ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ
МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ
INTERNATIONAL UNIVERSITY

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2022 (3) 4

Қазан-желтоқсан

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншіктенуші: «Халықаралық ақпараттық технологиялар университеті» АҚ (Алматы қ.).
Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің Ақпарат комитетінде – **20.02.2020** жылы берілген.
№ KZ82VPY00020475 мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: ақпараттық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологияларға арналған.
Мерзімділігі: жылына 4 рет.
Тиражы: 100 дана
Редакцияның мекенжайы: 050040, Алматы қ-сы, Манас к-сі, 34/1, 709-кабинет, тел: +7 (727) 244-51-09).
E-mail: ijict@iitu.edu.kz Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

---

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09). E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

АҚПАРАТТЫҚ КОММУНИКАЦИЯЛЫҚ ЖЕЛІЛЕР ЖӘНЕ КИБЕРҚАУІПСІЗДІК

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И КИБЕРБЕЗОПАСНОСТЬ

INFORMATION AND COMMUNICATION NETWORKS AND CYBERSECURITY

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 3. Is. 4. Number 12 (2022). Pp. 41–56
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/*10.54309/IJICT.2022.12.4.004*

УДК 004.056.55, 535.92

SECURITY ANALYSIS OF THE DISTRIBUTION OF QUANTUM KEYS IN PASSIVE OPTICAL NETWORKS

A.E. Nasylbekova[1]*, I. Khlevna[2]

Aiym Y. Nassylbekova — master student of the «Radio Engineering, electronics and telecommunications», International Information Technology University
ORCID: 0000-0002-9055-3498. E-mail: 33198@iitu.edu.kz.
I. Khlevna — d.tech.science, professor, Taras Shevchenko National university of Kyiv (Ukraine)

Abstract. The need for security for end users has led to the installation of Quantum Key Distribution (QKD) in one-to-many access networks such as passive optical networks. In networks, the presence of optical power splitters makes the secure key rate issues more important. However, research on QKD in access networks has mostly focused on implementation issues rather than developing a protocol to increase the key rate. Since the safe key rate is theoretically limited by the protocol, studies without protocol development cannot overcome the safe key rate limit given by the protocol. This necessitates research to develop a protocol. This article proposes a new approach that provides a secure increase in key transfer rate over the conventional protocol. A secure key rate formula in a passive optical network is proposed by extending the secure key rate formula based on the BB84 protocol with a honeypot state. For a passive optical network, a method is proposed that includes collaboration between end users. We then show that this method can mitigate the photon number division (PNS) attack, which is critical in the well-known BB84 trap protocol. In particular, the proposed scheme allows multiphoton states to serve as secure keys, unlike the conventional BB84 decoy

protocol. Numerical simulations show that our proposed scheme outperforms the BB84 honeypot protocol in terms of secure key speed.

Keywords: cybersecurity, passive optical systems, quantum distribution, photons, BB84 protocol

For citation A.E. Nasylbekova, I. Khlevna. Security analysis of the distribution of quantum keys in passive optical networks // INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2022. Vol. 3. Is. 4. Number 12. Pp. 41–56 (In Russ.). DOI: *10.54309/IJICT.2022.12.4.004.*

ПАССИВТІ ОПТИКАЛЫҚ ЖЕЛІЛЕРДЕГІ КВАНТТЫҚ КІЛТТЕРІНІҢ БӨЛУІНІҢ ҚАУІПСІЗДІК ТАЛДАУЫ

А.Е. Насылбекова[1*], I. Khlevna[2]

Насылбекова Айым Ермековна — «Радиотехника, электроника және телекоммуникациялар» кафедрасының магистранты, Халықаралық ақпараттық технологиялар университеті
ORCID: 0000-0002-9055-3498. E-mail: 33198@iitu.edu.kz.
I. Khlevna — д. тек.ғылым, Профессор, Тарас Шевченко Атындағы Киев Ұлттық университеті (Украина)

Аннотация. Түпкі пайдаланушылар үшін қауіпсіздік қажеттілігі пассивті оптикалық желілер сияқты бір-көп қолжетімділік желілерінде кванттық кілттерді таратуды (QKD) орнатуға әкелді. Желілерде оптикалық қуат бөлгіштерінің болуы қауіпсіз кілт жылдамдығы мәселелерін маңыздырақ етеді. Дегенмен, қол жеткізу желілеріндегі QKD бойынша зерттеулер негізгі жылдамдықты арттыру үшін хаттаманы әзірлеуге емес, негізінен іске асыру мәселелеріне бағытталған. Қауіпсіз кілт жылдамдығы хаттамамен теориялық тұрғыдан шектелгендіктен, хаттаманы әзірлемеген зерттеулер хаттамамен берілген қауіпсіз кілт жылдамдығының шегін жеңе алмайды. Бұл хаттаманы әзірлеу үшін зерттеуді қажет етеді. Бұл мақалада кәдімгі протоколға қарағанда кілтті тасымалдау жылдамдығын қауіпсіз арттыруды қамтамасыз ететін жаңа тәсіл ұсынылады. Атап айтқанда, пассивті оптикалық желідегі қауіпсіз кілт жылдамдығы формуласы BB84 протоколына негізделген қауіпсіз кілт жылдамдығы формуласын бал күйі күйімен кеңейту арқылы ұсынылады. Пассивті оптикалық желі үшін соңғы пайдаланушылар арасындағы ынтымақтастықты қамтитын әдіс ұсынылады. Содан кейін біз бұл әдіс белгілі BB84 тұзақ протоколында маңызды болып табылатын фотондар санын бөлу (PNS) шабуылын азайта алатынын көрсетеміз. Атап айтқанда, ұсынылып отырған схема кәдімгі BB84 жалған хаттамасынан айырмашылығы, мультифотон күйлеріне қауіпсіз кілттер ретінде қызмет етуге мүмкіндік береді. Сандық модельдеу біздің ұсынылған схема қауіпсіз кілт жылдамдығы бойынша BB84 протоколынан асып түсетінін көрсетеді.

Түйін сөздер: киберқауіпсіздік, пассивті оптикалық жүйелер, кванттық тарату, фотондар, BB84 протоколы

Дәйексөз үшін: А.Е. Насылбекова, I. Khlevna. Пассивті оптикалық желілердегі кванттық

кілттерінің бөлуінің қауіпсіздік талдауы // ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2022. Том. 3. Is. 4. Нөмірі 12. 41–56 бет (орыс тілінде). DOI: 10.54309/IJICT.2022.12.4.004.

АНАЛИЗ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕНИЯ КВАНТОВЫХ КЛЮЧЕЙ В ПАССИВНЫХ ОПТИЧЕСКИХ СЕТЯХ

А.Е. Насылбекова[1]*, I. Khlevna[2]

Насылбекова Айым Ермековна — магситрант факультета «Радиотехника, электроники и телекоммуникации», Университет международных информационных технологий
ORCID: 0000-0002-9055-3498. E-mail: 33198@iitu.edu.kz.
I. Khlevna — доктор технических наук, профессор, Киевский национальный университет имени Тараса Шевченко *(Украина)*

Аннотация. Потребность в обеспечении безопасности для конечных пользователей привела к установке квантового распределения ключей (Quantum Key Distribution — QKD) в сетях доступа «один ко многим», таких как пассивные оптические сети. В сетях наличие оптических разветвителей мощности делает вопросы безопасной скорости передачи ключей более важными. Однако исследования QKD в сетях доступа в основном были сосредоточены на вопросах реализации, а не на разработке протокола для повышения ключевой скорости. Поскольку безопасная ключевая скорость теоретически ограничена протоколом, исследования без разработки протокола не могут преодолеть предел безопасной ключевой скорости, заданный протоколом. Это вызывает необходимость исследований для разработки протокола. В этой статье предлагается новый подход, который обеспечивает безопасное повышение скорости передачи ключей по сравнению с обычным протоколом. В частности, предлагается формула безопасной ключевой скорости в пассивной оптической сети, расширяя формулу безопасной ключевой скорости на основе протокола BB84 с состоянием приманки. Для пассивной оптической сети предлагается способ, который включает сотрудничество между конечными пользователями. Затем мы показываем, что этот способ может смягчить атаку разделения числа фотонов (Photon Number Splitting - PNS), которая имеет решающее значение в известном протоколе-ловушке BB84. В частности, предлагаемая схема позволяет многофотонным состояниям служить безопасными ключами, в отличие от обычного протокола-ловушки BB84. Численное моделирование показывает, что предложенная нами схема превосходит протокол-приманку BB84 по скорости безопасного ключа.

Ключевые слова: кибербезопасность, пассивные оптические системы, квантовое распределение, фотоны, протокол BB84

Для цитирования: А.Е. Насылбекова*,* Iulia Khlevna. Анализ безопасности распределения квантовых ключей в пассивных оптических сетях // МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ.

2022. Том. 3. Is. 4. Номер 12. Стр. 41–56 (на русском языке). DOI: 10.54309/IJICT.2022.12.4.004.

Введение

Распределение квантовых ключей (QKD) привлекло большое внимание, поскольку оно обеспечивает новую парадигму безопасной связи. Приложение для соединений «точка-точка» (P2P) в магистральной сети является хорошим примером квантово-защищенных сетей. Для этого многие исследовательские группы провели и сообщили о теоретических и экспериментальных результатах QKD для сетей P2P (Хван, 2012; Бургуин и др., 2015). Ускоренные общенациональные полевые испытания QKD были проведены в ведущих странах (Пеев и др., 2009; Ван и др., 2010). В последнее время коммерциализированы системы QKD, основанные на протоколе BB84 (Чжао). Однако из-за различных сетевых структур между опорной сетью и сетью доступа этих результатов недостаточно для характеристики безопасности многопользовательских сетей. Для предоставления услуг конечным пользователям были проведены исследования для многопользовательских сетей (Фернандес и др., 2007; Чиурана и др., 2014; Фрёлих и др., 2013).

Целью сетей «точка-многоточка» является предоставление конечным пользователям более высокой безопасной скорости передачи ключей. Чтобы добиться этого, мы стремимся разработать способ совместной работы всех пользователей, чтобы снизить вероятность подслушивания. Мы предлагаем способ борьбы с атакой разделения числа фотонов (PNS) с помощью информации об обнаружении совпадений между конечными пользователями в нескольких точках. С помощью предложенной схемы мы показываем, что некоторые из импульсов, имеющих несколько фотонов, могут использоваться в качестве секретных ключей, в отличие от обычного протокола-ловушки BB84.

Тем не менее, большинство работ для многопользовательских сетей в основном сосредоточено на реализации сетей доступа QKD с протоколом-ловушкой BB84, потому что система QKD с протоколом-ловушкой BB84 проста в реализации и теоретически доказана ее безоговорочная безопасность. Вопросы реализации, такие как назначение длины волны и объединение между обычными и квантовыми каналами, рассматриваются в (Фернандес и др., 2017; Чиурана и др., 2014). Авторы в (Фрёлих, 2013) рассмотрели вопросы конфигурации, сравнивая нисходящие и восходящие сети квантового доступа. Они утверждали, что с точки зрения стоимости и осуществимости систем выгодно настраивать нисходящие сети квантового доступа, в которых передатчики расположены у конечных пользователей. Однако безопасная ключевая скорость исследований, может быть, в итоге ограничена без разработки протоколов. В протоколе BB84 критический фактор, ограничивающий скорость безопасного ключа, вызван атакой PNS. При атаке импульсы, имеющие несколько фотонов, называемые многофотонными состояниями, не могут генерировать безопасные ключи (Хван, 2003). Следовательно, только импульсы, имеющие один фотон, называемые однофотонными состояниями, могут генерировать безопасные ключи в

протоколе-ловушке BB84. Поскольку исследователи не рассматривали разработку протокола для смягчения атаки PNS, их производительность не может преодолеть ограничение независимо от системных конфигураций, таких как направление передачи. Недостаточность исследований для преодоления ограничения привела к необходимости исследований по разработке протокола.

В данной работе исследуются сети доступа, в которых имеется разветвитель, делающий структуру сети типа «один ко многим». Одним из таких примеров является пассивная оптическая сеть (Passive Optical Network - PON). На примере сети мы показываем, что вышеупомянутое ограничение можно преодолеть простым способом, используя характеристики PON: обнаружение совпадений между конечными пользователями может уменьшить количество секретных ключей, захваченных PNS-атакой. Следовательно, многофотонные состояния могут использоваться для генерации секретных ключей, которые считались непригодными для использования в качестве безопасных ключей. Поскольку стандартная PON обычно может быть развернута с максимальным коэффициентом разделения от 1 до 64 (Шим и др., 2012; Zhang и др., 2016), мы включили обнаружение совпадений в модель GLLP (Global Laboratory Leadership Programme) (Ma и др., 2005) и выполнили численные оценки для PON с 64 конечными пользователями.

Материалы и методы

Модель системы

Система QKD с ложным протоколом BB84 на PON состоит из одного терминала оптической линии (Optical Line Terminal – OLT), одного оптоволоконного канала и нескольких блоков оптической сети (Optical Network Unit – ONU), как показано на рисунке 1. Чтобы описать структуру, конкретные характеристики лазерного источника, канал и детектор, такие как распределение фотонов, генерируемых лазерным источником, потери в канале и вероятности обнаружения фотонов, моделируются типичным способом, как в (Ma и др., 2005).

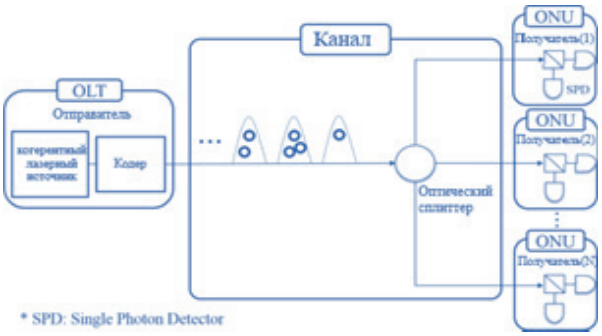

Рисунок 1 – Модель системы для общей системы PON нисходящего потока

Отправитель в OLT обладает когерентным лазерным источником с рандомизированной фазой и кодером для генерации квантовых состояний для сеанса

QKD. По характеристикам источника количество фотонов следует распределению Пуассона следующим образом:

$$\Pr(\text{количество фотонов} = i) = \frac{\mu^i}{i!}e^{-\mu} \quad (1)$$

где μ — среднее число фотонов источника.

Канал, рассматриваемый в этой статье, можно назвать квантовым каналом, потому что через него может быть доставлено квантовое состояние. Этот квантовый канал можно охарактеризовать своим внутренним коэффициентом пропускания. Пусть $T_к$ обозначает коэффициент пропускания квантового канала. Затем $T_к$ можно разложить на две части: коэффициент пропускания самого волокна, $T_в$, и коэффициент пропускания разветвителя, $T_р$.

$$T_к = T_в T_р = 10^{-\frac{\alpha l}{10}} 10^{-\frac{L_р}{10}} \quad (2)$$

где α, l и $L_р$ представляют собой коэффициент потерь в канале в дБ/км, расстояние оптического волокна в км и потери при расщеплении в дБ соответственно.

Квантовое состояние, достигшее ONU дополнительно страдает от внутреннего пропускания ONU. Внутренний коэффициент пропускания ONU, TONU, можно выразить следующим образом:

$$T_{ONU} = 10^{-\frac{L_{ONU}}{10}} \quad (3)$$

где L_{ONU} представляет внутренние потери ONU в дБ.

После внутренних оптических схем ONU квантовое состояние обнаруживается одним из двух детекторов одиночных фотонов (Single Photon Detector - SPD) в ONU. Эффективность обнаружения SPD можно обозначить как. С $\gamma_{общ}$, и уравнениями. (2) и (3), мы можем рассчитать общую квантовую эффективность обнаружения, $\gamma_{общ}$, квантового состояния, отправленного Отправителем:

$$\gamma_{общ} = \gamma_{обн} T_{ONU} T_к \quad (4)$$

Вышеупомянутое значение $\gamma_{общ}$ связано с коэффициентом пропускания одиночного фотона. Однако в реальной ситуации несколько фотонов могут быть переданы характеристиками лазерного источника в уравнении. (1). К сожалению, большинство обычных SPD могут разрешать только нулевые или ненулевые фотоны (Кок и др., 2007). Таким образом, мы не можем определить количество фотонов в входящем квантовом состоянии из события обнаружения. По этой причине эффективность обнаружения i-фотонных состояний, γ_i, может быть выражена следующим образом:

$$Y_i = 1 - (1 - \gamma_{общ})^i \quad (5)$$

Существует еще один фактор, вызывающий обнаружение SPD, а именно темновой счет SPD. Из-за темнового счета обнаружение может происходить на стороне Получателя даже при нулевых состояниях фотонов. Соответственно, чтобы вычислить условную вероятность того, что квантовое состояние будет обнаружено при заданном квантовом состоянии, нам необходимо принять во внимание γ_i и темновой счет. Мы определяем γ_i как условную вероятность обнаружения квантового состояния при заданном состоянии i-фотона, генерируемом лазерным источником:

$$\gamma_i = \Pr(\text{обнаружение} \mid \text{состояние i-фотона}) \quad (6)$$

Предполагая, что события обнаружения из двух разных источников, которые представляют собой переданное квантовое состояние и темновой счет, независимы, γ_i можно составить следующим образом:

$$Y_i = \gamma_i + Y_0 - \gamma_i Y_0 \quad (7)$$

где Y_0 — вероятность ложной тревоги, вызванной темновым счетом. То есть Y_0 соответствует вероятности (p) темнового счета в единицу времени, $p_{темн}$. Как и в (Хрг и др., 2005), $p_{темн}$ определяется как вероятность того, что среди двух детекторов на стороне Получателя произойдет хотя бы один темновой отсчет.

Пусть Q1 обозначает вероятность обнаружения i-фотонного состояния, называемую усилением i-фотонного состояния, как в (Ма и др., 2005). С γ_i и распределением Пуассона лазерного источника Q1 можно рассчитать следующим образом:

$$Q_i = \Pr(\text{обнаружение, состояние i-фотона}) = Y_i \frac{\mu^i}{i!} e^{-\mu} \quad (8)$$

Посредством обнаружения полученные состояния преобразуются в информацию, содержащую ошибки. Это можно смоделировать как квантовую частоту ошибок по битам (Quantum Bit Error Rate — QBER). Чтобы смоделировать QBER, нужно задать e_i как QBER состояния i-фотона. На QBER влияют два основных фактора: темновой счет и несовершенство системы. В случае темнового счета это вызывает ошибки с вероятностью. Поскольку темновые отсчеты двух детекторов на стороне Получателя независимы, в этой системе e_i равно 1/2. Для принятого квантового состояния может возникнуть ошибка с вероятностью, моделируемой как $e_{ош}$, характеризующая несовершенство системы. Исходя из вышеперечисленных особенностей,

$$e_i = \frac{e_0 Y_0 (1 - \gamma_i) + e_{ош} \gamma_i (1 - Y_0) + e_0 e_{ош} \gamma_i Y_0}{Y_I} \quad (9)$$

На основании уравнений. (8) и (9), мы можем рассчитать общий коэффициент усиления и QBER. Во-первых, общий коэффициент усиления Qμ представляет собой вероятность обнаружения лазерного источника со средним числом фотонов μ.

$$Q_\mu = \sum_{I=0}^{\infty} Q_I = 1 - (1 - Y_0)e^{-\gamma_{\text{общ}}\mu} \qquad (10)$$

Общий протокол QKD для PON

В этой статье рассматривается протокол QKD на основе протокола BB84 для PON нисходящего потока с помощью предложенного нами метода, который представляет собой этап оценки распределения числа фотонов с использованием характеристик PON. Для понимания предлагаемого метода мы кратко представляем ложный протокол BB84 QKD (Ma и др., 2005) на PON. Как и в большинстве случаев, предположим, что сеанс QKD создается между парой OLT и ONU. То есть существует N сеансов QKD, сгенерированных, если PON установлена с N ONU. Из-за вышеупомянутого предположения протокол является симметричным для каждой пары OLT и ONU.

Отправитель случайным образом выбирает среднее число фотонов лазерного источника, чтобы выбрать состояние приманки или сигнала. Затем Отправитель случайным образом генерирует слабые когерентные импульсы и модулирует их по четырем состояниям, используя либо фазовую, либо поляризационную модуляцию. Четыре состояния выбираются из двух оснований, которые Z = {|0> , |0>} или X = {|+> = (|0> + |1>)/ √ 2, |−> = (|0> − |1>)/ √ 2}. Затем модулированные импульсы отправляются Получателю.

Чтобы обнаружить полученное квантовое состояние, Получатель генерирует случайную последовательность битов, чтобы выбрать основу между основаниями Z и X.

После сеанса передачи Отправитель и Получатель объявляют время обнаружения и основную информацию по общедоступному каналу. Кроме того, Отправитель объявляет, к какому импульсу относится состояние приманки или сигнала. Здесь, исследуя коэффициенты обнаружения ложных и сигнальных состояний, блокируется тот факт, что Перехватчик намеренно передает больше многофотонных состояний, чем однофотонных состояний для атаки PNS. Затем обнаруженные результаты отсеиваются, чтобы отбросить измерения фотонов у Получателя, которые использовали базы, отличные от базисов Отправителя. Оставшаяся последовательность битов называется просеянным ключом.

Отправитель и Получатель сравнивают некоторые просеянные ключи, чтобы оценить QBER. Основываясь на предполагаемом QBER, Отправитель и Получатель рассчитывают соответствующую скорость безопасного ключа.

Чтобы сгенерировать окончательный ключ безопасности, Отправитель и Получатель выполняют постобработку, состоящую из исправления ошибок и усиления конфиденциальности, отправляя дополнительную информацию по общедоступному каналу.

Оценка распределения числа фотонов

Распределение числа фотонов можно оценить с помощью детекторов, разрешающих число фотонов (Маттиоли и др., 2016), или детекторов, не разрешающих число фотонов (Мородер и др., 2009; Бенатти и др., 2010). Очевидно, что первый лучше оценивает распределение. В этой работе мы рассматриваем наихудший сценарий, основанный на последнем параметре, чтобы оценить минимальный прирост производительности, который также может быть гарантирован для первого случая. Подчеркнем также, что последний случай более реалистичен из-за высокой стоимости использования детекторов, разрешающих число фотонов.

В качестве родственных работ авторы в (Мородер и др., 2009; Бенатти и др., 2010) оценивают распределение с не разрешающим детектором количества фотонов и переменным аттенюатором в сети точка-точка. В предлагаемом нами методе мы используем совместную работу ONU с не разрешающим определением количества фотонов. Таким образом, состояние фотонов, распределенное по многоточечной PON с помощью оптического сплиттера, вместо использования переменных аттенюаторов, можно совместно использовать для получения дополнительной информации о распределении числа фотонов, как обсуждается с конкретными подробностями ниже.

Когда распределение количества фотонов может быть оценено совместным измерением обнаружения фотонов на нескольких Получателях, мы можем ожидать увеличения скорости безопасного ключа, поскольку это может смягчить атаку PNS, которая приводит к генерации безопасных ключей из многофотонных состояний. Этого можно достичь, используя характеристики PON, которые обеспечивают обнаружение совпадений среди Получателей.

В PON многофотонное состояние может быть случайным образом направлено к Получателям в пределе частицеподобного поведения на оптическом разветвителе из-за того, что фотон неделим по своей природе (Curtacci и др., 2006). Эта характеристика генерирует обнаружение совпадений. Обнаружение совпадений предоставляет информацию о распределении количества фотонов в импульсе, отправленном OLT, Отправителем. Собрав всю информацию об обнаружении, Отправитель может оценить распределение обнаружений, например, количество обнаружений в одном Получателе, количество обнаружений в двух разных Получателях одним и тем же импульсом и так далее. Это предохраняет подслушивающего, то есть Перехватчика, от определенной атаки PNS, потому что делает предполагаемое распределение обнаружений отличным от теоретически рассчитанного распределения обнаружений с заданными системными параметрами. Таким образом, Перехватчик может выполнять PNS-атаку на ограниченную часть многофотонных состояний.

Для простоты понимания здесь рассмотрим, как оценка ограничивает атаку PNS, на примере. Предположим, что прослушивание происходит после сплиттера. В частности, есть два случая, может ли Перехватчик выполнить атаку PNS или нет. Безопасный случай — это многофотонные состояния, в которых Перехватчик не может провести PNS-атаку. Предположим, что имеется число N Получателей

и i-фотонное состояние, в котором i ≤ N. Тогда безопасный случай представляет i Получателей, обнаруживаемых в один и тот же временной интервал. Пример двухфотонного случая, i = 2, показан на рисунке 2(a). В этом случае два Получателя обнаруживают один фотон. Небезопасными случаями, когда Перехватчик может выполнять PNS-атаки, являются все случаи, когда одному Получателю может быть направлено более одного фотона. Пример для этого показан на рисунке 2 (b). В этом случае по крайней мере один Получатель получает несколько фотонов.

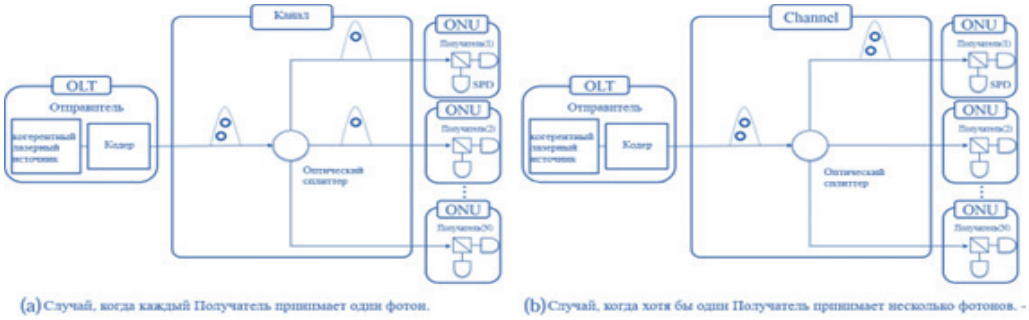

Рисунок 2 - Возможные случаи генерации импульса с несколькими фотонами

Для заданных системных параметров, таких как потери в канале обнаружения, внутренние потери Получателя и эффективность обнаружения УЗИП, мы можем рассчитать частоту обнаружения. После сеанса передачи Отправитель может оценить частоту обнаружения, приняв информацию об обнаружении от Получателя. Сравнивая рассчитанную и оценочную частоты обнаружения, если Перехватчик выполняет атаку PNS для всех многофотонных состояний, как если бы она делала это в обычной системе-ловушке BB84 QKD, она может быть обнаружена, поскольку два значения становятся разными. Предположим, что Перехватчик выполняет PNS-атаку на сейф. Затем уменьшается обнаружение совпадений среди Получателей.

Здесь мы добавляем новое поведение к обычному протоколу:

Мониторинг совпадений: накапливать статистику обнаружений совпадений i-Получатель, чтобы контролировать, отличается ли она от теоретически рассчитанного значения с заданными параметрами системы или нет.

Следовательно, Перехватчику следует провести PNS-атаку, за исключением безопасного случая, чтобы скрыть свое существование. То есть Отправитель и Получатель могут получить дополнительный безопасный ключ из некоторых многофотонных состояний, соответствующих безопасному случаю.

Безопасная ключевая ставка

В этом разделе мы явно указываем безопасные ключи в зависимости от возможных атак. Соответствующие результаты приведены в таблице 1. В таблице можно увидеть как изменяются распределение обнаружений совпадений и чисел фотонов в зависимости от вида атаки перед разделителем или после разделителя. Также учитывается есть ли управление разделителем при той или иной атаке.

Таблица 1 – Безопасные ключевые ставки для различных атак

Атака	Управление разделителем	Распределение обнаружений совпадений	Распределения чисел фотонов
Перед разделителем	НЕТ	Изменен	Изменен
			Без изменений
		Без изменений	Изменен
			Без изменений
	ДА	Изменен	Изменен
			Без изменений
		Без изменений	Изменен
			Без изменений
После разветвителя	НЕТ	Изменен	Изменен
			Без изменений
		Без изменений	Изменен
			Без изменений
	ДА	Изменен	Изменен
			Без изменений
		Без изменений	Изменен
			Без изменений

Результаты моделирования

Производительность системы с предложенным методом с точки зрения безопасной ключевой скорости оценивается численно в этом разделе. Для сравнения производительности используется обычный протокол BB84 с состоянием приманки. Поскольку атаки без изменения факторов мониторинга, таких как распределения, в основном рассматриваются в QKD, мы оцениваем безопасные значения ключей для соответствующих случаев. В частности, мы моделируем безопасные ключи с помощью уравнений. Для сравнения эффективности тарифов каждое моделирование проводится с оптимальным средним числом фотонов каждой системы. Мы проводим два численных моделирования в зависимости от параметров устройств и количества ONU в PON. Первое моделирование проводится с почти идеальными устройствами. Целью первого моделирования является обеспечение идеальной верхней границы с точки зрения безопасной скорости передачи ключей. Затем мы проводим второе моделирование, чтобы определить достижимую скорость безопасного ключа с учетом доступных в настоящее время устройств для сравнения с верхней границей.

Параметры моделирования, используемые в первом случае, следующие. В основном оптические потери в волокне составляют $\alpha = 0{,}2$ дБ/км, как и в обычном оптическом волокне. Каждый Получатель имеет идеальные SPD со 100 % эффективностью обнаружения, $\gamma_{обн} = 1$ и вероятностью темнового счета 0, $Y_0 = 0$. Внутри каждого Получателя нет оптических потерь, $L_{ONU} = 0$ дБ, и нет системной ошибки, $e_{ош} = 0$. При постобработке предполагается, что Получатель может выполнять идеальную коррекцию ошибок, что означает $f(E_\mu) = 1$. Результаты соответствующих оценок показаны на рисунке 3, где сплошными и пунктирными

линиями показаны системы QKD с предложенным и без предложенного метод соответственно. Поскольку расстояние между OLT и ONU составляет около 20 км или меньше в обычной PON, мы наносим результаты до 20 км. В случае системы QKD без предложенного метода для N = 8 и 64 оптимальное среднее число фотонов для достижения максимальной безопасной ключевой скорости составляет 1,001, полученное путем дифференцирования уравнения. Для N = 64 (8) оптимальное среднее число фотонов предлагаемой системы составляет 1,270 (1,220) без USD-атаки (Unambiguous State Discrimination – Однозначное различение Квантовых Состояний) и 1,190 (1,170) при USD-атаке. На расстоянии 20 км для N = 64 (8) скорость защищенного ключа увеличивается примерно на 25,54 % (21,44 %) при отсутствии USD атаки и на 21,35 % (18,82 %) при USD атаке. Причина, по которой мы можем получить дополнительные безопасные ключи, заключается в использовании многофотонных состояний в качестве секретных ключей в предлагаемом методе. По той же причине предлагаемый метод увеличивает используемое среднее число фотонов для генерации дополнительных секретных ключей, поскольку многофотонные состояния могут использоваться для генерации секретных ключей, что невозможно без предложенного нами метода.

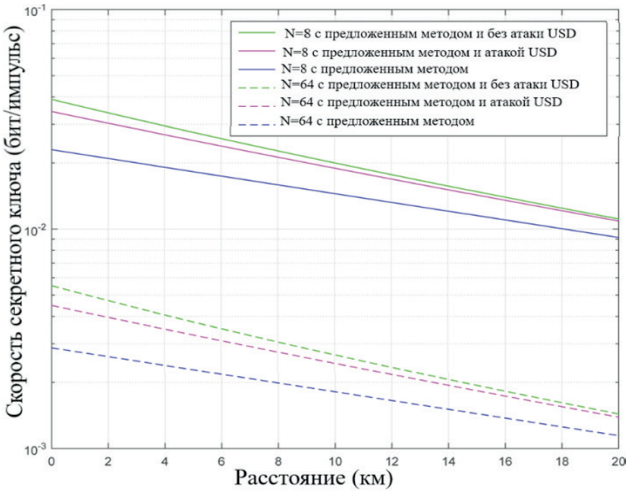

Рисунок 3 - Сравнение безопасной ключевой скорости между системой QKD с предложенным методом и без него при идеальной настройке

В случае второго моделирования учитываются реализуемые параметры. Предполагается, что те же потери в оптическом волокне, что и в предыдущем моделировании. Что касается SPD Получателя, то предполагается использование сверхпроводниковых SPD, для которых можно принять эффективность обнаружения 67 %, $\gamma_{обн}$ = 0,67 и вероятность темнового счета 1,6 × 10–6, Y0 = 1,6 × 10–6 [18]. L_{ONU}, ed и f (E_{μ}) установлены на 3 дБ, 2,3 % и 1,2 соответственно, что является типичными параметрами в экспериментальных результатах [19]. Соответствующий результат моделирования показан на рисунке 4. Для N =

64(8) оптимальное среднее число фотонов традиционной системы составляет 0,593 (0,592), а для предлагаемой системы — 0,630 (0,630) при отсутствии USD-атаки и 0,630 (0,630) при атаке USD соответственно. Здесь для N = 64(8) мы демонстрируем, что наша система обеспечивает выигрыш от 6,09 до 6,24 % (от 5,33 до 5,43 %) по сравнению с обычной системой в зависимости от типа атаки на 20 км. Мы видим незначительное снижение производительности из-за атаки USD.

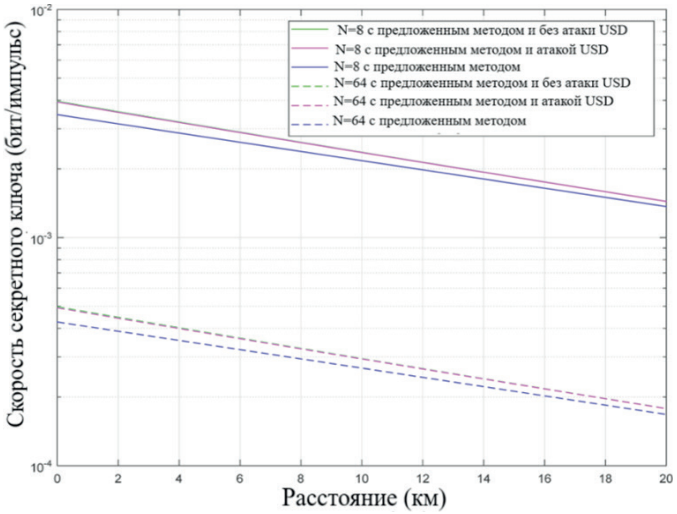

Рисунок 4 - Сравнение безопасной ключевой скорости между системой QKD с предлагаемым методом и без него в реализуемой настройке

Хотя сверхпроводниковые SPD демонстрируют высокую эффективность обнаружения, развертывание таких SPD в PON может быть обременительным из-за их стоимости. Чтобы рассмотреть более реалистичный сценарий, в котором мы используем более дешевые SPD, которые обычно дают более низкую эффективность детектора, мы также проводим больше симуляций, в которых эффективность детектора варьируется в широком диапазоне от 25 % до 100 %. На рисунке 5 показано усиление благодаря нашему протоколу в зависимости от эффективности детектора, когда мы предполагаем, что длина оптоволокна составляет 20 км и атака с помощью USD. Мы видим, что усиление увеличивается с эффективностью детектора, хотя эффективность детектора сильно зависит от стоимости SPD, которые мы можем использовать. Для большего N мы должны использовать более дешевые SPD при том же бюджете, а это приводит к снижению эффективности детектора. С другой стороны, чем больше N, тем выше коэффициент усиления, как показано на рисунке 5. Это означает, что при ограничении стоимости детектора (которое может зависеть от технологии реализации) на N может существовать оптимальное значение, при котором коэффициент усиления равен максимизирован. Таким образом, наш результат проливает свет на то, как на практике проектировать такие защищенные сети доступа.

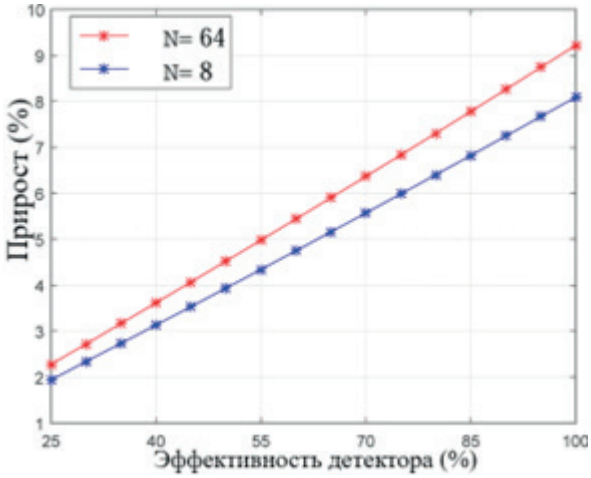

Рисунок 5 - Сравнение прироста защищенной ключевой скорости в зависимости от эффективности детектора

Заключение

В этой статье было исследовано, как повысить безопасную скорость передачи ключей QKD в многопользовательской сети, такой как PON. В частности, для достижения этого мы используем характеристики PON, которые обеспечивают обнаружение совпадений между ONU. Соответственно, было определено, что безопасные ключи можно использовать из многофотонных состояний, в отличие от обычного способа, при котором безопасный ключ генерируется только из однофотонных состояний. Для пригодных для использования многофотонных состояний мы тщательно анализируем количество информации, просочившейся к Перехватчику. Исходя из этого, мы предоставляем математическую модель безопасной ключевой скорости для QKD в PON. Проведены и представлены два различных численных моделирования для случаев идеальной и реализуемой установок. Результаты нашего моделирования показывают, что на расстоянии 20 км улучшение ключевой скорости в идеальной настройке составляет 21,35 %. Даже в реализуемом варианте выигрыш приличный: ~ 6,09 %. Кроме того, результаты показывают, что влияние USD атаки незначительно. Мы считаем, что наша работа может заложить прочную основу для дальнейших исследований QKD в многопользовательских сетях.

ЛИТЕРАТУРЫ

Ж.-П. Бургуин, Н. Гигов, Б.Л. Хиггинс, З. Ян, Э. Мейер-Скотт, А.К. Хандани, Н. Люткенхаус и Т. Дженневейн (2015). «Экспериментальное распределение квантового ключа с смоделированными потерями фотонов от земли к спутнику и ограничениями обработки». физ. Ред. А 92, — 052339 (2015). — С. 111–115.

Бенатти Ф., Фаннес М., Флореанини Р., Петритис Д. (2010). Квантовая информация, вычисления и криптография: вводный обзор теории, технологии и экспериментов. 808 (Спрингер, 2010). — С. 232–240.

С. Ван, В. Чен, З.-К. Инь, Ю. Чжан, Т. Чжан, Х.-В. Ли, Ф.-Х. Сюй, З. Чжоу, Ю. Ян, Д.-Дж. Хуанг,

Л.-Дж. Чжан, Ф.-Ю. Ли, Д. Лю, Ю.-Г. Ван, Г.-К. Го и З.-Ф. Хан (2010). «Полевые испытания сети распределения квантовых ключей с сохранением длины волны», Opt. лат. 35, 2454–2456 (2010). — С. 7–10.

Кок П., Манро В.Дж., Немото К., Ральф Т.С., Доулинг Дж.П., Милберн Г.Дж. (2007). «Линейные оптические квантовые вычисления с фотонными кубитами», Rev. Mod. физ. 79. —135 (2007). — С. 67–71.

Ф. Маттиоли, З. Чжоу, А. Гаггеро, Р. Гаудио, Р. Леони и А. Фиоре (2016). «Подсчет фотонов и аналоговая работа 24-пиксельного детектора разрешения числа фотонов на основе сверхпроводящих нанопроводов», Опт. Экспресс 24, 9067–9076 (2016). — С. 9–11.

Т. Мородер, М. Керти и Н. Люткенхаус (2009). "Распределение квантового ключа детектора-приманки", New J. Phys. 11. — 045008 (2009). — С. 89–92.

С. Ма, Б. Ци, Ю. Чжао, Х.-К. Ло (2005). «Практическое состояние приманки для квантового распределения ключей», Phys. Ред. A 72, 012326 (2005 г.). — С. 99–101.

М. Пеев, К. Паше, Р. Аллеом, К. Баррейро, Ж. Боуда, В. Бокслейтнер, Т. Дебюссхерт, Э. Диаманти, М. Дианати, Дж. Дайнс, С. Фазель, С. Фоссье, М. Фюрст, Ж.-Д. Готье, О. Гей, Н. Гизин, П. Гранжье, А. Хаппе, Ю. Хасани, М. Хентшель (2009). «The SECOQC сеть распространения квантовых ключей в Вене», New J. Phys. 11, 075001 (2009). —С. 76–80.

Р. Реннер (2008). "Безопасность распределения квантовых ключей", Int. J. Квантовая инф. 6. — 1–127 (2008). — С. 18–19.

Curtacci P., Garzia F., Cusani R. и Baccarelli E. (2006). «Анализ производительности различных многопользовательских оптических пассивных сетей для приложений квантовой криптографии», Proc. SPIE 6187, 61870U (2006 г.). — С. 45–47.

Фернандес В., Коллинз Р.Дж., Гордон К.Дж., Таунсенд П.Д., Буллер Г.С. (2007). Пассивный оптический сетевой подход к многопользовательскому распределению квантовых ключей с гигагерцовой тактовой частотой // IEEE J. Quantum Electron. 43, (2007). —С. 138–140.

Фрёлих Б., Дайнс Дж.Ф., Лукамарини М., Шарп А.В., Юань З., Шилдс А.Дж. (2013). «Квантовая сеть доступа». — Nature 501, 69–72 (2013). — С. 43–44.

X. Zhang, F. Lu, S. Chen, X. Zhao, M. Zhu, X. Sun (2016). «Схема удаленного кодирования, основанная на волноводной брэгговской решетке в микросхеме сплиттера PLC для мониторинга PON», Opt. Экспресс 24, 4351–4364 (2016). — С. 76–78.

Д. Хрг, А. Поппе, А. Федрицци, Б. Блауэнштейнер, Х. Хюбель и А. Цайлингер (2005). «Аспекты безопасности и моделирование практических платформ QKD», Квантовая физика природы Теория, эксперимент и интерпретация в сотрудничестве с 6-й европейский семинар QIPC, Австрия (2005 г.). — С. 121-123.

В.-Ю. Хван, «Распределение квантовых ключей с большими потерями: на пути к глобальной безопасной связи», Phys. Преподобный Летт. 91, 057901 (2003). — С. 32–35.

Ю. Чжао, «Квантовые защищенные коммуникационные сети: продукты и решения», — С. 13–20.

А. Чиурана, Х. Мартинес-Матео, М. Пеев, А. Поппе, Н. Валента, Х. Збинден, В. Мартин (20).1 «Квантовая городская оптическая сеть на основе мультиплексирования с разделением по длине волны», Опт. Экспресс 22, — 1576–1593 (2014). — С. 182–185.

П.В. Шор и Дж. Прескилл (2000). "Простое доказательство безопасности протокола распределения квантовых ключей BB84", Phys. Преподобный Летт. 85, 441 (2000). — С. 102–105.

Х. Шим, К. Чо, Ю. Такушима и Ю. Чанг (2012). «Рефлектометрия на основе корреляции для мониторинга в процессе эксплуатации 64-сплит TDM PON», Опт. Экспресс 20, 4921–4926 (2012). — С. 22–24.

REFERENCES

J.-P. Burguin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lutkenhaus and T. Jennevein (2015). "Experimental distribution of a quantum key with simulated photon losses from the earth to a satellite and processing restrictions". Phys. Ed. A 92, 052339 (2015). — Pp. 111–115.

Benatti F., Fannes M., Floreanini R., Petritis D. (2010). Quantum Information, Computing and Cryptography: an introductory review of theory, technology and experiments. 808 (Springer, 2010). — Pp. 232–240.

A. Chiurana, H. Martinez-Mateo, M. Peev, A. Poppe, N. Valenta, H. Zbinden, V. Martin (2014). "Quantum urban optical network based on wavelength division multiplexing", Opt. Express 22, 1576–1593 (2014). — Pp. 182–185.

Curtacci P., Garzia F., Cusani R. and Baccarelli E. (2006). "Performance analysis of various multi-user optical passive networks for quantum cryptography applications", Proc. SPIE 6187, 61870U (2006). — Pp. 45–47.

Frelich B., Dines J.F., Lucamarini M., Sharp A.V., Yuan Z., Shields A.J. (2013). "Quantum access network". — Nature 501, 69–72 (2013). — Pp. 43–44.

Fernandez V., Collins R.J., Gordon K.J., Townsend P.D., Buller G.S. (2007). Passive optical network approach to multi-user distribution of quantum keys with gigahertz clock frequency // IEEE J. Quantum Electron. 43, (2007). — Pp. 138–140.

D. Hrg, A. Poppe, A. Fedrizzi, B. Blauensteiner, H. Huebel and A. Zeilinger (2005). "Security aspects and modeling of practical QKD platforms", Quantum Physics of Nature Theory, Experiment and interpretation in collaboration with the 6th European Seminar QIPC, Austria (2005). — Pp. 121–123.

V.-Yu. Hwang (2003). "Distribution of quantum keys with large losses: on the way to global secure communication", Phys. Rev. Lett. 91. — 057901 (2003). — Pp. 32–35.

Kok P., Munro V.J., Nemoto K., Ralph T.S., Dowling J.P., Milburn G.J. (2007). "Linear optical quantum computing with photonic qubits", Rev. Mod. phys. 79. — 135 (2007). — Pp. 67–71.

S. Ma, B. Qi, Yu Zhao, H.-K. Lo (2005). "The practical state of bait for quantum key distribution", Phys. Ed. A 72. — 012326 (2005). — Pp. 99–101.

F. Mattioli, Z. Zhou, A. Gaggero, R. Gaudio, R. Leoni and A. Fiore (2016). "Photon counting and analog operation of a 24-pixel photon number resolution detector based on superconducting nanowires", Opt. Express 24, 9067-9076 (2016). — Pp. 9–11.

T. Moroder, M. Curti and N. Lutkenhaus (2009). "Distribution of the quantum key of the decoy detector", New J. Phys. 11, 045008 (2009). — Pp. 89–92.

M. Peev, K. Pasche, R. Alleom, K. Barreiro, J. Bouda, V. Boxleitner, T. Debusshert, E. Diamanti, M. Dianati, J. Dines, S. Fasel, S. Fossier, M. Furst, J.-D. Gauthier, O. Gay, N. Gizin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel (2009). "The SECOQC quantum Key distribution network in Vienna", New J. Phys. 11, 075001 (2009). — Pp. 76–80.

R. Renner, "Security of quantum key distribution", Int. J. Quantum Inf. 6. — 1–127 (2008). — Pp. 18–19.

H. Shim, K. Cho, Yu. Takushima and Yu. Chang (2012). "Correlation-based reflectometry for in-service monitoring of 64-split TDM PON", Opt. Express 20, 4921–4926 (2012). — Pp. 22–24.

P.V. Shor and J. Preskill (2000). "A simple proof of the security of the BB84 quantum Key Distribution Protocol", Phys. Venerable Lett. 85, 441 (2000). — Pp. 102–105.

S. Wang, V. Chen, Z.-K. Yin, Yu. Zhang, T. Zhang, H.-V. Li, F.-H. Xu, Z. Zhou, Yu Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Yu-G. Van, G.-K. Go and Z.-F. Khan (2010). "Field tests of a wavelength-conserved quantum key distribution network", Opt. lat. 35, 2454–2456 (2010). — Pp. 7–10.

Yu Zhao, "Quantum secure communication networks: products and solutions". — Pp. 13–20.

X. Zhang, F. Lu, S. Chen, X. Zhao, M. Zhu, X. Sun (2016). "Remote coding scheme based on a Bragg waveguide array in a PLC splitter chip for PON monitoring", Opt. Express 24, 4351–4364 (2016). — Pp. 76–78.

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

Подписано в печать 15.12.2022.
Формат 60x881/8. Бумага офсетная. Печать - ризограф.7,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59