Письма в ЖЭТФ, том 116, вып. 2, с. 128 – 132

Квантовое распределение ключей с недоверенными, открытыми для подслушивателя детекторами

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

[+]*Центр квантовых технологий, МГУ им. М. В. Ломоносова, 119899, Москва, Россия*

[*]*Институт физики твердого тела РАН, 142432 Черноголовка, Россия*

Поступила в редакцию 7 июня 2022 г.
После переработки 7 июня 2022 г.
Принята к публикации 9 июня 2022 г.

Предлагается простая, но принципиальная модификация протоколов квантового распределения ключей, сводящаяся к тому, что не требуется защищать от подслушивателя результаты работы лавинных детекторов; при этом сохраняются все криптографические свойства протоколов.

DOI: 10.31857/S1234567822140105, EDN: izoxyi

1. Введение. При квантовом распределении ключей (КРК) для гарантии стойкости распределяемых ключей принципиально важно, чтобы подслушиватель не имел доступа к передающей и приемной аппаратуре. На приемной стороне биты ключа получаются из фотоотсчетов однофотонных лавинных детекторов, к которым подслушиватель не должен иметь доступа, что требует определенных мер по защите детекторов от утечки информации при регистрации квантовых состояний.

Подслушиватель может получать информацию о том, какой детектор сработал, даже не имея прямого доступа к детекторам. Существует также обратное переизлучение детекторов в канал связи (*back-flash излучение*), измеряя которое подслушиватель может получать информацию о битах ключа, оставаясь не обнаруженным.

Особенно это относится к системам КРК, использующих сверхпроводящие детекторы. Из-за использования "сухих" криостатов, и их отнюдь не миниатюрных размеров, детекторы находятся за пределами основной приемной аппаратуры, и соединены с ней волокном и электрическими кабелями, поэтому достаточно сложно обеспечить их полную гарантированную изоляцию от внешнего мира.

В этой связи возникает принципиальный вопрос – можно ли создать такую систему КРК и гарантировать криптографическую стойкость ключей, в которой детекторы, вообще, являются открытыми, и более того, даже вынесены за пределы основной аппаратуры, и результаты отсчетов доступны подслушивателю[2)].

Ответ на данный принципиальный вопрос оказывается положительным и дается в данной работе.

Ниже речь пойдет о протоколе BB84 [1] в стандартной конфигурации точка-точка, использующим фазовое кодирование, в волоконных системах. В протоколе используются два базиса – прямой базис $+$ и сопряженный $\times$, и два состояния, отвечающие 0 и 1 в каждом базисе.

На передающей стороне (Алиса) случайно выбирается базис и состояние в нем. Выбор базиса и состояния происходит выбором относительной фазы в двух импульсах состояний. Всего используются 4 значения фазы. В базисе $+$ логическому биту 0^+ отвечает фаза $\varphi_A = 0$, 1^+ фаза $\varphi_A = \pi$, соответственно, в базисе $\times$, биту $0^\times$ отвечает фаза $\varphi_A = \frac{\pi}{2}$, и $1^\times$ фаза $\varphi_A = \frac{3\pi}{2}$.

В стандартной версии протокола на приемной стороне (Боб) выбирает только два значения фазы, отвечающих выбору базиса, $\varphi_B = 0$ – базис $+$, $\varphi_B = \frac{\pi}{2}$ – базис $\times$.

Алиса и Боб оставляют только те посылки, где базисы совпадали. На приемной стороне состояния из канала связи после прохождения интерферометра Маха–Цандера [2], поступают на детекторы. Вероятность отсчета на детекторах U и D пропорциональна разности фаз: в детекторе $U \propto \cos^2\left(\frac{\varphi_A-\varphi_B}{2}\right)$, в детекторе $D \propto \sin^2\left(\frac{\varphi_A-\varphi_B}{2}\right)$ (рис. 1). При совпадающих базисах, если Алиса посылает 0^+, то из-за конструктив-

[1)]e-mail: kirill.balygin@gmail.com

[2)]Во избежание недоразумений, отметим, что ниже речь будет идти не о системах квантовой криптографии типа twin-field (см. ниже), а о стандартной конфигурации системы типа точка-точка.

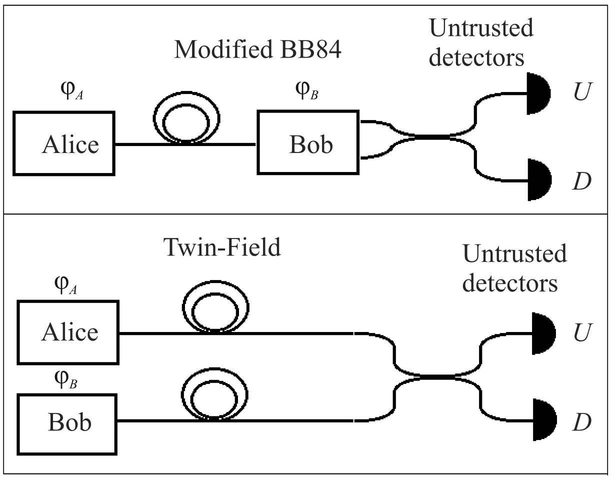

Рис. 1. Схематическое представление схем КРК для модифицированного протокола с недоверенными детекторами (верхняя часть рисунка) и протокола КРК twin-field (нижняя часть рисунка). На обоих рисунках: вероятность отсчета в детекторе U пропорциональна $\cos^2\left(\frac{\varphi_A-\varphi_B}{2}\right)$, соответственно, вероятность отсчета в детекторе D пропорциональна $\sin^2\left(\frac{\varphi_A-\varphi_B}{2}\right)$

ной интерференции на детекторе U и деструктивной на детекторе D, срабатывает только детектор U. Если Алиса посылает 1^+, то срабатывает детектор D, отсчет на детекторе U отсутствует.

Аналогично в базисе $\times$. От состояния $0^\times$ срабатывает детектор D, а от состояния $1^\times$, детектор U.

Поскольку после передачи состояний значения базиса раскрываются (но не состояния в базисе), то, если бы подслушиватель имел доступ к детекторам и знал, какой из детекторов сработал, то подслушиватель знал бы весь передаваемый ключ. По этой причине для систем КРК в стандартном исполнении должна быть обеспечена защита детекторов – подслушиватель не должен иметь ни прямого, ни косвенного доступа к ним.

2. Неформальные причины стойкости модифицированного протокола. Приведем модифицированный протокол с недоверенными детекторами и обсудим неформальные причины стойкости нового протокола.

Идея состоит в том, чтобы использовать на приемной стороне случайный выбор не двух значений фаз, а четырех значений фаз, по две в каждом базисе. Значения фаз и соответствующие им детекторы, где возникает отсчет, приведены ниже.

$$\text{базис} + \begin{cases} \text{бит } 0 \quad \varphi_A = 0 & \begin{cases} \varphi_B = 0 \to U \\ \varphi_B = \pi \to D \end{cases} \\ \text{бит } 1 \quad \varphi_A = \pi & \begin{cases} \varphi_B = 0 \to D \\ \varphi_B = \pi \to U \end{cases} \end{cases}, \quad (1)$$

$$\text{базис} \times \begin{cases} \text{бит } 0 \quad \varphi_A = \frac{\pi}{2} & \begin{cases} \varphi_B = \dfrac{\pi}{2} \to U \\ \varphi_B = \dfrac{3\pi}{2} \to D \end{cases} \\ \text{бит } 1 \quad \varphi_A = \frac{3\pi}{2} & \begin{cases} \varphi_B = \dfrac{3\pi}{2} \to U \\ \varphi_B = \dfrac{\pi}{2} \to D \end{cases} \end{cases}. \quad (2)$$

В каждом базисе, например, в базисе +, если Алиса посылает 0 ($\varphi_A = 0$), то в зависимости от случайного выбора фаз Бобом ($\varphi_B = 0$ или $\varphi_B = \pi$), который неизвестен Еве даже после раскрытия базисов, Ева, которая не знает фазы Боба, будет "видеть", как случайно срабатывает один из детекторов U или D для каждого значения бита 0 или 1 (см. формулы (1), (2)). Аналогично для других состояний.

Таким образом, введение Бобом в каждом базисе дополнительной случайности, которая неизвестна Еве, позволяет открыть отсчеты детекторов для подслушивателя, при этом Ева не будет знать передаваемый бит ключа.

Открытость детекторов для подслушивателя можно пояснить на языке теории информации.

В стандартном протоколе Алиса выбирает базис и бит внутри этого базиса, которые неизвестны Еве. Боб выбирает только базис, который Еве также неизвестен. В итоге, до раскрытия базисов Еве неизвестно три бита информации. При раскрытии базисов Алиса и Боб раскрывают по одному биту информации. В итоге, из трех бит остается один бит, который неизвестен Еве. Данный бит является общим секретом Алисы и Боба. При известном базисе данный бит Боб узнает по отсчету детектора.

В модифицированном протоколе, Алиса до раскрытия базисов имеет два бита информации, неизвестных Еве. Боб также имеет два бита информации до раскрытия базисов. После раскрытия базисов Алиса и Боб раскрывают по одному биту информации. Остается два бита, неизвестных Еве. Если Еве разрешить доступ к отсчетам в детекторах, то после отсчета детектора Ева получит еще один бит информации. В итоге остается еще один бит информации, неизвестный Еве, и который будет фигурировать в ключе. Естественно, Боб также знает, в каком детекторе произошел отсчет, но, кроме этого, Боб знает свой выбор фазы, что позволяет ему идентифицировать посланный Алисой бит. Ева не знает выбор фазы Боба, а видит только отсчет детектора в данном базисе. Но при известном базисе и не известной фазе Боба, Ева не может узнать, видя только отсчет детектора, передаваемый бит Алисы.

Интересно сравнить наш протокол с активно развиваемым протоколом twin-field [3, 4][3)], в котором детекторы также являются недоверенными и доступными (открытыми) для подслушивателя.

В схеме twin-field (см. рис. 1) Алиса и Боб в каждом из двух базисов независимо и равновероятно выбирают два значения фаз, например, в базисе $+$ $0 \to \varphi_A = 0$ и $1 \to \varphi_A = \pi$, аналогично для Боба $0 \to \varphi_B = 0$ и $1 \to \varphi_B = \pi$. Поскольку интерференционный сигнал на детекторе U пропорционален $\cos^2\left(\frac{\varphi_A-\varphi_B}{2}\right)$, на детекторе D $\sin^2\left(\frac{\varphi_A-\varphi_B}{2}\right)$, то при одинаковых фазах срабатывает детектор U, а при разных – детектор D. Детекторы открыты для подслушивателя.

Алиса генерирует два бита информации, неизвестных подслушивателю, – один бит для выбора базиса, второй для логического значения 0 или 1 в внутри базиса. Аналогично Боб генерирует два бита информации, неизвестных Еве. После раскрытия базисов – Алиса и Боб раскрывают по одному биту информации. Остается из 4-х бит два бита, неизвестных Еве. После отсчета детектора U или D Ева получает еще один бит информации. Остается один неизвестный Еве бит информации, который является общим секретом Алисы и Боба.

В отличии от Евы, Алиса и Боб, зная отсчет детектора, а также зная, какой бит они посылали, получают общий бит. Например, Алиса посылала 0, и Боб 0. Сработал детектор U. Такое событие имеет место, если они посылали одинаковые биты (каждый из них знает, что было послано), поэтому заранее договорившись, Алиса и Боб будут иметь общий бит 0. Если Алиса посылала 1, а Боб 1, то также сработает детектор U, и они будут считать общим битом 1. Ева "видит" только отсчет детектора U, и не будет знать общего бита, поскольку отсчет в детекторе U мог иметь место как от $A = 0,\ B = 0$, так и от $A = 1,\ B = 1$.

В этом состоит неформальная теоретико-информационная причина получения общего секретного бита Алисой и Бобом.

3. Формальное доказательство стойкости. Основная идея при формализации недоверенных, доступных для Евы детекторов, состоит к сведению нового протокола к эквивалентному протоколу, использующему стандартный протокол BB84 с доставкой Еве дополнительных квантовых состояний, которые говорят ей об отсчете того или иного детектора.

[3)]Идея интерференции состояний из разных источников в КРК была высказана еще в 1997 г. [5], такая система была названа КРК на базе квантового компаратора.

Рассмотрим стандартный протокол BB84. После измерений Боба детекторами, которые недоступны Еве, Боб после получения отсчета – результата 0 или 1, правильного или нет, в каждом базисе, сообщает его Еве, меняя случайно и равновероятно переставляя детекторы U или D. Например, если сработал детектор U, то Боб случайно и равновероятно выбирает детектор D или U и сообщает свой выбор Еве.

Данная процедура эквивалентна модифицированному протоколу, когда Боб случайно в каждом базисе выбирает одно из двух значений фаз, приводящее к случайной перестановке (для Евы) отсчетов в детекторах U или D.

Далее ограничимся однофотонным случаем и одинаковой квантовой эффективностью детекторов, чтобы излишне не загромождать выкладки техническими деталями. Учет неравной квантовой эффективности детекторов может быть сделан методом, представленным в работах [6, 7].

Таким образом, достаточно рассмотреть протокол BB84, дополненный информацией для Евы, связанной со случайной перестановкой детектора, который сработал. Из-за симметрии ситуации по базисам, достаточно рассмотреть ситуацию в одном базисе, например, в базисе $+$. Результаты в другом базисе $\times$ получаются унитарным преобразованием информационных состояний.

Воспользуемся ЭПР-версией протокола (см. детали, например, [6]). Алиса готовит ЭПР состояние, свою подсистему X, Алиса оставляет ее у себя как эталонную, а подсистему Y направляет Бобу. Подсистема Y подвергается атаке Евы в квантовом канале связи. Алиса делает измерения в базисе X, при этом случайно и равновероятно возникает состояние, отвечающее 0 или 1. После измерения подсистема Боба Y из-за структуры ЭПР состояние переходит в состояние, отвечающее 0 или 1. ЭПР состояние имеет стандартный вид

$$|\Phi^+\rangle_{XY} = \frac{1}{\sqrt{2}}\left(|0\rangle_X \otimes |0\rangle_Y + |1\rangle_X \otimes |1\rangle_Y\right). \quad (3)$$

Отметим, что структура ЭПР состояния одинакова как в базисе $+$, так и в базисе $\times$, поэтому индекс базиса опускаем.

Любое преобразование входного квантового состояния в выходное описывается действием супероператора – вполне положительного отображения [8]. Любой супероператор унитарно представим (см. детали в [9]). Последнее означает, что любой супероператор реализуется запутыванием входного состояния с вспомогательным ($|E\rangle_E$) при помощи унитарного оператора U_{BE}, который определяется Евой.

После атаки Евы, описываемой унитарным преобразованием U_{BE}, получаем

$$U_{BE}\left(|\Phi^+\rangle_{XY}\otimes|E\rangle_E\right)= \tag{4}$$

$$\frac{1}{\sqrt{2}}|0\rangle_X\otimes\Big\{\sqrt{1-Q}|0\rangle_Y\otimes|\Phi_0\rangle_E+\sqrt{Q}|1\rangle_Y\otimes|\Theta_0\rangle_E\Big\}+$$

$$+\frac{1}{\sqrt{2}}|1\rangle_X\otimes\Big\{\sqrt{1-Q}|1\rangle_Y\otimes|\Phi_1\rangle_E+\sqrt{Q}|0\rangle_Y\otimes|\Theta_1\rangle_E\Big\}.$$

Состояния Евы нормированы, поэтому коэффициенты выбраны в виде $1-Q$ и Q для сохранения нормировки. Как будет видно ниже, величина Q имеет смысл вероятности ошибки на приемной стороне.

Алиса и Боб делают измерения в одинаковом базисе. Алиса в базисе $\{|0\rangle_X,|1\rangle_X\}$, Боб соответственно в базисе $\{|0\rangle_Y,|1\rangle_Y\}$. В итоге возникает состояние Алиса–Боб–Ева, которое описывается матрицей плотности, с учетом (3), (4) получаем

$$\rho_{XYE}= \tag{5}$$

$$=\frac{1}{2}|0\rangle_{XX}\langle 0|\otimes\{(1-Q)|0\rangle_{YY}\langle 0|\otimes|\Phi_0\rangle_{EE}\langle\Phi_0|+$$

$$+Q|1\rangle_{YY}\langle 1|\otimes|\Theta_0\rangle_{EE}\langle\Theta_0|\}+$$

$$+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes\{(1-Q)|1\rangle_{YY}\langle 1|\otimes|\Phi_1\rangle_{EE}\langle\Phi_1|+$$

$$+Q|0\rangle_{YY}\langle 0|\otimes|\Theta_1\rangle_{EE}\langle\Theta_1|\}.$$

Как было показано ранее (например, [6]), для оптимальной атаки Евы, состояния $\{|\Phi_0\rangle_E,|\Phi_1\rangle_E\}$ и состояния $\{|\Theta_0\rangle_E,|\Theta_1\rangle_E\}$ лежат в ортогональных подпространствах, и ${}_E\langle\Theta_0|\Theta_1\rangle_E={}_E\langle\Phi_0|\Phi_1\rangle_E=1-2Q$. Оптимальность понимается в смысле – максимум информации Евы о передаваемом ключе, при наблюдаемой ошибке Q на приемной стороне.

Интерпретация (5) достаточно простая. С вероятностью $\frac{1}{2}$ Алиса посылает 0 или 1. Боб с вероятностью $1-Q$ получает правильный отсчет, у Евы оказывается состояние $|\Phi_0\rangle_E$. С вероятностью Q Боб получает ошибочный результат, у Евы оказывается состояние $|\Theta_0\rangle_E$. Аналогично для случая, когда Алиса посылала 1.

4. Модификация протокола. Пусть Боб получил отсчет 0 (неважно, правильный или ошибочный), т.е. сработал детектор U. Боб сообщает Еве случайно и равновероятно одно из ортогональных состояний $|U\rangle_D$ и $|D\rangle_D$. Сказанное означает, что Еве доставляется матрица плотности

$$\rho_D=\frac{1}{2}\left(|U\rangle_{DD}\langle U|+|D\rangle_{DD}\langle D|\right). \tag{6}$$

Таким образом, при регистрации Бобом 0 (верхний детектор) Еве доставляется состояние (6). Измерение состояния (6) дает Еве равновероятно детектор U или D в соответствии с (1), (2).

Аналогичная ситуация будет, если Боб зарегистрировал отсчет 1 в детекторе D (неважно, верный или ошибочный), Ева равновероятно будет “видеть” детектор U или D – “видеть” после измерения (6) состояние U или D.

В итоге матрица плотности ρ_{XYE} заменяется на ρ_{XYED}:

$$\rho_{XYED}= \tag{7}$$

$$=\frac{1}{2}|0\rangle_{XX}\langle 0|\otimes\{(1-Q)|0\rangle_{YY}\langle 0|\otimes|\Phi_0\rangle_{EE}\langle\Phi_0|\otimes\rho_D+$$

$$+Q|1\rangle_{YY}\langle 1|\otimes|\Theta_0\rangle_{EE}\langle\Theta_0|\otimes\rho_D\}+$$

$$+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes\{(1-Q)|1\rangle_{YY}\langle 1|\otimes|\Phi_1\rangle_{EE}\langle\Phi_1|\otimes\rho_D+$$

$$+Q|0\rangle_{YY}\langle 0|\otimes|\Theta_1\rangle_{EE}\langle\Theta_1|\otimes\rho_D\}.$$

5. Длина ключа, недоверенные детекторы. Согласно [10] длина секретного ключа в асимптотическом пределе длинных последовательностей имеет вид (учет конечной длины передаваемых последовательностей может быть сделан методом, предложенным в работе [7], чтобы не загромождать изложением техническими деталями, рассматриваем асимптотический случай)

$$\ell\geq H(\rho_{XED}|\rho_{ED})-H(\rho_{XY}|\rho_Y). \tag{8}$$

Формула (8) имеет простую интерпретацию: $H(\rho_{XED}|\rho_{ED})$, нехватка информации Евы в битах о эталонной битовой строке X Алисы, при условии, что Ева имеет в своем распоряжении квантовые системы ED; $H(\rho_{XY}|\rho_Y)$ – нехватка информации Боба о строке Алисы, при условии, что Боб имеет в своем распоряжении битовую строку Y – строку с ошибками. Разность нехваток информаций Евы и Боба о битовой строке Алисы составляет общий секрет Алисы и Боба.

Соответствующие частичные матрицы плотности, фигурирующие в (8), имеют вид

$$\rho_{XED}=\mathrm{Tr}_Y\{\rho_{XYED}\}= \tag{9}$$

$$=\frac{1}{2}|0\rangle_{XX}\langle 0|\otimes\{(1-Q)|\Phi_0\rangle_{EE}\langle\Phi_0|\otimes\rho_D+$$

$$+Q|\Theta_0\rangle_{EE}\langle\Theta_0|\otimes\rho_D\}+$$

$$+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes\{(1-Q)|\Phi_1\rangle_{EE}\langle\Phi_1|\otimes\rho_D+$$

$$+Q|\Theta_1\rangle_{EE}\langle\Theta_1|\otimes\rho_D\}.$$

$$\rho_{ED}=\mathrm{Tr}_{XY}\{\rho_{XYED}\}= \tag{10}$$

$$= \frac{1}{2}\left\{(1-Q)|\Phi_0\rangle_{EE}\langle\Phi_0| \otimes \rho_D + Q|\Theta_0\rangle_{EE}\langle\Theta_0| \otimes \rho_D\right\} +$$
$$+\frac{1}{2}\left\{(1-Q)|\Phi_1\rangle_{EE}\langle\Phi_1| \otimes \rho_D + Q|\Theta_1\rangle_{EE}\langle\Theta_1| \otimes \rho_D\right\}.$$

Далее

$$\rho_{XY} = \mathrm{Tr}_{ED}\{\rho_{XYED}\} = \tag{11}$$
$$= \frac{1}{2}|0\rangle_{XX}\langle 0|\left\{(1-Q)|0\rangle_{YY}\langle 0| + Q|1\rangle_{YY}\langle 1|\right\} +$$
$$+ \frac{1}{2}|1\rangle_{XX}\langle 1|\left\{(1-Q)|1\rangle_{YY}\langle 1| + Q|0\rangle_{YY}\langle 0|\right\}.$$
$$\rho_Y = \mathrm{Tr}_{XED}\{\rho_{XYED}\} = \frac{1}{2}\left\{|0\rangle_{YY}\langle 0| + |1\rangle_{YY}\langle 1|\right\}. \tag{12}$$

Вычисляя собственные числа (9)–(12), находим для условных энтропий фон Неймана

$$H(\rho_{XED}|\rho_{ED}) = H(\rho_{XED}) - H(\rho_{ED}) = \tag{13}$$
$$= H(\rho_{XE} \otimes \rho_D) - H(\rho_E \otimes \rho_D) = H(\rho_{XE}) - H(\rho_E) =$$
$$= 1 + h(Q) - 2h(Q) = 1 - h(Q).$$
$$H(\rho_{XY}|\rho_Y) = H(\rho_{XY}) - H(\rho_Y) = h(Q). \tag{14}$$

Окончательно с учетом (13), (14) для длины ключа получаем

$$\ell = 1 - 2h(Q). \tag{15}$$

Таким образом, длина секретного ключа в модифицированном протоколе оказывается такой же, как и в стандартном протоколе BB84 [1, 10]. Критическая ошибка Q_c, при которой длина ключа обращается в нуль равна $Q_c \approx 11\,\%$, $1 = 2h(Q_c)$, т.е. модификация протокола не “портит” криптографические свойства протокола.

6. Заключение. Для систем, где технически сложно обеспечить криптографическую защиту детекторов, найдено радикальное решение, сводящее к модификации протокола таким образом, что позволяет сделать детекторы недоверенными, и даже полностью доступными для наблюдения результатов отсчетов подслушивателем. Причем предлагаемая модификация не требует каких-либо радикальных изменений протокола и самой системы квантового распределения ключей. Приведенная аналогия с протоколом twin-field позволяет на качественном теоретико-информационном уровне объяснить причины секретности ключей при открытых для подслушивателя детекторах.

Кроме того, открытость детекторов позволяет обеспечить естественную защиту от атаки detector mismatch, открытость детекторов делает данную атаку полностью неэффективной.

Отметим в заключение, что данная модификация достигается без существенных изменений аппаратуры системы КРК и не приводит к снижению скорости распределяемых ключей.

Один из авторов (С. П. Кулик) выполнял исследование при поддержке Междисциплинарной научно-образовательной школы Московского университета “Фотонные и квантовые технологии. Цифровая медицина”.

---

1. C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, Bangalore, India (1984), p. 175.
2. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).
3. M. Lucamarini, L. M. Yuan, J. F. Dynes, and A. J. Shields, Nature **557**, 400 (2018).
4. S. N. Molotkov and I. V. Sinilshchikov, Laser Phys. Lett. **16**, 105205 (2019).
5. S. N. Molotkov, Pis’ma v ZhETF **66**, 736 (1997).
6. S. N. Molotkov, Laser Phys. Lett. **18**, 045202 (2021).
7. С. Н. Молотков, ЖЭТФ **160**(3), 327 (2021).
8. K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory*, Springer Verlag, Berlin (1983).
9. W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).
10. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich (2005); arXiv:0512258.