Письма в ЖЭТФ, том 121, вып. 6, с. 503 – 512 

# О трудоемкости перебора в квантовой криптографии с теоретико-информационно стойкой аутентификацией

*С. П. Кулик*[+], *С. Н. Молотков*[*1)]

[+]*Центр квантовых технологий, МГУ имени М. В. Ломоносова, 119991 Москва, Россия*

[*]*Институт физики твердого тела имени Ю. А. Осипьяна РАН, 142432 Черноголовка, Россия*

Поступила в редакцию 26 декабря 2024 г.
После переработки 10 февраля 2025 г.
Принята к публикации 10 февраля 2025 г.

Стойкость систем квантового распределения ключей базируется не только на детектировании атак на квантовые состояния, которое гарантируется фундаментальными законами квантовой теории, но и на обеспечении целостности классических сообщений, передаваемых по вспомогательному классическому каналу связи. Для детектирования вторжений в классический канал связи используется процедура аутентификации. Теоретико-информационная аутентификация гарантирует обнаружение вторжений в классический канал связи независимо от вычислительных и технических возможностей нарушителя, включая квантовый вычислитель.

В работе впервые простыми средствами решен принципиальный для квантовой криптографии вопрос о связи между абстрактным критерием стойкости систем КРК с теоретико- информационной аутентификацией и сложностью поиска квантовых ключей.

DOI: 10.31857/S0370274X25030234, EDN: RDSOJG

**Введение.** В квантовой криптографии используются два открытых и доступных для прослушивания канала связи [1]. Квантовый канал доступен для вторжения и модификации передаваемых квантовых состояний. Классический канал является открытым, но должен быть аутентичным и используется для вспомогательных сообщений между Алисой и Бобом. Аутентичность классического канала означает обеспечение целостности – неизменяемости передаваемых открытых классических сообщений.

Финальным продуктом квантового распределения ключей (КРК) является "квантовый" ключ, который в явном виде даже не фигурирует в критерии стойкости, основанном на различимости квантовых состояний. Ключ называется $\varepsilon$-секретным, если следовое расстояние между квантовым состоянием, описывающим реальную ситуацию КРК, и состоянием для идеальной ситуации не превышает $\varepsilon$.

Реальная ситуация – сеанс квантового распределения ключей с вторжением нарушителя в квантовый канал связи, и аутентификацией в классическом канале связи, при которой возможна подмена сообщений.

Идеальная ситуация – сеанс квантового распределения ключей без вторжения в квантовый канал связи, и аутентификация без подмены сообщений в классическом канале связи.

Критерий стойкости, основанный на следовом расстоянии является довольно абстрактным.

При использовании квантового ключа для криптографических целей интересна не малость следового расстояния сама по себе, а трудоемкость – сложность поиска квантового ключа, который используется в дальнейших приложениях, например, в шифровании.

*Вопрос о том, как сложность поиска квантовых ключей зависит от величины следового расстояния, является принципиальным для квантовой криптографии. Ответ на данный вопрос долгое время отсутствовал, что приводило к эмоциональным дискуссиям в научном сообществе [2–6].*

Впервые ответ на данный вопрос был получен в работах [7–9], где были представлены явные аналитические выражения, связывающие величину следового расстояния с трудоемкостью – числом шагов перебора до определения квантового ключа.

*При этом в [7–9] считалось, что классический аутентичный канал является идеальным – нарушитель не вторгается в канал и не производит подмены классических сообщений. В реальной ситуации аутентификация не является идеальной, и нарушитель может подменять классические сообщения,*

[1)]e-mail: sergei.molotkov@gmail.com

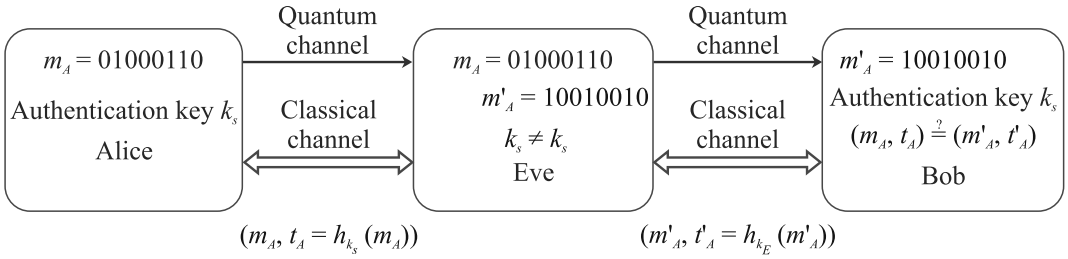


Рис. 1. Иллюстрация атаки *Man-in-the-Middle*. Нарушитель разрывает квантовый и классический каналы связи и генерирует отдельные ключи Алиса–Ева и Ева–Боб. Такая атака не обнаруживается, если классический канал не обеспечивает аутентичность – немодифицируемость открытых классических сообщений

*что может приводить к нарушению целостности передаваемых сообщений.*

Нарушитель может производить атаку человек посредине – *Man-in-the-Middle* (рис. 1) [10–12]. Без атак на классический канал связи нарушитель может атаковать только состояния в квантовом канале. Если нарушитель может подменять еще и классические сообщения, то круг атак расширяется. Крайне сложно, установить критерий $\varepsilon$-секретности для сложного составного процесса. Абстрактный критерий секретности, основанный на следовой метрике, обладает одним важным и удобным свойством. Оказывается, что критерий секретности может быть разложен на критерии секретности между отдельными элементарными процессами. Для отдельных процессов можно вычислить следовое расстояние, тогда следовое расстояние между составными реальными и идеальными процессами оказывается ограничено суммой следовых расстояний между отдельными процессами [13].

Поскольку КРК по исходному замыслу [1, 14] должно обеспечивать безусловную секретность (unconditional security) распределяемых ключей, которая основана на фундаментальных законах квантовой механики, а не на ограниченных вычислительных или технических возможностях нарушителя, то и аутентификация должна быть теоретико-информационно стойкой, и гарантировать обнаружение вторжений в классический канал связи, независимо от технических и вычислительных ограничений нарушителя.

Теоретико-информационная аутентификация впервые была предложена Simmons [15], а затем Wegman, Carter [16]. В фундаментальной работе Wegman и Carter [16] было показано, что теоретико-информационная аутентификация может быть достигнута с использованием класса специальных хеш-функций [16–28].

Теоретико-информационная аутентификация *гарантирует* обнаружение вторжений в классический канал связи независимо от технических возможностей подслушивателя, даже при наличии у него полномасштабного квантового компьютера.

*Для теоретико-информационной аутентификации требуется общий ключ $k_s$ у Алисы и Боба, поэтому при первом запуске системы Алисе и Бобу должен быть доставлен общий стартовый ключ $k_s$.* Теоретико-информационная аутентификация исследовалась в ряде работ [16–28].

В работе [13] было показано, что после запуска системы с использованием общего стартового ключа возможно практически сколь угодно долгое квантовое распределение ключей, до следующего перезапуска системы.

**Трудоемкость с теоретико-информационной аутентификацией в КРК.** *Вопрос о том, как изменится трудоемкость поиска квантового ключа для полного следового критерия секретности КРК с учетом атак нарушителя как на квантовый, так и на классический каналы связи, до сих пор остается открытым.*

*Ответ на данный вопрос является принципиальным как для понимания теоретической стойкости систем КРК, так и для практических применений квантовой криптографии.*

Как было показано ранее [13], суммарная величина параметра стойкости $\varepsilon$ для КРК с теоретико-информационной аутентификацией ограничена сверху суммой двух следовых расстояний.

1) Первое расстояние ($\varepsilon_{QKD}$) – расстояние между квантовыми состояниями реального и идеального сеансов КРК, но с идеальной аутентификацией без вторжений в классический канал связи.

2) Второе расстояние ($\varepsilon_{Aut}$) – расстояние между реальной и идеальной ситуациями при передаче классических сообщений, но без атак на квантовый канал связи – квантовые состояния.

**В чем состоит принципиальная разница между ситуациями 1) и 2)?** Наивная точка зре-

ния сводится к тому, для случая, когда возможны атаки как на квантовый, так и классический каналы связи, а также комбинированные атаки, то суммарный параметр $\varepsilon$-секретности, который будет входить в трудоемкость, равен сумме $\varepsilon = \varepsilon_{QKD} + \varepsilon_{Aut}$.

Однако, более детальные рассуждения сразу наталкиваются на сомнения.

В ситуации 1) нарушитель имеет в своем распоряжении квантовую систему $\rho_E^k$, коррелированную с ключом $k$ – битовой строкой, распределенной в конце сеанса КРК у Алисы и Боба. Нарушитель производит измерения над квантовой системой $\rho_E^k$ и получает "слепок", ключа Алисы и Боба – битовую строку $y$, коррелированную с ключом $k$. Степень корреляции определяется совместным распределением вероятностей $P_{KY}(k, y)$, а также условными распределениями вероятностей $P_{K|Y}(k|y)$ и $P_{Y|K}(y|k)$.

Далее, имея распределение вероятностей, нарушитель начинает опробовать ключи в соответствии с апостериорным распределением, начиная с самого вероятного ключа. Подсчет числа шагов опробования и определяет трудоемкость поиска ключа (см. подробности в [7]).

Важно подчеркнуть, что такой способ действия нарушителя и способ подсчета трудоемкости, работает потому, что квантовая система $\rho_E^k$ и битовая строка $y$ являются "прямыми" побочными переменными для нарушителя – **напрямую зависящими от ключа** $k$. Такова ситуация только при атаках на квантовый канал связи.

Напомним, что классический канал является открытым, вся передаваемая по нему информация доступна нарушителю. Сообщения содержат информацию о согласовании базисов, оценки вероятности ошибок, коррекции ошибок, усиления секретности очищенных ключей. Нарушитель, зная передаваемые сообщения и их хэш-значения, может их подменять. Классическая информация, передаваемая по классическому каналу связи также играет роль *побочной информации* для нарушителя.

Однако имеется принципиальная разница между классической и квантовой побочной информацией. Классические сообщения лишь **косвенно коррелированы с ключом** $k$.

*Далеко не очевидно, как определять трудоемкость поиска ключа в такой ситуации. Ввиду важности вопроса требуется строгий вывод соотношений, который базируется на аккуратном рассмотрении, а не на эвристических качественных соображениях.*

Ниже будет установлена прямая связь между критерием стойкости, основанным на следовом расстоянии между состоянием $\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}}$, отвечающим реальному квантовому распределению ключей и реальному классическому каналу с возможной подменой сообщений, и состоянием $\rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}$, отвечающим идеальному квантовому распределению ключей без нарушителя, и идеальной аутентификации сообщений в классическом канале без подмены сообщений нарушителем.

**Почти сильно $\varepsilon$-универсальные хеш-функции $\varepsilon - ASU_2$ – $\varepsilon$ almost strongly universal functions.** Приведем необходимые сведения для дальнейшего рассмотрения сведения о хэш-функциях, которые используются при теоретико-информационной аутентификации [16–28]. Теоретико-информационная аутентификация позволяет двум пользователям Алисе и Бобу обеспечить целостность передаваемой информации через открытый канал связи. При аутентификации вместе с открытым сообщением $m \in \mathcal{M} = \{0,1\}^\mu$ посылается его хеш-значение (далее тег) $t \in \mathcal{T} = \{0,1\}^\tau$, ($|\mathcal{T}| \ll |\mathcal{M}|$), $t = h_{k_s}(m)$, которое имеет меньшую длину.

Теоретико-информационная аутентификация требует общего секретного ключа у двух пользователей. Хеш-функция выбирается случайно из множества хеш-функций $\mathcal{H} = \{h_{k_s}\}_{k_s \in \mathcal{K}_s}$ в зависимости от ключа, $k_s \in \mathcal{K}_s = \{0,1\}^{\kappa_s}$, который должен выбираться равновероятно.

Под теоретико-информационной аутентификацией понимается такая аутентификация, при которой вероятность подмены сообщения (impersonation) без знания ключа $k_s$ – нахождение *допустимой пары* $(t, m)$ и равновероятном выборе ключей $k_s$ не превышает величины $\Pr_{k_s}\{t = h_{k_s}(m)\} = \frac{1}{|\mathcal{T}|}$.

Далее, вероятность подмены сообщения (substitution) без знания ключа $k_s$ – замены истинного сообщения после наблюдения пары $(t, m)$ на другую пару $(t', m')$, не превышает величины $P_{k_s}[t = h_{k_s}(m), t' = h_{k_s}(m')] < \frac{\varepsilon}{|\mathcal{T}|}$.

Из определений $\varepsilon$-$\mathrm{ASU}_2$ хеш-функций следует, что вероятность замены (substitution) $(m, t) \to (m', t')$, точнее условная вероятность, без знания ключа, и при наблюдении пары $(m, t)$, *не зависит от вычислительных возможностей подслушивателя, а зависит только от свойств множества хеш-функций* $\mathcal{K}_s$, *и не превосходит* $P_{k_s}[t' = h_{k_s}(m')|t = h_{k_s}(m)] < \varepsilon$.

Семейство функций $\varepsilon$-$\mathrm{ASU}_2$ может быть реализовано различными способами. Применительно к теоретико-информационной аутентификации в квантовой криптографии необходима экономия ключей

аутентификации – минимизация множества $|\mathcal{K}_s|$. Для семейства $\varepsilon$-$\mathrm{ASU}_2$ хеш-функций известны соотношения между параметрами $\varepsilon$, $|\mathcal{K}_s|$, $|\mathcal{T}|$ [29], которые накладывают ограничения на объем множества ключей $|\mathcal{K}_s|$, при заданных $\varepsilon$, $|\mathcal{T}|$.

Для экономии ключей аутентификации используется реализация $\varepsilon$-$\mathrm{ASU}_2$ функций на основе композиции хеш-функций $\varepsilon$-$\mathrm{AXU}_2$ и шифрования хеш-значения одноразовым ключом (см. детали в [13, 29]). Для функций $\varepsilon$-$\mathrm{AXU}_2$ используется один и тот же ключ во время всех сеансов аутентификации. Ключ для шифрования тега используется как одноразовый в каждом сеансе аутентификации.

**Следовое расстояние между квантовыми состояниями – ситуациями.** Ранее было показано в [13], после КРК с теоретико-информационной аутентификацией расстояние между двумя ситуациями не более

$$||\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}} - \rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}||_1 \le \varepsilon_{Aut}+\varepsilon_{QKD}, \quad (1)$$

где параметры $\varepsilon_{Aut}+\varepsilon_{QKD}$ включают все неидеальности отдельных процессов [13]. Параметр $\varepsilon_{QKD}$ описывает процесс КРК при идеальной аутентификации, $\varepsilon_{QKD} = \varepsilon_F+\varepsilon_{\mathrm{corr}}+\varepsilon_{\mathrm{sec}}$, где $\varepsilon_F$ отвечает за неидеальность выбора хеш-функций при усилении секретности в КРК, $1-\varepsilon_{\mathrm{corr}}$ определяет вероятность корректности протокола КРК – совпадению ключей у Алисы и Боба, $\varepsilon_{\mathrm{sec}}$ параметр секретности сеанса КРК (см. детали в [14]).

Далее нам потребуются матрицы плотности для реальной и идеальной ситуаций КРК. Матрицы плотности для реальной и идеальной ситуаций имеют квантово-классическую форму

$$\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}} = \sum_{k_s\in\mathcal{K}_s} P_{K_s}(k_s)|k_s\rangle_{K_sK_s}\langle k_s|$$

$$\sum_{k_A\in\{0,1\}^\ell}\sum_{k_B\in\{0,1\}^\ell} P_{K_AK_B}(k_A,k_B)\rho_E^{k_Ak_B}\otimes$$

$$|k_A\rangle_{AA}\langle k_A|\otimes|k_B\rangle_{BB}\langle k_B|\otimes\rho^{R^A_{Aut}}(k_A,k_s)\otimes\rho^{R^B_{Aut}}(k_B,k_s),$$

где $\ell$ – длина секретного ключа, $|k_A\rangle_A = |k_{1A}\rangle_A|k_{2A}\rangle_A...|k_{\ell A}\rangle_A$ и $|k_B\rangle_B = |k_{1B}\rangle_B|k_{2B}\rangle_B...|k_{\ell B}\rangle_B$ – квантовые состояния, отвечающие ключам Алисы и Боба, которые, вообще говоря, могут отличаться в конце сеанса КРК из-за атаки Евы. $P_{K_s}(k_s)$ – функция распределения стартового ключа аутентификации, $P_{K_AK_B}(k_A,k_B)$ – функция распределения финальных ключей Алисы и Боба, $\rho_E^{k_Ak_B}$ – квантовое состояние Евы, коррелированное с ключами $(k_A,k_B)$, $\rho^{R^A_{Aut}}(k_A,k_s)$, $\rho^{R^B_{Aut}}(k_B,k_s)$ – квантовые состояния сопоставленные классическим сообщениям от Алисы к Бобу, от Боба к Алисе при аутентификации в конце сеанса, открытые сообщения зависят от сеанса КРК (финального ключа).

Считаем, как и ранее [13], что проверка целостности сообщений происходит в конце сеанса КРК. Сначала Алиса и Боб проводят сеанс КРК, включая обмен открытыми классическими сообщениями, затем в конце сеанса перепосылаются все накопленные открытые сообщения $m$ вместе с их хэш-значениями $(m, t = h_{k_s}(m))$, которые могут подменяться нарушителем $(m, t = h_{k_s}(m)) \to (m', t')$.

Матрицы плотности $\rho^{R^A_{Aut}}(k_A,k_s)$, $\rho^{R^B_{Aut}}(k_B,k_s)$ в базисе $|m\rangle_A|t\rangle_A|m'\rangle_E|t'\rangle_E$ $(m \ne m', t \ne t')$ имеют недиагональные матричные элементы,

$$\rho^{R^A_{Aut}}(k_A,k_s) = \quad (2)$$

$$\sum_{((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M'T'}))_{OK}} P^{R_A}_{MTM'T'}(m,t,m',t' \mid k_A)$$

$$|m\rangle_{MM}\langle m|\otimes|t\rangle_{TT}\langle t|\otimes|m'\rangle_{M'M'}\langle m'|\otimes|t'\rangle_{T'T'}\langle t'|,$$

символическая запись $((m,t),(m',t')) \in ((\mathcal{MT}),(\mathcal{M'T'}))_{OK}$ означает, что суммирование происходит только по тем значениям подменных сообщений, которые прошли проверку на приемной стороне. Не прошедшие проверку сообщения отбрасываются. Аналогичный вид имеет матрица плотности $\rho^{R^B_{Aut}}(k_B,k_s)$, описывающая передачу классических сообщений от Боба к Алисе. Далее, квантовое состояние для идеальной ситуации КРК и идеального классического канала без подмены сообщений

$$\rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}} = \sum_{k_s\in\mathcal{K}_s}\frac{1}{|\mathcal{K}_s|}|k_s\rangle_{K_sK_s}\langle k_s| \quad (3)$$

$$\sum_{k_A\in\{0,1\}^\ell}\sum_{k_B\in\{0,1\}^\ell}\frac{\delta_{k_A,k_B}}{|\mathcal{K}_A|}|k_A\rangle_{AA}\langle k_A|\otimes|k_B\rangle_{BB}$$

$$\langle k_B|\otimes\rho^{I^A_{Aut}}(k_A,k_s)\otimes\rho^{I^B_{Aut}}(k_B,k_s)\otimes\rho_E,$$

$$\rho^{I^A_{Aut}}(k_A,k_s) = \quad (4)$$

$$\sum_{((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M'T'}))_{OK}} P^{I_A}_{MTM'T'}(m,t,m',t' \mid k_A)$$

$$|m\rangle_{MM}\langle m|\otimes|t\rangle_{TT}\langle t|\otimes|m'\rangle_{M'M'}\langle m'|\otimes|t'\rangle_{T'T'}\langle t'|,$$

где распределение вероятностей $P^{I_A}_{MTM'T'}(m,t,m',t'|k_A)$ для идеального классического канала без подмены сообщений является диагональным по $(m,t,m',t')$, т.е. $P^{I_A}_{MTM'T'}(m,t,m',t' \mid k_A) \propto \delta_{m,m'}\delta_{t,t'}$. Отметим, что в суммировании в (2), (4) фигурируют только слагаемые $((m_A, t_A = h_{k_s}(m_A)),(m'_A, t'_A = h_{k_s}(m'_A)))$,

$((m_B, t_B = h_{k_s}(m_B), (m'_B, t'_B = h_{k_s}(m'_B)))$, это означает, что проверка на аутентификацию пройдена, хотя была возможна подмена.

Аналогичный вид имеет матрица плотности $\rho^{I^B_{Aut}}(k_B, k_s)$, описывающая передачу классических сообщений от Боба к Алисе для идеального классического канала связи без подмены сообщений.

$$\rho_E = \sum_{k_A \in \{0,1\}^\ell} \sum_{k_A \in \{0,1\}^\ell} P_{K_A K_B}(k_A, k_B) \rho_E^{k_A k_B}.$$

Здесь $\rho^{I^A_{Aut}}(k_A)$ и $\rho^{I^B_{Aut}}(k_B)$ – матрицы плотности, отвечающие набору классических сообщений и их тегов от Алисы к Бобу, и от Боба к Алисе, которые передаются через идеальный классический канал с аутентификацией без подмены сообщений Евой. Функция распределения ключей Алисы и Боба отвечает равновероятному распределению ключей, ключи Алисы и Боба совпадают ($\frac{\delta_{k_A,k_B}}{|\mathcal{K}_A|}$), распределение стартовых ключей также равновероятное, квантовая система Евы $\rho_E$ не связана – некоррелирована с ключами. Матрицы плотности $\rho^{I^A_{Aut}}(k_A, k_s)$, $\rho^{I^B_{Aut}}(k_B, k_s)$, сопоставленные классическим сообщениям, имеют диагональную структуру [13], так как нет подмены сообщений.

**Средняя вероятность угадывания ключей.** *Следовый критерий (1) в явном виде не содержит ключей, которые после КРК используются в различных криптографических целях. Конечная цель нарушителя – узнать ключ, который появляется в результате КРК.*

Нарушитель производит измерения над своим *квантовым состоянием, полученным при атаке на квантовые состояния Алисы, данные состояния непосредственно коррелированным с ключом.* В результате нарушитель имеет в своем распоряжении побочные переменные $(y_A, y_B)$ – битовые строки, *напрямую* коррелированные с ключами $(k_A, k_B)$, а также все открытые сообщения и их теги, которые лишь *косвенно* связаны с ключом.

Найдем сначала среднюю вероятность угадывания по ключам. Для краткости изложения введем следующие обозначения:

$$(K, K_s, M, T, Y) \leftrightarrow (k_A, k_B, k_s, m_A, t_A, m'_A, t'_A, m_B, t_B, m'_B, t'_B, y_A, y_B),$$

$$(K|K_s, M, T, Y) \leftrightarrow (k_A, k_B|k_s, m_A, t_A, m'_A, t'_A, m_B, t_B, m'_B, t'_B, y_A, y_B), \quad (5)$$

где $m_A, t_A, m_B, t_B$ – исходные сообщения и их теги от Алисы к Бобу и от Боба к Алисе, $m'_A, t'_A, m'_B, t'_B$ – соответствующие подменные сообщения и их теги. Побочные переменные $(y_A, y_B)$ – битовые строки, которые получаются при измерениях нарушителя над квантовой системой $\rho_E^{k_A,k_B}$. Имея набор побочных переменных, нарушитель по некоторому решающему правилу, пытается определить значения ключей $k_{AB} = (k_A, k_B)$. Поскольку ключ Боба привязан к ключу Алисы и совпадает с ключом Алисы с вероятностью не менее $1 - \varepsilon_{\text{corr}}$, то множество значений $k_{AB}$ есть $|\mathcal{K}_A|$.

Поскольку матрицы плотности (2)–(4) имеют квантово-классический вид, естественно выбрать измерения, которые также имеют квантово-классическую структуру, хотя для дальнейший выводов это не принципиально. Пусть имеется полное измерение над всей квантовой системой Алиса–Ева–Боб, которое задается операторно-значными мерами

$$\mathcal{F}(K, K_s, M, T, Y) = \quad (6)$$

$$= |k_s\rangle_{K_s K_s}\langle k_s| \otimes |k_A\rangle_{K_A K_A}\langle k_A| \otimes |k_B\rangle_{K_B K_B}\langle k_B| \otimes$$
$$\otimes |m_A\rangle_{M_A M_A}\langle m_A| \otimes |t_A\rangle_{T_A T_A}\langle t_A| \otimes$$
$$\otimes |m'_A\rangle_{M'_A M'_A}\langle m'_A| \otimes |t'_A\rangle_{T'_A T'_A}\langle t'_A| \otimes$$
$$\otimes |m_B\rangle_{M_B M_B}\langle m_B| \otimes |t_B\rangle_{T_B T_B}\langle t_B| \otimes$$
$$\otimes |m'_B\rangle_{M'_B M'_B}\langle m'_B| \otimes |t'_B\rangle_{T'_B T'_B}\langle t'_B| \otimes \mathcal{M}_E^{y_A y_B}.$$

Операторно-значные меры реализуют разложение единицы, которое является формальным описанием измерения

$$I_{K_s} \otimes I_{K_A} \otimes I_{K_B} \otimes I_M \otimes I_T \otimes I_{M'} \otimes I_{T'} \otimes I_E = \quad (7)$$
$$= \sum_{K, K_s, M, T, Y} \mathcal{F}(K, K_s, M, T, Y).$$

Воспользуемся известным соотношением между следовым расстоянием и функцией распределения результатов измерений [30]

$$||\rho_{ABE}^{R^A_{Aut} R^B_{Aut} R^{AB}_{QKD}} - \rho_{ABE}^{I^A_{Aut} I^B_{Aut} I^{AB}_{QKD}}||_1 = \quad (8)$$

$$\max_{\mathcal{F}} \sum_{K, K_s, M, T, Y} |\mathrm{Tr}\{\mathcal{F}(K, K_s, M, T, Y) \rho_{ABE}^{R^A_{Aut} R^B_{Aut} R^{AB}_{QKD}}\} -$$
$$- \mathrm{Tr}\{\mathcal{F}(K, K_s, M, T, Y) \rho_{ABE}^{I^A_{Aut} I^B_{Aut} I^{AB}_{QKD}}\}|.$$

Данная граница достижима [30], т.е. существуют оптимальные измерения, для которых имеет место знак равенства. Для произвольных измерений следовое расстояние в правой части (8) не превосходит следового расстояния, для дальнейших выкладок этого факта достаточно.

Измерение приводит к распределению вероятностей для реальной и идеальной ситуаций

$$P^R(K,K_s,M,T,Y) = \\ = \mathrm{Tr}\{\mathcal{F}(K,K_s,M,T,Y)\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}}\}, \quad (9)$$

$$P^I(K,K_s,M,T,Y) = \\ = \mathrm{Tr}\{\mathcal{F}(K,K_s,M,T,Y)\rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}\}. \quad (10)$$

После сеанса КРК легитимные пользователи имеют ключи $(k_A,k_B)$, общий ключ аутентификации $k_s$, которые недоступны нарушителю. Нарушитель после измерений имеет в своем распоряжении набор побочных переменных $(M,T,Y)$, которые коррелированы с ключами легитимных пользователей.

Цель нарушителя, имея побочные переменные и применяя некоторое решающее правило $\mathcal{G}$, узнать истинные значения ключей Алисы и Боба – для краткости "угадать" $(k_A,k_B)$, т.е., имея $(M,T,Y)$, нарушитель принимает решение о реальных ключах $(\hat{k}_A,\hat{k}_B)=\mathcal{G}(M,T,Y)$. Если $(\hat{k}_A,\hat{k}_B)=(k_A,k_B)$, то гадываение (решение нарушителя) является успешным. Данное решение реализуется при помощи аутентификации с ключом $k_s$, который неизвестен нарушителю.

Для вычисления средней вероятности угадывания по всем ключам необходимо просуммировать по всем случайным реализациям ключа $k_s$. Поскольку побочные переменные также являются случайными величинами, то также необходимо провести усреднение только по тем значениям побочных переменных, при которых угадывание было успешным, получаем

$$\mathrm{Pr}_{\mathrm{Guess}} = \sum_{K_s} \sum_{(M,T,Y)\,:\,\mathcal{G}(M,T,Y)=(k_A,k_B)} P^R(K_s,M,T,Y)P^R(K|K_s,M,T,Y) = \quad (11)$$

$$= \sum_{K_s} \sum_{(M,T,Y)\,:\,\mathcal{G}(M,T,Y)=(k_A,k_B)} P^R(K,K_s,M,T,Y),$$

здесь $P^R(K_s,M,T,Y)$ – функция распределения $K_s,M,T,Y$ и $P^R(K|K_s,M,T,Y)$ – функция условного распределения, $P^R(K,K_s,M,T,Y)=P^R(K_s,M,T,Y)P^R(K|K_s,M,T,Y)$. *В сумме фигурируют только те оценки, для пары ключей, для которых оценка совпадает с истинными ключами* $(\hat{k}_a,\hat{k}_B)=(k_A,k_B)$. *Как будет видно ниже, для вычисления верхней границы вероятности правильного угадывания ключей* $Pr_{Guess}$ *явный вид решающего правиле не потребуется, находим*

$$\sum_{K_s} \sum_{(M,T,Y)\,:\,\mathcal{G}(M,T,Y)=(k_A,k_B)} \big(P^R(K,K_s,M,T,Y) - P^I(K,K_s,M,T,Y)\big) \le$$

$$\le \sum_{K_s} \sum_{\substack{(M,T,Y)\,:\,\mathcal{G}(M,T,Y)=(k_A,k_B) \\ \left(P^R(K,K_s,M,T,Y) - P^I(K,K_s,M,T,Y)\right)>0}} \big(P^R(K,K_s,M,T,Y) - P^I(K,K_s,M,T,Y)\big) \le \quad (12)$$

$$\le \sum_{\substack{K,K_s,M,T,Y \\ \left(P^R(K,K_s,M,T,Y) - P^I(K,K_s,M,T,Y)\right)>0}} \big(P^R(K,K_s,M,T,Y) - P^I(K,K_s,M,T,Y)\big) =$$

$$= \sum_{K,K_s,M,T,Y} \frac{1}{2}|P^R(K,K_s,M,T,Y) - P^I(K,K_s,M,T,Y)| \le$$

$$\le ||\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}} - \rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}||_1 \le \varepsilon_{Aut}+\varepsilon_{QKD}, \quad (13)$$

в (12) использовано соотношение между распределениями вероятностей $P_1(x)$ и $P_2(x)$ [31],

$$\frac{1}{2}\sum_x |P_1(x)-P_2(x)| = \sum_{x:(P_1(x)-P_2(x))>0} (P_1(x)-P_2(x)). \quad (14)$$

Измерения над идеальным квантовым состоянием дают

$$P^I(K,K_s,M,T,Y)=\mathrm{Tr}\{\mathcal{F}(K,K_s,M,T,Y)\rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}\}= \tag{15}$$

$$=\frac{1}{|\mathcal{K}_s|}\frac{1}{|\mathcal{K}_A|}P_{M_A}(m_A)P_{M_B}(m_B)\delta_{k_A,k_B}\delta_{m'_A,m_A}\delta_{m'_B,m_B}\delta_{t'_A,t_A}\delta_{t'_B,t_B}\delta_{t_A,h_{k_s}(m_A)}\delta_{t_B,h_{k_s}(m_B)}P_{Y_AY_B}(y_A,y_B),$$

$$P_{Y_AY_B}(y_A,y_B)=\sum_{k_A,k_B}P_{K_AK_B}(k_A,k_B)\mathrm{Tr}_E\left\{\mathcal{M}_E^{y_Ay_B}\rho_E\right\}=\sum_{k_A,k_B}P_{K_AK_B}(k_A,k_B)P_{Y_AY_B|K_AK_B}(y_A,y_B|k_A,k_B), \tag{16}$$

$$\sum_{y_A,y_B}P_{Y_AY_B}(y_A,y_B)=1.$$

С учетом (12)–(16) для (11), находим

$$\mathrm{Pr}_{\mathrm{Guess}}=\sum_{K_s}\sum_{(M,T,Y):\,\mathcal{G}(M,T,Y)=(k_A,k_B)}P^I(K,K_s,M,T,Y)+||\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}}-\rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}||_1\leq \tag{17}$$

$$\leq\sum_{K,K_s,M,T,Y}P^I(K,K_s,M,T,Y)+||\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}}-\rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}||_1\leq$$

$$\leq\frac{1}{|\mathcal{K}_A|}+||\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}}-\rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}||_1\leq\frac{1}{|\mathcal{K}_A|}+\varepsilon_{Aut}+\varepsilon_{QKD}.$$

Таким образом, вероятность угадывания ключей после КРК с теоретико-информационной аутентификацией превышает вероятность простого угадывания $\frac{1}{|\mathcal{K}_A|}=\frac{1}{2^\ell}$ не более, чем на $\varepsilon_{Aut}+\varepsilon_{QKD}$.

**Трудоемкость поиска ключей при заданной вероятности успеха после сеанса КРК с теоретико-информационной аутентификацией.** Средняя вероятность угадывания по ключам является достаточно грубой характеристикой в том смысле, что не дает информации о сложности – числе шагов перебора до определения истинного ключа. Более важной характеристикой является число шифр-сообщений до первого прочитанного. Пусть каждое сообщение шифруется своим ключом, полученным в КРК.

Пусть у нарушителя, в его пользу, имеется критерий читаемости, т.е. если нарушитель в результате опробования ключей нашел правильный, то сообщение считается прочитанным. Пусть задается только переборное множество ключей, и заданная вероятность успеха – вероятность того, что ключ попадает в переборное множество. Вопрос, который нас будет интересовать – какова трудоемкость (число шагов) перебора (опробования) ключей до определения истинного ключа.

Пусть подслушиватель, не зная ключа аутентификации $k_s$, но имея набор побочных переменных $s_i=$ $=(M,T,Y)_i=(m_A,m'_A,t_A,t'_A,m_B,m'_B,t_B,t'_B,,y_A,y_B)_i$, *часть которых напрямую, а часть косвенно,* связанных с истинными ключами $(k_A,k_B)$, для каждого шифр-сообщения опробовает $1\leq N\leq|\mathcal{K}_A|$ первых наиболее вероятных ключей.

Считаем, в пользу подслушивателя, что ему известны сами распределения вероятностей. Подслушиватель при данном значении побочных переменных $s_i$ упорядочивает первые $N$ ключей в порядке убывания условных вероятностей. Кроме того, задается вероятность успеха $\pi_0$ (см. ниже). Пусть упорядочение условных апостериорных вероятностей *при заданных* $s_i$ есть

$$P^R(k_{1(s_i)}|s_i)\geq P^R(k_{2(s_i)}|s_i)\ldots\geq P^R(k_{N(s_i)}|s_i), \tag{18}$$

где $P^R(k_{\ell(s_i)}|s_i)=\sum_{k_s}P^R(k_{\ell(s_i)}|k_s,s_i)$ – вероятность усредненная по всем значениям ключа аутентификации, $(\ell=1,...,N)$.

Номера исходных ключей $m(s_i)$ при упорядочивании вероятностей зависят от $s_i$, где обозначено для краткости $k_{m(s_i)}=(k_A,k_B)_{m(s_i)}$, где $1(s_i),2(s_i),\ldots|\mathcal{K}_A|(s_i))$ является перестановкой номеров исходных ключей.

Задача состоит в вычислении среднего числа опробований до первого удачного вскрытия шифра – определения истинного ключа. Для первого сообщения опробуются первые $N$ наиболее вероятных ключей из полного множества ключей $|\mathcal{K}_A|$, если ключ найден, то процесс завершен – успех. Если ключ после $N$ опробований не найден, опробование прекращается, и ожидается второе сообщение, и т.д. до определения истинного ключа. Пусть последовательность побочной переменной у подслушивателя в серии испытаний есть

$$\mathbf{s}=(s_1,s_2\ldots s_i\ldots),\quad s_i\in S, \tag{19}$$

здесь индекс $i$ нумерует сообщения, этот же индекс нумерует побочные переменные $s_i$, которые возникают у нарушителя для данного сообщения, $S$ – множество *всевозможных значений побочных переменных*, которые они принимают после измерений нарушителя.

Пусть соответствующая последовательность переборных множеств первых $N$ наиболее вероятных ключей, привязанных к каждому набору побочных переменных $s_1$, $s_2$ .... $s_{|\mathcal{K}_A|}$, есть

$$\mathbf{K} = (\mathcal{K}_1, \mathcal{K}_2, \dots \mathcal{K}_i \dots), \tag{20}$$

здесь каждое множество $\mathcal{K}_i$ зависит от значения $s_i$: $\mathcal{K}_i = \{k_{1(s_i)}, k_{2(s_i)} \dots k_{N(s_i)}\}$.

Вероятность, подчиняющаяся геометрическому распределению, последовательности длины $j$ при данных побочных переменных, до первого определения ключа есть

$$P(j) = \pi(N, s_{j+1}) \prod_{i=0}^{j} (1 - \pi(N, s_i)), \quad \pi(N, s_i) = \sum_{\{k_{m(s_i)} \in \mathcal{K}_i\}} P^R(k_{m(s_i)}|s_i). \tag{21}$$

Формула (24) дает вероятность определения ключа на $j$ шаге, при условии, что на предыдущих $j-1$ шагах ключ не был найден.

Далее, пусть

$$\mathcal{K}_i = \{k_{m(s_i)} : P(k_{1(s_i)}|s_i) \geq P(k_{2(s_i)}|s_i) \dots \geq P(k_{M(s_i)}|s_i); \quad m(s_i) = 1 \dots N\}, \tag{22}$$

т.е. упорядочение в $\mathcal{K}_i$ зависит однозначно от побочной переменной $s_i$. Другими словами, расстановка индексов $m(s_i)$ и условных вероятностей в множестве всевозможных значений ключей $\mathcal{K}$ задается побочной переменной $s_i$, множества $\mathcal{K}_i$ и $\mathcal{K}$ одинаковы, точнее говоря, различаются только перестановкой ключей.

Средняя трудоемкость по всем побочным переменным, последние при разных $j$ независимы, дает

$$G(N, K|S) = \mathbf{E}\left(G(N, K|\mathbf{s})\right) = \mathbf{E}\left(N \sum_{j=0}^{\infty} \left(j\pi(N, s_{j+1}) \prod_{i=0}^{j} (1 - \pi(N, s_i))\right) + \right. \tag{23}$$

$$\left. + \sum_{j=0}^{\infty} \sum_{m=1}^{N} \left(m \frac{P(k_{m(s_{j+1})}|s_{j+1})}{\pi(N, s_{j+1})} \pi(N, s_{j+1}) \prod_{i=0}^{j} (1 - \pi(N, s_i))\right)\right) =$$

$$= \frac{(1 - \pi(N))N}{\pi(N)} + \frac{1}{\pi(N)} \sum_{m=1}^{N} mp(m), \tag{24}$$

где в (23) $G(N, K|\mathbf{s})$ трудоемкость при условии конкретного наблюдаемого набора побочных переменных (см. формулу (19)), а для средней величины трудоемкости по всем наблюдениям побочных переменных введено обозначений $G(N, K|S)$, где символ $S$ указывает лишь на тот факт, что средняя трудоемкость зависит от совокупности наблюдаемых побочных переменных. Далее, $\mathbf{E}(\dots)$ обозначает среднее по всем независимым реализациям побочных переменных $s_i$

$$\mathbf{E}(\dots) = \sum_{s_1 \in S} P^R(s_1) \sum_{s_2 \in S} P^R(s_2) \dots \sum_{s_i \in S} P^R(s_i) \dots (\dots). \tag{25}$$

Величины в (24) имеют следующий смысл: $\pi(N)$ – средняя вероятность успеха (нахождения ключа шифрования) – вероятность попасть случайному ключу $k_1$ в переборное множество – множество наиболее вероятных ключей, которые опробоваются. $G(N, K|S)$ – средняя сложность (в опробованиях) – среднее число актов – шагов опробования внутри переборного множества опробования.

Индекс $m(s_j)$ определяет шаг опробования ключей и принимает значение при фиксированном $s_j$ – $\{m(s_j) = 1(s_j), 2(s_j) \dots N(s_j)\}$. Данная запись символизирует тот факт, что при данном $s_j$ осуществляется перестановка ключей таким образом, что для первого ключа $k_{1(s_j)}$ условная вероятность максимальная. Для второго $k_{2(s_j)}$, соответственно, $P^R(k_{1(s_j)}|s_j) \geq P^R(k_{2(s_j)}|s_j)$, и .т.д.

$$p(m) = \sum_{s_i \in S} P^R(s_i) P^R(k_{m(s_i)}|s_i), \quad \pi(N) = \sum_{m=1}^{N} p(m) = \sum_{m=1}^{N} \sum_{s_i \in S} P^R(s_i) P^R(k_{m(s_i)}|s_i), \tag{26}$$

вероятность зависит только от номера шага $m$ опробования. С учетом (26) находим

$$\sum_{m=1}^{N} m \sum_{s_i \in S} P^R(s_i) P^R(k_{m(s_i)}|s_i) = \sum_{m=1}^{N} m \cdot p(m). \tag{27}$$

*В выражение (24) входят величины* $\pi(N)$, $\frac{1}{\pi(N)}$ *и* $\sum_{m=1}^{N} mp(m)$. *Для оценки нижней границы трудоемкости в (23), (24) требуется нижняя оценка* $\sum_{m=1}^{N} mp(m)$, *а для величины* $\pi(N)$, *входящей как в числитель, так и в знаменатель нужны как нижняя, так и верхняя оценка.*

Учитывая правую часть (21), (26) и (27), а также то, что множества $\mathcal{K}_i$ и $\mathcal{K}$ одинаковы с точностью до перестановки, и, тот факт, что шаг опробования $m$ и ключ опробования $k(m)$, при заданных побочных переменных $s$, в силу (22) однозначно связаны, прямым вычислением получаем цепочку соотношений

$$\pi(N) = \sum_{s\in S} P^R(s)\pi(N,s) = \sum_{s\in S}\sum_{k(m)\in\mathcal{K}} P^R(s)P^R(k(m)|s) = \tag{28}$$

$$= \sum_{s\in S}\sum_{m=1}^{N} \left(P^R(k(m),s) - P^I(k(m),s)\right) + \sum_{s\in S}\sum_{m=1}^{N} P^I(k(m),s) =$$

$$= \frac{N}{|\mathcal{K}_A|} + \sum_{s\in S}\sum_{m=1}^{N} \left(P^R(k(m),s) - P^I(k(m),s)\right) \le \frac{N}{|\mathcal{K}_A|} + \frac{1}{2}\sum_{s\in S}\sum_{m=1}^{N} |P^R(k(m),s) - P^I(k(m),s)| \le$$

$$\le \frac{N}{|\mathcal{K}_A|} + ||\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}} - \rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}||_1 \le \frac{N}{|\mathcal{K}_A|} + \varepsilon_{Aut} + \varepsilon_{QKD}.$$

Для оценки нижней границы аналогичными выкладками, как в (28), получаем

$$\pi(N) = \sum_{s\in S} P^R(s)\pi(N,s) \ge \frac{N}{|\mathcal{K}_A|} - ||\rho_{ABE}^{R^A_{Aut}R^B_{Aut}R^{AB}_{QKD}} - \rho_{ABE}^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}||_1 \ge \frac{N}{|\mathcal{K}_A|} - (\varepsilon_{Aut} + \varepsilon_{QKD}). \tag{29}$$

Далее находим

$$\sum_{s\in S}\sum_{m=1}^{N} mP^R(s)P^R(k(m)|s) = \tag{30}$$

$$= \frac{N(N+1)}{2|\mathcal{K}_A|} + \sum_{s\in S}\sum_{m=1}^{N} m\left(P^R(k(m),s) - P^I(k(m),s)\right) \ge \frac{N(N+1)}{2|\mathcal{K}_A|} - \sum_{s\in S}\sum_{k\in\mathcal{K}}^{|\mathcal{K}_A|} \frac{1}{2}|m\left(P^R(k,s) - P^I(k,s)\right)| \ge$$

$$\ge \frac{N(N+1)}{2|\mathcal{K}_A|} - N\sum_{s\in S}\sum_{k\in\mathcal{K}} \frac{1}{2}|\left(P^R(k,s) - P^I(k,s)\right)| \ge \frac{N(N+1)}{2N} - (\varepsilon_{Aut} + \varepsilon_{QKD}).$$

В (30) использовано равенство

$$\sum_{s\in S}\sum_{m=1}^{N} mP^I(k(m),s) = \sum_{s\in S} P^I(s)\sum_{m=1}^{N} mP^I(k(m)|s) = \sum_{s\in S} P^I(s)\frac{1}{|\mathcal{K}_A|}\sum_{m=1}^{N} m = \frac{N(N+1)}{2|\mathcal{K}_A|}.$$

Здесь учтено, что для идеального случая переходная вероятность $P^I(k(m)|s) = \frac{1}{|\mathcal{K}_A|}$ не зависит от побочных переменных $s$, сумма $\sum_{m=1}^{N} m = \frac{N(N+1)}{2}$ есть сумма арифметической прогрессии, и условие нормировки вероятности $\sum_{s\in S} P^I(s) = 1$.

С учетом оценок, приведенных выше (28)–(30), в итоге получаем

$$Q(K|S,\pi_0) = \min_{\{N:\pi(N)\ge\pi_0\}} G(K|S,N) \ge \left(1 - \frac{\varepsilon_{Aut} + \varepsilon_{QKD}}{\pi_0}\right)\left(\frac{|\mathcal{K}_A|(1 - 4(\varepsilon_{Aut} + \varepsilon_{QKD})) + 1}{2}\right). \tag{31}$$

Таким образом, трудоемкость частичного перебора после сеанса КРК с теоретико-информационной аутентификацией явным образом выражается через следовое расстояние (1).

*Важно отметить, ответ на поставленный в начале работы вопрос основан на строгих выкладках, а не на качественных интуитивных соображениях, поэтому может быть надежно использован в дальнейших исследованиях и применениях систем КРК.*

**Заключение.** Интересно сделать некоторые оценки. Пусть заданная вероятность успеха $\pi_0 = \frac{1}{2}$. Для реальных систем достижимые величины $\varepsilon_{QKD} \approx 10^{-7} \div 10^{-9}$, аналогично $\varepsilon_{Aut} \approx 10^{-7} \div 10^{-9}$. Число шагов опробований до первого прочтения сообщения – определения истинного ключа имеет порядок $\approx \frac{1}{4} 2^{\ell}(1 - 16(10^{-7} \div 10^{-9}))$. При длине ключа $\ell = 256$ бит число шагов перебора практически равно числу шагов перебора по всему ключевому пространству $\approx 2^{254} \approx 10^{76}$.

Выражаем благодарность И. М. Арбекову, сотрудникам ИнфоТекс, СФБ Лаборатории, коллегам по Академии криптографии Российской Федерации за интерес к работе, многочисленные обсуждения, советы и поддержку.

**Финансирование работы.** Данная работа финансировалась за счет средств бюджета института (Кулик С. П. – Центр Квантовых Технологий Московского государственного университета имени М. В. Ломоносова, Молотков С. Н. – Институт физики твердого тела имени Ю. А. Осипьяна Российской академии наук). Никаких дополнительных грантов на проведение или руководство данным конкретным исследованием получено не было.

**Конфликт интересов.** Авторы данной работы заявляют, что у них нет конфликта интересов.

1. C. H. Bennett and G. Brassard, *Quantum cryptography: public key distribution and coin tossing*, in *Proceedings of IEEE International Conference on Computers7*, Systems and Signal Processing, Bangalore, India (1984), p. 175.
2. H. P. Yuen, Phys. Rev. A **82**, 062304 (2010).
3. H. P. Yuen, arXiv:1109.1051 [quant-ph].
4. H. P. Yuen, arXiv:1109.2675 [quant-ph].
5. H. P. Yuen, arXiv:1109.1066 [quant-ph].
6. R. Renner, 1209.2423 [quant-ph].
7. И. М. Арбеков, С. Н. Молотков, ЖЭТФ **152**(1(7)), 62 (2017).
8. И. М. Арбеков, Математические вопросы криптографии **7**(1), 39 (2016).
9. С. Н. Молотков, ЖЭТФ **150**(5(11)), 903 (2016).
10. A. Abidin and J.-Å. Larsson, Int. J. Quantum Inf. **7**(5), 1047 (2009).
11. M. Peev, C. Pacher, T. Lorünser, M. Nölle, A. Poppe, O. Maurhart, M. Suda, A. Fedrizzi, R. Ursin, and A. Zeilinger, Int. J. Quantum Inf. **7**, 1401 (2009).
12. C. Pacher, A. Abidin, T. Lornser, M. Peev, R. Ursin, A. Zeilinger, and J-Å. Larsson, Quantum Information Processing **15**(1), 327 (2012); arXiv:1209.0365.
13. S. N. Molotkov, Laser Phys. **34**, 045202 (2024).
14. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. (2005).
15. G. Simmons, Proc. IEEE **76**(5), 603 (1988).
16. M. N. Wegman and L. Carter, J. Comput. Syst. Sci., **22**, 265 (1981).
17. M. Atici and D. R. Stinson, *Universal hashing and multiple authentication*, in N. Koblitz (editor), CRYPTO 96. LNCS, Springer, Berlin (1996), v. 1109, p. 16.
18. J. Bierbrauer, T. Johansson, G. Kabatianskii, and B. Smeets, *On families of hash functions via geometric codes and concatenation*, in D. Stinson (editor), CRYPTO '93. LNCS, Springer, Berlin (1994), v. 773, p. 331.
19. B. den Boer, J. Comput. Security **2**, 65 (1993).
20. H. Krawczyk, *LFSR-based hashing and authentication*, in Y. Desmedt (editor), CRYPTO 94. LNCS, Springer, Berlin (1994), v. 839, p. 129.
21. H. Krawczyk, *New hash functions formessage authentication*, in L. C. Guillou and J. J. Quisquater (editors), EUROCRYPT 95. LNCS, Springer, Berlin (1995), v. 921, p. 301.
22. D. R. Stinson, *Universal hashing and authentication codes*, in J. Feigenbaum (editor), CRYPTO 91. LNCS, Springer, Berlin (1992), v. 576, p. 74.
23. D. R. Stinson, J. Comput. Syst. Sci. **48**, 337 (1994).
24. D. R. Stinson, Congr. Numer. **114**, 7 (1996).
25. D. R. Stinson, J. Combin. Math. Combin. Comput. **42**, 3 (2002).
26. A. Abidin and J-Å. Larsson, *New universal hash functions*, in S. Lucks and F. Armknecht (editors), WEWoRC 2011. LNCS, Springer, Berlin (2012), v. 7242, p. 99.
27. P. Rogaway, J. Cryptol. **12**(2), 91 (1999).
28. A. Abidin and J-Å. Larsson, Quantum Inf. Process. **13**, 2155 (2014).
29. Ch. Portmann, IEEE Trans. Inform. Theory **60**(7), 4383 (2014).
30. M. M. Wilde, arXiv:1106.1445v6 [quant-ph] 2 Dec 2015.
31. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Second Edition, A. J. Wiley & Sons, Inc., Publication, Hoboken, New Jersey (2006).