Демонстрация сети квантового распределения ключа в городских оптоволоконных линиях связи

Е.О.Киктенко, Н.О.Пожар, А.В.Дуплинский, А.А.Канапин, А.С.Соколов, С.С.Воробей, А.В.Миллер, В.Е.Устимчик, М.Н.Ануфриев, А.С.Трушечкин, Р.Р.Юнусов, В.Л.Курочкин, Ю.В.Курочкин, А.К.Федоров

Представлены результаты реализации сети квантового распределения ключей (КРК) с использованием стандартных волоконных каналов связи в Москве. Разработанная сеть КРК основана на парадигме доверенных повторителей и позволяет генерировать общий ключ между пользователями через промежуточный доверенный узел. Основной особенностью сети является объединение установок, использующих два типа кодирования – поляризационное и фазовое. Одним из возможных применений разработанной сети КРК является непрерывное обновление ключей в существующих симметричных устройствах шифрования с периодом обновления до 14 с.

Ключевые слова: *квантовое распределение ключей связи, волоконные каналы связи, поляризационное и фазовое кодирования.*

1. Введение

За последние десятилетия был достигнут значительный прогресс в теории, экспериментальных исследованиях и технологии квантового распределения ключей (КРК) [1–3]. Тем не менее существует ряд проблем, таких как небольшое расстояние, низкая скорость генерации ключей, практическая безопасность систем КРК и т. д. [1–3]. Для реализации КРК между несколькими (более чем двумя) пользователями необходимо создавать сети КРК [4]. Существует целый ряд крупных проектов по созданию таких сетей, в частности в США, Европе, Китае и Японии [5–13]. Сети КРК имеют ряд перспективных приложений, например создание защищенных распределенных баз данных [14]. Прежде всего они гарантируют теоретико-информационную безопасность связи между узлами, а также могут использоваться для непрерывного обновления ключей в доступных в настоящее время симметричных устройствах шифрования.

Е.О.Киктенко. Российский квантовый центр, Россия, 143025 Москва, Сколково, ул. Новая, 100; Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул. Губкина, 8; Московский государственный технический университет им. Н.Э.Баумана, Россия, 105005 Москва, 2-я Бауманская ул., 5

Н.О.Пожар, М.Н.Ануфриев. Российский квантовый центр, Россия, 143025 Москва, Сколково, ул. Новая, 100; Московский государственный технический университет им. Н.Э.Баумана, Россия, 105005 Москва, 2-я Бауманская ул., 5

А.В.Дуплинский. Российский квантовый центр, Россия, 143025 Москва, Сколково, ул. Новая, 100; Московский физико-технический институт (государственный университет), Россия, Московская обл., 141700 Долгопрудный, Институтский пер., 9

А.А.Канапин. Российский квантовый центр, Россия, 143025 Москва, Сколково, ул. Новая, 100; Московский государственный университет им. М.В.Ломоносова, Россия, 119991 Москва, Воробьевы горы

А.С.Соколов, С.С.Воробей, А.В.Миллер, В.Е.Устимчик, Р.Р.Юнусов, В.Л.Курочкин, Ю.В.Курочкин, А.К.Федоров. Российский квантовый центр, Россия, 143025 Москва, Сколково, ул. Новая, 100;
e-mail: veu@rqc.ru; y.kurochkin@gmail.com

А.С.Трушечкин. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул. Губкина, 8

Поступила в редакцию 7 июля 2017 г., после доработки – 10 августа 2017 г.

Одной из наиболее важных проблем в развитии сетей КРК является генерация секретных ключей за пределами лаборатории. Как следствие, важно использовать протокол КРК, который гарантирует секретность в городских оптоволоконных каналах связи, имеющих значительные потери. Данное обстоятельство является одним из наиболее важных отличительных факторов экспериментов по квантовому распределению ключа в городских условиях. Важно отметить, что процедуры постобработки просеянных ключей также являются неотъемлемой частью работы сетей КРК [15, 16].

Цель настоящей работы – экспериментальная демонстрация сетей КРК для систем с различными типами кодирования квантовых состояний в городских условиях. Квантовое распределение ключей реализовано с применением «темного» оптоволокна со значительными потерями, которое проложено совместно с использующимися линиями связи. Одним из возможных применений разработанной сети КРК является непрерывное обновление ключей в доступных в настоящее время симметричных устройствах шифрования. Российские стандарты шифрования предполагают использование ключей длиной 256 бит, поэтому с учетом использования сетей КРК они могут обновляться примерно каждые 14 с.

2. Сеть КРК

В настоящей работе был использован подход SECOQC [6], который определяет сеть КРК как инфраструктуру, основанную на соединениях КРК типа точка–точка. Тогда любые два узла сети могут сгенерировать общий ключ на информационно-теоретическом уровне стойкости. Сетевой протокол (в рассматриваемом случае – три узла и два канала КРК) работает следующим образом (рис.1). Узлы 1 и 2, а также узлы 2 и 3 генерируют свои секретные ключи k_{12} и k_{23}. Эти ключи хранятся в памяти соответствующих узлов. Используя квантовый генератор случайных чисел, узел 1 генерирует ключ K и затем пересылает его в зашифрованном при помощи одноразового блокнота виде $K \oplus k_{12}$ на промежуточный доверенный узел (узел 2). Используя сгенерированный ранее ключ

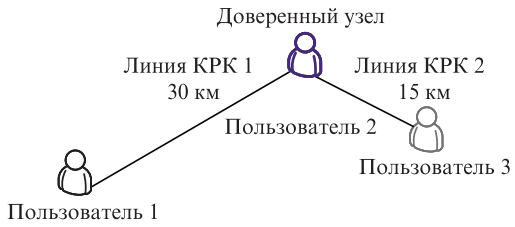

Рис.1. Схема сети КРК, в которой квантовые ключи распределяются между тремя пользователями через промежуточный доверенный узел.

k_{23}, узел 2 передает $K \oplus k_{23}$ в узел 3. В результате произвольные узлы (и все узлы вместе) в сети КРК могут получить общий секретный ключ. Для гарантии отправления полученных ключей конкретным узлом может применяться информационно-теоретически безопасная аутентификация [6].

Созданная сеть КРК позволяет получать общий квантовый ключ для пользователей с различными оптическими схемами КРК, реализующими поляризационное и фазовое кодирования. Основой для данного эксперимента является недавно представленное модульное устройство КРК [15]. Его функционирование осуществляется при помощи плат National Instruments (NI) программного обеспечения с открытым исходным кодом на LabView для управления и работы, алгоритмами с открытым исходным кодом на Python для постобработки и протокола с открытым исходным кодом для внешних приложений [16–18]. Устройство КРК может работать с любыми однофотонными детекторами. Внешние драйверы однофотонных детекторов, фазовых модуляторов и детекторов синхронизации реализованы как съемные модули. Каждое устройство может использовать до четырех детекторов и шести универсальных портов для подключения лазеров, фазовых или амплитудных модуляторов. Программное решение, отвечающее за управление системой, пишется с использованием среды LabVIEW.

Управление электрооптическими модуляторами осуществляется при помощи платы PCIe-7811R (NI), установленной в персональных компьютерах [15]. Полупроводниковый лазер LDI-DFB2.5G, управляемый FPGA-платой Spartan-6, генерирует оптические импульсы с частотой следования 10 МГц на стандартной телекоммуникационной длине волны излучения 1.55 мкм. Были использованы однофотонные детекторы ID230 [19]. Светоделители, зеркало Фарадея, циркуляторы, переменный оптический аттенюатор, модуляторы фазы и интенсивности, применяемые в схемах, являются стандартными оптическими компонентами.

Первое звено созданной сети КРК генерирует квантовые ключи с использованием схемы поляризационного кодирования на основе протокола BB84 [20]. В этой установке используется эффект Поккельса в низковольтных

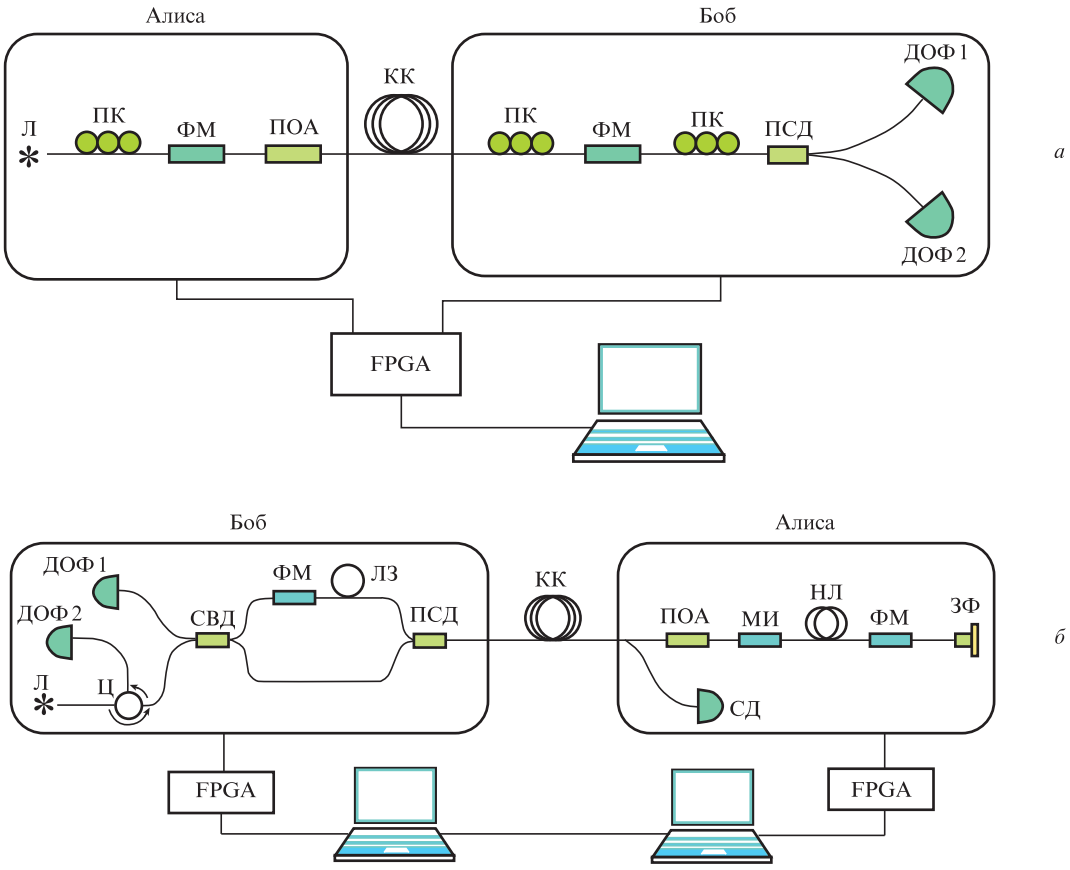

Рис.2. Схемы первого звена КРК для генерации квантовых ключей с использованием схемы поляризационного кодирования (Л – источник излучения; ПК – поляризационный контроллер; ФМ – фазовый модулятор; ПОА – переменный оптический аттенюатор; КК – квантовый канал (городская оптоволоконная линия); ПСД – поляризационный светоделитель; ДОФ – детектор одиночных фотонов) (*а*) и второго звена КРК, использующего схему фазового кодирования (Ц – циркулятор; СВД – светоделитель; ЛЗ – линия задержки; НЛ – накопительная линия; СД – синхронизирующий детектор; МИ – модулятор интенсивности; ЗФ – зеркало Фарадея) (*б*).

электрооптических фазовых модуляторах на основе кристалла $LiNbO_3$ (рис.2,*а*). Отметим, что этот метод позволяет использовать один лазерный источник, тогда как большинство реализаций поляризационного кодирования сталкиваются с проблемой различимости импульсов, испущенных разными источниками [21]. Кроме того, требуются только два однофотонных детектора, в отличие от стандартных схем поляризационного кодирования с четырьмя детекторами. Это звено обеспечивает обмен ключами на расстоянии до 30 км (в городском оптоволокне с потерями на уровне 13 дБ, среднее число фотонов в импульсе $\mu_{\rm pol} = 0.02$) при скорости генерации просеянного ключа около 0.1 Кбит/с.

Второе звено использует схему фазового кодирования для КРК (рис.2,*б*), реализующую протокол BB84, которая уже испытывалась для КРК в условиях городских оптоволоконных линий [22]. Это звено позволяет генерировать секретные ключи на расстоянии до 15 км (в городских оптоволоконных линиях с потерями на уровне 7 дБ, среднее количество фотонов в импульсе $\mu_{\rm ph} = 0.03$), при этом скорость генерации ключа составляет около 0.2 Кбит/с.

На рис.3 представлена зависимость среднего значения квантового уровня ошибок (quantum bit error rate (QBER)) от времени (данные за 6 ч). Изменение значения QBER вызвано внешними факторами (механическими и температурными воздействиями). Видно, что реальная доля ошибок в просеянном ключе составляет несколько процентов, что слишком велико для прямых приложений, например для использования в качестве ключей при шифровании одноразовым блокнотом или для обновления ключа в симметричных шифрах. Чтобы устранить

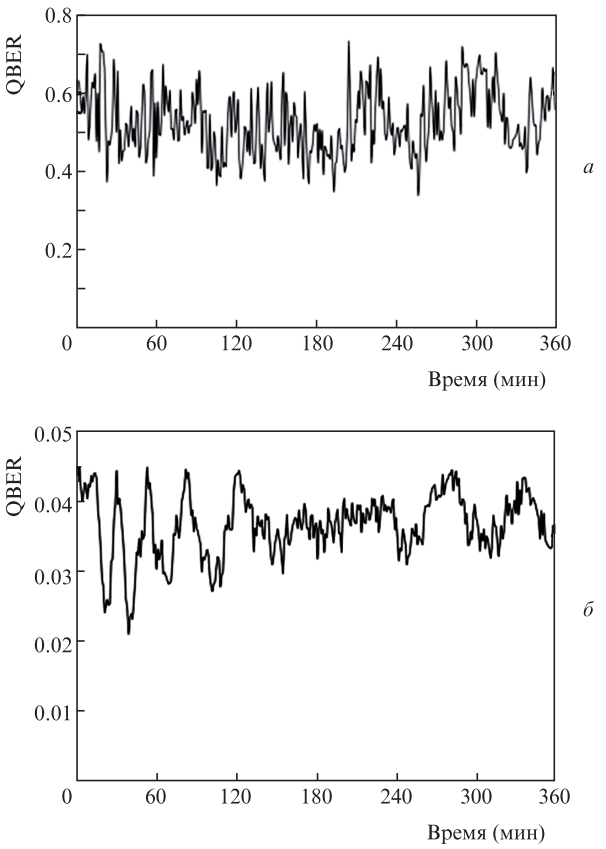

Рис.3. Среднее значение QBER в зависимости от времени (6 ч) для установки кодирования поляризации (*а*) и для установки фазового кодирования (*б*).

эту долю ошибок, а также уменьшить потенциальную информацию перехватчика до незначительных величин, мы используем процедуру постобработки, описанную ниже.

3. Скорость генерации секретного ключа

Просеянные ключи из обеих линий КРК являются входными данными для процедуры постобработки, которая состоит из согласования информации, оценки параметров, усиления секретности и проверки подлинности [16]. Процедура состоит из ряда этапов.

1. Просеянные ключи от звеньев КРК проходят этап согласования информации на основе метода, описанного в работе [17] и использующего низкоплотностные коды проверки на четность [23–25]. Отметим, что этот метод позволяет выполнять сверку информации с очень грубой или даже отсутствующей оценкой QBER. Кроме того, слепой протокол согласования информации позволяет значительно повысить эффективность процедуры исправления ошибок и уменьшить ее интерактивность [17].

2. После выполнения этапа согласования информации все еще существует определенная вероятность того, что не все ошибки исправлены. Чтобы обнаружить возможные оставшиеся ошибки, мы реализуем последующий протокол верификации с использованием универсальных хэш-функций [26]. Вероятность наличия ошибок после успешной проверки блока ключа длиной $\sim$1 Мбит ограничена величиной $\varepsilon_{\rm ver} = 2 \times 10^{-11}$ с использованием хэш-тега длиной 50 бит. Подробное описание протокола верификации представлено в работе [26]. Получившаяся на этом этапе общая двоичная последовательность называется проверенным ключом.

3. На стадии оценки параметров стороны получают фактический уровень QBER для своих блоков ключа путем непосредственного сравнения ключей до и после согласования информации. Фактически этот шаг выполняется «на стороне Боба», где модификация просеянного ключа была осуществлена на предыдущем этапе. Если значение QBER оказалось выше критического значения, необходимого для эффективного усиления конфиденциальности, пользователи останавливают протокол. В противном случае проверенные ключевые блоки переходят на стадию усиления секретности, а оценка значения QBER используется в следующих циклах согласования информации [16].

4. Стадия усиления секретности используется для уменьшения потенциальной информации противника о проверенных блоках до незначительного количества [16]. Это достигается путем укорочения входного ключа. Длина секретного ключа задается следующим выражением:

$$L_{\rm sec} = L_{\rm ver}\,\hat{Y}_1[1 - h(\hat{q}_1)] - {\rm leak}_{\rm ec} - 5\log_2(1/\varepsilon_{\rm pa}), \qquad (1)$$

где $L_{\rm ver}$ – длина верифицированного ключа; $\hat{Y}_1$ – оценка доли бит просеянного ключа, полученых из однофотонных импульсов; $\hat{q}_1$ – оценка QBER для однофотонных импульсов;

$$h(q) = -q\log_2 q - (1-q)\log_2(1-q)$$

– бинарная энтропийная функция; lea$k_{\rm ec}$ – общее количество бит, раскрытых при согласовании информации и на этапе верификации; $\varepsilon_{\rm pa}$ – вероятность неудачи на стадии усиления секретности, возникающая вследствие конечно-

сти длины поступающего верифицированного ключа. В нашей процедуре мы приняли $\varepsilon_{\text{pa}} = 10^{-12}$.

Оценка для $\hat{Y}_1$ выглядит следующим образом:

$$\hat{Y}_1 = \frac{\eta\mu - p_2}{\eta\mu}, \tag{2}$$

где η – коэффициент пропускания квантового канала; μ – интенсивность лазерных импульсов; $p_2 = \mathrm{e}^{-\mu}\mu^2/2$ – вероятность двухфотонного излучения при генерации когерентных импульсов [27]. Данная оценка получена в предположении, что «Ева» может выполнять атаку с разделением числа фотонов, а также другие операции с пересылаемыми квантовыми состояниями, однако не имеет возможности влиять на установки «Алисы» и «Боба» (например, модифицировать интенсивность посылаемых сигналов «Алисы» или эффективность детектора «Боба»). В уравнении (2) мы также пренебрегли вероятностью излучения сигнала с числом фотонов $n > 2$. Это предположение разумно, т. к. в наших установках КРК используются импульсы очень низкой интенсивности ($\mu_{\text{pol}} = 0.02$ и 0.03). Оценка QBER в однофотонных импульсах в предположении, что все ошибки появляются только в них, задается выражением

$$\hat{q}_1 = \frac{q}{\hat{Y}_1}, \tag{3}$$

где q – значение QBER, полученное на этапе оценки параметров.

После вычисления длины конечного ключа (для каждого верифицированного блока) в соответствии с методом, представленным в [16], может быть выполнено усиление секретности: блок секретного ключа вычисляется как результат применения универсальной хэш-функции второго порядка по отношению к проверенному ключу. В нашей процедуре постобработки используется хэширование Теплица [28, 29]. Получившийся ключ называют секретным ключом.

5. Наконец, стороны проверяют подлинность своего классического канала путем обмена хэш-значениями всего входящего трафика. В нашей системе мы используем хэширование Теплица в комбинации с одноразовым блокнотом. Длина хэш-значения l_{auth} была установлена равной 40 бит, что ограничивает вероятность успешной атаки посредника на уровне

$$\epsilon_{\text{auth}} = 2 \times 2^{-l_{\text{auth}}} < 2 \times 10^{-12}. \tag{4}$$

Если аутентификация пройдена, стороны резервируют $2l_{\text{auth}}$ бит своих секретных ключей для следующего этапа постобработки. Тогда мы получаем следующее выражение:

$$L_{\text{fin}} = L_{\text{sec}} - 2\,l_{\text{auth}}, \tag{5}$$

где L_{fin} – количество бит финального ключа, который может использоваться в криптографических целях. Это конечный продукт КРК.

Уровень секретности итогового ключа

$$\epsilon_{\text{QKD}} = \epsilon_{\text{ver}} + \epsilon_{\text{pa}} + \epsilon_{\text{auth}} < 2.3 \times 10^{-11}. \tag{6}$$

Отметим, что уровень секретности ключа, распределенного по сети КРК с N узлами, определяется следующим выражением:

$$\epsilon_{\text{QKD Net}} = (N-1)(\epsilon_{\text{QKD}} + \epsilon_{\text{auth}}). \tag{7}$$

Здесь дополнительное слагаемое ϵ_{auth} обусловлено необходимостью дополнительной проверки подлинности. Для нашей сети КРК с $N = 3$ имеем $\epsilon_{\text{QKD Net}} < 5 \times 10^{-11}$.

Скорость генерации финального секретного ключа длиной L_{fin} может быть определена следующим образом:

$$R_{\text{fin}} = L_{\text{fin}}/\tau, \tag{8}$$

где τ – время, необходимое для генерации. Применяя нашу процедуру постобработки к экспериментально сгенерированным ключам, мы получаем, что первая линия КРК обеспечивает обмен ключами на протяжении более 30 км при скорости генерации финального ключа около 0.02 Кбит/с. Вторая линия КРК позволяет генерировать секретные ключи на расстоянии, превышающем 15 км, причем скорость генерации финального ключа составляет примерно 0.1 Кбит/с. Отметим, что скорость генерации ключа в парадигме доверенного повторителя ограничена минимальной скоростью генерации во всех используемых линиях. Таким образом, для нашей сети КРК скорость генерации ключа между Пользователем 1 и Пользователем 3 составляет около 0.02 Кбит/с.

Основным применением квантово-распределенных ключей является непрерывное обновление ключей в доступных в настоящее время симметричных устройствах шифрования. Российские стандарты шифрования предполагают использование ключей длиной 256 бит, поэтому с учетом использования сетей КРК они могут обновляться примерно каждые 14 с. Данный период обновления ограничен скоростью генерации ключей.

4. Заключение

В работе приведено подробное описание реализованной сети КРК, основанной на парадигме доверенного повторителя. Разработанная сеть КРК была протестирована с использованием стандартных оптоволоконных линий связи в Москве. Важно отметить, что сеть соединяет пользователей с двумя разными оптическими схемами – фазового и поляризационного кодирования.

При создании сети применялось «темное» оптоволокно, проложенное совместно с использующимися линиями связи, которые создают паразитные засветки на телекоммуникационной длине волны. В качестве одного из звеньев сети выступает устройство, основанное на однопроходной схеме распределения ключа. Такая схема, в отличие от автокомпенсационной, позволяет посылать непрерывные последовательности импульсов, однако нуждается в стабилизации относительно флуктуации состояния поляризация в квантовом канале, вызванной внешними факторами (механические и температурные воздействия). В отличие от лабораторных условий, испытания на реальной городской линии связи требуют регулярной подстройки параметров и калибровки. Проведенные испытания подтвердили способность системы компенсировать внешние воздействия в условиях реальных городских линий связи [21], что позволяет в будущем внедрять устройства в существующую инфраструктуру.

Основным применением таких квантовых ключей является непрерывное обновление ключей в доступных в настоящее время симметричных устройствах шифрования.

Работа выполнена при поддержке Российского научного фонда (грант № 17-71-20146).

1. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys*., **74**, 145 (2002).
2. Lo H.-K., Curty M., Tamaki K. *Nat. Photonics*, **8**, 595 (2014).
3. Diamanti E., Lo H.-K., Yuan Z. *npj Quantum Information*, **2**, 16025 (2016), doi: 10.1038/npjqi.2016.25.
4. Salvail L., Peev M., Diamanti E., Alleaume R., Lütkenhaus N., Laenger T. *J. Comput. Sec*., **18**, 61 (2010).
5. Elliott C., Colvin A., Pearson D., Pikalo O., Schlafer J., Yeh H. *Proc. SPIE*, **5815**, 138 (2005).
6. Peev M. et al. *New J. Phys*., **11**, 075001 (2009).
7. Stucki D., Legre M., Buntschu F., Clausen B., Felber N., Gisin N., Henzen L., Junod P., Litzistorf G., Monbaron P., Monat L., Page J.-B., Perroud D., Ribordy G., Rochas A., Robyr S., Tavares J., Thew R., Trinkler P., Ventura S., Voirol R., Walenta N., Zbinden H. *New J. Phys*., **13**, 123001 (2011).
8. Chen T.-Y., Liang H., Liu Y., Cai W.-Q., Ju L., Liu W.-Y., Wang J., Yin H., Chen K., Chen Z.-B.,et al. *Opt. Express*, **17**, 6540 (2009).
9. Chen T.-Y., Wang J., Liang H., Liu W.-Y., Liu Y., Jiang X., Wang Y., Wan X., Cai W.-Q., Ju L., Chen L.-K., Wang L.-J., Gao Y., Chen K., Peng C.-Z., Chen Z.-B., Pan J.-W. *Opt. Express*, **18**, 27217 (2010).
10. Wang S., Chen W., Yin Z.-Q., Zhang Y., Zhang T., Li H.W., Xu F.-X., Zhou Z., Yang Y., Huang D.-J., Zhang L.-J., Li F.-Y., Liu D., Wang Y.-G., Guo G.-C., Han Z.-F. *Opt. Lett*., **35**, 2454 (2010).
11. Sasaki M. et. al. *Opt. Express*, **19**, 10387 (2011).
12. Frohlich D., Dynes J.F., Lucamarini M., Sharpe A.W., Yuan Z., Shields A.J. *Nature*, **501**, 69 (2013).
13. Zhang Q. http://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete.
14. Kiktenko E.O., Pozhar N.O., Anufriev M.N., Trushechkin A.S., Yunusov R.R., Kurochkin Y.V., Lvovsky A.I., Fedorov A.K. ArXiv:1705.09258.
15. Sokolov A.S., Miller A.V., Kanapin A.A., Rodimin V.E., Losev A.V., Trushechkin A.S., Kiktenko E.O., Pozhar N.O., Fedorov A.K., Kurochkin V.L., Kurochkin Y.V. ArXiv:1612.04168.
16. Kiktenko E.O., Trushechkin A.S., Kurochkin Y.V., Fedorov A.K. *J. Phys. Conf. Ser*., **741**, 012081 (2016).
17. Kiktenko E.O., Trushechkin A.S., Lim C.C.W., Kurochkin Y.V., Fedorov A.K. ArXiv:1612.03673.
18. Kiktenko E.O., Trushechkin A.S., Anufriev M.N., Pozhar N.O., Fedorov A.K. https://dx.doi.org/10.5281/zenodo.200365 (2016).
19. ID Quantique, www.idquantique.com.
20. Bennet C.H., Brassard G. *Proc. IEEE Intern. Conf. Computers, Systems and Signal Processing* (Bangalore, India) (New York: IEEE, 1984, p. 175).
21. Duplinskiy A., Ustimchik V., Kanapin A., Kurochkin Y. *Proc. SPIE*, **10224**, 102242W (2016).
22. Kurochkin V.L., Kurochkin Y.V., Miller A.V., Sokolov A.S., Kanapin A.A. *Proc. SPIE*, **10224**, 102242U (2016).
23. Gallager R. *IRE Trans. Inf. Theory*, **8**, 21 (1962).
24. MacKay D.J.C. *IEEE Trans. Inf. Theory*, **45**, 399 (1999).
25. Krovetz T., Rogaway P. *Lect. Notes Comp. Sci*., **2015**, 73 (2001).
26. Kiktenko E.O., Trushechkin A.S., Fedorov A.K. ArXiv:1705.06664 [quant-ph].
27. Lutkenhaus N. *Phys. Rev. A*, **61**, 052304 (2000).
28. Krawczyk H. *Lect. Notes Comp. Sci*., **839**, 129 (1994).
29. Krawczyk H. *Lect. Notes Comp. Sci*., **921**, 301 (1995).