Письма в ЖЭТФ, том 100, вып. 6, с. 457 – 464 © 2014 г. 25 сентября

О стойкости волоконной квантовой криптографии при произвольных потерях в канале связи: запрет измерений с определенным исходом

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии РФ, 121552 Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия

Поступила в редакцию 8 августа 2014 г.

Нестрогая однофотонность источника квантовых состояний вместе с потерями в линии связи открывают возможность для атаки с измерениями с определенным исходом (UM-измерениями), что приводит к потере секретности. Проблема стойкости протоколов квантового распределения ключей в канале с большими потерями до сих пор остается открытой. Предлагается радикальное решение данной проблемы путем исключения возможности для подслушивателя вообще проводить UM-измерения. Проблема решается за счет подсчета классических реперных импульсов. Сохранение числа классических синхроимпульсов приводит к невозможности проводить UM-измерения. При этом потери в канале связи считаются заранее неизвестными и могут изменяться на протяжении серии посылок.

DOI: 10.7868/S0370274X1418012X

Введение. В современных системах волоконной квантовой криптографии (системах квантового распределения ключей) секретность ключей гарантируется *даже при идеальных детекторах без собственных темновых шумов* лишь при определенных длинах линии связи, не превышающих некоторую критическую длину [1]. Это связано *с совместным действием двух факторов*. Во-первых, в качестве источника информационных квантовых состояний используется сильно ослабленное излучение лазера – когерентное состояние $|\alpha\rangle$ ($\mu = |\alpha|^2 \approx 0.1{-}0.5$ – среднее число фотонов), которое является не строго однофотонным состоянием, а квазиоднофотонным с пуассоновским распределением по числу фотонов. Во-вторых, имеются потери в линии связи.

Информационные квантовые состояния, в которые кодируется информация о будущем ключе, представляют собой набор неортогональных линейно-независимых когерентных состояний $\{|\varphi_i\rangle = |\alpha_i\rangle\}_{i=1}^{N}$[2)]. Неортогональность необходима для невозможности достоверной различимости состояний. Линейная независимость состояний является необходимым и достаточным условием существования измерений с определенным исходом (*Unambiguous Measurements*, UM) [2].

Любое измерение в квантовой механике дается некоторым разложением единицы, которое является формальным описанием измерения при помощи физического устройства. Разложение единицы id для UM измерений имеет вид

$$\mathrm{id} = \sum_{j=1}^{N+1} \mathcal{M}_j, \tag{1}$$

где $\mathcal{M}_j$ – операторно-значные меры (*Positive Operator Valued Measure*, POVM). Для UM-измерений имеет место свойство

$$\Pr(j|i) = \mathrm{Tr}\{|\varphi_i\rangle\langle\varphi_i|\mathcal{M}_j\} = P_j\delta_{ji}, \quad i = 1,\dots N, \tag{2}$$

$$\Pr(N+1|i) = \mathrm{Tr}\{|\varphi_i\rangle\langle\varphi_i|\mathcal{M}_{N+1}\} = P_{?i}, \quad i = 1,\dots N.$$

Измерения означают, что если произошел один из $1,\dots,N$ (*conclusive*) исходов, то состояние идентифицируется однозначно, но с вероятностью меньшей единицы. Если произошел $N+1$ (*inconclusive*) исход, то невозможно сказать, от какого состояния был данный исход.

Если канал имеет потери, т.е. часть состояний не достигает приемной стороны, то подслушиватель может действовать следующим образом. Он разрывает канал связи вблизи передающей и приемной станций (напомним, что квантовый канал связи в кванто-

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

[2)] В реальности используются пакеты когерентных состояний, а не одномодовые когерентные состояния. Однако поскольку оптическая схема линейна, достаточно рассматривать одну моду когерентных состояний, чтобы не усложнять выкладки несущественными деталями.

вой криптографии не контролируется). Вблизи передающей станции подслушиватель осуществляет UM-измерения. Если получен определенный исход, то он сообщает своему партнеру вблизи приемной стороны, какой результат получен. Партнер готовит соответствующее состояние и посылает к приемнику. Если получен неопределенный исход (?), то к приемнику ничего не посылается. При этом если вероятность потерь в канале связи равна вероятности неопределенного исхода ($\Pr(?) = \Pr(\text{Loss})$), то число состояний, достигающих приемной стороны в присутствии подслушивателя и без него, не меняется. При этом подслушиватель знает все передаваемые состояния и не производит ошибок на приемной стороне, т.е. остается недетектируемым. Система не обеспечивает секретность ключей, начиная с некоторого уровня потерь в линии связи.

Таким образом, UM-измерения разрушают секретность протоколов квантовой криптографии. До сих пор данная проблема остается актуальной. Ниже приводятся краткий анализ основных протоколов и причина их неустойчивости по отношению к UM-измерениям, а также новый протокол, который запрещает UM-измерения.

Краткий анализ основных протоколов квантового распределения ключей с фазовым кодированием. *Протокол B92.* Данный протокол был предложен в [3]. Он использует пару неортогональных состояний. Квантовый ансамбль есть $\{p_0 = p_1 = \frac{1}{2}, |\varphi_0\rangle, |\varphi_1\rangle\}$, где $p_{0,1}$ – вероятности появления состояний. Оптимальные UM-измерения, минимизирующие вероятность неопределенного исхода (*inconclusive*) [2], имеют вид

$$\begin{aligned} &\mathrm{id} = \mathcal{M}_0 + \mathcal{M}_1 + \mathcal{M}_?, \quad \mathcal{M}_0 = \frac{\mathrm{id} - |\varphi_1\rangle\langle\varphi_1|}{1 - |\langle\varphi_0|\varphi_1\rangle|}, \\ &\mathcal{M}_1 = \frac{\mathrm{id} - |\varphi_0\rangle\langle\varphi_0|}{1 - |\langle\varphi_0|\varphi_1\rangle|}, \quad \mathcal{M}_? = \mathrm{id} - \mathcal{M}_0 - \mathcal{M}_1. \end{aligned} \tag{3}$$

Вероятность неопределенного исхода с учетом того, что $p_0 = p_1$, есть

$$\Pr(?) = |\langle\varphi_0|\varphi_1\rangle|. \tag{4}$$

Если используется фазовое кодирование когерентных состояний, то $|\varphi_0\rangle = |e^{i\varphi_0}\alpha\rangle$ и $|\varphi_1\rangle = |e^{i\varphi_1}\alpha\rangle$. Соответственно вероятность неопределенного исхода $\Pr(?) = \exp\left(-\frac{\mu|e^{i\varphi_0} - e^{i\varphi_1}|^2}{2}\right)$, а вероятность потерь в канале $\Pr(\text{Loss}, L) = \exp\{-\mu[T(L)]\}$, где $\mu = |\alpha|^2$ – среднее число фотонов (типичные значения $\mu = 0.1{-}0.5$), $T(L) = 10^{-\delta L/10}$, L – длина линии связи, δ – константа затухания (типичные значения $\delta = 0.2$ дБ/км для одномодового волокна SMF-28).

Протокол не секретен, если $\Pr(\text{Loss}, L) \geq \Pr(?)$. Отсюда получаем ограничения на длину линии связи L_c, до которой гарантируется секретность передаваемых ключей. При длинах линии связи $L \geq L_c$ подслушиватель знает весь ключ, не производит ошибок на приемной стороне и остается недетектируемым.

Протокол BB84 и протоколы GUS на геометрически однородных состояниях. Протокол BB84 был предложен в [4]. На сегодняшний день он является наиболее изученным (см. [5–7]). Данный протокол использует два сопряженных базиса ($+$ и $\times$) с ансамблями состояний внутри каждого из них: $\{p_0(+) = p_1(+) = \frac{1}{2}, |\alpha\rangle, |-\alpha\rangle\}$, $\{p_0(\times) = p_1(\times) = \frac{1}{2}, |i\alpha\rangle, |-i\alpha\rangle\}$.

Возможно обобщение данного протокола на большее число информационных состояний – GUS протоколы (*Geometrically Uniform States*) [8]. Состояния в протоколе BB84 описываются точками в комплексной плоскости α и расположены на окружности радиуса $|\alpha|$ через равные углы. Все состояния могут быть получены из одного состояния, например $|\alpha\rangle$, последовательными унитарными поворотами. Так, $|i\alpha\rangle = U(\frac{\pi}{2})|\alpha\rangle$, $|-\alpha\rangle = U^2(\frac{\pi}{2})|\alpha\rangle$, $|-i\alpha\rangle = U^3(\frac{\pi}{2})|\alpha\rangle$. Числа базисов ($N_b$) и состояний ($2N_b$) могут быть бóльшими, чем $N_b = 2$ в протоколе BB84. Из-за геометрически однородной структуры информационных состояний для данного семейства протоколов имеется точное аналитическое решение для оптимальных UM-измерений [2]. Увеличение числа состояний уменьшает вероятность определенных исходов (соответственно увеличивает вероятность inconclusive исходов). Тем не менее при любом N_b имеется критическая длина линии связи, при превышении которой протокол теряет секретность. Подслушиватель знает весь ключ, не производит ошибок на приемной стороне и не детектируется.

Данное семейство протоколов удобно тем, что геометрически однородная структура делает их прозрачными для анализа стойкости. Казалось бы, увеличивая число базисов, можно увеличить длину линии связи до произвольной величины. Вместе с тем даже при идеальных фотодетекторах без темновых шумов увеличение числа базисов приводит к снижению эффективности генерации ключа. При $N_b \to \infty$ критическая длина формально $L_c \to \infty$. Однако при этом и скорость генерации ключа стремится к нулю. Поэтому данное семейство протоколов не решает проблему секретности при больших длинах линии связи (соответственно при больших потерях).

Протоколы DPS и COW. Протокол DPS (*Differential Phase Shift*) [9–11] и производный от DPS протокол COW (*Coherent One Way*) [12–15] также представляют собой попытки "запретить" UM-измерения. При этом протокол DPS является аналогом протокола, используемого в классических телекоммуникациях. В протоколе DPS информация о ключе кодируется в относительную разность фаз серии ослабленных когерентных состояний:

$$|e^{i\varphi_1}\alpha_1\rangle \otimes |e^{i\varphi_2}\alpha_2\rangle \otimes \ldots \otimes |e^{i\varphi_{n-1}}\alpha_{n-1}\rangle \otimes |e^{i\varphi_n}\alpha_n\rangle,$$

где $\varphi_i = -\pi, \pi$. Значение i-го бита ключа равно 0 при $\varphi_i - \varphi_{i+1} = 0, 2\pi$ и 1 при $\varphi_i - \varphi_{i+1} = \pm\pi$.

Поскольку в протоколе нет базисов, скорость генерации ключа не падает с ростом длины серии. Измерения с определенным исходом "запрещены" в том смысле, что их невозможно проводить над отдельной посылкой. Однако остается возможность осуществлять UM-измерения сразу над всей серией. При этом вероятность определенного исхода, по-видимому, экспоненциально падает с длиной серии. Замечено также, что при больших потерях и длинных сериях вовсе не обязательно пытаться проводить UM-измерения сразу над всей серией. Можно разбить всю последовательность на достаточно короткие серии и проводить UM-измерения над ними. В таком случае критическая ошибка протокола, до которой гарантируется секретное распределение ключей, стремится к нулю. Последнее является настораживающим обстоятельством. Из-за взаимной связи отдельных посылок для данного протокола не работает квантовая теорема de Finetti (детали см. в [7]), которая позволяет свести анализ стойкости протокола к атакам на отдельные посылки. Поэтому на сегодняшний день стойкость протокола до конца не изучена (см., например, [1], где данный протокол был назван вызовом для теоретиков).

Протокол COW [12–15] является, на наш взгляд, усложнением протокола DPS. Он использует ту же идею взаимной зависимости отдельных посылок при обнаружении подслушивания. В этом протоколе используется три состояния: два информационных, $|\text{vac}\rangle \otimes |\alpha\rangle$ для 0 и $|\alpha\rangle \otimes |\text{vac}\rangle$ для 1, а также одно контрольное, $|\alpha\rangle \otimes |\alpha\rangle$, где $|\text{vac}\rangle$ – вакуумное состояние поля (пустая посылка). Стойкость данного протокола также до конца не исследована. Сложность возникает из-за тех же причин, что и для протокола DPS.

Релятивистская квантовая криптография в открытом пространстве. Релятивистская квантовая криптография полностью решает проблему секретности при передаче ключей через открытое пространство в канале с произвольными потерями [16]. Единственным ограничением являются только темновые шумы однофотонных детекторов. (Напомним, что для упомянутых выше протоколов потеря секретности имеет место *даже при идеальных однофотонных детекторах* при превышении потерь над критическим значением.) Релятивистская квантовая криптография, кроме фундаментальных запретов квантовой механики на различимость квантовых состояний, использует дополнительные фундаментальные ограничения, диктуемые релятивистской причинностью [16]. Данные протоколы были специально разработаны для распределения ключей в открытом пространстве. Кроме ошибок на приемной стороне при детектировании действий подслушивателя, протоколы [16] фиксируют задержки состояний в канале. При этом возникает дополнительный параметр в задаче – расстояние между приемной и передающей станциями. На первый взгляд фиксирование задержек требует общей синхронизации часов на передающей и приемной стороне, которая должна проводиться через классический не контролируемый легитимными пользователями канал связи. Однако оказалось [16], что можно регистрировать задержки без общей синхронизации часов, используя двухпроходный вариант схемы измерений (см. реализацию протокола в [17]). Протокол гарантирует секретность ключей при произвольных потерях в канале связи и не строго однофотонном источнике информационных квантовых состояний. Можно считать, что релятивистская квантовая криптография для открытого пространства полностью решает проблему запрета UM-измерений. Физически картина достаточно прозрачна. Для UM-измерений требуется доступ к квантовому состоянию как целому. Если квантовое состояние размазано в пространстве-времени Минковского (имеет конечную протяженность), то доступ подслушивателя к состоянию как целому эквивалентен доступу (просмотру) к конечной части пространства-времени. Это требует конечного времени из-за существования предельной скорости распространения сигналов. Последнее неизбежно приводит к задержкам (сдвигу) времени измерений на приемной стороне, которые и фиксируются.

К сожалению, релятивистскую квантовую криптографию в открытом пространстве практически нельзя перенести на волоконные системы. Поскольку скорость распространения в волокне примерно в 1.5 раза меньше, чем в открытом пространстве, приходится сильно растягивать в пространстве квантовые состояния, чтобы подслушиватель не мог скомпенсировать задержки по времени, связанные с разностью скоростей распространения света в волокне и открытом пространстве.

Новый протокол – квантовое распределение ключей с классическим реперным состоянием. Как показывает вышеприведенный анализ, проблема потери секретности в канале с потерями до сих пор не нашла внятного решения. Так или иначе все попытки сводятся к увеличению числа информационных состояний, чтобы "запретить" (точнее, уменьшить) влияние UM-измерений, что приводит к увеличению вероятности неопределенных исходов. В протоколах DPS и COW информация размазывается на всю передаваемую последовательность. Однако это не запрещает проводить UM-измерения сразу над всей последовательностью. Размазывание информации на всю последовательность приводит к тому, что протокол становится сложным для анализа стойкости. Для данных протоколов, несмотря на их интенсивное исследование, неизвестна даже критическая ошибка в канале без потерь. Для протокола DPS имеются частичные результаты в однофотонном случае. Было показано [11], что когда однофотонное состояние размазывается на n посылок, критическая ошибка оказывается довольно низкой ($\approx 4.12\,\%$). Для протокола COW результаты в однофотонном случае нам неизвестны. Напомним, что для протокола BB84 в однофотонном случае критическая ошибка составляет $\approx 11\,\%$. Как показывает опыт исследования других протоколов, при переходе к квазиоднофотонным когерентным состояниям величина критической ошибки может только уменьшиться.

Поскольку состояния во всех посылках связаны между собой, перестает работать квантовая теорема де Финетти [7], которая позволяет свести анализ стойкости протокола к анализу состояний в отдельных посылках. И наконец, частные результаты по исследованию стойкости протокола в канале с потерями показывают, что критическая ошибка, до которой можно гарантировать секретность ключей, стремится к нулю с ростом потерь. Это является косвенным указанием на то, что протокол не обеспечивает секретность ключей при больших длинах линии связи и потерях.

Хотя протоколы DPS и COW используются в европейских и японских системах квантовой криптографии [9–15], неопределенность с их криптостойкостью представляет собой зыбкую основу для систем гарантированной стойкости.

Ниже предлагается принципиально новое решение проблемы UM-измерений в квантовой криптографии. Реализация и, особенно, анализ стойкости этого протокола являются достаточно простыми, что важно при практическом использовании. *Предыдущие протоколы были направлены на уменьшение роли UM-измерений. "Запрет" UM-измерений означал лишь уменьшение вероятности определенных исходов и, соответственно, увеличение вероятности неопределенных исходов. В нашем протоколе проблема решается радикально полным запретом (без кавычек) UM-измерений.*

Идея состоит в совмещении квантовой части протокола с классической частью. В любой системе квантовой криптографии (волоконной или в открытом пространстве) используется интенсивный световой классический импульс синхронизации. В качестве этого импульса применяется интенсивное (классическое) когерентное состояние $|\alpha_{cl}\rangle$ (среднее число фотонов макроскопически велико: $\mu_{cl} = |\alpha_{cl}|^2 \gg 1$) с той же или иной длиной волны, что и информационные состояния. В некоторых системах такой импульс вообще передается по отдельной вспомогательной линии. Наличие подобного интенсивного состояния связано с технической частью протокола – стробированием лавинных детекторов. Вообще говоря, оно не входит в квантовую криптографическую часть протокола. *При этом интенсивность состояния всегда такова, что все синхроимпульсы в каждой серии посылок должны быть зарегистрированы. В противном случае система сигнализирует о сбое синхронизации и вся серия посылок выбрасывается.* Поскольку интенсивное классическое состояние всегда присутствует, имеет смысл напрямую использовать его в квантовой криптографической части протокола. Опишем сначала протокол, а затем приведем его реализацию и анализ стойкости.

Протокол.

1. Передается длинная серия отдельных независимых посылок. Каждая посылка состоит из пары сдвинутых по времени при помощи интерферометра Маха–Цандера (см. ниже) состояний: информационного, $|e^{i\varphi_{0,1}}\alpha_q\rangle$ ($|\alpha_q|^2 < 1$), и интенсивного классического, $|\alpha_{cl}\rangle$ ($|\alpha_{cl}| \gg 1$) – $|e^{i\varphi_{0,1}}\alpha_q\rangle \otimes |\alpha_{cl}\rangle$. Информация о битах ключа кодируется в фазу квантового состояния: $0 \to \varphi_0$, $1 \to \varphi_1$.

2. Потери $T(L)$ в канале связи могут меняться во время передачи ключей.

3. При прохождении через канал связи с линейными потерями когерентные состояния ослабляются *самоподобным* образом: $|e^{i\varphi_{0,1}}\alpha_q\rangle \otimes |\alpha_{cl}\rangle \to |e^{i\varphi_{0,1}}\alpha[T(L)]_q\rangle \otimes |\alpha[T(L)]_{cl}\rangle$.

4. На приемной стороне состояния при помощи светоделителя (см. ниже) разделяются на два канала:

$$|e^{i\varphi_{0,1}}\alpha[T(L)]_q\rangle \otimes |\alpha[T(L)]_{cl}\rangle \to$$

$$\to \begin{pmatrix} |e^{i\varphi_{0,1}}\frac{\alpha[T(L)]_q}{\sqrt{2}}\rangle \otimes |\frac{\alpha[T(L)]_{cl}}{\sqrt{2}}\rangle \\ |e^{i\varphi_{0,1}}\frac{\alpha[T(L)]_q}{\sqrt{2}}\rangle \otimes |\frac{\alpha[T(L)]_{cl}}{\sqrt{2}}\rangle \end{pmatrix}.$$

5. Калиброванным классическим фотодетектором измеряется интенсивность во временном окне отвечающем классическому когерентному состоянию во втором канале (см. п. 4). При регистрации оценивается интенсивность и одновременно вырабатывается импульс синхронизации для стробирования лавинных детекторов (см. ниже).

6. Поскольку соотношение амплитуд классического и квантового когерентного состояний $\left(\zeta = \frac{|\alpha_{cl}|^2}{|\alpha_q|^2}\right)$ известно публично и является открытым параметром протокола, измерение “на ходу” интенсивности классического когерентного состояния $|\alpha_{cl}[T(L)]/\sqrt{2}|^2$ позволяет ослабить его в $\frac{|\alpha_{cl}[T(L)]|^2}{|\alpha_q[T(L)]|^2}$ раз во временном окне, отвечающем классическому состоянию в первом канале (см. п. 4). При этом происходит переход интенсивного состояния $|\frac{\alpha_{cl}[T(L)]}{\sqrt{2}}\rangle \to |\frac{\alpha_q[T(L)]}{\sqrt{2}}\rangle$. В итоге в первом канале возникает пара одинаковых с точностью до фазового множителя состояний: $|e^{i\varphi_{0,1}}\frac{\alpha_q[T(L)]}{\sqrt{2}}\rangle \otimes |\frac{\alpha_q[T(L)]}{\sqrt{2}}\rangle$.

7. На приемной стороне происходит декодирование: на состояние $|e^{i\varphi_{0,1}}\frac{\alpha_q[T(L)]}{\sqrt{2}}\rangle$ случайным образом накладывается компенсирующая фаза. После этого пара направляется на интерферометр Маха–Цандера, на выходе которого два состояния интерферируют друг с другом (конструктивно и деструктивно на двух выходах) и регистрируются в центральном временном окне лавинными однофотонными детекторами. *Принципиально важно, что интерферируют друг с другом исходное квантовое когерентное состояние и ослабленное до того же уровня состояние, произошедшее из интенсивного когерентного состояния.*

8. Через открытый канал проверяются числа посланных и зарегистрированных классических импульсов. При обнаружении несовпадения их чисел, вся серия отбрасывается. При совпадении числа посланных и зарегистрированных классических импульсов протокол продолжается аналогично другим протоколам квантового распределения ключей.

Таким образом, в данном протоколе UM-измерения реально запрещены. Поскольку информация о ключе кодируется в фазу ослабленных когерентных состояний, подслушиватель должен различать одно из неортогональных состояний $|e^{\varphi_0}\alpha_q\rangle$ и $|e^{\varphi_1}\alpha_q\rangle$ (считаем в пользу подслушивателя, что фаза α_q известна, например из классического состояния). В случае неопределенного исхода при различении информационных квантовых состояний подслушиватель не может блокировать интенсивное классическое состояние (иначе вся серия будет отброшена). Поэтому взамен ослабленного информационного квантового состояния подслушиватель вынужден будет послать вместо истинного состояния, например $|e^{i\varphi_0}\alpha_q\rangle$, некоторое состояние наугад, что приведет при интерференции с ослабленным классическим импульсом к ошибке. Таким образом, подслушиватель никогда не сможет узнать весь ключ и не производить ошибок на приемной стороне. Если бы не было классического импульса, с которым осуществляется “сбивка” на интерферометре, подслушиватель мог бы блокировать посылки, в которых получен неопределенный исход (?) при UM-измерениях. При наличии классического реперного состояния UM-измерения приводят к ошибкам на приемной стороне. Поэтому исключается ситуация, которая имеет место в других протоколах, приведенных выше, когда, начиная с некоторых потерь, подслушиватель знает весь ключ, не производит ошибок на приемной стороне и не детектируется.

Волоконная реализация протокола. Реализация протокола приведена на рис. 1. Лазер формирует локализованный по времени интенсивный импульс когерентного состояния $|\alpha\rangle$ ($|\alpha|^2 \gg 1$). Интерферометр Маха–Цандера с разной длиной плеч преобразует одно состояние в два сдвинутых по времени. В нижнем плече интерферометра встроен постоянный аттенюатор, который ослабляет состояние, проходящее по нижнему плечу, до квазиоднофотонного уровня $|\alpha_q\rangle$ ($|\alpha|^2 < 1$). На выходе интерферометра возникает пара когерентных состояний: интенсивное классическое и квантовое, $|\alpha_q\rangle \otimes |\alpha_{cl}\rangle$. Далее пара состояний проходит через фазовый модулятор. В момент прохождения квантового состояния к фазовому модулятору прикладывается импульс напряжения, что приводит к появлению дополнительной фазы у квантового когерентного состояния, $|e^{i\varphi_{0,1}}\alpha_q\rangle \otimes |\alpha_{cl}\rangle$. Затем состояния направляются в канал связи. Оба состояния проходят в канале одинаковую эволюцию. На приемной стороне пара состояний разделяется светоделителем на два канала. Во втором канале во временном окне, отвечающем интенсивному состоянию, происходит детектирование классического состояния калиброванным детектором. По протекающему фототоку “на ходу” оценивается интенсивность классического состояния. По величине интенсивности вырабатывается импульс напряжения на модулятор интенсивности, который ослабляет классическое состояние в первом канале до уровня квазиоднофотонного. Далее пара состояний поступает на фазовый модулятор, который изменяет относительную фазу, а затем – на интерферометр, который сдвигает

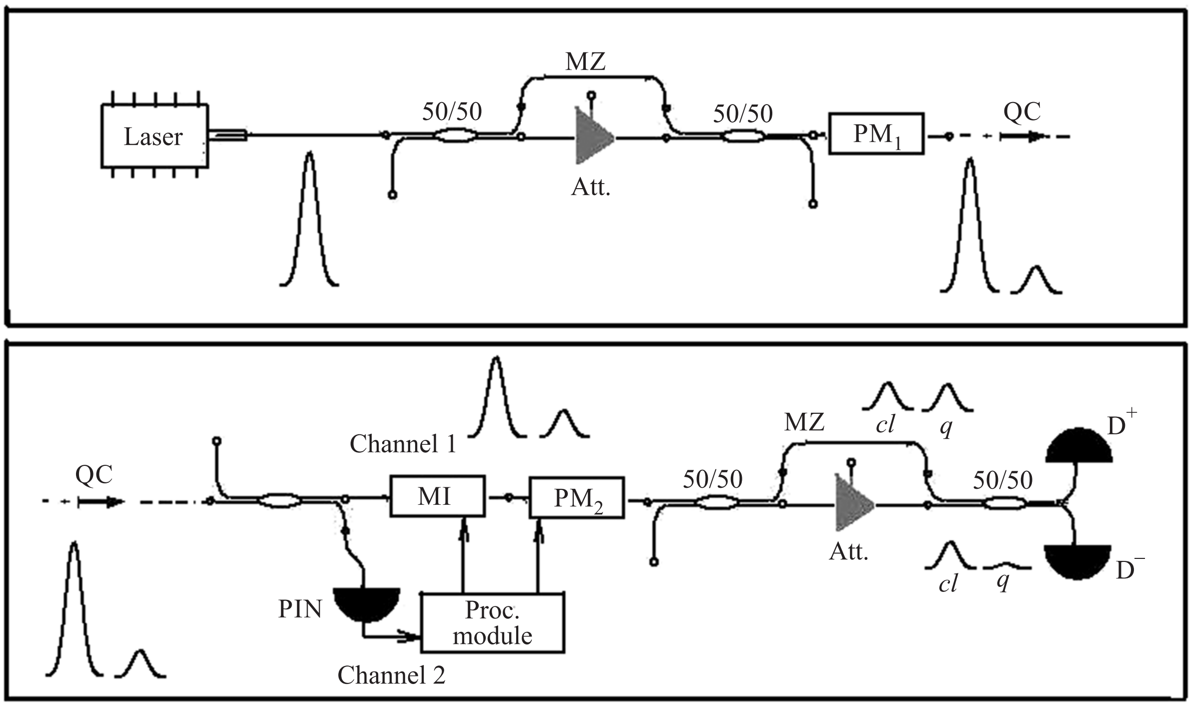

Рис. 1. Функциональная схема волоконной части системы: Laser – источник когерентных состояний, 50/50 – симметричные светоделители, MZ – интерферометры Маха–Цандера с разной длиной плеч, MI – быстрый модулятор интенсивности, $\mathrm{PM}_{1,2}$ – фазовые модуляторы, q, cl – состояния, происходящие из классического интенсивного и ослабленного когерентных состояний, Att. – медленный управляемый аттенюатор, proc. module – модуль управляющей электроники для выработки синхроимпульса и оценки интенсивности классического когерентного состояния, PIN – калиброванный детектор, $\mathrm{D}^{\pm}$ – лавинные однофотонные детекторы, QC – квантовый канал связи

пару состояний друг относительно друга и приводит к конструктивной и деструктивной интерференции.

Постоянный (точнее, медленный) управляемый аттенюатор в интерферометре Маха–Цандера на приемной стороне играет двоякую роль. Во первых, он нужен для того, чтобы обеспечить некоторый постоянный уровень ослабления в коротком плече. Это связано с тем, что быстрые модуляторы интенсивности (MI на схеме) обеспечивают коэффициент ослабления не более 60 db. Быстрый аттенюатор (MI) нужен, чтобы совместно с постоянным аттенюатором набрать требуемый коэффициент ослабления. Во-вторых, если потери в канале за время передачи серии не меняются, то требуемый коэффициент ослабления может быть набран только при помощи постоянного аттенюатора.

Анализ стойкости протокола относительно UM-измерений. Возможны три типа атак: 1) унитарная атака, 2) атака со светоделителем, 3) атака с UM-измерениями. Стойкость относительно первых двух атак гарантируется неортогональностью состояний. Полный анализ слишком объемен. На данный момент достаточно показать, что в канале связи с произвольными и неизвестными потерями протокол устойчив относительно UM-атаки.

Поскольку подслушиватель не может блокировать классическое реперное состояние, а измерения информационного квантового состояния имеют вероятность неопределенного исхода (см. формулу (4))

$$\Pr(?) = |\langle e^{i\varphi_0}\alpha_q|e^{i\varphi_1}\alpha_Q\rangle|, \tag{5}$$

условная энтропия в асимптотическом пределе длинных передаваемых последовательностей в пересчете на одну посылку равна

$$H(X|Y_E) = (1-p) + p\Pr(?), \tag{6}$$

где $0 \le p \le 1$ – доля посылок, в которых подслушиватель использует UM-измерения, X – передаваемая битовая строка, Y_E – битовая строка подслушивателя. Иначе говоря, в доле посылок p из-за невозможности блокировать посылки с неопределенным исходом (?) подслушиватель вместо истинных квантовых состояний вынужден посылать квантовые состояния наугад, что приведет в этих посылках к вероятности ошибки 1/2. Условная энтропия Шеннона между легитимными пользователями в пересчете на посылку равна

$$H(X|Y) = h(Q), \;\; h(Q) = -Q\log Q - (1-Q)\log(1-Q),$$
$$Q = \frac{1}{2}p\Pr(?), \qquad (7)$$

где Q – наблюдаемая ошибка на приемной стороне, которая вызвана подслушивателем из-за UM-измерений, Y – битовая строка на приемной стороне. Длина секретного ключа есть (см., например, [7])

$$R(p,Q) \geq H(X|Y_E) - H(X|Y) = (1-p) + p\Pr(?) - h(Q). \qquad (8)$$

При идеальных фотодетекторах без темновых шумов ошибка Q обусловлена только UM-измерениями и равна $Q = \frac{1}{2}p\Pr(?)$. Формула (8) имеет интуитивно прозрачную интерпретацию. Величина $H(X|Y_E)$ есть количество бит информации, которых не хватает подслушивателю, чтобы знать передаваемую битовую строку X целиком, если он имеет в своем распоряжении только строку Y_E. Аналогично $H(X|Y)$ – количество бит информации, которых не хватает приемнику, чтобы знать передаваемую битовую строку X целиком, имея в своем распоряжении строку Y. Разница этих условных информаций представляет секретный ключ, который неизвестен подслушивателю. Поскольку $\Pr(?)$ является параметром протокола и определяется только структурой информационных состояний, а параметр p находится в руках подслушивателя, удобно переписать (8), используя наблюдаемую ошибку и $\Pr(?)$. С учетом того что $p = 2Q/\Pr(?)$, имеем

$$R[\Pr(?), Q] \geq 1 - h(Q) - 2Q\left(\frac{1}{\Pr(?)} - 1\right). \qquad (9)$$

На рис. 2 показаны зависимости длины секретного ключа от наблюдаемой ошибки Q при различных значениях параметра $\Pr(?)$.

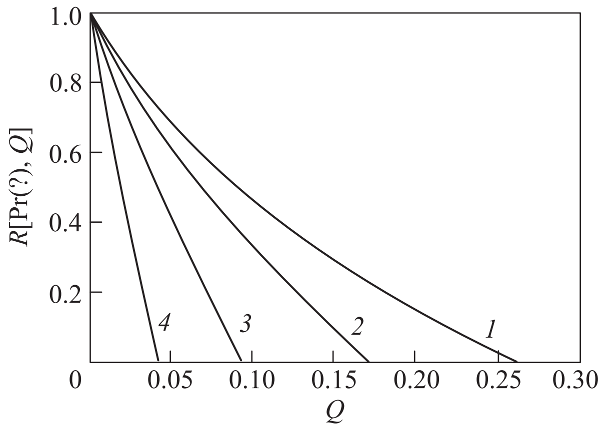

Рис. 2. Зависимости длины секретного ключа $R[\Pr(?), Q]$ в пересчете на одну позицию от наблюдаемой ошибки на приемной стороне. Значения параметра $\Pr(?)$ для кривых *1*, *2*, *3*, *4* составляют 0.75, 0.5, 025, 0.1 соответственно

Заключение. Таким образом, перенос классического импульса синхронизации из технической части системы в криптографическую совместно с измерением "на ходу" его интенсивности и последующим ослаблением до уровня квантового информационного состояния позволяет реально запретить подслушивателю проводить UM-измерения, которые в других системах приводят к потере секретности при наличии потерь в канале связи. Отметим, что в данной схеме снимается требование на потери, которые в предыдущем варианте [18] считались заранее известными. Здесь потери в линии не предполагаются заранее известными и могут меняться при передаче ключей даже в каждой отдельной посылке. Кроме того, в протоколе каждая посылка не зависит от предыдущей, что делает анализ стойкости протокола достаточно простым и позволяет провести его до конца.

Выражаю благодарность Д.А. Кронбергу и С.П. Кулику за полезные обсуждения, а также коллегам по Академии криптографии РФ за постоянную поддержку.

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
2. A. Chefles, arXiv/quant-ph: 9807022; A. Chefles and S. M. Barnett, arXiv/quant-ph: 9807023.
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, *Interferometric Quantum Key Distribution System*, April 26 (1994), Date of Patent, Patent Number 5.307.410.
4. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
5. D. Mayers, J. ACM **48**, 351 (2001).
6. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
7. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. 2005.
8. S. N. Molotkov, JETP Lett. **95**, 332 (2012).
9. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).

10. H. Takesue, S.W. Nam, Q. Zhang, R.H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photon. **1**, 343 (2007).
11. K. Wen, K. Tamaki, and Y. Yamamoto, arXiv/quant-ph: 0806.2684.
12. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, arXiv:quant-ph/0506097.
13. C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, arXiv:quant-ph/0609090.
14. C. Branciard, N. Gisin, and V. Scarani, arXiv:quant-ph/0710.4884.v2.
15. D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, arXiv:quant-ph/08095264.
16. S. N. Molotkov, JETP **112**, 370 (2012); JETP Lett. **94**, 469 (2011); JETP Lett. **96**, 342 (2012).
17. I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, arXiv:quant-ph/1403.3122; Las. Phys. Lett. **11**, 065203 (2014).
18. S. N. Molotkov, JETP Lett. **93**, 747 (2011).