Письма в ЖЭТФ, том 103, вып. 12, с. 883 – 890

О противодействии атаке с яркими состояниями в двухпроходной системе квантовой криптографии

К. А. Балыгин[+], *А. Н. Климов*[+*], *А. В. Корольков*[×], *С. П. Кулик*[+], *С. Н. Молотков*[×○∇1)]

[+] *Физический факультет, МГУ им. Ломоносова, 119991 Москва, Россия*

[*] *Институт общей физики РАН им. Прохорова, 119991 Москва, Россия*

[×] *Академия Криптографии Российской Федерации, 121552 Москва, Россия*

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

[∇] *Факультет вычислительной математики и кибернетики МГУ им. Ломоносова, 119991 Москва, Россия*

Поступила в редакцию 10 марта 2016 г.
После переработки 13 мая 2016 г.

Секретность ключей в системах квантовой криптографии, в отличие от математических алгоритмов криптографии, гарантируется фундаментальными законами квантовой механики. Однако криптостойкость таких систем, которые являются распределенным физическими устройствами, принципиально зависит от способа их реализации и, особенно, от калибровки и контроля критических параметров. Самым важным параметром является число фотонов в информационных квазиоднофотонных состояниях в линии связи. Для ряда систем была явно продемонстрирована уязвимость по отношению к атаке с яркими состояниями. В данной работе предложен и реализован метод, гарантирующий стойкость относительно такого рода атак, кроме того, впервые получена связь наблюдаемых физических параметров, используемых и получаемых при контроле квантовых состояний, с длиной финальных секретных ключей.

DOI: 10.7868/S0370274X16120109

Введение. К настоящему времени для многих протоколов квантовой криптографии доказано, что они гарантируют секретность ключей *при любых атаках на квантовый канал связи*. При таких атаках подслушиватель не имеет ни прямого, ни косвенного доступа к приемной (клиенту) и передающей (серверу)[2)] аппаратуре, но может производить любые манипуляции с квантовыми состояниями в канале (подменять посылаемые состояния) и с самим квантовым каналом связи (например, заменять его каналом с меньшими потерями). При этом подразумевается, что все параметры протокола, например число фотонов или фазовый сдвиг *в посылаемом в канал состоянии*, строго поддерживаются аппаратурой. Другой тип атак подразумевает, что подслушиватель (Ева) может через квантовый канал связи активно воздействовать на аппаратуру, посылая зондирующее излучение на детекторы (атака с ослеплением детекторов), фазовые модуляторы и т.д., что в результате может дать, через знание состояния аппаратуры, непосредственный доступ к ключевой последовательности. Таким образом, доказательство секретности ключей, в отличие от доказательств при атаках только на квантовый канал, должно учитывать практическую реализацию системы. До конца вопрос криптостойкости при атаках активного зондирования до сих пор не решен на требуемом уровне.

Чтобы гарантировать секретность ключей (при атаках только на квантовый канал), необходимо быть уверенным, что в канал связи выходят состояния, которые предписаны протоколом. В двухпроходных системах (волоконных и работающих через открытое пространство [1–3]), на прямом проходе в канал выходят контролируемые интенсивные (классические) состояния, которые не несут никакой информации о ключе. На стороне клиента часть состояния используется для синхронизации, а остальная ослабляется до квазиоднофотонного уровня, модулируется (уже несет информацию о ключе) и, после от-

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

2)Во избежании путаницы, которая возникает для двухпроходных систем, будем называть сервером ту часть системы, где находится интерферометр Маха–Цандера. Часть, где находится зеркало, – клиентом. К одному серверу через коммутатор могут подключаться несколько клиентов.

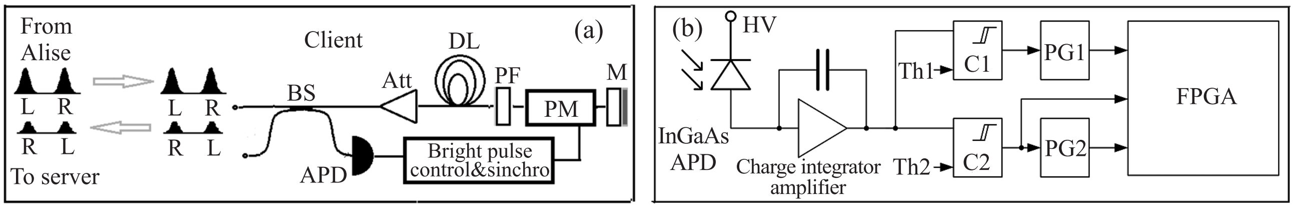

Рис. 1. (a) – Блок-схема клиента с контролем ярких импульсов: L(R) и R(L) – пара входных классических импульсов и ослабленных квазиоднофотонных, APD – лавинный фотодиод, BS – волоконный светоделитель, Att – медленный волоконный аттенюатор, DL – волоконная линия задержки, PF – поляризационный фильтр, PM – фазовый модулятор, M – волоконное зеркало. (b) – Блок-схема детектора входных импульсов у клиента: APD – лавинный фотодиод, HV – напряжение смещения, Charge Integrator Amplifier (CIA) – зарядово-чувствительный усилитель, Th1, 2 – независимо выставляемые пороги генерации синхроимпульсов и детектирования ярких импульсов, C1, 2 – компараторы, PG1, 2 – одновибраторы, FPGA – ПЛИС (Программируемая Логическая Интегральная Схема)

ражения от зеркала, направляется обратно в канал связи к серверу (рис. 1). Чтобы гарантировать, что в канал связи выходят квазиоднофотонные состояния, которые требует протокол, нужно знать в точности, какие состояния приходят из канала связи. Однако состояние канала связи может меняться, как само по себе от внешних факторов, так и от действий подслушивателя. Поскольку существующие волоконные аттенюаторы достаточно медленные, технически сложно и измерять интенсивности входных состояний в каждой посылке, и затем ослаблять их на "лету" до квазиоднофотонного уровня.

Атака с яркими состояниями. Прежде, чем сформулировать задачу, нам потребуется описать атаку с яркими состояниями. Такая атака является критической для двухпроходных систем. Использование в двухпроходных системах детектора классических состояний, приходящих к клиенту, как для синхронизации, так и для регистрации числа ярких, превышающих некий порог, входных импульсов, является обязательным для защищенных систем [4]. Классические интенсивные когерентные состояния, которые вышли из интерферометра на сервере (см., например, [2]), несут полную информацию о разности хода и относительной фазе. Нет фундаментальных запретов на полное измерение данных состояний и Ева может приготовить пару идентичных когерентных состояний, но с существенно большей интенсивностью, которые после ослабления на стороне клиента на определенную величину вернутся на сервер и произведут интерференцию без ошибок.

Если на стороне клиента нет контроля интенсивности входных импульсов, а ослабление установлено на определенную величину, зависящую от длины линии, то при достаточно большой интенсивности ярких импульсов Евы, даже после ослабления на стороне клиента, в канал выйдут интенсивные классические состояния, которые уже несут информацию о ключе. Измерение этих состояний позволит Еве получить полную информацию о кодированных состояниях клиента, а затем послать на сервер пару таких состояний с уменьшенной интенсивностью. При такой атаке Ева будет знать весь ключ и не произведет ошибок. Поэтому без правильного детектирования интенсивности входных состояний невозможно гарантировать секретность ключей. Например, было экспериментально продемонстрировано [4], что широко разрекламированная швейцарская система Clavis-2 уязвима относительно такой атаки.

Формулировка задачи. Поскольку Ева может атаковать произвольное число посылок, причем с разной интенсивностью, то наиболее общий подход предполагает, что интенсивность входных импульсов от Евы к клиенту подчиняется распределению $P_{\mathrm{Eve}}(\mu)$. Причем данное распределение вероятностей известно только Еве. Поскольку аттенюатор выставляется на определенное ослабление на всю серию посылок, то на выходе в канал связи пойдут состояния с распределением $P(\mu)$, которое получается из $P_{\mathrm{Eve}}(\mu)$ ослаблением в фиксированное число раз. Контроль входных состояний сводится к аппаратному вычислению

$$I(\mu_{th}) = \int_0^\infty P(\mu) f_{\mu_{th}}(\mu) d\mu,$$

и если $I(\mu_{th})$ превышает некоторое значение, то принимается решение о наличии в данной посылке состояния, с превышением интенсивности, $f_{\mu_{th}}(\mu)$ – некоторая функция (рис. 2), описывающая порого-

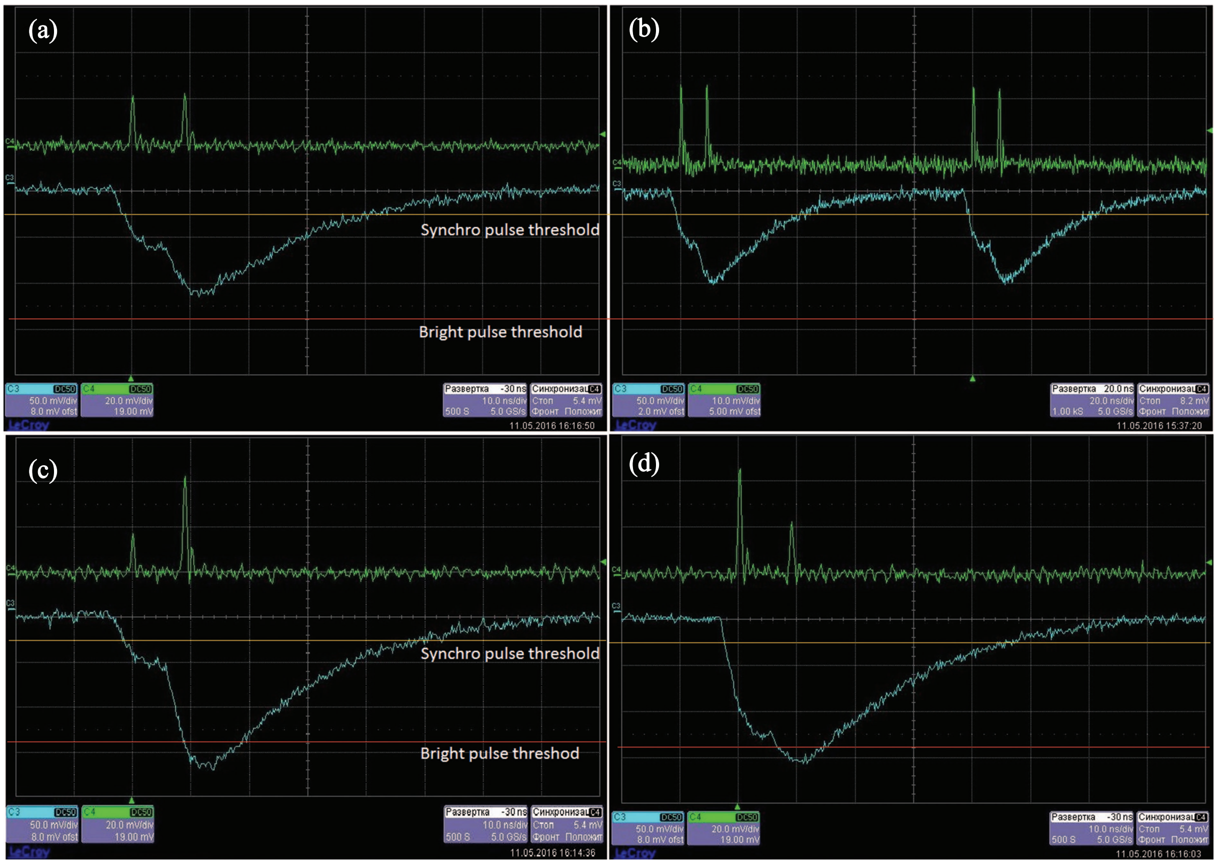

Рис. 2. (Цветной онлайн) Осциллограммы сигналов на выходе APD (с дополнительным усилением) (верхняя кривая) и на выходе CIA (нижняя кривая). (a), (b) – Штатная работа детектора при различных (1 и 10 МГц) частотах повторения входных импульсов. (c), (d) – Наложение зондирующего импульса на второй и первый рабочий импульс. Видно, что при этом интегральный сигнал превышает порог детектирования ярких импульсов

вые свойства детектора, которая зависит от μ_{th} (порога), задаваемого клиентом (см. ниже). Здесь μ – число фотонов в линии. Дальнейшая задача состоит в: 1) реализации системы контроля интенсивности выходных состояний – определения наблюдаемого значения $I(\mu_{th})$; 2) установлении связи наблюдаемого значения $I(\mu_{th})$ с длиной секретного ключа. Говоря неформально, требуется получить ответ на вопрос – какое дополнительное количество информации получит подслушиватель и какую длину секретного ключа можно доказательно получить, если в серии зарегистрировано n_G ярких импульсов? При этом необходимо учесть неидеальность порогового детектора, т.е. отличие его характеристики от идеальной (типа $\theta(\mu - \mu_{th})$). Для реального детектора не все импульсы с $\mu > \mu_{th}$ будут зарегистрированы. В такой постановке задачи неважно, чем вызван зарегистрированный яркий импульс – изменением состояния линии или действиями Евы.

В данной работе, насколько нам известно, впервые дается систематический ответ на данные вопросы. Предложена и экспериментально реализована система контроля ярких импульсов, получена зависимость длины секретного ключа от количества ярких импульсов и характеристик порогового детектора, причем данная связь получена в общем виде. Наш метод, в отличие от используемого в других системах (см. [3]*), доказуемо гарантирует криптостойкость относительно данного вида атак.*

Связь длины секретного ключа с наблюдаемым порогом $I(\mu_{th})$. Дальнейшая логика наших действий состоит в следующем. Сначала получим выражение для длины секретного ключа, считая интенсивность μ известной. Далее, используя полученное выражение и, зная аппаратную пороговую функцию $f_{\mu_{th}}(\mu)$, установим связь длины секретного ключа с наблюдаемой величиной $I(\mu_{th})$, в которую входит произвольное неизвестное распределение Евы $P(\mu)$.

Критерием секретности в квантовой криптографии является следовое расстояние, которое связывается со сглаженной квантовой min энтропией Реньи [5]. Пусть μ задано, имеет место (см. детали в [6])

$$\frac{1}{2}||\rho_{XE}^{(n)}(\mu) - \rho_U^{(n)} \otimes \rho_E^{(n)}(\mu)||_1 <$$

$$< \frac{1}{2}\sqrt{2^{-(H_{\min}^{\varepsilon}(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu)C(\mu)) - R_n(\mu))}} \le \varepsilon,$$

n – длина последовательности. Для min энтропии справедливо неравенство [5]

$$H_{\min}^{\varepsilon}(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu)C(\mu)) \ge$$

$$\ge H_{\min}^{\varepsilon}(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu)) - H_{\max}(C(\mu)) =$$

$$= H_{\min}^{\varepsilon}(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu)) - \mathrm{leak}_n(\mu),$$

где $C(\mu)$ символизирует всю совокупность информации Евы, получаемую при коррекции ошибок ($\mathrm{leak}_n(\mu)$ – утечка информации в битах). Длина ε-секретного ключа в битах равна

$$R_n(\mu) \ge H_{\min}^{\varepsilon}(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu)) - \mathrm{leak}_n(\mu).$$

Далее, чтобы не загромождать выкладки, рассмотрим асимптотический предел – число посылок стремится к бесконечности $n \to \infty$ (отметим, что данные результаты обобщаются и на случай конечных последовательностей), при этом $\varepsilon \to 0$. В этом пределе сглаженные энтропии Реньи стремятся к энтропиям фон Неймана [5], имеем

$$H_{\min}^{\varepsilon}(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu)) \to H(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu)),$$

$$H(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu)) = n(H(\rho_{XE}(\mu)) - H(\rho_E(\mu))),$$

$$\rho_{XE}^{(n)}(\mu) = \rho_{XE}^{\otimes n}(\mu), \quad \rho_E^{(n)}(\mu) = \rho_E^{\otimes n}(\mu),$$

$$\rho_E(\mu) = \mathrm{Tr}_X\{\rho_{XE}(\mu)\}.$$

Вся информация об атаках Евы заключена в $H(\rho_{XE}^{(n)}(\mu)|\rho_E^{(n)}(\mu))$, которая неформально описывает нехватку информации Евы относительно ключа. Матрица плотности после атаки Евы имеет вид

$$\rho_{XE}(\mu) =$$

$$= \sum_x P_X(x)|\varphi_x(\mu)\rangle_{BB}\langle\varphi_x(\mu)| \otimes |E_x(\mu)\rangle_{EE}\langle E_x(\mu)|,$$

$$|\varphi_x(\mu)\rangle_B| \otimes |E_x(\mu)\rangle_E = U_{BE}(|\varphi_x^{(0)}(\mu)\rangle_B| \otimes |E(\mu)\rangle_E),$$

где $|E(\mu)\rangle_E$ – вспомогательное состояние Евы, $P_X(x)$ – вероятность выбора состояния x на сервере, исходные когерентные состояния

$$|\varphi_x^{(0)}(\mu)\rangle_B = |\sqrt{\mu}\rangle_L \otimes |e^{i\theta_x}\sqrt{\mu}\rangle_R,$$

(L и R – индексы временных окон, см. детали в [7] и рис. 1) состояния в линии после клиента, унитарный оператор U_{BE} описывает действия Евы на состояния в канале связи после их выхода от клиента.

Без контроля интенсивности Ева может направить к клиенту интенсивные состояния с $\mu_{\mathrm{clas}} \gg 1$, такие, что даже после ослабления $\mu_{\mathrm{clas}} \to \mu \gg 1$ состояния все равно еще интенсивные. При больших μ когерентные состояния сколь угодно близки к ортогональным $|\langle\sqrt{\mu}|e^{i\theta}\sqrt{\mu}\rangle|^2 = e^{-\mu|1-e^{i\theta}|^2} \to 0$. В пользу Евы считаем, что состояния ортогональны, а значит достоверно различимы без возмущения, могут быть скопированы с вероятностью единица, т.е. Ева может добиться, чтобы

$$|\varphi_x^{(0)}(\mu)\rangle_B| \otimes |E(\mu)\rangle_E \to |\varphi_x^{(0)}(\mu)\rangle_B \otimes |\varphi_x^{(0)}(\mu)\rangle_E.$$

Для таких посылок условная энтропия фон Неймана равна нулю $H(\rho_{XE}(\mu)) - H(\rho_E(\mu)) = 0$, нехватка информации о состоянии для Евы – нуль, такая посылка не секретна.

Учет распределения по μ. Пока мы считали μ фиксированным. Интенсивность выходных импульсов в канале μ подчиняется неизвестному распределению $P(\mu)$, известному только Еве – разные посылки могут иметь разную интенсивность, что сервер и клиент воспринимают как случайность. В этом случае матрица плотности $\rho_{XE}(\mu)$ становится

$$\overline{\rho}_{XE} = \int_0^{\infty} P(\mu)\rho_{XE}(\mu)d\mu =$$

$$= \sum_x \int_0^{\infty} P(\mu)(|\varphi_x(\mu)\rangle_{BB}\langle\varphi_x(\mu)| \otimes$$

$$\otimes |E_x(\mu)\rangle_{EE}\langle E_x(\mu)|)d\mu. \quad (1)$$

Если бы распределение $P(\mu)$ было известно, то можно было напрямую использовать выражение для длины ключа, которое приобретает вид

$$R_n \ge (H(\overline{\rho}_{XE}) - H(\overline{\rho}_E)) - \mathrm{leak}_n, \; H(\rho) = -\mathrm{Tr}\{\rho\log_2\rho\}$$

$H(\rho)$ – энтропия фон Неймана, leak_n – информация в битах, потраченная на исправление ошибок для последовательности длины $n \to \infty$. *Проблема в состоит том, что распределение $P(\mu)$ находится в руках*

Евы и неизвестно серверу и клиенту. Как, не зная вида распределения, можно гарантировать секретность ключей? Наш подход состоит в следующем. Пусть из общего числа посылок (n) зарегистрировано

$$n_G = n\int_{\mu_c}^{\infty} P(\mu) f_{\mu_{th}}(2\mu) d\mu$$

ярких входных импульсов, интенсивность которых, превышает μ_c на импульс (*в данной реализации* $\mu_{th} = 2\mu_c$, *т.к. пороговая функция измеряет интенсивность в паре импульсов, а распределение* $P(\mu)$ *относится к числу фотонов в одном информационном импульсе, см. ниже*). В остальных $n_{OK} = n - n_G$ превышение не обнаружено. Наша задача состоит в том, чтобы связать длину секретного ключа с неизвестным распределением $P(\mu)$ и заданной аппаратной пороговой функцией детектора $f_{\mu_{th}}(2\mu)$, параметрически зависящей от порога μ_{th}, и желательно универсальным образом, не зависящим от протокола. Преобразуем (1) к виду

$$\overline{\rho}_{XE} = \int_0^{\mu_c} P(\mu)\rho_{XE}(\mu) d\mu + \int_{\mu_c}^{\infty} P(\mu)\rho_{XE}(\mu) d\mu. \quad (2)$$

Далее в пользу Евы, считаем, что при $\mu > \mu_c$ ей достоверно известны состояния, что означает замену

$$\rho_{XE}(\mu) \to \rho_{XX} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n} |x\rangle_{BB}\langle x| \otimes |x\rangle_{EE}\langle x|,$$

$$|x\rangle_{B,E} = |x_1\rangle_{B,E} \otimes |x_2\rangle_{B,E} \otimes \ldots |x_n\rangle_{B,E}.$$

Консервативно в пользу Евы, чем больше μ, тем лучше различимы квантовые состояния, тем меньше условная квантовая энтропия фон Неймана, тем меньше длина секретного ключа, поэтому законна замена в первом слагаемом в (2)

$$\int_0^{\mu_c} P(\mu)\rho_{XE}(\mu) d\mu \to \rho_{XE}(\mu_c)\int_0^{\mu_c} P(\mu) d\mu.$$

Далее из условия нормировки

$$1 = \int_0^{\mu_c} P(\mu) d\mu + \int_{\mu_c}^{\infty} P(\mu) d\mu,$$

учитывая, что $(0 \le f_{\mu_{th}}(2\mu) \le 1)$ и $f_{\mu_{th}}(2\mu)$ – растущая функция μ, и $(0 \le P(\mu) \le 1)$, получаем

$$n_G = n\int_{\mu_c}^{\infty} P(\mu) f_{\mu_{th}}(2\mu) d\mu \ge n f_{\mu_{th}}(2\mu_c)\int_{\mu_c}^{\infty} P(\mu) d\mu,$$

$$\int_{\mu_c}^{\infty} P(\mu) d\mu \le \delta_G, \quad \int_0^{\mu_c} P(\mu) d\mu \ge 1 - \delta_G,$$

где $\delta_G = \frac{n_G}{n f_{\mu_{th}}(2\mu_c)}$ – доля зарегистрированных ярких импульсов, подправленная неидеальностью детектора ярких импульсов. Для консервативной оценки матрицы плотности Еве получаем

$$\overline{\rho}_{XE} \to (1-\delta_G)\cdot\rho_{XE}(\mu_c) + \delta_G\cdot\rho_{XX},$$

для условной энтропии и длины секретного ключа $r = \lim_{n\to\infty}\frac{R_n}{n}$ в пересчете на одну посылку,

$$H(\overline{\rho}_{XE}|\overline{\rho}_E) = (1-\delta_G)\cdot H(\rho_{XE}(\mu_c)|\rho_E(\mu_c)) +$$

$$+\,\delta_G\cdot H(\rho_{XX}|\rho_X), \quad H(\rho_{XX}|\rho_X) = 0,$$

$$r \ge (1-\delta_G)\cdot H(\rho_{XE}(\mu_c)|\rho_E(\mu_c)) - \mathrm{leak}. \quad (3)$$

Вся информация об используемом протоколе распределения ключей и атаках Евы на квантовый канал связи заключена во втором сомножителе – нехватка информации Евы о ключе. Первый сомножитель дает изменение длины ключа при регистрации n_G ярких импульсов. Последнее слагаемое есть уменьшение длины ключа за счет информации (в пересчете на посылку), выдаваемой в открытый классический канал при коррекции ошибок. *Данная формула носит универсальный характер – не зависит от протокола, и справедлива при любой аппаратной пороговой функции.* Нужно отметить, что данная длина ключа получается следующим образом. Пусть передана последовательность длины n (при совпадающих базисах). Далее, при коррекции ошибок, публично раскрывается $n\cdot\mathrm{leak}$ бит. Пусть зарегистрировано n_G ярких входных импульсов. После вычисления $n\cdot r$ производится сжатие (хеширование универсальными функциями второго порядка [5]) битовой строки длиной n до строки длины $n\cdot r$, которая и есть секретный ключ.

Экспериментальная реализация. Блок-схема детектора входных импульсов у клиента показана на рис. 1. Фототок лавинного фотодиода (APD), работающего в линейном режиме, усиливается зарядовочувствительным усилителем (CIA) с постоянной времени разряда ≈ 30 нс (для оптической разности хода ≈ 10 нс и времени между посылками не менее 100 нс). Амплитуда сигнала на выходе CIA пропорциональна суммарной энергии в двух оптических импульсах и показана на осциллограммах на рис. 2. Далее сигнал с CIA поступает на компараторы C1, 2. C1 предназначен для выработки импульса синхронизации, а C2 – для детектирования ярких импульсов. При превышении заданного порога на выходе C1, 2 формируется выходной сигнал, который запускает одновибраторы PG1, 2, а также поступает в ПЛИС для измере-

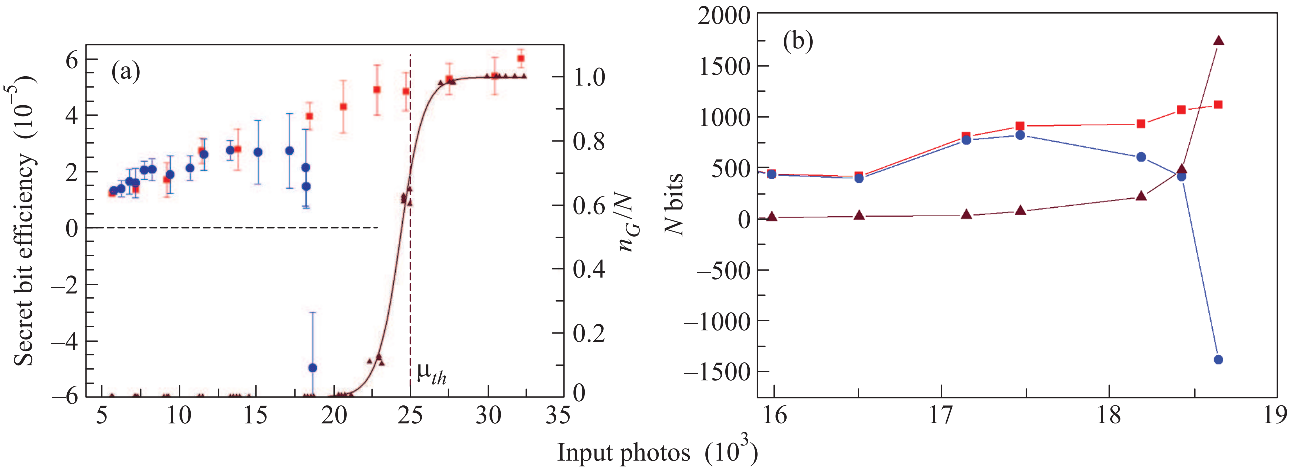

Рис. 3. (Цветной онлайн) Зависимости длины секретного ключа и пороговой функции в зависимости *от числа фотонов в паре импульсов* на входе клиента (*Input photons*). (a) – Secret bit efficiency – r (3) – доля секретных бит в пересчете на одну посылку в серии из $N = 27962000$ посылок. Квадратными маркерами показана нормированная длина секретного ключа r без учета вычитания ярких импульсов ((3) без первого множителя). Круглыми маркерами показана нормированная длина секретного ключа r с учетом ярких импульсов (3). Каждая точка получалась усреднением по 5 сериям посылок N. Сплошной линией показана нормированная (n_G/N) аппаратная пороговая функция. Коэффициент аттенюации на стороне клиента равен $att = 3.1 \cdot 10^4$. Значение порога $\mu_{th} = N_c/att = 25 \cdot 10^3/3.1 \cdot 10^4 = 0.8$ фотонов *на два импульса*, в каждом импульсе не более $\mu_c = 0.4$ фотона (см. пояснения в тексте). При обработке сырого ключа системой использовалось значение $\mu_c = 0.4$ (3). Треугольными маркерами показано число регистрируемых ярких импульсов. Значение аппаратной пороговой функции $f_{\mu_{th}}(\mu)$ в пороге равно $f_{\mu_{th}}(\mu_{th}) = 0.7$. (b) – Детальная зависимость длины секретного ключа от числа зарегистрированных ярких импульсов. Треугольные маркеры – число зарегистрированных ярких импульсов в серии $N = 27962000$ послылок. Число секретных бит из серии посылок $N = 27962000$: квадратные маркеры – без вычитания ярких импульсов, круглые маркеры – с учетом вычитания ярких импульсов. Длина ключа r вычислялась по формуле (11) [6]. Отрицательная длина ключа (3) и, соответственно, секретная эффективность означают невозможность сгенерировать секретный ключ при числе ярких импульсов больше критического

ния его длительности. Использование APD позволяет уменьшить интенсивность входных импульсов и, соответственно, засветок, связанных с отражениями и рэлеевским рассеянием в линии. Нужно отметить следующие важные моменты.

1. Импульсы синхронизации вырабатываются на каждый входной импульс и подсчитываются в ПЛИС для сравнения с общим числом импульсов, посланных сервером в данной серии. При несовпадении числа синхроимпульсов текущая серия не используется.

2. Согласно исходной последовательности, информационная фаза накладывается клиентом случайно на разные импульсы (L или R, рис. 1). Это запрещает Еве перераспределять энергию между двумя импульсами, чтобы иметь возможность получить на выходе информационный импульс с удвоенной интенсивностью. Если бы фаза выставлялась всегда на один импульс, то Ева могла бы вместо двух импульсов послать один с удвоенной интенсивностью, чтобы затем на выходе “считать” с него фазу, а второй сколь угодно слабый, чтобы сохранить суммарную энергию ниже порога и, соответственно, недетектируемость вторжения. В этом случае пришлось бы выбрать порог $\mu_{th} = \mu_c/2$ и снижать интенсивность рабочих импульсов, что привело бы к уменьшению эффективности генерации секретных ключей.

Измерение аппаратной пороговой функции в канале ярких импульсов. Для определения длины секретного ключа требуется знание аппаратной пороговой функции $f_{\mu_{th}}(2\mu)$. Для ее измерения, при фиксированном пороге Th2, на вход подавались серии импульсов калиброванной интенсивности (задано μ) и производился подсчет регистрируемых ярких импульсов. Характерный вид пороговой кривой приведен на рис. 3. Таким образом, величине порога Th2 может быть поставлено в соответствие число фотонов на входе клиента. Измерение пороговой характеристики до начала генерации серии информационных импульсов позволяет оценить среднее число фотонов в импульсе, приходящее к клиенту, и оперативно следить за пропусканием линии.

Моделирование атаки с яркими состояниями. Связь длины ключа с порогом, числом ярких импульсов и числом фотонов в линии. При конфигурировании системы, для заданной длины линии связи, на стороне сервера выбирается такая интенсивность в каждой посылке, которая обеспечивает устойчивую синхронизацию на стороне клиента. При этом среднее входное число фотонов может быть измерено непосредственно или по пороговой характеристике. Затем выбирается коэффициент ослабления на стороне клиента, чтобы при этой интенсивности в линию выходило $\mu \approx 0.3$ фотона в импульсе. Данное число фотонов обеспечивает на длине линии (25 км) для протокола [6] оптимальную скорость генерации секретного ключа, в отсутствии вторжений в линию. И, наконец, устанавливается минимальное значение порога регистрации ярких импульсов, при котором они отсутствуют.

Для описанного штатного режима работы аппаратуры клиента, атака с яркими состояниями моделировалась следующим образом. Сервер посылает в линию состояния с различной интенсивностью, в том числе выше штатной. Наличие ярких импульсов приведет к их регистрации, что будет учтено при получении секретного ключа (см. выше). Чем больше число регистрируемых ярких импульсов (n_G), тем меньшую длину секретного ключа можно получить (см. рис. 3). При некотором критическом числе ярких импульсов, длина секретного ключа становится отрицательной, что означает невозможность сгенерировать ключ. *Важно, что система гарантирует секретность ключа, даже при наличии ярких импульсов. Т.е. никогда не будет такой ситуации, что ключ получен, а на самом деле он не секретен. Если ключ получен (его длина больше нуля), то он секретен, что гарантируется системой (см. анализ выше).*

Главное требование к системам квантовой криптографии состоит в доказуемой гарантии секретности ключей. Скорость генерации также важна, но это вторичное, по отношению к секретности, требование. Скорость генерации определяется первым слагаемым в (3), которое содержит два сомножителя. На рис. 3 приведены зависимости (r) эффективности генерации секретного ключа при различных значениях входной интенсивности на сторону клиента на реальной системе с длиной канала связи 25 км (см. [7]). Генерация ключа происходила по протоколу на геометрически однородных состояниях с четырьмя базисами (см. детали в [6]). Данный протокол устойчив к потерям и гарантирует секретность ключей вплоть до потерь 0.999 (напомним, что длина линии в 100 км стандартного одномодового волокна с потерями 0.2 дБ/км дает потери 0.99). Контроль ярких входных импульсов не позволяет подслушивателю “подсунуть” более интенсивные состояния. Из-за того, что пороговая функция не есть ступенчатая функция, при надлежащем выборе порога система начинает с определенной вероятностью регистрировать яркие состояния еще до достижения порога.

Заключение.

1. В системе Clavis-2 *серии посылок, в которых зарегистрированы яркие состояния целиком выкидываются* [4]. Более аккуратный анализ (см. выше) показывает, что регистрация n_G ярких импульсов, хоть и ведет к уменьшению длины секретного ключа (3), но не обнуляет его (при числе ярких импульсов меньше критического), что принципиально. *Даже если в каждой серии есть яркие импульсы (но их число меньше критического), то генерация ключа продолжается, при этом гарантируется его секретность, что принципиально.* Длина ключа явно зависит от реализации – аппаратной пороговой функции $f_{\mu_{th}}(2\mu)$.

2. В отличии от Clavis-2, где используется два детектора, и протоколы BB84 и SARG [4], которые подвержены еще и атакам с ослеплением одного из двух детекторов [8], а также атаке *detectors mismatch* (основанной на разных свойствах детекторов [9]), наша система не подвержена данным атакам, т.к. в системе один детектор и устойчивый к данным атакам протокол.

3. Протокол на геометрически однородных состояниях [6] с четырьмя базисами гарантирует секретность ключей вплоть до полных потерь 0.999, которые включают потери и в приемной части системы, в отличие от [2].

Авторы благодарят И.В. Радченко за полезные подробности, касающиеся работы, “вскрытия” системы Clavis-2, и обсуждение атак на аппаратуру двухпроходных квантово-криптографических систем. Работа выполнена при поддержке гранта РНФ # 16-12-00015.

---

1. D. S. Bethune and W. P. Risk, New J. Phys. **4**, 42.1 (2002).
2. A. Müller, T. Herzog, B. Hüttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
3. I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Laser. Phys. Lett. **11**, 065203 (2014).

4. S. Sajeed, I. Radchenko, S. Kaiser, J.-Ph. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015); arXiv:1412.8032 [quant-ph].
5. R. Renner, arXiv:0512258 [quant-ph].
6. С. Н. Молотков, Письма в ЖЭТФ **101**, 579 (2015).
7. К. А. Балыгин, А. Н. Климов, С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **103**, 496 (2016).
8. V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, arXiv:1009:2663 [quant-ph].