DOI: 10.22184/1993-7296.FRos.2024.18.4.282.294

Влияние точности квантового состояния поляризации одиночных фотонов на величину битовой ошибки квантового распределения ключа

Д. Н. Фроловцев[1], *А. В. Демин*[2]
[1] *Физический факультет, МГУ им. М. В. Ломоносова, г. Москва, Россия*
[2] *Всероссийский научно-исследовательский институт оптико-физических измерений (ФГБУ «ВНИИОФИ»), г. Москва, Россия*

В работе анализируется эффективность меры качества квантового состояния (фиделити) для оценки величины сырой битовой ошибки, вносимой состоянием поляризации источника одиночных фотонов. Анализ проведен для протоколов квантового распределения ключа BB84 и BBM92. Теоретически и экспериментально показано, что при уменьшении фиделити от 1 до 0 в протоколе BB84 величина сырой битовой ошибки линейно возрастает от 0 до 1, а в протоколе BBM92 – от 0 до 1/2. Подробно описаны экспериментальные установки для исследования влияния фиделити на величину битовой ошибки.

Ключевые слова: метрология квантовых состояний, фиделити, квантовое распределение ключа, спонтанное параметрическое рассеяние света

Статья получена: 10.02.2024
Статья принята: 15.03.2024

1. ВВЕДЕНИЕ

Развитие оптической платформы для квантовых вычислений [1, 2] и квантовой технологии [3–6] требует метрологического обеспечения составных элементов: источников одиночных фото-

Influence of Quantum State Fidelity of a Single Photon Source on the Bit Error Rate in Quantum Key Distribution

D. N. Frolovtsev[1], *A. V. Demin*[2]
[1] *Faculty of Physics, Lomonosov Moscow State University, Moscow, Russia*
[2] *All-Russian Research Institute of Optical and Physical Measurements (VNIIOFI), Moscow, Russia*

The paper analyzes the efficiency of a quantum state fidelity to assess the raw bit error value introduced by the polarization state of a single photon source. The analysis was performed for the quantum key distribution schemes BB84 and BBM92. It has been shown theoretically and experimentally that when the fidelity is decreased from 1 to 0 in the BB84 scheme, the raw bit error value linearly increases from 0 to 1, and in the BBM92 scheme – from 0 to 1/2. The experimental setups for determine the influence of fidelity on the bit error value are described in detail.

Keywords: quantum state metrology, fidelity, quantum key distribution, spontaneous parametric light scattering

Article received: February 10, 2024
Article accepted: March 15, 2024

1. INTRODUCTION

The development of an optical platform for quantum computing [1, 2] and quantum technology [3–6] requires metrological support for its constituent elements: single photon sources [7], single photon detectors [8], interferometers [9], polarization plates, filters, etc. to assess the value of errors introduced by the system components. To ensure the specifications of the photon source tools in the

нов [7], детекторов одиночных фотонов [8], интерферометров [9], поляризационных пластин, фильтров и т.д. для оценки величины ошибок, вносимых составными частями системы. Для обеспечения характеристик приборной базы источников фотонов в квантово-оптических технологиях [10] предложено использовать параметры $g^{(2)}$ [11] и Грангиера α [12, 13], связанные со статистикой фотонов источника. В настоящей работе анализируется источник ошибок при квантовом распределении ключа, связанный не со статистикой фотонов, а с неточным совпадением квантового состояния поляризации, приготавливаемого источником, и «идеального».

Для цели метрологического обеспечения квантовых состояний поляризации источников одиночных фотонов в фотонных пар предлагается использовать меру качества воспроизведения источником требуемого квантового состояния – фиделити [14] (англ. *fidelity*) [14]. Фиделити является мерой близости двух квантовых состояний – требуемого в практической задаче квантового состояния и состояния фотонов, генерируемых используемым на практике источником. Математически величину фиделити F определяют выражением

$$F=|\langle\psi_t|\psi_r\rangle|^2,$$

где $|\psi_t\rangle$ – требуемое от источника квантовое состояние фотонов, $|\psi_r\rangle$ – реально генерируемое квантовое состояние. Если источник генерирует фотоны в смешанном состоянии $\hat{\rho}$, то фиделити определяют как

$$F=|\langle\psi_t|\hat{\rho}|\psi_r\rangle|^2.$$

Цель работы – показать, что величину сырой битовой ошибки, вносимой неидеальным квантовым состоянием поляризации фотонов при квантовом распределении ключа можно оценить на основании единственного параметра – фиделити.

Кратко опишем применение фиделити в квантовых коммуникациях для определения уровня битовой ошибки в протоколах квантового распределения ключа. В разделе 2 теоретически и экспериментально исследуется использование фиделити в протоколе BB84 [15], а в разделе 3 – в протоколе BBM92 [16]. В разделе 4 подведены итоги работы.

2. КВАНТОВАЯ ПЕРЕДАЧА КЛЮЧА ПО ПРОТОКОЛУ BB84

Впервые идея квантовой криптографии была предложена Ч. Беннеттом и Ж. Брассардом

quantum optical technologies [10], it is proposed to use the parameters $g^{(2)}$ [11] and Grangier's α [12, 13] related to the statistics of source photons. This paper analyzes the source of errors in the case of quantum key distribution that is associated not with the photon statistics, but with the inaccurate preparation of the quantum polarization state by the source and the "ideal" one.

In order to provide metrological support of quantum polarization states of the single photon sources in the photon pairs, it is proposed to use a quality measure for the source reproduction of the required quantum state, namely fidelity [14]. Fidelity is a proximity measure for two quantum states: the quantum state required in a practical problem and the state of photons generated by the source used in practice. Mathematically, the fidelity value F is determined by the following expression:

$$F=|\langle\psi_t|\psi_r\rangle|^2,$$

where $|\psi_t\rangle$ is the quantum photon state required from the source, $|\psi_r\rangle$ is an actually generated quantum state. If the source generates photons in a mixed state $\hat{\rho}$, then fidelity is determined as follows:

$$F=|\langle\psi_t|\hat{\rho}|\psi_r\rangle|^2.$$

The purpose of this paper is to show that the raw bit error rate introduced by the non-ideal quantum photon polarization state in the case of quantum key distribution can be estimated on the basis of a single parameter, namely fidelity.

We will briefly describe the application of fidelity in quantum communications to determine the bit error level in the quantum key distribution schemes. On a theoretical and experimental level, section 2 examines the use of fidelity in the BB84 scheme [15], and section 3 – in the BBM92 scheme [16]. Section 4 provides the summarization of research.

2. QUANTUM KEY TRANSFER USING THE BB84 SCHEME

The concept of quantum cryptography was first proposed by C. Bennett and G. Brassard in 1984 [15]. The aim of the scheme is to generate an identical random bit sequence between two placeholders (called Alice and Bob). The communication channel security is determined by the fact that when listening to the quantum channel, the placeholders can reliably register the sequence compromise

в 1984 году [15]. Целью протокола является формирование идентичной случайной битовой последовательности у двух абонентов (называемых Алисой и Бобом). Защищенность канала связи определяется тем, что при прослушивании квантового канала абоненты могут гарантированно зарегистрировать по величине битовой ошибки компрометацию последовательности третьим абонентом, называемом обычно Евой [17]. Напомним, что в протоколе можно выделить три этапа.

На первом этапе Алиса приготавливает одиночные фотоны. Для этого она случайным образом выбирает базис кодирования – лабораторный или диагональный. Затем выбирает случайное число – «0» или «1» и приготавливает одиночный фотон с поляризацией, случайное число. В лабораторном базисе «0» и «1» кодируется горизонтальной $|H\rangle$ и вертикальной $|V\rangle$ поляризацией фотона, а в диагональном базисе – состояниям линейной поляризации фотона ±45° к горизонтали: «0» соответствует состоянию поляризации $|D\rangle=\left(|H\rangle+|V\rangle\right)/\sqrt{2}$, а «1» соответствует состоянию поляризации $|A\rangle=\left(|H\rangle-|V\rangle\right)/\sqrt{2}$. Процедура случайного выбора поляризационного базиса и бита информации повторяется для каждого фотона, приготавливаемого Алисой.

На втором этапе Алиса посылает приготовленные фотоны по квантовому каналу Бобу, который производит измерение их поляризации в случайно выбранном базисе. Затем абоненты по открытому каналу сообщают друг другу, в каких базисах (лабораторном или диагональном) они проводили измерения, и оставляют у себя только результаты в совпадающем базисе. Таким образом у абонентов формируется сырой ключ. Если используемые Алисой и Бобом приборы идеальны и отсутствует подслушивание, сырые ключи у абонентов идентичны. Как следует из теоремы о запрете клонирования [18] квантового состояния, прослушивание квантового канала ведет к наличию ошибок в сыром ключе. Например, если некоторая любопытная персона (называемая Евой) непрерывно ведет прослушивание, проводя измерения состояния поляризации фотонов в квантовом канале в случайно выбранном базисе и передавая Бобу вместо изначального фотона результат своих измерений, то Алиса и Боб должны зарегистрировать возрастание ошибки до 25%. Если Ева измеряет не каждый фотон, а только часть из потока, посылаемого Алисой Бобу, то величина вносимой ошибки уменьшается, хотя Ева узнает меньше информации о ключе. Допустимым количеством информации, принципиально доступной злоумышленнику третьей стороне, обычно называемой Евой, на основе битовой ошибки [17]. Напомним, что протокол можно разделить на три этапа.

At the first stage, Alice prepares the single photons. To do this, she randomly selects a coding basis: a laboratory or diagonal one. Then she selects a random number ("0" or "1") and prepares a single photon with polarization, a random number. In the laboratory basis, "0" and "1" are encoded by the horizontal $|H\rangle$ and vertical $|V\rangle$ photon polarization, and in the diagonal basis – by the states of photon linear polarization ±45° to the horizontal: "0" corresponds to the polarization state $|D\rangle=\left(|H\rangle+|V\rangle\right)/\sqrt{2}$, and "1" corresponds to the polarization state $|A\rangle=\left(|H\rangle-|V\rangle\right)/\sqrt{2}$. The random selection procedure for a polarization basis and an information bit is repeated for each photon prepared by Alice.

At the second stage, Alice sends the prepared photons through a quantum channel to Bob, who measures their polarization in a randomly selected basis. Then the subscribers use an open channel to inform each other in which basis (laboratory or diagonal) they have performed the measurements, and keep only the results in the matching basis. In this way, a raw key is generated for the subscribers. If the devices used by Alice and Bob are ideal and there is no eavesdropping, the subscribers' raw keys are identical. As follows from the no-cloning theorem [18] of a quantum state, listening to the quantum channel leads to the available errors in the raw key. For example, if some curious person (called Eve) is constantly listening while taking measurements of the photon polarization state in the quantum channel in a randomly selected basis and transmitting the measurement results to Bob instead of the original photon, then Alice and Bob should register an increase in the error up to 25%. If Eve measures not every photon, but only a part of the flow sent by Alice to Bob, then the introduced error value is decreased, although Eve learns less information about the key. The permissible amount of information that is fundamentally accessible to the attackers, as well as the methods applied to enhance the key secrecy [9, 19], determine the maximum permissible error level.

Any errors in the key generation process occur not only due to the eavesdropping, but also due to the inevitable equipment imperfection. For example, if Alice uses a source that produces photons with an error, then Bob will receive erroneous bits in the raw key as a result of measurements.

кам, а также используемыми методами усиления секретности ключа [9, 19] и определяется максимально допустимый уровень ошибки.

Ошибки при генерировании ключа возникают не только из-за прослушивания, но и из-за неизбежной неидеальности оборудования. Например, если Алиса использует источник, приготавливающий фотоны с погрешностью, то Боб в результате измерений получит ошибочные биты в сыром ключе.

Пусть источник фотонов Алисы приготавливает одиночные фотоны в состоянии поляризации $|\psi\rangle=\alpha|H\rangle-\beta|V\rangle$ вместо $|H\rangle$. Боб при регистрации поляризации фотонов в лабораторном базисе с вероятностью $|\langle\psi|H\rangle|^2=|\alpha|^2=F$, где F – фиделити, получит правильный результат измерения – фотон имеет горизонтальную поляризацию. С вероятностью $|\langle V|\psi\rangle|^2=|\beta|^2=1-F$ Боб зарегистрирует вертикальную поляризацию фотона, и в ключе возникнет ошибка. Аналогичные соотношения между фиделити и величиной битовой ошибки имеют место и при приготовлении Алисой остальных состояний $|V\rangle$, $|D\rangle$ и $|A\rangle$. Таким образом, при уменьшении фиделити увеличивается вероятность ошибки.

Схема экспериментальной установки для исследования влияния точности приготовления квантового состояния источником на величину битовой ошибки приведена на рис. 1. Установка имитирует работу системы квантового распределения ключа с помощью одиночных фотонов по протоколу BB84 от Алисы к Бобу. Одиночные фотоны приготавливаются с помощью спонтанного параметрического рассеяния света (СПР) [20] в кристалле ppKTP. В качестве накачки используется лазер с длиной волны 405 нм. В результате СПР рождается пара фотонов с длиной волны 810 нм, один из которых отражается поляризационным светоделителем и регистрируется детектором одиночных фотонов. Это событие сигнализирует о том, что источник Алисы приготовил одиночный фотон. С помощью полуволновой пластинки Алиса задает направление поляризации одиночного фотона (табл. 1).

Let Alice's photon source produce the single photons in a polarization state $|\psi\rangle=\alpha|H\rangle-\beta|V\rangle$ instead of $|H\rangle$. When registering the photon polarization in a laboratory basis with the probability of, where F is fidelity, Bob will obtain the correct measurement resultL the photon has horizontal polarization. If the probability is $|\langle V|\psi\rangle|^2=|\beta|^2=1-F$, then Bob will register the vertical photon polarization, and an error will appear in the key. Similar relations between fidelity and the bit error value are developed when Alice prepares the remaining states $|V\rangle$, $|D\rangle$ and $|A\rangle$. Thus, as fidelity decreases, the probability of error is increased.

The experimental setup layout to determine the influence of the quantum state preparation accuracy by the source on the bit error value is shown in Fig. 1. The setup simulates the operation of a quantum key distribution system using the single photons according to the BB84 scheme from Alice to Bob. The single photons are prepared using the spontaneous parametric light scattering (SPLS) [20] in a ppKTP crystal. A laser with a wavelength of 405 nm is used for pumping. As a result of SPLS, a pair of photons with a wavelength of

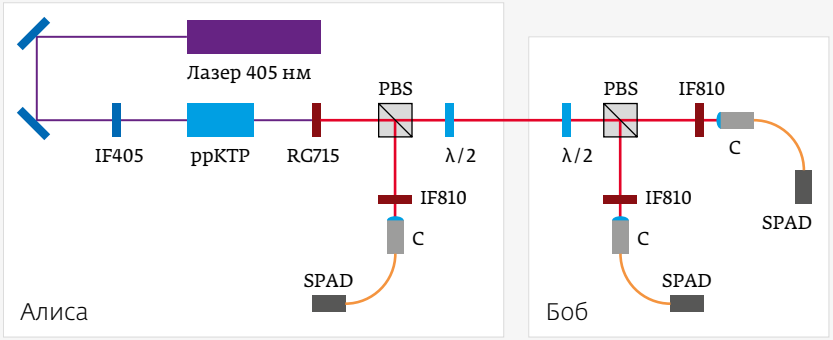

Рис. 1. *Схема экспериментальной установки для определения влияния фиделити на величину сырой битовой ошибки: IF405 – интерференционный фильтр, ppKTP – нелинейный кристалл трифосфата калия с регулярной доменной структурой, RG715 – светофильтр из цветного стекла, PBS – поляризационный светоделитель, IF810 – полосовой интерференционный светофильтр, C – оптоволоконный коллиматор, SPAD – детектор одиночных фотонов, λ/2 – полуволновая пластинка*

Fig. 1. *The experimental setup layout to determine the fidelity influence on the raw bit error value: IF405 – interference filter, ppKTP – nonlinear crystal of potassium triphosphate with a regular domain structure, RG715 – color glass filter, PBS – polarization beam splitter, IF810 – bandpass interference filter, C – fiber optic collimator, SPAD – single photon detector, λ/2 – half-wave plate*

Для моделирования неидеальности приготовления состояния поляризации источником одиночных фотонов полуволновая пластинка Алисы дополнительно поворачивается на некоторый угол θ, а плоскость поляризации поворачивается на угол 2θ. В результате фиделити приготовленного состояния поляризации принимает значение $F=\cos^2 2\theta$.

Боб регистрирует одиночные фотоны в лабораторном и диагональном базисах, выбирая измерительный базис с помощью своей полуволновой пластинки. Для каждого базиса измерения проводятся при двух положениях волновой пластинки, при которых детекторы «меняются местами», что позволяет учесть в расчетах их разную квантовую эффективность. Соответствующие положения волновой пластинки представлены в табл. 2.

Для измерений в лабораторном базисе полуволновая пластинка установлена с углом поворота 0° или 45°. В первом случае прошедший через поляризационный светоделитель Боба фотон соответствует биту «0», а отраженный светоделителем – биту «1». При положении пластинки 45° значения битов противоположные – прошедшему фотону соответствует «1», а отраженному – «0».

Измерения в диагональном базисе Боб производит при положении полуволновой пластинки 22,5° или (22,5°+45°). При положении пластинки прошедший через светоделитель Боба фотон соответствует биту «1», а отраженный – «0». При положении пластинки (22,5°+45°) прошедший через светоделитель фотон соответствует биту «0», а отраженный – «1».

Измерение величины битовой ошибки в зависимости от величины фиделити производились следующим образом. В соответствии с выбранным значением фиделити определялось значение угла θ. Затем Алиса приготавливала состояние поляризации одиночных фотонов, устанавливая свою полуволновую пластинку в соответствии с табл. 1. Для каждого состояния поляризации, приготавливаемого Алисой, Боб производил измерение битовой ошибки. Для этого Боб устанавливал свою полуволновую пластинку для измерения поляризации в базисе, совпадающем с базисом Алисы, и производил измерение вероятности ошибки (получения значения бита, противоположного задаваемому Алисой) в течение 20 с. Скорость счета коррелированных с триггерным фототсчетом Алисы одиночных фотонов детекторами Боба ~500 фотоотсчетов в секунду. Результаты измерений четырех значений битовой ошибки – для лабораторного и диагонального базисов, в каждом базисе измерения

Таблица 1. Положение полуволновой пластинки Алисы для приготовления состояний поляризации фотонов с заданным значением фиделити для квантового распределения ключа по протоколу BB84

Table 1. Position of the Alice's half-wave plate for preparing photon polarization states with a given fidelity value for the quantum key distribution using the BB84 scheme

Угол поворота полуволновой пластинки Алисы Rotation angle of the Alice's half-wave plate	Значение передаваемого бита Transmitted bit value	Базис Basis
0+θ	0	Лабораторный Laboratory
45°+θ	1	Лабораторный Laboratory
22,5°+θ	0	Диагональный Diagonal
22,5°+45°+θ	1	Диагональный Diagonal

810 nm is generated, one of which is reflected by a polarizing beam splitter and recorded by a single photon detector. This event notifies that the Alice's source has prepared a single photon. Using a half-wave plate, Alice sets the polarization direction of a single photon (Table 1). To simulate the non-ideal preparation of the polarization state by the single photon source, the Alice's half-wave plate is additionally rotated by a certain angle θ, and the polarization plane is rotated by an angle 2θ. As a result, the fidelity of the prepared polarization state takes on the value $F=\cos^2 2\theta$.

Bob detects the single photons in the laboratory and diagonal basis while selecting the measurement basis using his half-wave plate. For each basis, the measurements are performed at two positions of the wave plate, in which the detectors "swap their places" that makes it possible to consider their various quantum efficiencies in the calculations. The relevant positions of the wave plate are given in Table 2.

For the measurements in a laboratory basis, the half-wave plate is installed with a rotation angle 0° or 45°. In the first case, the photon passed through the Bob's polarization beam splitter corresponds to the "0" bit, and the photon reflected by the beam splitter corresponds to the "1" bit. When the plate

производились для двух положений полуволновой пластинки Боба, – усреднялись, и вычислялась вероятность битовой ошибки p_{err}:

$$p_{err} \frac{N_{err}^{L1} + N_{err}^{L2} + N_{err}^{D1} + N_{err}^{D2}}{N_{norm}^{L1} + N_{norm}^{L2} + N_{norm}^{D1} + N_{norm}^{D2}},$$

где $N_{err}^{L1,\,2/D1,\,2}$ – количество ошибочно полученных Бобом битов, а $N_{norm}^{L1,\,2/D1,\,2}$ – общее количество полученных Бобом битов (включая ошибочные и правильный). Индексы *L1*, *L2*, *D1*, *D2* соответствуют измерению Бобом в лабораторном (*L*) и диагональном базисе (*D*), числа 1 и 2 соответствуют различным положениям пластин из табл. 2.

Измеренная величина битовой ошибки в зависимости от фиделити представлена на рис. 2. Полученные экспериментальные данные подтверждают, что фиделити позволяет однозначно определить величину битовой ошибки, вносимой источником, в протоколе BB84.

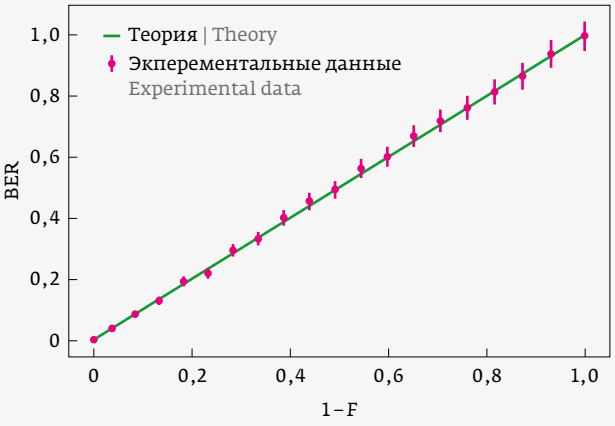

Рис. 2. *Зависимость величины битовой ошибки (BER) от фиделити F (зеленая кривая – теоретическая зависимость, красные точки – экспериментально измеренные данные)*

Fig. 2. *Dependence of the bit error rate (BER) on fidelity F (green curve – theoretical dependence, red dots – experimentally measured data)*

3. КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА С ПОМОЩЬЮ ПРОТОКОЛА BBM92

Рассмотрим влияние величины фиделити на величину битовой ошибки при квантовом распределении ключа по протоколу BBM92 [16]. В протоколе используются пары квантово-запутанных частиц. Для определенности будем считать, что используется is positioned at 45° the bit values are opposite: the transmitted photon corresponds to “1”, and the reflected photon corresponds to “0”.

Таблица 2. Положение волновых пластинок при измерении состояния поляризации одиночных фотонов Бобом в протоколе BB84 (четвертьволновая пластинка не использовалась), и обоими абонентами в протоколе BBM92
Table 2. Position of wave plates when measuring the polarization state of single photons by Bob in the BB84 scheme (a quarter-wave plate has not been used), and by both subscribers in the BBM92 scheme

Базис Basis	Первое положение пластинок First position of the plates	Второе положение пластинок Second position of the plates
Лабораторный Laboratory	Полуволновая пластинка: 0°, Четвертьволновая пластинка: 0° Прошедший поляризационный светоделитель фотон соответствует биту «0», отраженный – «1» Half-wave plate: 0°, Quarter wave plate: 0° The photon that has passed through the polarization beam splitter corresponds to the “0” bit, the reflected one – to “1”	Полуволновая пластинка: 45°, Четвертьволновая пластинка: 0° Прошедший поляризационный светоделитель фотон соответствует биту «1», отраженный – «0» Half-wave plate: 45°, Quarter wave plate: 0° The photon that has passed through the polarization beam splitter corresponds to the “1” bit, the reflected one – to “0”
Диагональный Diagonal	Полуволновая пластинка: 22,5°, Четвертьволновая пластинка: 45° Прошедший поляризационный светоделитель фотон соответствует биту «0», отраженный – «1» Half-wave plate: 22.5°, Quarter wave plate: 45° The photon that has passed through the polarization beam splitter corresponds to the “0” bit, the reflected one – to “1”	Полуволновая пластинка: –22,5°, Четвертьволновая пластинка: 45° Прошедший поляризационный светоделитель фотон соответствует биту «1», отраженный – «0» Half-wave plate: –22,5°, Quarter wave plate: 45° The photon that has passed through the polarization beam splitter corresponds to the “1” bit, the reflected one – to “0”

ются пары частиц в поляризационном состоянии Бэлла $|\Phi^{(+)}\rangle=\left(|HH\rangle+|VV\rangle\right)/\sqrt{2}$. Алиса и Боб получают по одному из запутанных фотонов. Источник запутанных фотонов может быть внешним, или же находиться у одного из абонентов. После того, как абоненты получили по одному фотону из запутанной пары, Алиса и Боб производят измерения поляризации фотонов. Для этого у каждого из абонентов имеется измеритель, аналогичный измерителю, используемому Бобом в протоколе BB84, рассмотренном выше. С вероятностью 1/2 Алиса производит измерения поляризации фотона в лабораторном базисе, и с вероятностью 1/2 в диагональном. Независимо те же самые действия проделывает Боб. Затем Алиса и Боб, сообщают друг другу базис, в котором были произведены измерения, но не сообщают конкретные результаты измерений.

Ошибки в созданном ключе появляются из-за прослушивания, а так же в случае использования некачественного источника запутанных фотонов, генерирующего фотонные пары в отличающемся от $|\Phi^{(+)}\rangle$ состоянии, задаваемом матрицей плотности $\hat{\rho}$. Проанализируем ошибки, возникающие из-за отклонения квантового состояния фотонных пар от $|\Phi^{(+)}\rangle$.

Для этого матрицу плотности поляризационного состояния источника представим в виде

$$\hat{\rho}=F|\Phi^{(+)}\rangle\langle\Phi^{(+)}|+(1-F)\hat{\rho}_{\perp}, \qquad (4)$$

где $F=\langle\Phi^{(+)}|\hat{\rho}|\Phi^{(+)}\rangle$ есть величина *Фиделити*, а $\hat{\rho}_{\perp}$ удовлетворяет условиям $\langle\Phi^{(+)}|\hat{\rho}_{\perp}|\Phi^{(+)}\rangle=0$, $\mathrm{Tr}\,\hat{\rho}_{\perp}=1$ и квазиположительной определенности.

Для нахождения вероятности ошибки, выразим квантовые состояния, соответствующие событию ошибки ($|HV\rangle$, $|VH\rangle$, $|AD\rangle$ и $|DA\rangle$) в базисе состояний Бэлла:

$$\begin{aligned}
|HV\rangle&=\frac{1}{\sqrt{2}}\left(|\psi^{(+)}\rangle+|\psi^{(-)}\rangle\right)\\
|VH\rangle&=\frac{1}{\sqrt{2}}\left(|\psi^{(+)}\rangle-|\psi^{(-)}\rangle\right)\\
|AD\rangle&=\frac{1}{\sqrt{2}}\left(|\Phi^{(-)}\rangle+|\psi^{(-)}\rangle\right)\\
|DA\rangle&=\frac{1}{\sqrt{2}}\left(|\Phi^{(-)}\rangle-|\psi^{(-)}\rangle\right).
\end{aligned} \qquad (5)$$

Находя вероятности измерения состояний в (5) по матрице плотности (4), получим значение сырой битовой ошибки:

$$\begin{aligned}
p_{er}&=\frac{1}{2}\left(p_{HV}+p_{VH}\right)+\frac{1}{2}\left(p_{AD}+p_{DA}\right)=\\
&=\left(1-F\right)\left(1+\langle\psi^{(-)}|\hat{\rho}_{\perp}|\psi^{(-)}\rangle\right)/2.
\end{aligned} \qquad (6)$$

Bob makes measurements in the diagonal basis when the half-wave plate is position at an angle of 22.5° or (22,5°+45°). When the plate is positioned at the photon passed through the Bob's beam splitter corresponds to the "1" bit, and the reflected photon corresponds to the "0" bit. When the plate is positioned at (22.5°+45°) the photon passed through the beam splitter corresponds to the "0" bit, and the reflected photon corresponds to "1".

The measurement of the bit error rate depending on the fidelity value was performed as follows. In accordance with the selected fidelity value, the angle value θ was determined. Then Alice prepared the polarization state of single photons by installing her half-wave plate in accordance with Table 1. For each polarization state prepared by Alice, Bob made a bit error measurement. To do this, Bob installed his half-wave plate to measure polarization in a basis that coincided with the Alice's basis, and measured the error probability (receipt of a bit value opposite to that set by Alice) for 20 seconds. The counting rate for the single photons correlated with the trigger Alice's photocount by the Bob's detectors is ~500 photocounts per second. The measurement results for four bit error values (for the laboratory and diagonal basis, the measurements in each basis were performed for two positions of the Bob's half-wave plate) were averaged, and the bit error probability was calculated p_{err}:

$$p_{err}=\frac{N_{err}^{L1}+N_{err}^{L2}+N_{err}^{D1}+N_{err}^{D2}}{N_{norm}^{L1}+N_{norm}^{L2}+N_{norm}^{D1}+N_{norm}^{D2}},$$

where $N_{err}^{L1,2/D1,2}$ is the number of bits erroneously received by Bob, and $N_{norm}^{L1,2/D1,2}$ is the total number of bits received by Bob (including erroneous and correct bits). The indices *L*1, *L*2, *D*1, *D*2 correspond to the Bob's measurement in the laboratory (*L*) and diagonal (*D*) basis, the numbers 1 and 2 correspond to various plate positions according to Table 2.

The measured value of the bit error depending on the fidelity is given in Fig. 2. The experimental data obtained confirm that fidelity makes it possible to unambiguously determine the bit error value introduced by the source in the BB84 scheme.

3. QUANTUM KEY DISTRIBUTION USING THE BBM92 SCHEME

We will consider the influence of fidelity value on the bit error value during the quantum key distribution using the BBM92 scheme [16]. The scheme

В силу того, что $\mathrm{Tr}\hat{\rho}_\perp = 1$ и значения элементов на диагонали матрицы $\hat{\rho}_\perp$ лежат в диапазоне от 0 до 1, то $0 \le \langle \psi^{(-)} | \hat{\rho}_\perp | \psi^{(-)} \rangle \le 1$. Таким образом,

$$\frac{1-F}{2} \le p_{er} \le \left(1-F\right), \tag{7}$$

то есть фиделити определяет диапазон возможных значений величины битовой ошибки в протоколе BBM92.

Пусть в протоколе BBM92, используется т. н. двухкристальный источник фотонных пар [21], генерирующий фотонные пары в поляризационном состоянии

$$|\psi\rangle = \cos\theta_0 |HH\rangle + e^{i\varphi} \sin\theta_0 |VV\rangle, \tag{8}$$

где θ_0 и φ – параметры, задаваемые направлением эллипса поляризации и эллиптичностью поляризации накачки. Фиделити для данного квантового состояния равна:

$$F = \frac{1}{2}\left(1 + \cos 2\theta_0 \cos\varphi\right), \tag{9}$$

и оптимальными значениями являются $\theta_0 = \pi/4$ и $\varphi = 0$, при которых $F = 1$. Вероятность ошибки, как можно проверить прямой подстановкой, равна $p_{er} = \left(1-F\right)/2$.

Из-за наличия механизмов декогеренции [22] двухкристальный источник может генерировать фотонные пары в смешанном состоянии. Такой источник описывается матрицей плотности [23]

$$\hat{\rho} = F|\Phi^{(+)}\rangle\langle\Phi^{(+)}| + (1-F)|\Phi^{(-)}\rangle\langle\Phi^{(-)}|, \tag{10}$$

и величина битовой ошибки снова равна $p_{er} = \left(1-F\right)/2$. Таким образом, двухкристальная схема при погрешностях в ее настройки вносит минимально возможную величину битовой ошибки, допускаемой выражением (6).

Схема установки для исследования влияния фиделити квантового состояния источника на величину битовой ошибки при квантовом распределении ключа по протоколу BBM92 представлена на рис. 3. В качестве источника поляризационно-запутанных фотонных пар используется двухкристальная схема. Непрерывный лазер, излучающий на длине волны 405 нм, последовательно проходит через компенсатор формы пучка накачки, полуволновую и кварцевую пластинки, и проходит через интерференционный светофильтр. Полученное излучение падает на двойной кристалл BBO. Пары поляризационно-запутанных фотонов

uses the pairs of quantum entangled particles. For the sake of argument, we will assume that the pairs of particles in the Bell polarization state are used $|\Phi^{(+)}\rangle = \left(|HH\rangle + |VV\rangle\right)/\sqrt{2}$. Alice and Bob each receive one of the entangled photons. The source of entangled photons can be external, or located at one of the subscribers. After the subscribers have each received one photon from the entangled pair, Alice and Bob measure the photon polarization. To do this, each subscriber has a meter similar to the meter used by Bob in the BB84 scheme discussed above. With the probability of 1/2, Alice measures the photon polarization in the laboratory basis, and with the probability of 1/2 – in the diagonal basis. Bob performs the same activities independently. Then Alice and Bob tell each other the basis in which the measurements have been made, but do not provide the specific measurement results.

Any errors in the developed key occur due to the eavesdropping, as well as in the case of using a low-quality source of entangled photons that generates the photon pairs in a state different from $|\Phi^{(+)}\rangle$ determined by the density matrix $\hat{\rho}$. Let us analyze the errors occurred due to the quantum state deviation of photon pairs from $|\Phi^{(+)}\rangle$.

To do this, we represent the density matrix of the source polarization state as follows:

$$\hat{\rho} = F|\Phi^{(+)}\rangle\langle\Phi^{(+)}| + (1-F)\hat{\rho}_\perp, \tag{4}$$

where $F = \langle\Phi^{(+)}|\hat{\rho}|\Phi^{(+)}\rangle$ is the *fidelity value*, and $\hat{\rho}_\perp$ meets the conditions of $\langle\Phi^{(+)}|\hat{\rho}_\perp|\Phi^{(+)}\rangle = 0$, $\mathrm{Tr}\hat{\rho}_\perp = 1$ and quasi-positive determinacy.

To obtain the error probability, we express the quantum states relevant to the error event($|HV\rangle$, $|VH\rangle$, $|AD\rangle$ and $|DA\rangle$) in the basis of Bell states:

$$\begin{aligned}
|HV\rangle &= \frac{1}{\sqrt{2}}\left(|\psi^{(+)}\rangle + |\psi^{(-)}\rangle\right)\\
|VH\rangle &= \frac{1}{\sqrt{2}}\left(|\psi^{(+)}\rangle - |\psi^{(-)}\rangle\right)\\
|AD\rangle &= \frac{1}{\sqrt{2}}\left(|\Phi^{(-)}\rangle + |\psi^{(-)}\rangle\right)\\
|DA\rangle &= \frac{1}{\sqrt{2}}\left(|\Phi^{(-)}\rangle - |\psi^{(-)}\rangle\right).
\end{aligned} \tag{5}$$

Having determined the probabilities of state measurements in (5) using the density matrix (4), we obtain the raw bit error value:

$$\begin{aligned}
p_{er} &= \frac{1}{2}\left(p_{HV} + p_{VH}\right) + \frac{1}{2}\left(p_{AD} + p_{DA}\right) =\\
&= \left(1-F\right)\left(1 + \langle\psi^{(-)}|\hat{\rho}_\perp|\psi^{(-)}\rangle\right)/2.
\end{aligned} \tag{6}$$

распространяются под углом 3° по отношению к накачке.

Один из полученных фотонов направляется на установку Алисы, а другой – Боба. У абонентов имеются волновые пластинки и поляризационный светоделитель, позволяющие им выбирать базис и производить поляризационные измерения. Одиночные фотоны регистрируются детекторами одиночных фотонов.

Величина фиделити экспериментально регулировалась путем наклона пластинки P, изменяющей фазу в состоянии (8). Величина $\theta_0 = \pi/4$. При каждом установленном положении пластинки P проводилась процедура квантовой томографии

Due to the fact that $\mathrm{Tr}\,\hat{\rho}_\perp = 1$ and the element values on the matrix diagonal $\hat{\rho}_\perp$ lie in the range from 0 to 1, then $0 \le \langle \psi^{(-)} | \hat{\rho}_\perp | \psi^{(-)} \rangle \le 1$. Thus,

$$\frac{1-F}{2} \le p_{er} \le \left(1-F\right), \qquad (7)$$

that is fidelity determines the range of possible bit error values in the BBM92 scheme.

Let the BBM92 scheme use the so-called double-crystal source of photon pairs [21], generating the photon pairs in a polarization state

$$|\psi\rangle = \cos\theta_0 |HH\rangle + e^{i\varphi} \sin\theta_0 |VV\rangle, \qquad (8)$$

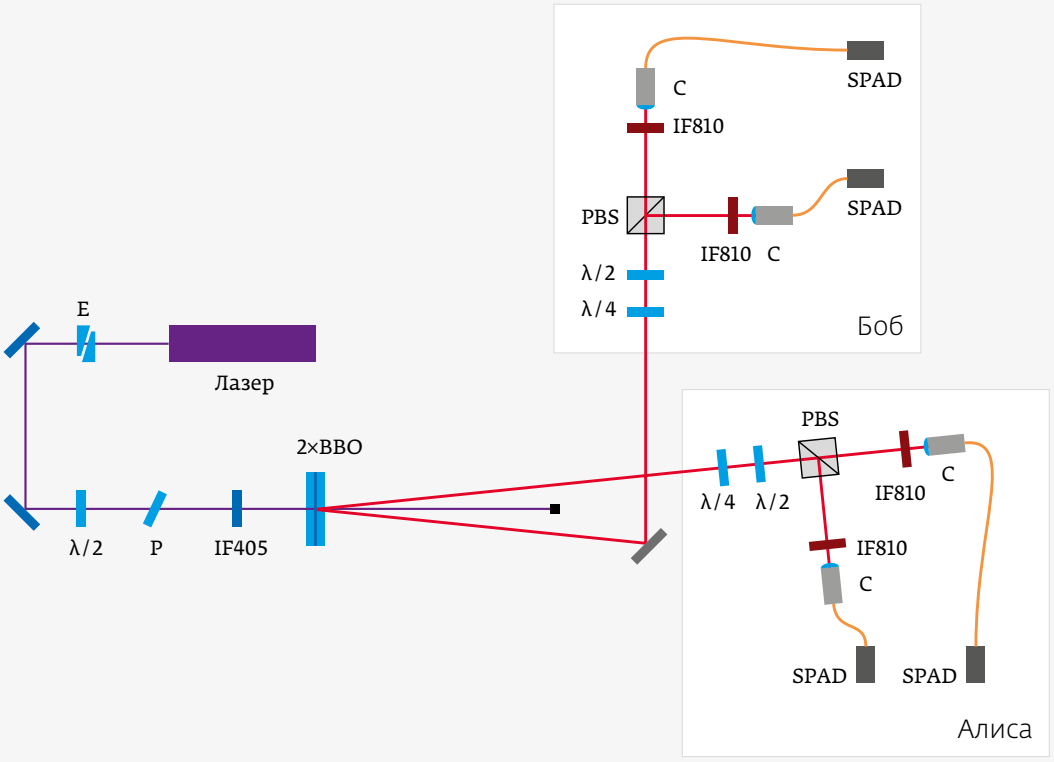

Рис. 3. *Схема экспериментальной установки для исследования зависимости величины битовой ошибки от фиделити при использовании протокола BBM92: Laser – лазер, излучающий на длине волны 405 нм; E – призменный компенсатор формы пучка накачки; λ/2, λ/4 – полу- и четвертьволновые пластинки; P – кварцевая пластинка, регулирующая эллиптичность поляризации накачки; IF405 и IF810 – интерференционный полосовой светофильтр на длину волны 405 нм и 810 нм, соответственно; 2×BBO – двойной кристалл BBO, PBS – поляризационный светоделитель; C – оптоволоконный коллиматор; SPAD – детектор одиночных фотонов*

Fig. 3. *The experimental setup layout to study the bit error value dependence on fidelity when using the BBM92 scheme: Laser – a laser emitting at a wavelength of 405 nm; E – prism pump beam shape compensator; λ/2, λ/2 – half- and quarter-wave plates; P – quartz plate that regulates the pump polarization ellipticity; IF405 and IF810 – interference bandpass filters for the wavelengths of 405 nm and 810 nm, respectively; 2×BBO – double BBO crystal, PBS – polarization beam splitter; C – fiber optic collimator; SPAD – single photon detector*

поляризационного состояния фотонных пар [24]. Время одного томографического измерения составляло 60 с, общая скорость счета коррелированных фотонов (без поляризационной фильтрации) – ≈300 фотоотсчетов в секунду. На основании восстановленной методом функции правдоподобия матрицы плотности $\hat{\rho}$, по формуле (2) вычислялась величина фиделити состояния источника $\hat{\rho}$ и состояния $|\Phi^{(+)}\rangle$. Затем производилось измерение величины битовой ошибки по аналогичной для BB84 процедуре, с дополнительным усреднением по измерениям Алисы.

Для измерения вероятности битовой ошибки волновые пластинки Алисы и Боба устанавливались для измерения состояния поляризации одиночных фотонов в совпадающих базисах – лабораторном или диагональном. Для четырех возможных комбинаций положений пластинок из табл. 2 производилось измерение вероятности получения несовпадающих битов (в течение 10 с каждое). Затем полученные измерения вероятности ошибки усреднялись по комбинациям пластинок и по двум совпадающим базисам, давая вероятность битовой ошибки в протоколе BBM92.

На рис. 4 представлена экспериментально измеренная зависимость величины битовой ошибки от фиделити. Из рисунка видно, что на основании значения фиделити действительно можно прогнозировать вклад в величину битовой ошибки, вносимый источником квантового света.

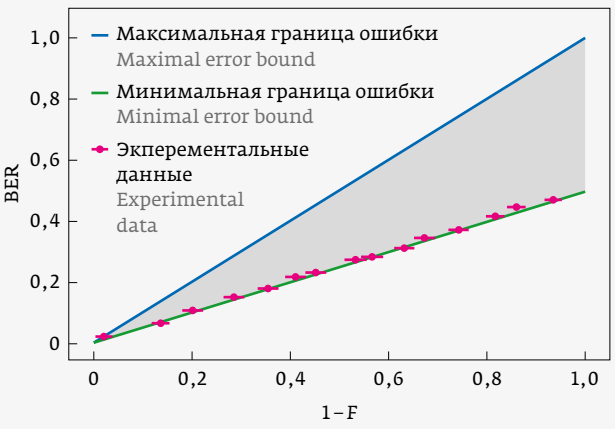

Рис. 4. *Зависимость величины битовой ошибки от фиделити при использовании протокола BBM92 (закрашенная область – множество допустимых значений величины битовой ошибки согласно выражению (6); красные точки – экспериментальные данные, полученные с использованием двухкристальной схемы)*

Fig. 4. *Dependence of the bit error value on fidelity when using the BBM92 scheme (shaded area is the set of permissible values of the bit error value according to the expression (6); red dots are the experimental data obtained using a double-crystal circuit)*

4. ЗАКЛЮЧЕНИЕ

В работе теоретически и экспериментально показано, что измерение фиделити позволяет определить величину одного из ключевых параметров системы квантового распределения ключа – величину сырой битовой ошибки, вносимой источником.

Для протокола BB84 теоретически и экспериментально показано, что при уменьшении фиделити от 1 до 0, величина сырой битовой ошибки линейно возрастает от 0 до 1.

Для протокола BBM92 теоретически показано, что величина битовой ошибки лежит в диапазоне от $\left(1-F\right)/2$ до 1–F. Экспериментально продемонстрировано, что при использовании двухкристального источника поляризационно-запутанных фотонных пар величина сырой битовой ошибки принимает минимально допускаемое величиной фиделити значение, и при уменьшении фиделити от 1 до 0 сырая битовая ошибка линейно возрастает от 0 до 1/2.

where θ_0 and φ are the parameters specified by the polarization ellipse direction and the pumping polarization ellipticity. Fidelity for a given quantum state is equal to the following:

$$F=\frac{1}{2}\left(1+\cos 2\theta_0 \cos\varphi\right), \qquad (9)$$

and the optimal values are $\theta_0=\pi/4$ and $\varphi=0$, at which F=1. The error probability of, as can be verified by direct substitution, is equal to $p_{er}=\left(1-F\right)/2$.

Due to the availability of decoherence mechanisms [22], a double-crystal source can generate the photon pairs in a mixed state. Such a source is described by the density matrix [23] as follows:

$$\hat{\rho}=F|\Phi^{(+)}\rangle\langle\Phi^{(+)}|+(1-F)|\Phi^{(-)}\rangle\langle\Phi^{(-)}|, \qquad (10)$$

and the bit error value is again equal to $p_{er}=\left(1-F\right)/2$. Thus, a double-crystal circuit with the errors in its settings introduces the minimum possible bit error value allowed by the expression (6).

The setup layout to study the fidelity influence of the source quantum state on the bit error

Таким образом, использование критерия *фиделити* в качестве стандарта квантового состояния, генерируемого источником запутанных фотонов является целесообразным.

Отметим, что полученные результаты применимы для протоколов BB84 и BBM92, основанных не только на использовании поляризационной степени свободы фотона, но и при использовании другой степени свободы с двумя дискретными базисными состояниями, например, при фазовом кодировании [25] или кодировании двумя значениями проекции орбитального момента света [26].

БЛАГОДАРНОСТИ

Авторы выражают благодарность А. С. Чиркину за обсуждение работы и ценные замечания.

ПОДДЕРЖКА

Работа выполнена при финансовой поддержке гранта Российского научного фонда, уникальный номер проекта РНФ № 21-12-00155.

REFERENCES

1. **Vaughan O.** A platform for quantum computing. *Nature Electronics* 6, no. 5 (2023): 337–337. DOI: 10.1038/s41928-023-00974-4.
2. **Fldzhyan S. A., Saygin M.Yu., Kulik S. P.** Programmable heralded linear optical generation of two-qubit states. *Physical Review Applied* 20, no. 5 (2023): 054030. DOI: 10.1103/PhysRevApplied.20.054030.
3. **Wang J., Sciarrino F., Laing A., Thompson M. G.** Integrated photonic quantum technologies. *Nature Photonics* 14, no. 5 (2020): 273–284. DOI: 10.1038/s41566-019-0532-1.
4. **Struchalin G. I., Zagorovskii Ya.A., Kovlakov E. V., Straupe S. S., Kulik S. P.** Experimental estimation of quantum state properties from classical shadows. *PRX Quantum* 2, no. 1 (2021): 010307. DOI: 10.1103/PRXQuantum.2.010307.
5. **Moiseev E. S., Tashchilina A., Moiseev S. A., and Sanders B. C.** Broadband quantum memory in a cavity via zero spectral dispersion. *New Journal of Physics* 23, no. 6 (2021): 063071. DOI: 10.1088/1367-2630/ac0754.
6. **Kalash M., Chekhova M. V.** Wigner function tomography via optical parametric amplification. *Optica* 10, no. 9 (2023): 1142–1146. DOI: 10.1364/OPTICA.488697.
7. **Mironov Y. B., Kazantsev S. Y., Shakhovoy R. A., Kolesnikov O. V., Mashkovtseva L. S., Zaitcev A. I., Korobov A. V.** *Analysis of single photon sources with quantum key distribution systems development prospects.* H&ES Reserch. 2021;13(6):22–33. DOI: 10.36724/2409-5419-2021-13-6-22-33.
8. **Миронов Ю. Б., Казанцев С. Ю., Шаховой Р. А., Колесников О. В., Машковцева Л. С., Зайцев А. И., Коробов А. В.** Анализ перспектив развития источников одиночных фотонов в системах квантового распределения ключей. Наукоемкие технологии в космических исследованиях Земли. 2021;13(6):22–33. DOI: 10.36724/2409-5419-2021-13-6-22-33.
9. **Shu H.** Solve single photon detector problems. *Quantum*. 2023 Nov 21;7:1187. DOI: 10.22331/q-2023-11-21-1187.
10. **Reutov A, Tayduganov A, Mayboroda V, Fat'yanov O.** Security of the decoy-state BB84 protocol with imperfect state preparation. Entropy. 2023 Nov 17;25(11):1556. DOI: 10.3390/e25111556.
11. **Chunnilall CJ, Degiovanni IP, Kück S, Müller I, Sinclair AG.** Metrology of single-photon sources and detectors: a review. *Optical Engineering*. 2014 Aug 1;53(8):081910. DOI: 10.1117/1.OE.53.8.081910.
12. **Waks E, Santori C, Yamamoto Y.** Security aspects of quantum

value in the case of quantum key distribution using the BBM92 scheme is shown in Fig. 3. The double-crystal circuit is used as a source of polarization-entangled photon pairs. A continuous wave laser emitting at a wavelength of 405 nm passes sequentially through a pump beam shape compensator, half-wave and quartz plates, and passes through an interference filter. The resulting radiation is incident on a double crystal. The pairs of polarization-entangled photons are propagated at an angle 3° of relative to the pump.

One of the received photons is sent to the Alice's setup, and the other one is sent to the Bob's setup. The subscribers have the wave plates and a polarization beam splitter, allowing them to select a basis and make the polarization measurements. The single photons are recorded by the single photon detectors.

The fidelity value was experimentally adjusted by tilting the plate P, changing the phase in a state (8). The value was $\theta_0 = \pi/4$. At each established position of the plate P, a quantum tomography procedure of the polarization state of photon pairs was performed [24]. The duration of one tomographic measurement was 60 seconds, the total counting rate of correlated photons (without any polarization filtering) was ≈300 photocounts per second. Based on the density matrix $\hat{\rho}$ reconstructed by the likelihood function method, the formula (2) was used to calculate the fidelity value of the source state $\hat{\rho}$ and state $|\Phi^{(+)}\rangle$. Then the bit error value was measured using a procedure similar to BB84, with additional averaging based on the Alice's measurements.

To measure the bit error probability, the Alice's and Bob's waveplates were set up to measure the polarization state of single photons in the matching bases (laboratory or diagonal). For four possible combinations of plate positions given in Table 2, the probability of receiving mismatched bits was measured (within 10 seconds each). The resulting error probability measurements were then averaged across the plate combinations and across two matching bases to obtain the BBM92 bit error probability.

Figure 4 shows the experimentally measured dependence of the bit error on fidelity. The figure shows that the fidelity value can be used as the basis for possible prediction of contribution to the bit error made by the quantum light source.

4. CONCLUSION

On the theoretical and experimental level, the paper shows that the fidelity measurement makes

При поддержке: МИНПРОМТОРГ РОССИИ; Министерство науки и высшего образования Российской Федерации; ЭЛЕМЕНТ

Организаторы: НИИМЭ; ПРОГРЕСС

Генеральный партнер: ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Инновационный партнер: АСТРОН

Партнеры: Итэлма; Fostec; НИИТМ; МИФИ

Оператор: ПрофКонференции

Генеральный информационный партнер: ТЕХНОСФЕРА

РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА 2024
10 лет

Сириус
федеральная территория

23–28 сентября 2024

6 дней	**2500+** участников	**850+** компаний	**13** секций
25 круглых столов	**850+** докладов	**125+** экспозиций	**1000** м^2 выставочных площадей

10 лет вместе!

Российский форум «Микроэлектроника 2024» – синергия уникальных событий

- Предконференции
- Научная конференция «ЭКБ и микроэлектронные модули»
- Деловая программа
- Школа молодых ученых
- Выставка «Виртуальная среда микроэлектроники»
- Культурная программа

MICROELECTRONICA.PRO

ПОДПИСЫВАЙТЕСЬ И БУДЬТЕ В КУРСЕ ВСЕХ ПОСЛЕДНИХ НОВОСТЕЙ!

+7 495 641 57 17 | microelectronica.pro | info@microelectronica.pro

key distribution with sub-Poisson light. *Physical Review A*. 2002 Oct 22;66(4):042315. DOI: 10.1103/PhysRevA.66.042315.
13. **Grangier P, Roger G, Aspect A.** Experimental evidence for a photon anticorrelation effect on a beam splitter: a new light on single-photon interferences. *Europhysics Letters*. 1986 Feb 15;1(4):173. DOI: 10.1209/0295-5075/1/4/004.
14. ETSI standard. ETSI GS QKD 011 V1.1.1 (2016-05), Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems. URL: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/011/01.01.01_60/gs_QKD011v010101p.pdf
15. **Jozsa R.** Fidelity for mixed quantum states. *Journal of modern optics* 41, no. 12 (1994): 2315–2323. DOI: 10.1080/09500349414552171.
16. **Bennett C. H., Brassard G.** An update on quantum cryptography. In *Workshop on the theory and application of cryptographic techniques*, pp. 475–480. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984. DOI: 10.1007/3-540-39568-7_39.
17. **Bennett C. H., Brassard G., Mermin N. D.** Quantum cryptography without Bell's theorem. *Physical review letters* 68, no. 5 (1992): 557. DOI: 10.1103/PhysRevLett.68.557.
18. **Kulik S. P.** Quantum cryptography. *Photonics Russia*. 2010;4(2):36–41. **Кулик С. П.** Квантовая криптография. *ФОТОНИКА*. 2010;4(2):36–41.
19. **Wootters W. K., Zurek W. H.** A single quantum cannot be cloned. *Nature* 299, no. 5886 (1982): 802–803. DOI: 10.1038/299802a0.
20. **Lo H.-K., Ma X., Chen K.** Decoy state quantum key distribution. *Physical review letters* 94, no. 23 (2005): 230504. DOI: 10.1103/PhysRevLett.94.230504.
21. **Couteau C.** Spontaneous parametric down-conversion. *Contemporary Physics* 59, no. 3 (2018): 291–304. DOI: 10.1080/00107514.2018.1488463.
22. **Kwiat P. G., Waks E., White A. G., Appelbaum I., Eberhard P. H.** Ultrabright source of polarization-entangled photons. *Physical Review A* 60, no. 2 (1999): R773. DOI: 10.1103/PhysRevA.60.R773.
23. **Altepeter J. B., Jeffrey E. R., Kwiat P. G.** Phase-compensated ultra-bright source of entangled photons. *Optics Express* 13, no. 22 (2005): 8951–8959. DOI: 10.1364/OPEX.13.008951.
24. **Rangarajan R., Goggin M., Kwiat P. G.** Optimizing type-I polarization-entangled photons. *Optics express* 17, no. 21 (2009): 18920–18933. DOI: 10.1364/OE.17.018920.
25. **Frolovtsev D. N., Magnitskii S. A., Demin A. V.** Measurement Method of the Polarization-Entangled States of Biphotons Using a Quantum Tomograph. *Measurement Techniques* 64, no. 10 (2022): 809–816. DOI: 10.1007/s11018-022-02008-5. **Фроловцев, Д.Н., Магницкий С.А., Демин А. В.** Методика измерений поляризационно-запутанных состояний бифотонов с помощью квантового томографа. *Измерительная техника* 10 (2023): 21–27. DOI: 10.32446/0368-1025it.2021-10-21-27.
26. **Pathak N. K, Chaudhary S, Sangeeta, Kanseri B.** Phase encoded quantum key distribution up to 380 km in standard telecom grade fiber enabled by baseline error optimization. *Scientific Reports*. 2023 Sep 22;13(1):15868. DOI: 10.1038/s41598-023-42445-y.
27. **Spedalieri F. M.** Quantum key distribution without reference frame alignment: Exploiting photon orbital angular momentum. *Optics communications*. 2006 Apr 1;260(1):340–6. DOI: 10.1016/j.optcom.2005.10.001.

АВТОРЫ

Фроловцев Д. Н., научный сотрудник, Физический факультет, МГУ им. М. В. Ломоносова, г. Москва
Демин А. В., к. т. н., с.н.с., Всероссийский научно-исследовательский институт оптико-физических измерений (ФГБУ «ВНИИОФИ»), г. Москва, Россия.

ЛИЧНЫЙ ВКЛАД АВТОРОВ

Д. Н. Фроловцев – 70% (теоретические расчеты, проведение эксперимента, обработка результатов эксперимента, анализ полученных результатов, написание текста статьи); А. В. Демин – 30% (анализ полученных результатов, написание текста статьи).

КОНФЛИКТ ИНТЕРЕСОВ

Авторы декларируют отсутствие конфликта интересов.

it possible to determine the value of one of the key parameters of a quantum key distribution system, namely the raw bit error rate introduced by the source.

For the BB84 scheme, it has been theoretically and experimentally shown that as the fidelity is decreased from 1 to 0, the raw bit error rate increases linearly from 0 to 1.

For the BBM92 scheme, it has been theoretically shown that the bit error value is within the range from $(1-F)/2$ to $1-F$. It has been experimentally demonstrated that when using a double-crystal source of polarization-entangled photon pairs, the raw bit error value takes on the minimum value allowed by the fidelity, and when the fidelity decreases from 1 to 0, the raw bit error is linearly increased from 0 to 1/2.

Thus, application of *the fidelity* criterion as a standard for the quantum state generated by a source of entangled photons is appropriate.

It should be noted that the results obtained are applicable for the BB84 and BBM92 schemes, based not only on the application of the polarization freedom degree of the photon, but also when using another degree of freedom with two discrete basis states, for example, in the case of phase encoding [25] or encoding with two projection values of the orbital light moment [26].

ACKNOWLEDGMENTS

The authors express their gratitude to A. S. Chirkin for discussion of this paper and valuable comments.

SUPPORT

The paper has been prepared with the financial support in the form of a grant from the Russian Science Foundation, unique RSF project number No. 21-12-00155.

AUTHORS

Frolovtsev D. N., Researcher, Department of Physics, Lomonosov Moscow State University, Moscow, Russia
Demin A. V., Cand. of Technical Sciences, Researcher, FGBI "VNIIOFI", Moscow, Russia.

PERSONAL CONTRIBUTION OF THE AUTHORS

D. N. Frolovtsev – 70% (theoretical calculations, conducting the experiment, processing the results of the experiment, analyzing the results obtained, writing the text of the article); A. V. Demin – 30% (analyzing the results obtained, writing the text of the article).

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.


weldex
23-Я МЕЖДУНАРОДНАЯ ВЫСТАВКА СВАРОЧНЫХ МАТЕРИАЛОВ, ОБОРУДОВАНИЯ И ТЕХНОЛОГИЙ
8–11 ОКТЯБРЯ 2024
МОСКВА КРОКУС ЭКСПО ПАВИЛЬОН 1
– СОТНИ НОВИНОК ОБОРУДОВАНИЯ ДЛЯ СВАРКИ, РЕЗКИ, ПАЙКИ
– ДЕМОНСТРАЦИЯ ПРОДУКЦИИ В ДЕЙСТВИИ
– НАЦИОНАЛЬНЫЕ ЧЕМПИОНАТЫ ПО СВАРКЕ И КОНФЕРЕНЦИИ
ПОЛУЧИТЕ БИЛЕТ ПО ПРОМОКОДУ
tehnosphera
Одновременно и на одной площадке с
2-й Международной выставкой крепежа и оснастки
FASTENEX
Международной выставкой оборудования и инструмента
TOOL MASH
Посещение выставок бесплатно по билету на Weldex
ITE ОРГАНИЗАТОР ORGANISER
0+
+7 499 750 08 28
WELDEX@ITE.GROUP