ЖЭТФ, 2019, том 155, вып. 1, стр. 54–61

СОХРАНЕНИЕ ЭНЕРГИИ ПРИ РАСПРЕДЕЛЕННОЙ ИНТЕРФЕРЕНЦИИ — ГАРАНТИЯ ДЕТЕКТИРОВАНИЯ АТАКИ С ОСЛЕПЛЕНИЕМ ДЕТЕКТОРОВ В КВАНТОВОЙ КРИПТОГРАФИИ

С. Н. Молотков*

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Академия криптографии Российской Федерации
121552, Москва, Россия

Факультет вычислительной математики и кибернетики,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 30 августа 2018 г.,
после переработки 30 августа 2018 г.
Принята к публикации 4 сентября 2018 г.

Атака с ослеплением лавинных однофотонных детекторов является одним из методов квантового хакинга систем квантового распределения ключей (КРК). Атака была экспериментально продемонстрирована для различных систем КРК, использующих как фазовое, так и поляризационное кодирование. При такой атаке подслушиватель знает весь ключ, не производит ошибок и не детектируется. Однако при фазовом кодировании некоторые существенные особенности статистики фотоотсчетов на приемной стороне не были учтены. В работе показано на уровне фундаментальных принципов, что в системах с фазовым кодированием данная атака приводит к изменению статистики фотоотсчетов и детектированию подслушивателя. Получены выражения для длины секретного ключа при такой атаке. При этом не требуется никаких изменений в конструкции и управляющей электронике системы КРК с фазовым кодированием, а достаточно лишь изменений при обработке результатов регистрации квантовых состояний. В то же время уязвимость и компрометация секретных ключей в системах КРК с поляризационным кодированием являются существующим фактом, а не потенциальной угрозой.

DOI: 10.1134/S0044451019010048

1. ВВЕДЕНИЕ

Секретность ключей в квантовой криптографии гарантируется фундаментальными запретами квантовой механики на различимость квантовых состояний, а не техническими или вычислительными ограничениями подслушивателя. Поэтому часто говорится, что квантовая криптография обеспечивает безусловную секретность ключей. Однако нужно понимать, что данное утверждение подразумевает, что подслушиватель не имеет прямого или даже косвенного доступа к передающей и приемной аппаратуре, где происходит приготовление и детектирование квантовых состояний. Когда подслушиватель имеет доступ только к передаваемым квантовым состояниям в канале связи, безусловная секретность действительно имеет место. Атаки на квантовые состояния в канале связи подробно исследовались, поэтому можно считать, что в этом случае безусловная секретность доказана для ряда протоколов квантового распределения ключей. Системы квантового распределения ключей (КРК) являются открытыми системами. Подслушиватель может внешним излучением зондировать состояние фазовых модуляторов, модуляторов интенсивности, лавинных однофотонных детекторов и пр., которые несут информацию о передаваемом ключе. Одним из критических элементов является однофотонный лавинный детектор (APD). Было экспериментально продемонстрировано на различных системах КРК, что они уязвимы

* E-mail: sergei.molotkov@gmail.com

относительно атаки с ослеплением лавинных детекторов [1–16]. При такой атаке Ева знает весь ключ, не производит ошибок на приемной стороне и не детектируется, система не гарантирует секретность ключей. Данная атака реализуется на сегодняшнем технологическом уровне, в отличие от других потенциальных атак, которые требуют, например, долгосрочной квантовой памяти.

Исходно атака с ослеплением детекторов была придумана для КРК с поляризационным кодированием, впоследствии по инерции была перенесена и на системы с фазовым кодированием. В результате ошибочно считается, что все системы КРК уязвимы.

В литературе возникли дискуссии о том, как противодействовать атаке с ослеплением детекторов. Были предложены технические изменения системы детектирования путем изменения нагрузочных сопротивлений, порога дискриминации, случайного изменения квантовой эффективности лавинных детекторов и пр. [16–19].

Попытки «решения» проблемы уязвимости по отношению к атаке с ослеплением на уровне технических изменений переводят системы КРК, которые должны гарантировать безусловную секретность ключей, в разряд систем, которые обеспечивают секретность лишь за счет технических ограничений подслушивателя. Поэтому проблема ослепления должна быть решена на уровне фундаментальных законов природы, а не на уровне технических «заплаток».

Ниже будет показано, что атака с ослеплением всегда детектируется в системах КРК, которые используют фазовый принцип кодирования. Атака детектируется по изменению статистики фотоотсчетов в боковых временны́х окнах при распределенной интерференции, что является следствием сохранения энергии — эквивалентно нормировке квантовых состояний (см. ниже) при распределенной в пространстве и времени интерференции. Изменение статистики отсчетов учитывается при обработке первичных ключей. Если изменение статистики не превышает некоторой критической величины, то можно получить ключ и гарантировать его секретность. При превышении изменений статистики фотоотсчетов выше критической величины секретный ключ получить нельзя. То есть никогда не будет ситуации, при которой ключ получен и считается секретным, а на самом деле таковым не является. В то же время системы КРК с поляризационным кодированием не обладают таким свойством и остаются уязвимыми по отношению к атаке с ослеплением лавинных детекторов.

2. ОБЩАЯ ИДЕЯ АТАКИ С ОСЛЕПЛЕНИЕМ ЛАВИННЫХ ДЕТЕКТОРОВ

Опишем кратко атаку с ослеплением детекторов на примере протокола BB84. Для других протоколов [4] анализ аналогичен. В протоколе BB84 квантовые состояния для 0 или 1 в каждом из двух базисов посылаются случайным образом. Базисы также выбираются равновероятно. Внутри базиса состояния ортогональны, т. е. достоверно различимы. Атака с ослеплением детекторов является вариантом атаки прием–перепосыл. Подслушиватель разрывает квантовый канал связи и использует регистрирующую аппаратуру, аналогичную аппаратуре Боба. Ева выбирает базис случайно. Возможны две ситуации для тех посылок, где базисы Алисы и Боба совпадают, так как остаются только те посылки, где их базисы совпадали: 1) базис Евы совпадает с базисом Алисы–Боба; 2) базис Евы не совпадает с базисом Алисы–Боба.

Вторая часть аппаратуры Евы используется для перепосылки подмененных состояний (fake states). Ева ослепляет лавинные детекторы Боба постоянным излучением лазера и перепосылает то состояние, которое она получила в результате измерений в выбранном ей базисе, но с другим числом фотонов (см. ниже).

В ситуации 1) Ева при измерении получает правильное состояние Алисы. Перепосыл состояния не приводит к ошибкам на стороне Боба.

В ситуации 2) Ева получает равновероятно результат 0 или 1 в неправильном базисе. И перепосылает то состояние, которое она получила в неправильном по отношению к Алисе–Бобу базисе. Если не ослеплять лавинные детекторы, то перепосыл состояний 0 или 1 в неправильном базисе с вероятностью 50 % приведет к ошибкам у Боба.

Цель атаки Евы — сделать так, чтобы перепосланные состояния в неправильном базисе вообще не производили отсчетов у Боба, а в случае совпадения базисов детекторы производили отсчеты. Данная цель достигается ослеплением лавинных детекторов.

3. ПРИНЦИП ОСЛЕПЛЕНИЯ ЛАВИННЫХ ДЕТЕКТОРОВ

В системах КРК в качестве однофотонных детекторов обычно используют лавинные фотодетекторы с низкими темновыми шумами, работающие в стробируемом режиме. В этом режиме на детек-

тор постоянно подается обратное смещение (U_{bias}, см. рис. *а*) через балластное сопротивление R_B, величина которого ниже напряжения пробоя. При этом детектор заперт и ток через него практически не течет (кроме темнового тока). В тот момент, когда ожидается прилет фотона, дополнительно к постоянному смещению на детектор подается короткий стробирующий импульс с амплитудой (U_{gate}), достаточной для выхода детектора в пробойный режим.

Когда на детектор попадает излучение, через него начинает протекать ток. Ток течет и через балластное сопротивление R_B, на котором падает напряжение $U_B = IR_B$. Полное напряжение на детекторе и балластном сопротивлении постоянно ($U_{APD} + U_B = U_{bias}$). Протекание тока через APD приводит к падению напряжения на нем. Начиная с некоторой интенсивности, ток через детектор приводит к падению напряжения, достаточному, чтобы импульс строба не переводил детектор в пробойный режим. Это ведет к тому, что APD переходит в линейный режим и становится не чувствительным к одиночным фотонам. В этом режиме амплитуда выходного электрического сигнала пропорциональна мощности входного оптического сигнала.

Ослепление детектора представляет собой подсветку детектора постоянным излучением мощностью, достаточной для перевода детектора в линейный режим. Подсветка импульсным излучением на фоне засветки приводит к изменению тока через детектор и выделению на нагрузочном сопротивлении сигнала, пропорционального мощности в импульсе.

Здесь важно отметить следующее: сигнал регистрируется только тогда, когда амплитуда импульса на входе дискриминатора (Discr.) превышает установленный порог, $U_b > U_{discr}$. Порог обычно устанавливается чуть выше уровня шумов. Сигнал регистрации возникает, если уровень оптического сигнала на фоне ослепляющего постоянного излучения превышает некоторую величину, $P > P_{th}$. Если уровень сигнала ниже порога, $P < P_{th}$, то сигнал регистрации отсутствует — детектор ослеплен.

Ниже будет показано, что для систем КРК с фазовым кодированием для того, чтобы атака с ослеплением не детектировалась, необходимо одновременно удовлетворить двум взаимоисключающим условиям: $P_f > P_{th}$ и $P_f/2 < P_{th}$ (P_f — интенсивность подмененного состояния (fake state)), что является следствием сохранения энергии — эквивалентно нормировке квантового состояния при распределенной интерференции.

4. ФАЗОВОЕ КОДИРОВАНИЕ В СИСТЕМАХ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Для демонстрации этого факта необходимо напомнить, как устроено фазовое кодирование в системах КРК на примере протокола BB84. В реальных системах КРК используется сильно ослабленное когерентное состояние. В канал поступают информационные состояния $|\alpha\rangle_1 \otimes |e^{i\varphi_A}\alpha\rangle_2$, где относительная фаза когерентных состояний, локализованных во временны́х окнах 1 и 2 (рис. *б,в*) равна

$$\begin{cases} 0^+ \to \varphi_A = 0, \\ 1^+ \to \varphi_A = \pi, \end{cases} \qquad \begin{cases} 0^\times \to \varphi_A = \dfrac{\pi}{2}, \\ 1^\times \to \varphi_A = \dfrac{3\pi}{2}. \end{cases}$$

На приемной стороне базис выбирается случайно: либо $+$, либо $\times$. В базисе $+$ относительная фаза $\varphi_B = 0$, в базисе $\times$ относительная фаза $\varphi_B = \pi/2$.

Перед детектированием состояния подвергаются преобразованию на интерферометре Маха – Цандера (МЦ, рис. *б,в*), который является унитарным преобразователем. При совпадающих базисах Алисы и Боба на входе в детекторы состояния имеют следующий вид, если Алиса посылала 0^+:

$$\begin{cases} \left|\frac{\alpha}{2}\right\rangle_1 \otimes |\alpha\rangle_2 \otimes \left|\frac{\alpha}{2}\right\rangle_3 \to D_1, \\ \left|\frac{\alpha}{2}\right\rangle_1 \otimes |\mathrm{vac}\rangle_2 \otimes \left|\frac{\alpha}{2}\right\rangle_3 \to D_2, \end{cases} \qquad \begin{cases} \left|\frac{\alpha}{2}\right\rangle_1 \to \frac{1}{4}\mathrm{Pr}_{detect}, & |\alpha\rangle_2 \to \mathrm{Pr}_{detect}, & \left|\frac{\alpha}{2}\right\rangle_3 \to \frac{1}{4}\mathrm{Pr}_{detect} : & D_1 \\ \left|\frac{\alpha}{2}\right\rangle_1 \to \frac{1}{4}\mathrm{Pr}_{detect}, & |\mathrm{vac}\rangle_2 \to 0, & \left|\frac{\alpha}{2}\right\rangle_3 \to \frac{1}{4}\mathrm{Pr}_{detect} : & D_2 \end{cases} . \quad (1)$$

Аналогично, если Алиса посылала состояние 1^+:

$$\begin{cases} \left|\frac{\alpha}{2}\right\rangle_1 \otimes |\mathrm{vac}\rangle_2 \otimes \left|\frac{\alpha}{2}\right\rangle_3 \to D_1, \\ \left|\frac{\alpha}{2}\right\rangle_1 \otimes |\alpha\rangle_2 \otimes \left|\frac{\alpha}{2}\right\rangle_3 \to D_2, \end{cases} \qquad \begin{cases} \left|\frac{\alpha}{2}\right\rangle_1 \to \frac{1}{4}\mathrm{Pr}_{detect}, & |\mathrm{vac}\rangle_2 \to 0, & \left|\frac{\alpha}{2}\right\rangle_3 \to \frac{1}{4}\mathrm{Pr}_{detect} : & D_1 \\ \left|\frac{\alpha}{2}\right\rangle_1 \to \frac{1}{4}\mathrm{Pr}_{detect}, & |\alpha\rangle_2 \to \mathrm{Pr}_{detect}, & \left|\frac{\alpha}{2}\right\rangle_3 \to \frac{1}{4}\mathrm{Pr}_{detect} : & D_2 \end{cases} . \quad (2)$$

Аналогичные выражения имеют место при совпадающих базисах $\times$. При не совпадающих базисах находим

$$\begin{cases} \left|\frac{\alpha}{2}\right\rangle_1 \otimes \left|\frac{\alpha}{\sqrt{2}}\right\rangle_2 \otimes \left|\frac{\alpha}{2}\right\rangle_3 \to D_1, \\ \left|\frac{\alpha}{2}\right\rangle_1 \otimes \left|\frac{\alpha}{\sqrt{2}}\right\rangle_2 \otimes \left|\frac{\alpha}{2}\right\rangle_3 \to D_2, \end{cases} \quad \begin{cases} \left|\frac{\alpha}{2}\right\rangle_1 \to \frac{1}{4}\mathrm{Pr}_{detect}, \quad \left|\frac{\alpha}{\sqrt{2}}\right\rangle_2 \to \frac{1}{2}\mathrm{Pr}_{detect}, \quad \left|\frac{\alpha}{2}\right\rangle_3 \to \frac{1}{4}\mathrm{Pr}_{detect} : D_1 \\ \left|\frac{\alpha}{2}\right\rangle_1 \to \frac{1}{4}\mathrm{Pr}_{detect}, \quad \left|\frac{\alpha}{\sqrt{2}}\right\rangle_2 \to \frac{1}{2}\mathrm{Pr}_{detect}, \quad \left|\frac{\alpha}{2}\right\rangle_3 \to \frac{1}{4}\mathrm{Pr}_{detect} : D_2 \end{cases}. \quad (3)$$

Вероятность детектирования (1), (2) во временны́х окнах 1, 2 и 3 при совпадающих базисах ($|\alpha|^2$ — среднее число фотонов в состоянии, см. рисунок): в боковых окнах 1 и 3 $\mathrm{Pr}_{detect} \propto |\alpha|^2/4$, в информационном окне 2 на детекторе, где имеет место конструктивная интерференция, $\mathrm{Pr}_{detect} \propto |\alpha|^2$, на втором детекторе, где возникает деструктивная интерференция, $\mathrm{Pr}_{detect} \equiv 0$.

Независимо от того, совпадают или нет базис входных состояний и базис на приемной стороне, вероятности детектирования (3) в боковых окнах 1 и 3 равны, $\mathrm{Pr}_{detect} \propto |\alpha|^2/4$, так как эти окна не подвержены интерференции на интерферометре МЦ. В информационном окне 2 сумма вероятностей детектирования на обоих детекторах, $\mathrm{Pr}_{detect} \propto |\alpha|^2/2$, есть константа.

Интерферометр МЦ является унитарным преобразователем. Отсюда следует, что отношение суммы вероятностей фотоотсчетов в центральном временно́м окне 2 в двух детекторах к вероятности отсчетов в любом боковом окне и на любом детекторе должно быть равно 1/4 (чтобы не загромождать выкладки, считаем, что квантовые эффективности детекторов одинаковы, все дальнейшее обобщается на случай детекторов с разной эффективностью). Фактически, это фундаментальное следствие унитарности, а в данном контексте это сохранение полной энергии на входе и выходе интерферометра МЦ, или, что эквивалентно, сохранение нормировки квантовых состояний. На входе интерферометра МЦ энергия состояния в двух временны́х окнах есть $|\alpha|^2 + |\alpha|^2$. На обоих выходах интерферометра сумма энергий состояний по всем временны́м окнам равна: (боковые окна) $4(|\alpha|^2/4)$ + (центральные окна) $|\alpha_u|^2 + |\alpha_d|^2 = |\alpha|^2$. Здесь $|\alpha_u|^2 = |\alpha|^2 \cos^2(\varphi/2)$ — среднее число фотонов на верхнем детекторе, $|\alpha_d|^2 = |\alpha|^2 \sin^2(\varphi/2)$ — на нижнем, φ — разность фаз, набираемая состояниями при проходе по верхнему и нижнему плечам интерферометра (см. (1)–(3)). При идеальной интерференции $\varphi = 0$ — максимум на нижнем детекторе, или $\varphi = \pi$ — максимум на верхнем детекторе. Сумма интенсивностей по двум детекторам в центральном временно́м окне всегда есть константа $|\alpha|^2$.

Таким образом, энергия состояний на входе интерферометра в двух временны́х окнах распределяется по трем временны́м окнам на двух выходах интерферометра. Суммарная энергия по всем временны́м окнам на двух выходах интерферометра всегда равна энергии на входе, что является проявлением закона сохранения энергии при распределенной интерференции. В квантовой физике интерферометр МЦ является унитарным преобразователем, что гарантирует сохранение суммарной нормировки квантовых состояний на выходах интерферометра при распределенной интерференции.

5. СОХРАНЕНИЕ ЭНЕРГИИ ПРИ РАСПРЕДЕЛЕННОЙ ИНТЕРФЕРЕНЦИИ И ДЕТЕКТИРОВАНИЕ АТАКИ

Ева всегда перепосылает те состояния, которые она получила, т. е. состояния вида $|\alpha_E\rangle_1 \otimes |e^{i\varphi_E}\alpha_E\rangle_2$, фаза φ_E выбирается в соответствии с (1), (2) и с тем, какой исход получен. Среднее число фотонов $|\alpha_E|^2$ в состоянии выбирается таким, чтобы в случае совпадения базисов подслушивателя и легитимных пользователей в центральном временно́м окне 2 (см. рисунок) имел место фотоотсчет. Для этого интенсивность должна быть $|\alpha_E|^2 > P_{th}$. Если базисы не совпадали, то в этом случае в центральном временно́м окне (см. (3)) не будет идеальной конструктивной и идеальной деструктивной интерференции на обоих детекторах. На оба детектора приходят состояния с одинаковым средним числом фотонов $(1/2)|\alpha_E|^2$. Если интенсивность состояний такова, что $(1/2)|\alpha_E|^2 < P_{th}$, то отсчетов не будет. Соответственно, при несовпадении базисов не будет и ошибок на приемной стороне. Таким образом, если лавинный детектор ослеплен, то при регистрации только в центральном временно́м окне при перепосыле состояний с интенсивностью $(1/2)|\alpha_E|^2 < P_{th}$ и $|\alpha_E|^2 > P_{th}$ ошибочных отсчетов не будет. Отсчеты будут только в тех посылках, в которых базисы Алисы–Боба и Евы совпадали. В этих посылках подслушиватель знает все передаваемые состояния, не производит ошибок на приемной стороне и не детектируется. Система КРК оказывается не

секретной. Однако, если дополнить протокол измерениями в боковых окнах 1 и 3 на любом лавинном детекторе, то атака с ослеплением всегда детектируется. Если интенсивность подмененных состояний (fake states) выбрана так, что $P_{th} < |\alpha_E|^2 < 2P_{th}$, то отсчетов в боковых временны́х окнах (где интенсивность равна $(1/4)|\alpha_E|^2 < P_{th}$ независимо от того, совпадают или нет базисы Алисы–Боба и Евы) не будет, поскольку интенсивность на детекторах равна $(1/4)|\alpha_E|^2 < P_{th}$, что заведомо меньше пороговой величины (см. (1)–(3)), начиная с которой возникают фотоотсчеты. При ослеплении детекторов интенсивность подмененных состояний удовлетворяет условию $P_{th} < |\alpha_E|^2 < 2P_{th}$, при этом отсчеты в боковых окнах 1 и 3 полностью исчезают, т. е. соотношение вероятностей отсчетов в центральном информационном временно́м окне и боковых окнах изменяется. Таким образом, при фазовом кодировании подслушиватель не может не производить ошибок и не изменять статистику фотоотсчетов с учетом отсчетов в боковых временны́х окнах.

При несовпадающих базисах отсчетов при интенсивности $(1/2)|\alpha_E|^2$ не должно быть, т. е. $(1/2)|\alpha_E|^2 < P_{th}$. При совпадающих базисах интенсивность на детекторе равна $|\alpha_E|^2$, при этом должны быть отсчеты, так как $|\alpha_E|^2 > P_{th}$. Интенсивность в боковых временны́х окнах равна $(1/4)|\alpha_E|^2$ и не зависит от интерференции, т. е. от совпадения или несовпадения базисов Алисы–Боба и Евы, поэтому ослепление детекторов приведет к полному отсутствию фотоотсчетов, если требовать отсутствия ошибок при несовпадающих базисах, т. е. соблюдения условия $P_{th} < |\alpha_E|^2 < 2P_{th}$.

Таким образом, два условия: 1) отсутствие ошибок в центральном временно́м окне — $P_{th} < |\alpha_E|^2 < 2P_{th}$; 2) сохранение отношения вероятностей в боковых окнах и центральном временно́м окне — $|\alpha_E|^2 > 4P_{th}$, оказываются очевидно несовместимыми. Откуда следует, что подслушиватель принципиально не может знать весь ключ и не изменять статистики фотоотсчетов, т. е. оставаться недетектируемым. При этом в системах КРК с фазовым кодированием это гарантируется на уровне фундаментальных принципов, а не технических «заплаток» в системе.

6. ДЛИНА СЕКРЕТНОГО КЛЮЧА В АСИМПТОТИЧЕСКОМ ПРЕДЕЛЕ ДЛИННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПРИ АТАКЕ С ОСЛЕПЛЕНИЕМ ДЕТЕКТОРОВ

Не существует универсального метода вычисления длины секретного ключа для всех видов атак. Поэтому нужно проверять всевозможные атаки, вычислять для них длину ключа и выбирать минимальную по разным атакам. После детектирования атаки возникает вопрос: можно ли получить секретный ключ и какой длины? Общая формула для длины секретного ключа безотносительно к типу атаки имеет вид [20]

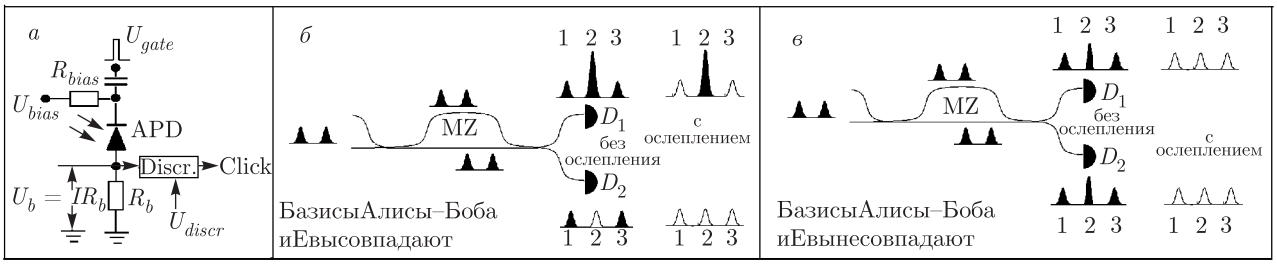
$$\ell_n = n\left(H^{\varepsilon}_{min}(X|E) - \mathrm{leak}_n\right), \tag{4}$$

где n — число зарегистрированных посылок в совпадающих базисах, $leak_n$ — число битов, израсходованных на коррекцию ошибок в первичных ключах, ε — параметр секретности, который назначается легитимными пользователями, $H^{\varepsilon}_{min}(X|E)$ — сглаженная минимальная энтропия (см. детали в [20]), содержащая всю информацию об атаке Евы. Неформально $H^{\varepsilon}_{min}(X|E)$ дает нехватку информации Евы в битах в пересчете на посылку о битовой строке длины n. Атака с ослеплением является атакой прием–перепосыл. Ева случайным образом в каждой из зарегистрированных посылок с вероятностью q решает, ослеплять детекторы или нет. Параметр q известен только Еве. Проявлением атаки служит изменение доли фотоотсчетов в боковых временны́х окнах по отношению к доле в центральном временно́м окне. Без ослепления отношение вероятности отсчета в боковом окне к вероятности в центральном окне должно быть 1/4.

Сначала рассмотрим асимптотический предел длинных последовательностей, $n \to \infty$, в этом пределе параметр q — вероятность отсчетов в центральном окне — известен точно, поскольку нет флуктуаций, связанных с конечной длиной. По сути, имеет место бернуллиевская схема испытаний. В доле зарегистрированных посылок q детекторы ослеплялись, а в доле $1-q$ — нет. То есть в nq посылках биты ключа известны, в $n(1-q)$ посылках — неизвестны. Отношение числа отсутствующих отсчетов в боковых окнах n_{side} к суммарному числу зарегистрированных отсчетов в центральных временны́х окнах в обоих детекторах (при этом неточность балансировки интерферометра не важна, так как суммарное число отсчетов в обоих детекторах есть константа, что дает

$$\lim_{n\to\infty} \frac{n_{side}}{n} = \frac{1}{4}q.$$

Соответственно для матрицы плотности Алиса–Ева имеем



а) Функциональная схема включения лавинного детектора (APD), R_b — нагрузочное сопротивление (типичные значения 50–100 Ом), с которого снимается напряжение — сигнал детектирования U_b; Discr. — дискриминатор, значение порогового напряжения дискриминации 10–100 мВ; U_{gate} — импульс стробирующего напряжения. *б*) Фотоотсчеты при фазовом кодировании в различных временны́х окнах на лавинном детекторе при совпадающих базисах Алисы–Боба и Евы без ослепления и с ослеплением детекторов. Временное окно 2 является информационным окном. Вероятность фотоотсчета зависит от интерференции состояний, прошедших по верхнему и нижнему путям интерферометра Маха – Цандера (MZ); D_1 и D_2 — лавинные детекторы. Фотоотсчеты во временны́х окнах 1 и 3 не зависят от выбора базиса. *в*) Фотоотсчеты в различных временны́х окнах без ослепления и с ослеплением детекторов, при не совпадающих базисах Алисы–Боба и Евы

$$\rho_{XE}(q) = \frac{1}{2}q \times$$
$$\times \{|0\rangle_{XX}\langle 0| \otimes |0\rangle_{EE}\langle 0| + |1\rangle_{XX}\langle 1| \otimes |1\rangle_{EE}\langle 1|\} +$$
$$+ \frac{1}{2}(1-q)\left\{|0\rangle_{XX}\langle 0| \otimes \frac{|0\rangle_{EE}\langle 0| + |1\rangle_{EE}\langle 1|}{2} + \right.$$
$$\left. + |1\rangle_{XX}\langle 1| \otimes \frac{|0\rangle_{EE}\langle 0| + |1\rangle_{EE}\langle 1|}{2}\right\}, \quad (5)$$

где $|0,1\rangle_X$ — состояния Алисы для 0 и 1, $|0,1\rangle_E$ — состояния Евы. В первом слагаемом, которое отвечает ситуации с ослеплением детекторов, соответствие между битами Алисы и Евы однозначное. Во втором слагаемом, которое отвечает за ситуацию без ослепления детекторов, каждому биту Алисы равновероятно отвечает 0 или 1 у Евы. Это означает, что в этих посылках Ева может только угадывать передаваемый бит Алисы.

Согласно [20], длина ключа в асимптотическом пределе бесконечно длинных последовательностей имеет вид

$$\lim_{n\to\infty}\left(\frac{\ell_n}{n}\right) = \lim_{n\to\infty}\frac{1}{n}\left(H(\rho_{XE}^{n\otimes}\rho_E^{n\otimes}) - \mathrm{leak}_n\right) =$$
$$= 1 - q - \mathrm{leak}, \quad (6)$$

где leak — информация на посылку, затраченная на исправление ошибок, которые могут возникать, например, за счет неточной балансировки интерферометра и других неидеальностей аппаратуры.

7. ДЛИНА СЕКРЕТНОГО КЛЮЧА ПРИ КОНЕЧНОЙ ДЛИНЕ ПОСЛЕДОВАТЕЛЬНОСТИ

При конечном числе n зарегистрированных отсчетов точное значение параметра q Алисе и Бобу неизвестно. В этом случае сглаженная условная минимальная энтропия определяется как

$$H_{min}^{\varepsilon}(\rho_{XE}^{n\otimes}|\rho_E^{n\otimes}) =$$
$$= \max_{\{q:\,\Pr\{|q-\overline{q}|\le\delta\}>1-\varepsilon(n,\delta)\}} H_{min}(\rho_{XE}^{n\otimes}(\overline{q})|\rho_E^{n\otimes}(\overline{q})), \quad (7)$$

где максимум определяется по тем матрицам плотности, у которых параметр $\overline{q}$ отстоит от истинного значения на величину не более δ и с вероятностью не менее $1-\varepsilon(n,\delta)$. Величина $\overline{q}$ определяется полным числом отсутствующих отсчетов в боковых окнах ($(1/4)n\overline{q}$) в последовательности длины n. Пусть истинное значение вероятности равно q. В бернуллиевской схеме при числе испытаний n число отсутствующих отсчетов в боковых окнах может быть любым от 0 до $n/4$, но с разной вероятностью. Вероятность того, что при истинном значении параметра бернуллиевской схемы q произойдет не более $\overline{k}$ отсчетов, равна

$$\Pr\{\overline{k}|n\} = \sum_{m=0}^{\overline{k}} C_n^m q^m (1-q)^{n-m},$$
$$C_n^m = \frac{n!}{m!(n-m)!}. \quad (8)$$

Соответственно, вероятность того, что число ослепленных посылок будет лежать в интервале $|k-\overline{k}| \le \delta$ есть

$$\Pr\{|q-\overline{q}|\le\delta\}=\Pr\left\{\left|\frac{k-\overline{k}}{n}\right|\le\delta\right\}>1-\varepsilon(n,\delta),$$
$$\varepsilon(n,\delta)=2e^{-2\delta^2 n},\quad \overline{q}=\frac{\overline{k}}{n},\quad q=\frac{k}{n}. \tag{9}$$

Поскольку матрицы плотности из этого множества имеют структуру тензорного произведения, в этом случае для сглаженной минимальной энтропии имеет место [20] соотношение

$$H_{min}^{\varepsilon(\delta,n)}(\rho_{XE}^{\otimes n}(q)|\rho_E^{\otimes n}(q))\ge n\left(H(\rho_{XE}(q)|\rho_E(q))-\right.$$
$$\left.-\ \mathrm{const}\cdot\sqrt{\frac{\log_2\left(\dfrac{1}{\varepsilon(\delta,n)}\right)}{n}}\right),\quad q=\overline{q}+\delta. \tag{10}$$

В итоге для длины секретного ключа получаем

$$\ell_n=n\left(1-\frac{\overline{k}}{n}-\delta(\varepsilon,n)-\mathrm{const}\cdot\sqrt{\frac{\log_2\left(\dfrac{1}{\varepsilon}\right)}{n}}\right), \tag{11}$$

где $\delta(\varepsilon,n)$ выражается через параметр ε, который задается легитимными пользователями.

8. ЗАКЛЮЧЕНИЕ

Таким образом, показано, что системы КРК с фазовым кодированием структурно устойчивы к атаке с ослеплением лавинных детекторов на уровне фундаментальных принципов, а не технических решений. При этом каких-то дополнительных технических изменений в системе КРК не требуется, достаточно лишь изменений на этапе обработки сырого ключа. Получены также выражения для длины секретного ключа в случае, когда обнаружена атака с ослеплением детекторов. Отметим, что системы КРК с поляризационным кодированием остаются уязвимыми по отношению к атаке с ослеплением лавинных детекторов, поскольку в таких системах не проводится преобразование состояний, которое приводит к распределенной интерференции — вся информация о передаваемом ключе сосредоточена в поляризации квантового состояния, локализованного в одном временном окне. По этой причине использование систем КРК с поляризационным кодированием, например, в банковской сфере [21], может привести к непредсказуемым последствиям.

Отметим, что исходная атака с ослеплением, предложенная в работах [1–15], приводит к исчезновению отсчетов в боковых временны́х окнах. Возможна модификация атаки с попыткой восстановления отсчетов в этих окнах. При модифицированной атаке подслушиватель может посылать подмененные состояния (fake states) в более ранний момент (временно́е окно на входе перед первым импульсом), а также в более поздний момент (после второго истинного импульса). Однако такая атака также детектируется, поскольку приводит к возникновению отсчетов в те моменты времени, где их не должно быть, что обнаруживается по контролю входных состояний, путем отвода части излучения на однофотонный детектор.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку и обсуждения, а также К. А. Балыгину, А. Н. Климову, С. П. Кулику, К. С. Кравцову за многочисленные и интенсивные обсуждения.

Работа поддержана проектом РНФ 16-12-00015 (продолжение).

ЛИТЕРАТУРА

1. L. Lydersen, C. Wiechers, Ch. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photon. **4**, 686 (2010); arXiv:1008.4593.

2. A. Vakhitov, V. Makarov, and Dag R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).

3. V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); arXiv:0511032.

4. V. Makarov and J. Skaar, Quant. Inf. Comp. **8**, 0622 (2008); arXiv:0702262.

5. V. Makarov, New J. Phys. **11**, 065003 (2009); arXiv: 0707.3987.

6. L. Lydersen, C. Wiechers, Ch. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photon. **4**, 801 (2010); arXiv:1012.0476.

7. L. Lydersen, C. Wiechers, Ch. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18** 27938 (2010); arXiv:1009.2663.

8. L. Lydersen, J. Skaar, and V. Makarov, J. Mod. Opt. **58**, 680 (2011); arXiv:1012.4366.

9. I. Gerhardt, Qin Liu, A. Lamas-Linares, J. Skaar, Ch. Kurtsiefer, and V. Makarov, Nature Commun. **2**, 349 (2011); arXiv:1011.0105.

10. S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, Opt. Express **19**, 23590 (2011); arXiv: 0809.3408.

11. L. Lydersen, V. Makarov, and J. Skaar, Appl. Phys. Lett. **98**, 231104 (2011).

12. L. Lydersen, M. K. Akhlaghi, A. Hamed Majedi, J. Skaar, and V. Makarov, New J. Phys. **13**, 113042 (2011); arXiv:1106.2396.

13. Qin Liu, A. Lamas-Linares, Ch. Kurtsiefer, J. Skaar, V. Makarov, and I. Gerhardt, Rev. Sci. Instr. **85**, 013108 (2014); arXiv:1307.5951.

14. M. G. Tanner, V. Makarov, and R. H. Hadfield, Opt. Express **22**, 6734 (2014); arXiv:1305.5989.

15. A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, arXiv:1601.00993.

16. C. Ci Wen Lim, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, IEEE J. Selected Topics in Quant. Electron. **21**, 1 (2015); arXiv:1408.6398.

17. Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature Photon. **4**, 800 (2010).

18. Z. L. Yuan, J. F. Dynes, and A. J. Shields, Appl. Phys. Lett. **99**, 196101 (2011).

19. N. Jain, B. Stiller, I. Khan, D. Elser, Ch. Marquardt, and G. Leuchs, Contemporary Phys. **57**, 3 (2016); arXiv:1512.07990.

20. R. Renner, PhD Thesis, ETH Zürich, arXiv: quant-ph:0512258 (2005).

21. A. V. Duplinskiy, E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, R. P. Ermakov, A. V. Brodsky, R. R. Unusov, V. L. Kurochkin, A. K. Fedorov, and Y. V. Kurochkin, arXiv:1712.09831.