}_G$, это оператор поворота вектора состояния квантового регистра в одной гиперплоскости на фиксированный угол, то поведение амплитуд в зависимости от числа итераций носит периодический характер.

Если интерпретировать эти числа как вероятности найти текущий ключ криптосистемы (или как в первом примере – извлечь из памяти КК определенную фотографию), то вероятность нахождения истинного ключа (или искомой фотографии) будет приближаться к единице. Однако, конечно, для выполнения процедуры *усиления амплитуды* совершенно необходимо использовать ККР, где преобразования типа *вычисление среднего* и *инверсия выделенного элемента* должны выполняться не перебором, а одновременно!

Как было отмечено выше, для эффективной при $N = 2^n \gg 1$ реализации алгоритма кубиты нужны не только для «записи» амплитуд состояния квантового регистра, но и для работы квантового шифратора – составной части блока U_ω (рисунок 1), в том числе для хранения открытого текста и криптограммы. Таким образом, число кубит, необходимых для реализации алгоритма, заметно превышает длину n искомого ключа.

В работе [23] достаточно подробно описан взлом при помощи АГ криптосистемы AES с различными, допустимым по стандарту, длинами ключей – 128, 192 и 256. В таблице 2 приводятся результаты расчета требуемого числа кубит для такого квантового криптоанализа, взятые из этой работы.

ТАБЛИЦА 2. Требуемое количество кубитов для выполнения криптоанализа по АГ для стандарта AES с различными длинами ключей

TABLE 2. Number of Qubits Required to Perform AG Cryptanalysis for AES with Different Key Lengths

Длина ключа, n	128	192	256
Количество кубитов	984	1112	1336

В настоящее время лидерами в построении КК являются компании Google и IBM: так, первая еще в 2018 г. реализовала КК с процессором Bristlecone на 72 кубитов [24], вторая же представила в 2023 г. квантовый процессор Heron, имеющий уже 133 кубита и анонсировала создание 1121-кубитного процессора Condor в 2024 г. [25].

Важно также отметить, что с увеличением количества кубитов в КК в них возрастает и вероятность ошибок при выполнении на гейтах различных операций. Поэтому пока весьма проблематично создание КК, содержащих более 100 кубитов,

что подтверждается и авторитетным мнением М. Дьяконова, изложенным им в зарубежной монографии [26].

Кроме того, даже при успешной реализации многобитового КК, из-за нереализуемости слишком большого числа требуемых операций АГ, можно выразить надежду на взлом в будущем, разве лишь, AES-128. Важно также отметить, что в работах, выполненных уже после изобретения АГ, было строго доказано, что не существует другого, более эффективного, чем АГ, метода, требующего менее $2^{n/2}$ итераций при выполнении поиска заданного элемента на неструктурированном множестве.

Заметим, что при попытке понимания эффективного использования АГ для «лобового» криптоанализа, наиболее сложным представляется интуитивно согласиться с возможностью неперебор-ного выполнения операции U_ω, то есть нахождения элемента «ω», обеспечивающего выполнение равенства $f(x, \omega) = y$. Интересно вспомнить, что один из профессоров, специализирующихся именно в квантовой физике, как-то сказал своему коллеге и тоже физику, что понять этот квантовый параллелизм невозможно, но, тем не менее, он работает. Можно привести один пример, который, хотя и не эквивалентен квантовой задаче, но, все же, немного поясняет невозможность полной замены физики математикой. Пусть имеется множество деревянных палочек различного, но близкого веса и похожих друг на друга. Лишь одна из этой кучи палочек сделана из железного дерева (с плотностью древесины ≥ 1000 кг/м³), которое тонет в пресной воде. Требуется отыскать эту палочку. Простейший метод – это поочередно опускать палочки в стакан и найти ту, что тонет. Однако более быстрый метод состоит в том, чтобы вывалить кучу этих палочек в ванну и взять ту, которая пошла на дно.

Еще более впечатляющие результаты дает использование КК при взломе криптосистем с открытым ключом (РША, Эль-Гамаля, Рабина и др.), где оно сводится к решению таких трудных задач теории чисел, как их факторизация и дискретное логарифмирование. Причем, если на обычном ПК их решение оказывается экспоненциально сложным, то КК решает эти задачи с полиномиальной зависимостью от длины ключа.

В работе П. Шора [27] приводится описание алгоритмов и оценка требуемого числа элементарных вычислений для решения этих задач. Поскольку описание данных алгоритмов оказывается достаточно сложным и требует знания, как минимум, основ квантовой физики и теории чисел, приведем здесь только оценки сложности вычислений, необходимых для взлома криптосистемы РША, представленные И. Голдовским в [28]:

– число операций для факторизации числа N – $O\left(n^2 \log_2 n \left(\log_2 \log_2 n\right)\right)$, где $n = \log_2 N$;

– требуемое количество кубит КК – $O(n^3 \log_2 n)$.

Из этих границ следует, что для взлома шифра РША придется при использовании ключей длиной N = 2048 обеспечить количество кубит, равное 4099. Для криптосистем на основе использования эллиптических кривых (требующих более короткий ключ) потребуется 1500 кубит для ключа длиной n = 256 и 2500 – для ключа длиной n = 512.

Так что в настоящее время можно говорить о реализуемости взлома криптосистемы РША с длиной ключа не более 1024 бита. В настоящее время в зарубежной криптографии появилась даже аббревиатура SNDL (*от англ.* Store Now-Decrypt Later) в надежде на прогресс в будущем квантовых компьютеров.

В связи с опасностью взлома криптосистем с открытым ключом при помощи КК появились так называемые *постквантовые* криптосистемы. К ним относится криптосистема Мак-Элис, основанная на экспоненциальной сложности от длины ключа алгоритма исправления ошибок для случайных линейных кодов, а также криптосистемы на основе использования *числовых решеток*.

3. АУТЕНТИФИКАЦИЯ МЕТОДА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ПО ПРОТОКОЛУ ДИФФИ – ХЕЛЛМАНА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ «СПАРИВАНИЯ» МОБИЛЬНЫХ УСТРОЙСТВ

3.1. Принцип формирования симметричного ключа по методу Диффи – Хеллмана

Метод Диффи – Хеллмана [29] позволяет использовать незащищенный от перехвата канал связи для формирования общего ключа шифрования с целью создания безопасного соединения между двумя корреспондентами. Этот метод нашел широкое применение в сетевых протоколах SSL/TLS, IPsec, PGP и др. [9]. Изложим кратко суть метода. Пользователи сети Алиса (*сокр. A*) и Боб (*сокр. B*) согласовывают параметры: p – простое число; g – элемент конечного поля $GF(p)$, порождающий группу, имеющий большой порядок, и выполняют следующий пошаговый протокол.

Шаг 1. Алиса генерирует элемент поля $x \in \in \{1, p-1\}$, вычисляет $X = g^x (\mathrm{mod} p)$ и посылает его Бобу.

Шаг 2. Боб генерирует элемент поля $y \in \in \{1, p-1\}$, вычисляет $Y = g^y (\mathrm{mod} p)$ и посылает его Алисе.

Шаг 3. Алиса вычисляет ключ $K_\mathrm{A} = Y^x (\mathrm{mod} p)$.

Шаг 4. Боб вычисляет ключ $K_\mathrm{B} = X^y (\mathrm{mod} p)$.

Несложно заметить, что ключи $K_\mathrm{A} = K_\mathrm{B}$. Величины X и Y, которыми обмениваются A и B по от-

крытым каналам, называются *значениями Диффи – Хеллмана* (*сокр*. DH-значениями).

Однако данный метод подвержен атаке, известной как «человек посередине». Алиса и Боб при выполнении протокола могут оказаться в ситуации, когда они устанавливают связь со злоумышленником – Евой, которая Алисе выдает себя за Боба, а Бобу представляется Алисой. Поэтому Алисе и Бобу требуется аутентифицировать ключи, сгенерированные по методу Диффи – Хеллмана.

Одним из направлений решения задачи аутентификации ключа является сертификация DH-значений удостоверяющим центром, что делается, например, в протоколе SSL/TLS. Проверка подлинности сертификата осуществляется с использованием открытого ключа, распространяемого в сети. Однако такой подход требует использования технологии PKI (*аббр. от англ.* Public Key Infrastructure, инфраструктура открытых ключей), что не всегда удобно для пользователей, особенно для пользователей мобильных сетей.

Другим подходом к решению задачи аутентификации ключа, распределяемого по методу Диффи – Хеллмана, является использование в целях аутентификации технологии *близкой аутентификации* (называемой иначе *спарингом).* Для этого пользователи *A* и *B* предварительно выполняют процедуру сопряжения своих мобильных устройств во время личной встречи. В результате они формируют двоичные последовательности $\boldsymbol{a}$ и $\boldsymbol{b}$, соответственно, которые впоследствии используют для взаимной аутентификации, в том числе и для аутентификации DH-значений. Предполагается, что нарушитель в момент сопряжения устройств удален от пользователей и не получает доступа к сообщениям, которыми обмениваются пользователи. Специфика решения задачи аутентификации этим способом состоит в том, что пользователи не могут непосредственно использовать вырабатываемые последовательности ни для шифрования, ни для аутентификации, так как эти последовательности содержат определенный процент ошибок (то есть несовпадений бит).

Другой способ выработки аутентифицирующих последовательностей может заключаться в использовании *квантовой телепортации*.

Ниже приводятся результаты исследования аутентификации DH-значений с использованием аутентифицирующих последовательностей независимо от способа их получения.

3.2. Сценарий спаривания мобильных устройств и аутентификации DH-значений

Задача получения пользователями идентичных последовательностей может быть решена на основе создания между пользователями дополнительного канала: визуального, акустического, вибрационного, тактильного, магнитометрического или даже канала квантовой телепортации.

Дополнительный канал образуется между двумя мобильными устройствами при личной встрече пользователей, при этом не требуется передача какой-либо информации по каналу связи, что затрудняет проведение атак со стороны злоумышленника. Для краткости будем называть обмен данными по дополнительному каналу с целью выработки аутентифицирующих последовательностей *близкой аутентификацией* на основе *сопряжения мобильных устройств*.

Поскольку участие пользователей при сопряжении неизбежно, решающими факторами в выборе способа сопряжения являются удобство использования, помехоустойчивость и минимальный объем передаваемых данных; сравнительная характеристика дополнительных каналов по этим критериям приведена в работах [30, 31]. На основе этих данных в наибольшей степени для решения задачи аутентификации подходят вибрационный и магнитометрический каналы.

Вибрационный канал. Его использование представляется возможным для устройств, содержащих в себе датчики акселерометра. Два содержащих их мобильных устройства необходимо встряхивать в одной руке примерно в течение 5 с. В это время осуществляется считывание информации о положении мобильного устройства в пространстве и преобразование ее в цифровой код. Два устройства (*A* и *B*), которые трясли вместе, на выходе получат схожие последовательности.

Магнитометрический канал. Пользователям необходимо удерживать два устройства вблизи друг к другу несколько секунд без выполнения каких-либо дополнительных операций. Устройства считывают собственные показания датчиков магнитометра и обмениваются ими. Сопряжение мобильных устройств с использованием магнитометрического канала, по сравнению с вибрационным, обеспечивает более высокую скорость работы (4,5 с), низкую вероятность ошибочной аутентификации и позволяет минимизировать участие пользователя в процессе сопряжения устройств, что указывает на преимущество магнитометрического канала для выработки случайных последовательностей [30].

Применение магнитометрического канала с целью выработки последовательностей, их использования для построения аутентифицирующих помехоустойчивых кодов (*сокр*. АП-кодов) и аутентификации ключей Диффи – Хеллмана достаточно полно было исследовано в работе [31].

В [32] был рассмотрен способ аутентификации DH-значений на основе использования универсальных хэш-функций, построенных путем ис-

пользования заранее выработанных пользователями аутентифицирующих последовательностей. В работе [33] аутентификация DH-значений осуществлялась на основе алгоритма Картера – Вегмана с одноразовым ключом, в качестве которого использовались аутентифицирующие последовательности, выработанные пользователями во время процедуры спаринга.

Перспективным способом получения аутентифицирующих последовательностей является, на наш взгляд, применение современных квантовых технологий и, в частности, технологии квантовой телепортации, которая интенсивно развивается в последние годы на основе использования теории ЭПР (*аббр. от* Эйнштейн, Подольский, Розен – авторы теории) [34]. Суть этого подхода состоит в осуществлении следующей процедуры.

Во время сопряжения мобильных устройств пользователи, используя специальное устройство, вырабатывают на ЭПР-пару «запутанных» кубит. Один кубит пары записывает в свою квантовую память пользователь *A*, а другой кубит – пользователь *B*. Во время процедуры телепортации, используя эти «запутанные» кубиты и дополнительный канал обмена (не квантовый), пользователи формируют аутентифицирующие последовательности. Перспективность данного подхода нам видится в том, что получение пар кубитов может быть выполнено пользователями на большом расстоянии между ними, и в этом случае необходимость в близкой аутентификации вообще отпадает. В настоящее время достигнуты дальности в процедуре телепортации: в свободном пространстве 1200 км [35], а по оптоволоконному кабелю – 44 км [36]. Однако нужно отметить, что полученные таким образом последовательности полностью не совпадают друг с другом. Точность совпадения квантовых состояний, переданных по волоконно-оптическому кабелю ~90 %. Конечно, многие вопросы телепортации, в частности хранение бит «запутанных» пар, пока окончательно не решены.

Рассмотрим более подробно сценарий сопряжения мобильных устройств, для формирования случайных последовательностей и аутентификации DH-значений с использованием магнитометрического канала, и смартфонов. Сценарий включает четыре этапа (рисунок 2).

1-й этап – этап сопряжения. Алиса и Боб располагают устройства достаточно близко друг к другу (практически касаются друг друга) и удерживают несколько секунд. В это время в каждом смартфоне производится измерение магнитного поля Земли по трем пространственным осям. Значения магнитного поля квантуются и из них формируются двоичные последовательности.

В процессе измерений поля между устройствами осуществляется локальный обмен данными, например, по каналу Bluetooth, для коррекции измерительных базисов устройств с целью обеспечения их идентичности. В итоге каждое устройство формирует случайную двоичную последовательность ***a*** или ***b*** необходимой длины. Эти последовательности пользователи записывают в память своих устройств и будут использовать по мере необходимости как ключи в процедуре аутентификации DH-значений. Обозначим $p_m = P(a_i \neq \neq b_i)$, где $i = 1, 2 \ldots L$ – номер символа в последовательностях, p_m – вероятность несовпадения бит в последовательностях ***a*** и ***b***.

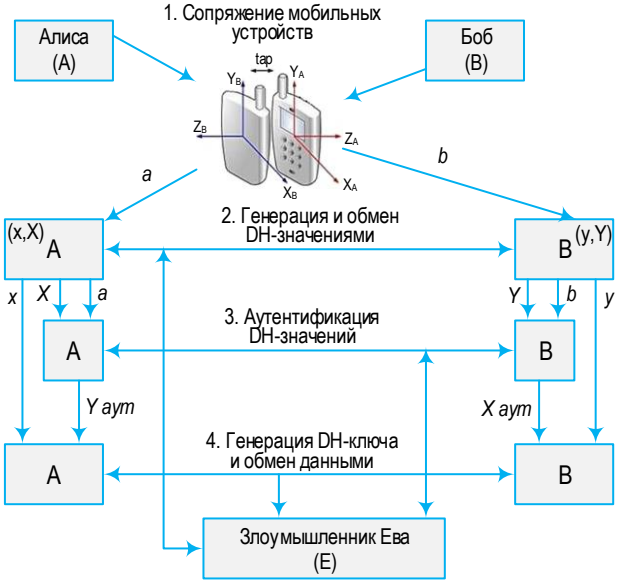

Рис. 2. Сценарий спаривания мобильных устройств и формирования ключа Диффи – Хеллмана с его аутентификацией

Fig. 2. Scenario of Pairing Mobile Devices and Formation of Diffie – Hellman Key with Its Authentication

В работе [30] подробно описан процесс сбора и коррекции данных магнитометров, в частности, предложен протокол Magpairing для создания корреспондентами *A* и *B* случайных последовательностей на основе магнитометрического канала и их использования для аутентификации DH-значений. Нами были проведены аналогичные исследования [37], которые подтвердили результаты этой работы; вероятность совпадения символов последовательностей, полученных от двух устройств в наших экспериментах составила 0,94.

Предполагается, что нарушитель (посторонний пользователь) также имеет магнитометр и может быть расположен достаточно близко к сопрягаемым устройствам, но не в точке сопряжения, поэтому сформировать последовательность, совпадающую с большой вероятностью с ***a*** и ***b*** он не может. Будем полагать, что вероятность несовпадения символов в последовательности, которую может сформировать нарушитель, с символами по-

следовательности легальных пользователей равна $p_e = P(a_i \neq e_i) = 1/2, i = 1, 2 \ldots L$, что соответствует обрыву канала.

2-й этап. Алиса и Боб вырабатывают секретные числа x и y, соответственно, вычисляют DH-значения и обмениваются ими, используя канал связи между A и B, контролируемый нарушителем, который может выполнять пассивные и активные атаки на передаваемую информацию.

3-й этап – аутентификация переданных по каналу DH-значений на основе использования последовательностей $\boldsymbol{a}$ и $\boldsymbol{b}$ в качестве ключа аутентификации для формирования и проверки аутентификаторов, передаваемых от A к B и обратно.

4-й этап. Если аутентификация DH-значений в обе стороны прошла успешно, то Алиса и Боб, используя имеющиеся у них случайные числа x и y, соответственно, вычисляют ключи по методу Диффи – Хеллмана.

Однако, как показано в [31], способ с использованием магнитометрического канала подвержен атаке «человек посередине» (см. п. 3.1); там также предложен способ устранения этой уязвимости на основе использования аутентифицирующих помехоустойчивых кодов. Дальнейшее развитие этот способ получил в работах [32, 33], где были предложены способы применения аутентифицирующих последовательностей $\boldsymbol{a}$ и $\boldsymbol{b}$ для формирования аутентификаторов по алгоритму Вегмана – Картера с использованием универсальных хэш-функций (WCA UH, *аббр. от англ.* Wegman-Carter Algorithm Universal Hash Function) и/или с одноразовым ключом (WCA OTP, *аббр. от англ*. Wegman-Carter Algorithm One Time Password) [38].

Способ аутентификации на основе алгоритмов WCA UH и WCA OTP схожи и отличаются эффективностью в плане расхода аутентифицирующих последовательностей $\boldsymbol{a}$ и $\boldsymbol{b}$, которые выработали корреспонденты на этапе близкой аутентификации. В то же время WCA UH представляет основу для обоих алгоритмов, поэтому рассмотрим далее детально способ аутентификации DH-значений на основе универсальных хэш-функций.

3.3. Аутентификация DH-значений на основе предварительно распределенных случайных последовательностей и алгоритма WCA UH

Рассмотрим этап аутентификации DH-значений согласно сценарию, показанному на рисунке 1.

Пользователь A разделяет DH-значение X на N блоков длиной m бит. Для каждого блока $\boldsymbol{u_i}$ вычисляется аутентификатор $\boldsymbol{w_i}$ длиной v бит ($i = 1, 2, \ldots, N$) на основе универсального класса хэш-функций и использования последовательности $\boldsymbol{a}$ в качестве ключа. Для аутентификации каждого следующего блока выбираются новый блок в последовательности $\boldsymbol{a}$.

Корреспондент B проводит аутентификацию DH-значения следующим образом. Для каждого принятого блока $\boldsymbol{u_i}$ вычисляется аутентификатор $\boldsymbol{w_i'}$ с использованием последовательности $\boldsymbol{b}$, который сравнивается с аутентификатором $\boldsymbol{w_i}$, полученным по каналу связи. Если $\boldsymbol{w = w_i'}$, то блок $\boldsymbol{u_i}$ аутентифицирован, и не аутентифицирован в противном случае. DH-значение считается аутентифицированным в целом, если среди N принятых блоков окажутся не аутентифицированными не более Δ блоков $1 \leq \Delta \leq N$.

Аутентификатор для каждого блока вычисляется согласно алгоритму WCA UH. Представим подблок $\boldsymbol{u}$, как элемент поля Галуа GF(2^m). Тогда аутентификатор $w = [u \times k_0 + k_1]_v$, где $k_0, k_1 \in \in GF(2^m)$ – ключи аутентификации. Знаки $\times, +$ обозначают, соответственно, умножение и сложение в конечном поле $GF(2^m)$, а $\lfloor \cdot \rfloor_v$ – «усечение», то есть выбор v левых или правых элементов последовательности в квадратных скобках. Блоки длиной m бит выбираются поочередно из последовательности $\boldsymbol{a}$. Для каждого очередного блока $\boldsymbol{u_i}$ формируется новый аутентификатор $\boldsymbol{w_i}$ с использованием новой пары ключей k_0 и k_1. Вероятность навязывания ложного блока при известных $\boldsymbol{u}$ и $\boldsymbol{w}$ для данного способа аутентификации определяется соотношением $P_s = 1/2^v$ [38].

Длина ключа аутентификации (минимальная длина последовательности $\boldsymbol{a}$), необходимая для аутентификации DH-значения: $L = 2mN$.

Будем считать, что нарушитель Ева может осуществить следующие атаки.

Атака *подмены.* Нарушитель перехватывает DH-значение $X = g^x$ длиной n_0 бит, передаваемое в виде подблоков u_i и аутентификаторов $w_i, i = 1,2, \ldots, N$. Генерирует ложное сообщение $X' = g^{x'}$, отличающееся от исходного в D блоках и формирует аутентификаторы к нему по следующему правилу:

– если блоки u_i в исходном и ложном сообщении совпали, он использует перехваченные аутентификаторы;

– если блоки не совпали, нарушитель формирует аутентификаторы случайным образом.

Атака *имперсонализации.* Ложное DH-значение $X' = g^{x'}$ создается нарушителем без предварительного приема истинного DH-значения от корреспондента A.

Оценку эффективности аутентификации DH-значения будем осуществлять по следующим параметрам:

P_f – вероятность ложного отклонения DH-значения в отсутствие навязывания; событие наступает, когда число неправильно аутентифицированных блоков равно Δ и более из-за несогласованности аутентифицирующих последовательностей $\boldsymbol{a}$ и $\boldsymbol{b}$;

P_i – вероятность *имперсонализации*; наступает, когда нарушитель создает ложное DH-значение (без предварительного приема истинного DH-значения), которое принимается как истинное;

P_s – вероятность подмены DH-значения; наступает, когда нарушитель создает ложное DH-значение, отличающегося от истинного в D блоках размерности m (обозначим вероятность этого события – $P_g(D)$), и навязывает его корреспонденту (вероятность обмана – $P_r(D)$); поскольку величина D определяется злоумышленником, то в худшем случае:

$$P_s = \max_D(P_g(D) \times P_r(D)); \quad (3)$$

P_d – вероятность навязывания ложного DH-значения:

$$P_d = \max(P_i, P_s); \quad (4)$$

L – длина ключа аутентификации (длина последовательностей $\boldsymbol{a}$ и $\boldsymbol{b}$), необходимая для аутентификации DH-значения длиной n_0 с заданными значениями $\tilde{P}_f, \tilde{P}_d$;

$W = vN$ – суммарная длина всех аутентификаторов DH-значения.

Вероятность P_f может быть оценена, как вероятность суммы событий, состоящих в том, что в принятой последовательности X из-за ошибок в аутентифицирующих последовательностях окажется не аутентифицированными $\Delta + 1$ и более блоков:

$$P_f(\Delta) = \sum_{i=\Delta+1}^{N} C_N^i p_b^i \times (1 - p_b)^{N-i}, \quad (5)$$

где p_b – вероятность несовпадения ключей (k_0, k_1) равна вероятности несовпадения блоков длиной $2m$ бит, выбранных их последовательностей $\boldsymbol{a}$ и $\boldsymbol{b}$ и равняется $p_b = 1 - (1 - p_m)^{2m}$ в предположении, что ошибки в битах распределены по закону Бернулли.

Вероятность успешной атаки *имперсонализации* можно получить, как оценку количества обнаруженных и необнаруженных ложных аутентификаторов в N блоках при их случайном генерировании. Учитывая, что вероятность успешного навязывания ложного аутентификатора длиной v символов при использовании универсальных хэш-функций равна $1/2^v$, можно записать:

$$P_f(\Delta) = \sum_{i=0}^{\Delta} C_N^i (\frac{1}{2^v})^{(N-i)} \times (1 - \frac{1}{2^v})^i. \quad (6)$$

Для оценки вероятности подмены P_s рассмотрим сомножители в (3).

Очевидно, что чем меньше отличаются истинное DH-значение X и ложное X', тем легче нарушителю реализовать атаку *подмены*. Заметим, что непосредственно значение X' нарушитель выбрать не может. Сначала он выбирает число x', затем находит значение экспоненты $X' = g^{x'} \bmod p$. Если x' выбирать случайно из множества чисел от 0 до p–1, то число X' будет также случайным числом из множества чисел от 0 до p–1. При большом значении модуля $p \approx 2^{256}$ нахождение отображения $x' \Leftrightarrow X'$ требует необозримо бóльших вычислительных затрат. Поэтому разумной стратегией для нарушителя будет случайный выбор числа x', что равносильно случайному выбору X'.

Вероятность случайного формирования нарушителем ложного DH-значения X', отличающегося от перехваченного значения X в D блоках, может быть найдена на основе комбинаторных рассуждений о выпадении одинаковых значений двух 2^m-гранных игральных костей при N бросаниях и записана как:

$$P_g(D) = C_N^D \left(\frac{1}{2^m}\right)^{N-D} \times \left(1 - \frac{1}{2^m}\right)^D. \quad (8)$$

Вероятность навязывания сформированного ложного DH-значения, отличающегося от истинного в D блоках, в зависимости от порога принятия решения Δ, можно оценить как:

$$P_r(\Delta) \le \sum_{i=0}^{\Delta} C_D^i (\frac{1}{2^v})^{(D-i)} \times (1 - \frac{1}{2^v})^i \sum_{j=0}^{t} C_{(N-D)}^j p_b^j \times \times (1 - p_b)^{(N-D-j)}, \quad (9)$$

где $t = \begin{cases} N - D, \text{если } \Delta - i \ge N - D. \\ \Delta - i, \text{если } \Delta - i < N - D \end{cases}$

Первая сумма в (9) характеризует вероятность фиксации на приеме i ложных аутентификаторов $(0 \le i \le \Delta)$, которые обнаруживаются, и D-i ложных аутентификаторов, которые не обнаруживаются. Вторая сумма – это вероятность несовпадения j $(0 \le j \le t)$ из N–D аутентификаторов исходного сообщения, которые нарушителем были переданы без изменений, а несовпадение произошло за счет несоответствия ключей в аутентифицирующих последовательностях $\boldsymbol{a}$ и $\boldsymbol{b}$.

Рассмотрим пример выбора параметров системы аутентификации, реализующей описанный выше способ. Пусть DH-значение, которое необходимо аутентифицировать, имеет длину 256 бит, вероятность несовпадения аутентифицирующих последовательностей p_m = 0,05. К системе аутентификации предъявлены требования: $\tilde{P}_f = \tilde{P}_d = 10^{-6}$.

Выберем несколько длин аутентифицируемых блоков m = 1, 2, 4, 8, 16, 32, среди которых будем искать удовлетворяющие заданным требованиям.

Используя соотношение (6), построим зависимость $P_f(\Delta)$ для выбранных длин блока аутентификации (рисунок 3). На пересечении кривых $P_f(\Delta, m)$ и прямой $P_f = 10^{-6}$ находим значения

порогов (Δ_{min} = 50, 46, 40, 30 для m = 1, 2, 4, 8, соответственно), при которых выполняется неравенство $P_f \le \tilde{P}_f$. Для m = 16 и 32 такие условия не выполняются, поэтому для дальнейшего исследования оставляем блоки с длинами 1, 2, 4, 8.

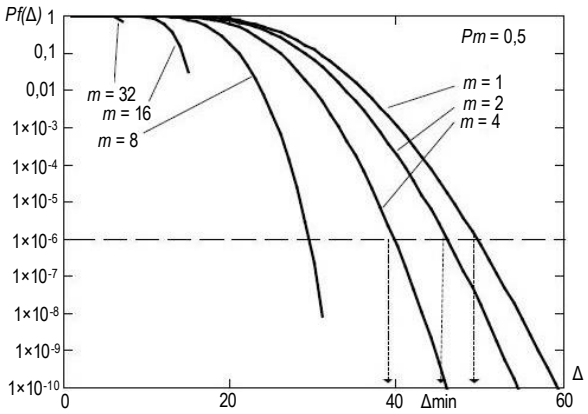

Рис. 3. Зависимость вероятности ложного отклонения DH-значения от порога Δ для разны длин x_0 аутентифицируемых блоков

Fig. 3. False Rejection Probability of the DH Value Dependence on the Threshold Δ for Different Lengths x_0 of Authenticated Blocks

Используя найденные значения Δ_{min}, построим зависимости $P_s(D) = P_g(D) \times P_r(D)$ для выбранных блоков длины m и всех аутентификаторов длины $v \le m$. Зависимости $P_g(D)$ и $P_r(D)$ рассчитываются согласно (8) и (9) (рисунок 4). По полученным зависимостям находим значения $P_s = \max_D P_s(D)$.

Максимумы кривых на рисунке 4 соответствуют вероятностям подмены в соответствии с соотношением (3) для разных значений длин аутентифицируемого блока (m) и аутентификатора (v). Вероятности ложного отклонения, подмены, имперсонализации, навязывания рассчитанные для этих значений представлены в таблице 3. Видим, что условию $\tilde{P}_f = \tilde{P}_d = 10^{-6}$ удовлетворяют только пары (m, v): (2,2) и (4,4).

В данном примере значение вероятности подмены, удовлетворяющее требованию $P_f \le 10^{-6}$, выполняется только при $m = v$, поэтому суммарная длина всех аутентификаторов равна длине DH-значения и равна W = 256 бит, а требуемая для аутентификации длина последовательностей ***a*** и ***b*** (длина ключа аутентификации) равна L = 512 бит.

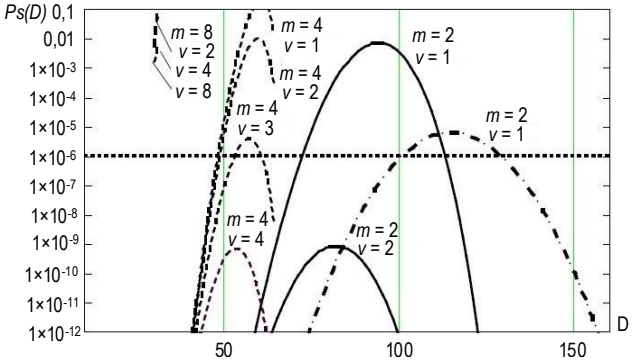

Рис. 4. Зависимость вероятности подмены от количества блоков, в которых различаются истинное и ложное DH-значения (D) для отобранных пар (m, v)

Fig. 4. Dependence of Substitution Probability on the Blocks Number in Which True and False DH-Values (D) Differ for the Selected Pairs (m, v)

ТАБЛИЦА 3. Значения вероятности ложного отклонения (P_f), подмены (P_s), имперсонализации (P_i) и навязывания (P_d) для пар (m,v)

TABLE 3. Values of the Probability of False Rejection (P_f), Substitution (P_s), Impersonation (P_i) and Imposition (P_d) for Pairs (m, v)

(m,v)	P_f	P_s	P_i	$P_d = \max(P_s', P_i)$
(1,1)	7,1×10^{-7} (+)	6,2×10^{-6} (-)	5,7×10^{-24} (+)	6,2×10^{-6} (-)
(2,2)	**1×10^{-6} (+)**	**8,1×10^{-10} (+)**	**1,4×10^{-20} (+)**	**8,1×10^{-10} (+)**
(2,1)	1×10^{-6} (+)	7,4×10^{-3} (-)	9,3×10^{-4} (-)	7,4×10^{-3} (-)
(4,4)	**6,5×10^{-7} (+)**	**6,8×10^{-10} (+)**	**2,7×10^{-13} (+)**	**6,8×10^{-10} (+)**
(4,3)	6,5×10^{-7} (+)	3,8×10^{-6} (-)	3,3×10^{-7} (+)	3,8×10^{-6} (-)
(4,2)	6,5×10^{-7} (+)	1×10^{-2} (-)	1,8×10^{-2} (-)	1×10^{-2} (-)
(4,1)	6,5×10^{-7} (+)	1,4×10^{-1} (-)	9,8×10^{-1} (-)	1,4×10^{-1} (-)

Таким образом, приведенное выше исследование показало, что, используя процедуру аутентификации спариванием на основе магнитометрического или вибрационного каналов, содержащих небольшой процент ошибок ≈ 5 %, можно достаточно надежно осуществить аутентификацию секретного ключа, распределяемого между мобильными устройствами по алгоритму Диффи – Хеллмана.

Продолжение следует…

Список источников

1. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
2. ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
3. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012.
4. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2012.
5. Бабаш А.В., Шанкин Г.П. Криптография. М.: Изд-во Солон-Р, 2002. 511 с.
6. Korjik V.I., Mukherjii A., Eremeev M.A., Moldovyan N.A. Fault-based analysis of flexible ciphers // Computer Science Journal of Moldova. 2002. Vol. 10. Iss. 2. PP. 223–236.

7. Korzhik V., Yakovlev V., Kovajkin Yu., Morales-Luna G. 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. DOI:10.14569/IJACSA.2012.030127

8. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие. СПб.: Издательский центр Интермедиа, 2016. 312 с. EDN:WEQWMN

9. Коржик В.И., Кушнир Д.В. Основы защиты информации в компьютерных системах. Методические указания к лабораторным работам. Часть 1. СПб: СПбГУТ, 1999. 17 с.

10. Alpern B., Schneider F.B. Key exchange using 'keyless cryptography' // Information Processing Letters. 1983. Vol. 16. Iss. 2. PP. 79-81. DOI:10.1016/0020-0190(83)90029-7

11. Korzhik V., Starostin V., Yakovlev V., Kabardov M., Krasov A. and Adadurov S. Advance in Keyless Cryptography // In: Ramakrishnan S., ed. Lightweight Cryptographic Techniques and Cybersecurity Approaches. IntechOpen, 2022. DOI:10.5772/intechopen.104429

12. Shannon C.E. Communication theory of secrecy systems // Bell System Technical Journal. 1949. Vol. 28. Iss. 4. PP. 656–715. DOI:10.1002/j.1538-7305.1949.tb00928.x

13. Vernam G.S. Secret signaling System. Patent US, no. 1310719A, 22.07.1919.

14. Лавриков И.В., Шишкин В.А. Какой объем данных можно безопасно обрабатывать на одном ключе в разных режимах? // Математические вопросы криптографии. 2019. Т. 10. № 2. С. 125–134 DOI:10.4213/mvk290

15. Williams C.P. Explorations in Quantum Computing. Texts in Computer Science. 2011. DOI:10.1007/978-1-84628-887-6.

16. Алгоритм Гровера. URL: http://www.youtube.com/watch?v=cQDpimNzKMo (дата обращения 10.05.2024)

17. Денисенко Д.В., Никитенкова М.В. Применение Квантового Алгоритма Гровера в задаче поиска ключа блочного шифра SDES // Журнал экспериментальной и теоретической физики. 2019. Т. 155. № 1. С. 32–53. DOI:10.1134/S0044451019010036. EDN:VRNRNG

18. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ. М.: Мир, 2006. 824 с.

19. Кайе Ф., Лафламм Р., Моска М. Введение в квантовые вычисления. М. – Ижевск: НИЦ «Регулярная и хаотическая динамика», Институт компьютерных исследований, 2012. 360 с.

20. Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information // Contemporary Physics. 2011. Vol. 52. Iss. 6. PP. 604–605 DOI:10.1080/00107514.2011.587535

21. Grover L.K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing (STOC'96, Philadelphia, USA, 22–24 May 1996). New York: ACM, 1996. DOI:10.1145/237814.237866

22. Запрягаев А. Квантовые компьютеры. URL: http//www.youtube.com/watch (дата обращения 10.05.2024)

23. Grassl M., Langenberg B., Roetteler M., Steinwandt R. Applying Grover's algorithm to AES: quantum resource estimates // arXiv:1512.04965v1 [quantum-ph]. 2015. DOI:10.48550/arXiv.1512.04965

24. A Preview of Bristlecone, Google's New Quantum Processor // Google Research. 2018. URL: https://research.google/blog/a-preview-of-bristlecone-googles-new-quantum-processor (Accessed 10.05.2024)

25. IBM представила свой мощнейший квантовый процессор Heron и первый модульный квантовый компьютер // 3Dnews. 2023. URL: https://3dnews.ru/1096936/ibm-predstavila-133kubitniy-kvantoviy-protsessor-heron-i-perviy-modulniy-kvantoviy-kompyuter (дата обращения 10.05.2024)

26. Dyakonov M.I. Is Fault-Tolerant Quantum Computation Really Possible? In: Future Trends in Microelectronics // arXiv:quant-ph/0610117v1. 2006. DOI:10.48550/arXiv.quant-ph/0610117

27. 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

28. Голдовский И. Посткванговая криптография. Готовимся сегодня? // ПЛАС. 2022. № 2(288). URL: https://plusworld.ru/journal/2022/plus-2-2022/postkvantovaya-kriptografiya-gotovimsya-segodnya (дата обращения 10.05.2024)

29. Diffe M., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22. Iss. 6. PP. 644–654. DOI:10.1109/TIT.1976.1055638

30. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. Vol. 1. Iss. 6. PP. 1304–1319. DOI:10.1109/TIFS.2015.2505626

31. Яковлев В.А. Аутентификация ключей, распределяемых методом Диффи – Хеллмана, для мобильных устройств на основе аутентифицирующих помехоустойчивых кодов и магнитометрических данных // Труды СПИИРАН. 2019. Т. 18. № 3. С. 705–740. DOI:10.15622/sp.2019.18.3.705-740. EDN:PRNILE

32. Yakovlev V., Korzhik V., Adadurov S. Authentication of Diffie-Hellman Protocol for Mobile Units Executing a Secure Device Pairing Procedure in Advance // Proceedings of the 29th Conference of Open Innovations Association (FRUCT, Tampere, Finland, 12–14 May 2021). 2021. PP. 385–392. EDN:DWHDGP

33. Яковлев В.А. Способ аутентификации значений Диффи – Хеллмана на основе предварительно распределенных случайных последовательностей и алгоритма аутентификации Вегмана – Картера с одноразовым ключом. // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 79–90. DOI:10.31854/1813-324X-2021-7-3-79-90. EDN:TBVSMD

34. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ. М.: Мир, 2006. 824 с.

35. Castelvecchi D. China's quantum satellite clears major hurdle on way to ultrasecure communications // Nature. 2017. DOI:10.1038/nature.2017.22142

36. Nield D. Quantum Teleportation Was Just Achieved With 90% Accuracy Over a 44km Distance // ScienceAlert. 2020. https://www.sciencealert.com/scientists-achieve-sustained-high-fidelity-quantum-teleportation-over-44-km (Accessed 10.05.2024)

37. Корпусов В.Д., Ольховой О.О., Яковлев В.А. Исследование датчика случайных чисел на основе магнитометра // VII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, Россия, 28 февраля–1 марта 2018). СПб.: СПбГУТ, 2018. С. 488–494. EDN:OVMQXN

38. Wegman M.N., Carter J.L. New Hash Functions and their Use in Authentication and Set Equality // Journal of Computer and System Sciences. 1981. Vol. 22. Iss. 3. PP. 265–279. DOI:10.1016/0022-0000(81)90033-7

References

1. GOST 28147-89 *Information processing systems. Cryptographic protection. Algorithm of cryptographic transformation*. (in Russ.)
2. GOST P 34.12-2015 *Information technology. Cryptographic data security. Block ciphers*. Moscow: Standartinform Publ.; 2015. (in Russ.)
3. GOST P 34.10-2012 *Information technology. Cryptographic data security. Generation and verification processes of electronic digital signature.* Moscow: Standartinform Publ.; 2012. (in Russ.)
4. GOST P 34.11-2012 *Information technology. Cryptographic data security. Hash-function.* Moscow: Standartinform Publ.; 2012. (in Russ.)
5. Babash A.V., Shankin G.P. *Cryptography*. Moscow: Solon-R Publ.; 2002. 511 p. (in Russ.)
6. Korjik V.I., Mukherjii A., Eremeev M.A., Moldovyan N.A. Fault-based analysis of flexible ciphers. *Computer Science Journal of Moldova*. 2002;10(2):223–236.
7. Korzhik V., Yakovlev V., Kovajkin Yu., Morales-Luna G. Secret Key Agreement Over Multipath Channels Exploiting a Variable-Directional Antenna. *International Journal of Advanced Computer Science and Applications*. 2012;3(1):172–178. DOI:10.14569/IJACSA.2012.030127
8. Korzhik V.I., Yakovlev V.A. *Fundamentals of Cryptography*. St. Petersburg: Intermedia Publ.; 2016. 312 p. (in Russ.) EDN:WEQWMN
9. Korzhik V.I., Kushnir D.V. *Fundamentals of information protection in computer systems. Methodical instructions for laboratory works. Part 1*. St. Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications Publ.; 1999. 17 p. (in Russ.)
10. Alpern B., Schneider F.B. Key exchange using 'keyless cryptography'. *Information Processing Letters*. 1983;16(2):79–81. DOI:10.1016/0020-0190(83)90029-7
11. Korzhik V., Starostin V., Yakovlev V., Kabardov M., Krasov A. and Adadurov S. Advance in Keyless Cryptography. *In: Ramakrishnan S., ed. Lightweight Cryptographic Techniques and Cybersecurity Approaches*. IntechOpen; 2022. DOI:10.5772/intechopen.104429
12. Shannon C.E. Communication theory of secrecy systems. *Bell System Technical Journal*. 1949;28(4):656–715. DOI:10.1002/j.1538-7305.1949.tb00928.x
13. Vernam G.S. *Secret signaling System*. Patent US, no. 1310719A, 22.07.1919.
14. Lavrikov L.V., Shishkin V.A. How much data may be safely processed on one key in different modes? *Mathematical Aspects of Cryptography.* 2019;10(2):125–134 (in Russ.) DOI:10.4213/mvk290
15. Williams C.P. *Explorations in Quantum Computing. Texts in Computer Science*. 2011. DOI:10.1007/978-1-84628-887-6.
16. *Grover algorithm*. (in Russ.) URL: http://www.youtube.com/watch?v=cQDpimNzKMo [Accessed 10.05.2024]
17. Denisenko D.V., Nikitenkova M.V. Application of Grover's Quantum Algorithm for SDES Key Searching. *Journal of Experimental and Theoretical Physics*. 2019;128(1):25–44. (in Russ.) DOI:10.1134/S1063776118120142. EDN:GGWKYZ
18. Nielsen M.A., Chuang I.L. *Quantum Computation and Quantum Information*. Cambridge Universities Press; 2001.
19. Kaye F., Laflamme R., Mosca M. *Introduction to quantum computing*. Moccow – Izhevsk: Regulyarnaya i haoticheskaya dinamika Publ.; Institut komp'yuternyh Issledovanij Publ.; 2012. 360 p. (in Russ.)
20. Nielsen M.A., Chuang I.L. Quantum computation and Quantum Information. *Contemporary Physics.* 2011;52(6):604–605. DOI:10.1080/00107514.2011.587535
21. Grover L.K. A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, STOC'96, 22–24 May 1996, Philadelphia, USA*. New York: ACM; 1996. DOI:10.1145/237814.237866
22. Zapryagaev A. *Quantum computers*. (in Russ.) URL: http//www.youtube.com/watch [Accessed 10.05.2024]
23. Grassl M., Langenberg B., Roetteler M., Steinwandt R. Applying Grover's algorithm to AES: quantum resource estimates. *arXiv:1512.04965v1 [quantum-ph]*. 2015. DOI:10.48550/arXiv.1512.04965
24. *Google Research*. A Preview of Bristlecone, Google's New Quantum Processor. 2018. URL: https://research.google/blog/a-preview-of-bristlecone-googles-new-quantum-processor [Accessed 10.05.2024]
25. *3Dnews*. IBM unveiled its most powerful quantum processor, Heron, and the first modular quantum computer. 2023. URL: https://3dnews.ru/1096936/ibm-predstavila-133kubitniy-kvantoviy-protsessor-heron-i-perviy-modulniy-kvantoviy-kompyuter [Accessed 10.05.2024]
26. Dyakonov M.I. Is Fault-Tolerant Quantum Computation Really Possible? In: Future Trends in Microelectronics. *arXiv:quant-ph/0610117v1*. 2006. DOI:10.48550/arXiv.quant-ph/0610117
27. 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
28. Goldovsky I. Post-quantum cryptography. Are we preparing today? *PLUS*. 2022;2(288). (in Russ.) URL: https://plusworld.ru/journal/2022/plus-2-2022/postkvantovaya-kriptografiya-gotovimsya-segodnya [Accessed 10.05.2024]
29. Diffe M., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976;22(6):644–654. DOI:10.1109/TIT.1976.1055638
30. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer. *IEEE Transactions on Information Forensics and Security*. 2016;1(6):1304–1319. DOI:10.1109/TIFS.2015.2505626
31. Yakovlev V.A. Authentication of Keys Distributed by the Diffie – Hellman Method for Mobile Devices Based on Authentication Codes and Magnetometric Data. *SPIIRAS Proceedings*. 2019;18(3):705–740. (in Russ.) DOI:10.15622/sp.2019.18.3.705-740. EDN:PRNILE

32. Yakovlev V., Korzhik V., Adadurov S. Authentication of Diffie-Hellman Protocol for Mobile Units Executing a Secure Device Pairing Procedure in Advance. *Proceedings of the 29th Conference of Open Innovations Association, FRUCT, 12–14 May 2021, Tampere, Finland*. 2021. p.385–392. EDN:DWHDGP

33. Yakovlev V. Method for Authentication of Diffie – Hellman Values Based on Pre-Distributed Random Sequences and Wegman – Carter One-Time Pad Algorithm. *Proceedings of Telecommunication Universities.* 2021;7(3):79–90. (in Russ.) DOI:10.31854/1813-324X-2021-7-3-79-90. EDN:TBVSMD

34. Nielsen M., Chang I. *Quantum computing and quantum information*. Moscow: Mir Publ.; 2006. 824 p. (in Russ.)

35. Castelvecchi D. China's quantum satellite clears major hurdle on way to ultrasecure communications. *Nature*. 2017. DOI:10.1038/nature.2017.22142

36. Nield D. Quantum Teleportation Was Just Achieved With 90% Accuracy Over a 44km Distance. *ScienceAlert*. 2020. https://www.sciencealert.com/scientists-achieve-sustained-high-fidelity-quantum-teleportation-over-44-km [Accessed 10.05.2024]

37. Korpusov V., Olkhovoy O., Yakovlev V. The Research of the Random Number Generator Based on the Magnetometer. *Proceedings of the VIIth International Conference on Infotelecommunications in Science and Education, 28 February – 1 Murch 2018, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2018. p.488–494. (in Russ.) EDN:OVMQXN

38. Wegman M.N., Carter J.L. New Hash Functions and their Use in Authentication and Set Equality. *Journal of Computer and System Sciences*. 1981;22:265–279. DOI:10.1016/0022-0000(81)90033-7

Статья поступила в редакцию 12.05.2024; одобрена после рецензирования 14.06.2024; принята к публикации 01.07.2024.
The article was submitted 12.05.2024; approved after reviewing 14.06.2024; accepted for publication 01.07.2024.

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

ИЗОТОВ Борис Викторович
кандидат технических наук, заместитель технического директора, начальник сектора защиты информации ЗАО «Научные приборы»
https://orcid.org/0009-0004-7081-3610

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.