ЖЭТФ, 2020, том 158, вып. 6 (12), стр. 1011–1031

О СТОЙКОСТИ СИСТЕМ КВАНТОВОЙ КРИПТОГРАФИИ С ФАЗОВО-ВРЕМЕННЫ́М КОДИРОВАНИЕМ К АТАКАМ АКТИВНОГО ЗОНДИРОВАНИЯ

С. Н. Молотков*

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

Академия криптографии Российской Федерации
121552, Москва, Россия

Центр квантовых технологий, Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 11 мая 2020 г.,
после переработки 11 мая 2020 г.
Принята к публикации 3 июля 2020 г.

Рассмотрена криптостойкость системы квантовой криптографии, использующей протокол с фазово-временны́м кодированием на ослабленных когерентных состояниях. Данный протокол имеет эффективную волоконную реализацию, при которой не требуется фазовый модулятор на приемной стороне, что не требует регулировки состояния поляризации при входе в приемную часть. Отсутствие фазового модулятора на приемной стороне исключает побочный канал утечки информации, связанный с активным зондированием фазового модулятора на приемной станции, что делает систему более устойчивой к таким атакам по сравнению с другими системами. Нестрогая однофотонность информационных состояний, а также утечка информации через побочные каналы учитывается обобщенным Decoy State-методом с учетом совместных коллективных измерений информационных квантовых состояний и квантовых состояний в побочных каналах. Получена оценка длины секретного ключа, которая выражается только через наблюдаемые величины на приемной станции и параметры квантовых состояний в побочных каналах.

DOI: 10.31857/S0044451020120019

1. ВВЕДЕНИЕ

Системы квантовой криптографии предназначены для создания общего секрета — секретного ключа, между пространственно-удаленными пользователями. Распределение ключей основано на передаче и измерении квантовых состояний. Попытки вторжения в квантовый канал связи приводят к возмущению состояний и ошибкам на приемной стороне [1].

Фундаментальные законы квантовой механики позволяют связать утечку информации к подслушивателю с наблюдаемым уровнем ошибок на приемной стороне [2, 3].

Для различных протоколов квантового распределения ключей были получены фундаментальные верхние границы утечки информации к подслушивателю при атаках на состояния в квантовом канале связи. Источник квантовых состояний — сильно ослабленное когерентное состояние — не является строго однофотонным источником, что приводит к ряду новых атак на передаваемые квантовые состояния, которые отсутствуют при строго однофотонном источнике [4]. Были разработаны методы, учитывающие не строго однофотонный источник квантовых информационных состояний [5–8].

На сегодняшний день применительно к атакам на передаваемые квантовые состояния в канале связи достигнуто достаточное понимание. При доказательстве секретности ключей в квантовой криптографии неявно предполагается, что приемная и передающая аппаратура абсолютно изолирована от внешнего мира.

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

Важным источником утечки информации в любой системе криптографии являются побочные каналы. В классических системах криптографии одним из таких каналов является побочное электромагнитное излучения электронной аппаратуры, которое можно детектировать дистанционно без непосредственного доступа к самой аппаратуре.

Для систем квантовой криптографии ситуация с побочными каналами утечки информации еще более деликатная, чем в классической криптографии. Системы квантовой криптографии являются открытыми системами в том смысле, что кроме детектирования побочного излучения передающей и приемной аппаратуры подслушиватель может активно зондировать состояние активных элементов (фазовых модуляторов, модулятора интенсивности, переизлучения лавинных детекторов и др.) внешним излучением через волоконную линию связи. Принципиальное отличие вторжения в квантовый канал связи от детектирования побочного излучения и активного зондирования аппаратуры состоит в том, что детектирование состояний в побочных каналах не приводит к ошибкам на приемной стороне, поскольку не возмущает передаваемых состояний.

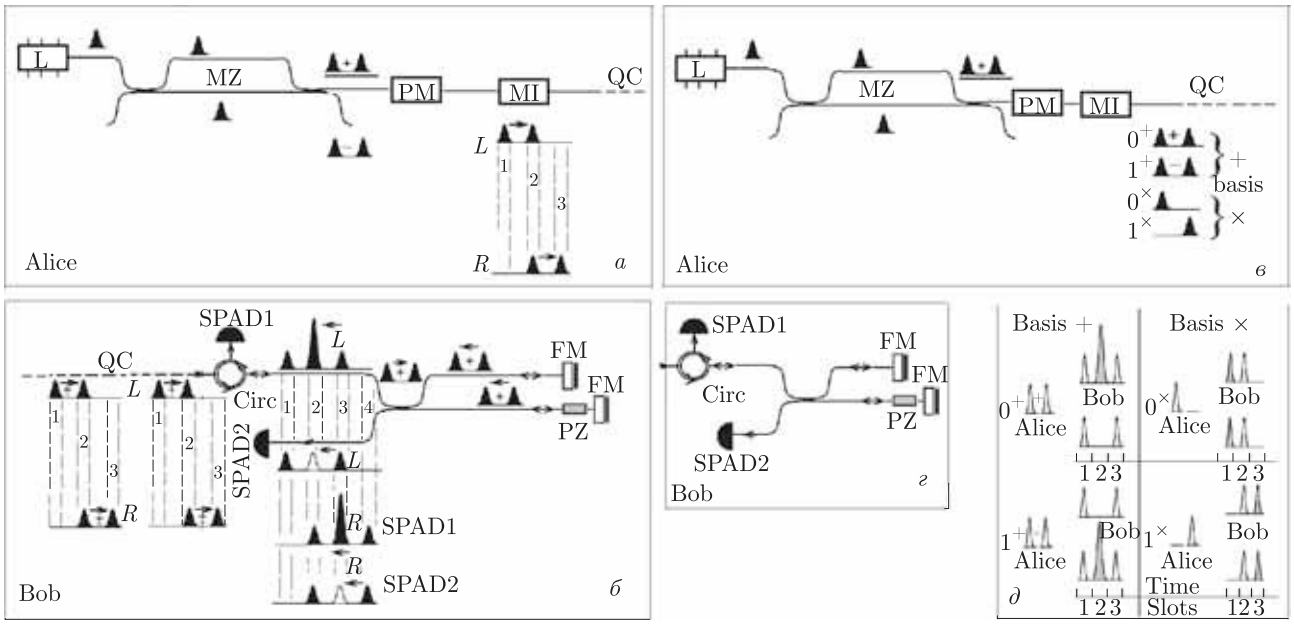
Дальнейшая логика доказательства секретности ключей с учетом побочных каналов утечки информации и не строго однофотонного источника информационных состояний будет состоять в следующем. Статистика лазерного излучения является пуассоновской по числу фотонов — в канале связи с пуассоновскими вероятностями присутствуют фоковские состояния с разным числом фотонов. Секретный ключ набирается только из однофотонной компоненты состояний. Информация, заключенная в многофотонных компонентах с числом фотонов $k \geq 2$ консервативно в пользу подслушивателя, считается известной подслушивателю. Наиболее общая атака подслушивателя на однофотонные состояния сводится к унитарной атаке, которая строится явно. Унитарная атака — это атака, при которой подслушиватель использует свое вспомогательное состояние ancilla и запутывает с передаваемым состоянием при помощи унитарного оператора. Искаженное информационное состояние подслушиватель направляет на приемную сторону, а свою подсистему оставляет в квантовой памяти. После измерений на приемной стороне, коррекции ошибок и усиления секретности подслушиватель проводит коллективные измерения над всей своей квантовой памятью.

Каждый побочный канал утечки представляет собой квантовое состояние, которое отражает состояние аппаратуры, фазовых модуляторов, модуляторов интенсивности, лавинных детекторов. В итоге в каждой посылке подслушиватель имеет в своем распоряжении дополнительные квантовые состояния, которые «привязаны» к информационным состояниям. Разумеется, что побочные каналы возникают и в том случае, когда в канале связи присутствуют состояния с числом фотонов $k \geq 2$, но информация, заключенная в этих посылках, и так отдается (консервативно считается известной) подслушивателю. Поэтому квантовые состояния в побочных каналах можно считать «привязанными» только к однофотонной компоненте информационных состояний.

Квантовые состояния из побочных каналов подслушиватель также сохраняет в квантовой памяти до конца протокола, а затем проводит совместные коллективные измерения над состоянием ancilla и квантовыми состояниями из побочных каналов.

Следующий шаг состоит в оценке доли однофотонной компоненты, которая достигает приемной стороны. В этом случае используется Decoy State-метод, который сводится к посылке случайным образом когерентных состояний с разным средним числом фотонов в разных посылках. Модуляция интенсивности когерентных состояний происходит при помощи модулятора интенсивности. Decoy State-метод основан на том факте, что подслушиватель, обнаружив в канале фоковское состояние с данными числом фотонов k, не может определить, из какого когерентного состояния и с каким средним числом фотонов происходит данная компонента. При наличии активного зондирования модулятора интенсивности подслушиватель может, пусть с некоторой вероятностью ошибки, определить, из какого состояния происходит данное число фотонов. По этой причине стандартный Decoy State-метод при атаке активного зондирования модулятора интенсивности должен быть модифицирован. Такая модификация будет сделана ниже.

При унитарной атаке на однофотонные состояния без побочных каналов утечки информации можно воспользоваться фундаментальными энтропийными соотношениями неопределенностей, которые связывают ошибку на приемной стороне с утечкой информации к подслушивателю. При этом не требуется явное построение атаки подслушивателя — унитарного оператора, состояния ancilla и пр. При наличии побочных каналов утечки информации приходится явно строить атаку на однофотонную компоненту состояний, поскольку побочные каналы не приводят к ошибкам на приемной стороне, и связь утечки информации с ошибками на приемной стороне «разрывается». Явное построение атаки необ-



а, б) Реализация системы с фазово-временным кодированием. *а*) Передающая сторона (Alice), L — лазер, работающий в CW-моде, MZ — интерферометр Маха – Цандера, MI — модулятор интенсивности, PM — фазовый модулятор. Весь оптический тракт на передающей станции выполнен на поляризационно сохраняющем волокне. *б*) Приемная часть (Bob), весь оптический тракт выполнен на стандартном одномодовом SM-волокне. Circ — волоконный поляризационно независимый циркулятор, SPAD1,2 — однофотонные лавинные детекторы, FM — фарадеевское зеркало, PZ — управляемый пьезоэлемент для выравнивания разности хода в верхнем и нижнем плечах интерферометра, QC — линия связи на основе SM-волокна. Стрелками показана эволюция состояний, а также формирование интерференции на приемной стороне. *в,г,д*) Реализация системы с протоколом BB84. *в*) Передающая станция, эволюция состояний. *г*) Приемная станция и эволюция состояний в прямом (индекс $+$) и сопряженном (индекс $\times$) базисах. *д*) Интерференция состояний на приемной стороне в прямом и сопряженном базисах

ходимо еще и потому, что квантовые состояния в побочных каналах «привязаны» в каждой посылке к искаженным информационным состояниям, что требует их явного знания.

2. ФАЗОВО-ВРЕМЕННО́Е КОДИРОВАНИЕ, ОДНОФОТОННЫЙ СЛУЧАЙ

Обсуждаемая ниже реализация квантовой криптографии с фазово-временным кодированием замечательна тем, что на приемной стороне не используется поляризационно-чувствительный элемент — фазовый модулятор, что делает систему более устойчивой к атакам активного зондирования по сравнению с другими системами. Кроме того, отсутствие поляризационно-чувствительных элементов на приемной стороне приводит к тому, что в системе не требуется регулировка поляризации состояний, поступающих на приемную сторону из квантового канала связи.

Далее, такая система позволяет реализовать, кроме протокола с фазово-временным кодированием, также протокол BB84 [9], что обеспечивает еще большую гибкость и универсальность системы.

В реальной системе информационными состояниями являются сильно ослабленные когерентные состояния. В протоколе фазово-временного кодирования используется два базиса L и R (см. пояснения на рисунке, индексы «L» и «R» соответствуют Left и Right), в каждом базисе имеется пара ортогональных состояний. Между базисами из-за перекрытия по времени состояния попарно неортогональны.

Состояния в базисе L имеют вид

$$0_L \to |\alpha\rangle_1 \otimes |\alpha\rangle_2, \quad 1_L \to |\alpha\rangle_1 \otimes |-\alpha\rangle_2, \qquad (1)$$

где индексы «1» и «2» отвечают за временное окно (см. рисунок), $|\alpha|^2 = \mu$ — среднее число фотонов в сильно ослабленном когерентном состоянии, $|\alpha|^2 = \mu \ll 1$. Аналогично, в базисе R

$$0_R \to |\alpha\rangle_2 \otimes |\alpha\rangle_3, \quad 1_R \to |-\alpha\rangle_2 \otimes |\alpha\rangle_3. \qquad (2)$$

Кодирование логических битов 0 и 1 в каждом базисе происходит в относительную фазу когерентных состояний во временных окнах 1 и 2 в базисе L и во временных окнах 2 и 3 в базисе R. Поскольку в каждой посылке импульсный лазер включается и выключается при формировании информационных состояний, фаза θ самого когерентного состояния (параметр $\alpha = e^{i\theta}|\alpha|$) является случайной. По этой причине подслушиватель видит в канале связи не чистые когерентные состояния, а их статистическую смесь. В базисе L имеем

$$\rho^x(\mu) = e^{-2\mu}\sum_{k=0}^{\infty}\frac{(2\mu)^k}{k!}|\Psi_k^x\rangle_{B\,B}\langle\Psi_k^x| = \\ = \sum_{k=0}^{\infty}P^{(k)}(\mu)|\Psi_k^x\rangle_{B\,B}\langle\Psi_k^x|, \quad (3)$$

$$P^{(k)}(\mu) = e^{-2\mu}\frac{(2\mu)^k}{k!},$$

$$|\Psi_k^x\rangle_B = \sqrt{\frac{k!}{2^k}}\sum_{m=0}^{k}e^{i\varphi_x m}\frac{|m\rangle_1\otimes|k-m\rangle_2}{\sqrt{m!(k-m)!}}, \quad (4)$$

где $x = 0, 1$; $\varphi_x = 0$ $(x = 0)$ и $\varphi_x = \pi$ $(x = 1)$, φ_x — относительная фаза состояний, локализованных во временных окнах 1 и 2, в которую кодируется информация о битах ключа; состояния $|m\rangle_1\otimes|k-m\rangle_2$ — фоковские состояния во временных окнах 1 и 2 (нижние индексы). В базисе R выражение для матрицы плотности аналогично (3), (4) с заменой индексов временных окон у состояний $(1, 2) \to (2, 3)$.

Секретный ключ набирается из однофотонной компоненты состояний. Информация, заключенная в многофотонных компонентах состояний (3), (4) консервативно в пользу подслушивателя, считается ему известной. Для однофотонной компоненты вторжение в канал связи приводит к возмущению и ошибкам на приемной стороне. Дальнейшая задача будет сводится к установлению связи вероятности ошибок на приемной стороне и количеством информации, которую может получить подслушиватель при данной наблюдаемой вероятности ошибок. В дальнейшем модифицированным Decoy State-методом будет оценена доля однофотонной компоненты на приемной стороне, из которой набирается секретный ключ.

Однофотонная компонента информационных состояний в левом базисе имеет вид

$$|0_L\rangle_X = \frac{1}{\sqrt{2}}\left(|1\rangle_1\otimes|0\rangle_2 + |0\rangle_1\otimes|1\rangle_2\right) = \\ = \frac{1}{\sqrt{2}}\left(|1\rangle_1 + |1\rangle_2\right), \quad (5)$$

$$|1_L\rangle_X = \frac{1}{\sqrt{2}}\left(|1\rangle_1\otimes|0\rangle_2 - |0\rangle_1\otimes|1\rangle_2\right) = \\ = \frac{1}{\sqrt{2}}\left(|1\rangle_1 - |1\rangle_2\right), \quad (6)$$

в правом базисе состояния равны

$$|0_R\rangle_X = \frac{1}{\sqrt{2}}\left(|1\rangle_2\otimes|0\rangle_3 + |0\rangle_2\otimes|1\rangle_3\right) = \\ = \frac{1}{\sqrt{2}}\left(|1\rangle_2 + |1\rangle_3\right), \quad (7)$$

$$|1_R\rangle_X = \frac{1}{\sqrt{2}}\left(|1\rangle_2\otimes|0\rangle_3 - |0\rangle_2\otimes|1\rangle_3\right) = \\ = \frac{1}{\sqrt{2}}\left(|1\rangle_2 - |1\rangle_3\right), \quad (8)$$

для экономии обозначений вакуумная компонента поля в соответствующих временных окнах опущена, далее $|1\rangle_i$ — однофотонное состояние, локализованное во временном окне i. В базисе L информационные состояния представляют собой суперпозицию однофотонных состояний во временных окнах 1 и 2, соответственно, в базисе R — суперпозицию во временных окнах 2 и 3. Внутри базиса информационные состояния ортогональны, поэтому достоверно различимы. Состояния из базисов L и R попарно неортогональны, достоверно неразличимы. Неортогональность состояний из разных базисов гарантирует, что вторжение подслушивателя в квантовый канал связи будет приводить к возмущению передаваемых состояний и появлению ошибок на приемной стороне. В отличие от протокола BB84, возмущение состояний будет приводить также к отсчетам в контрольных временных окнах [10, 11].

Унитарная атака на однофотонные состояния может быть представлена в виде

$$|\Psi_{0_L}\rangle_{XYQ} = |0_L\rangle_X\otimes U_{BE}(|0_L\rangle_Y\otimes|E\rangle_Q), \\ |\Psi_{1_L}\rangle_{XYQ} = |1_L\rangle_X\otimes U_{BE}(|1_L\rangle_Y\otimes|E\rangle_Q), \quad (9)$$

где $|E\rangle_Q$ — вспомогательное состояние Евы, ancilla; $|0_L\rangle_X$, $|1_L\rangle_X$ — эталонные состояния Алисы, недоступные подслушивателю, $|0_L\rangle_Y$, $|1_L\rangle_Y$ — состояния в квантовом канале связи, направленные к Бобу, доступные для атаки Евы.

Аналогичные уравнения получаются в базисе R. Запутывание информационного состояния и состояния ancilla Евы в базисе R получаются линейным преобразованием (9)–(11) из формул (5)–(8).

В базисе L находим (см. детали в [10, 11], далее индекс «L» для краткости опускаем)

$$|\Psi_0\rangle_{XYQ} = |0_L\rangle_X\otimes[|0_L\rangle_Y\otimes|\Phi_0\rangle_Q + |1_L\rangle_Y\otimes|\Theta_0\rangle_Q + \\ + |c_L\rangle_Y\otimes|\Lambda_0\rangle_Q], \quad (10)$$

$$|\Psi_1\rangle_{XYQ} = |1_L\rangle_X \otimes [|1_L\rangle_Y \otimes |\Phi_1\rangle_Q + |0_L\rangle_Y \otimes |\Theta_1\rangle_Q + \\ + |c_L\rangle_Y \otimes |\Lambda_1\rangle_Q]. \quad (11)$$

Разложение (10), (11) представляет собой разложение Шмидта в тензорном произведении пространств состояний Евы и Боба. Разложение в базисе R получается линейным преобразованием (9)–(11).

Нормировка состояний имеет вид (см. детали в [10,11])

$$\begin{aligned} {}_Q\langle\Phi_{0,1}|\Phi_{0,1}\rangle_Q &= (1-\zeta)(1-Q), \\ {}_Q\langle\Theta_{0,1}|\Theta_{0,1}\rangle_Q &= (1-\zeta)Q, \\ {}_Q\langle\Lambda_{0,1}|\Lambda_{0,1}\rangle_Q &= \zeta. \end{aligned} \quad (12)$$

Для дальнейшего удобно ввести нормированные состояния

$$\begin{aligned} \sqrt{(1-\zeta)(1-Q)}|\overline{\Phi}_{0,1}\rangle_Q &= |\Phi_{0,1}\rangle_Q, \\ \sqrt{(1-\zeta)Q}|\overline{\Theta}_{0,1}\rangle_Q &= |\Theta_{0,1}\rangle_Q, \\ \sqrt{\zeta}|\overline{\Lambda}_{0,1}\rangle_Q &= |\Lambda_{0,1}\rangle_Q, \end{aligned} \quad (13)$$

вместо (10), (11) с учетом (12), (13) получаем

$$|\Psi_0\rangle_{XYQ} = |0_L\rangle_X \otimes \sqrt{1-\zeta}\left[\sqrt{1-Q}|0_L\rangle_Y \otimes |\overline{\Phi}_0\rangle_Q + \right. \\ \left. + \sqrt{Q}|1_L\rangle_Y \otimes |\overline{\Theta}_0\rangle_Q\right] + \sqrt{\zeta}|c_L\rangle_Y \otimes |\overline{\Lambda}_0\rangle_Q, \quad (14)$$

$$|\Psi_1\rangle_{XYQ} = |1_L\rangle_X \otimes \sqrt{1-\zeta}\left[\sqrt{1-Q}|1_L\rangle_Y \otimes |\overline{\Phi}_1\rangle_Q + \right. \\ \left. + \sqrt{Q}|0_L\rangle_Y \otimes |\overline{\Theta}_1\rangle_Q\right] + \sqrt{\zeta}|c_L\rangle_Y \otimes |\overline{\Lambda}_1\rangle_Q. \quad (15)$$

Измерения на приемной станции в базисе L дается разложением единицы:

$$I_Y = |0_L\rangle_{YY}\langle 0_L| + |1_L\rangle_{YY}\langle 1_L| + |c_L\rangle_{YY}\langle c_L|, \quad (16)$$

где $|c_L\rangle_Y = |1\rangle_3$ — состояние во временном окне 3 в базисе L. Аналогичное разложение единицы, описывающее измерение в базисе R, имеет вид

$$I_Y = |0_R\rangle_{YY}\langle 0_R| + |1_R\rangle_{YY}\langle 1_R| + |c_R\rangle_{YY}\langle c_R|, \quad (17)$$

где $|c_R\rangle_Y = |1\rangle_1$ — состояние во временном окне 3 в базисе R.

Далее индекс «L» для краткости опускаем. После измерений в соответствующем базисе для матрицы плотности Алиса–Боб–Ева получаем

$$\rho_{XYQ} = \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-\zeta)[(1-Q)|0\rangle_{YY}\langle 0| \otimes \\ \otimes |\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + Q|1\rangle_{YY}\langle 1| \otimes |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|] + \zeta|c\rangle_Y \times \\ \times {}_Y\langle c|\otimes|\overline{\Lambda}_0\rangle_{QQ}\langle\overline{\Lambda}_0|] + \frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[(1-\zeta)[(1-Q)|1\rangle_Y \times \\ \times {}_Y\langle 1|\otimes|\overline{\Phi_1}\rangle_{QQ}\langle\overline{\Phi}_1| + Q|0\rangle_{YY}\langle 0|\otimes|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|] + \zeta|c\rangle_Y \times \\ \times {}_Y\langle c| \otimes |\overline{\Lambda}_1\rangle_{QQ}\langle\overline{\Lambda}_1|]. \quad (18)$$

Необходимо дать физическую интерпретацию матрицы плотности (18). Алиса с вероятностью $1/2$ посылает в канал состояние, отвечающее 0, и с вероятностью $1/2$ состояние, отвечающее 1.

Пусть Алиса посылала в базисе L состояние $|0\rangle_{YY}\langle 0|$ (в распоряжении Алисы остается эталонное состояние $|0\rangle_{XX}\langle 0|$). После атаки Евы и измерений Боба на приемной стороне Боб с вероятностью $(1-\zeta)(1-Q)$ видит состояние $|0\rangle_{YY}\langle 0|$, которое будет давать правильный исход измерений. Боб будет интерпретировать исход измерений как логический 0. При этом в распоряжении Евы окажется состояние $|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0|$.

Далее, с вероятностью $(1-\zeta)Q$ Боб видит состояние $|1\rangle_{YY}\langle 1|$, которое будет давать ошибочный исход измерений. Боб будет интерпретировать исход измерений как логическую 1. При этом в распоряжении Евы окажется состояние $|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|$.

Полная вероятность отсчетов как правильных, так и ошибочных в информационных временных окнах 1 и 2, будет равна $(1-\zeta)(1-Q)+(1-\zeta)Q = 1-\zeta$. Кроме отсчетов в информационных временных окнах 1 и 2, искаженные состояния будут давать отсчеты в контрольном временном окне 3 в базисе L (соответственно в контрольном окне 1 в базисе R). Невозмущенные состояния в базисе L никогда не дают отсчетов в контрольном временном окне 3.

Вероятность отсчетов в контрольном временном окне 3 равна ζ. При этом у Евы оказывается состояние $|\overline{\Lambda}_0\rangle_{QQ}\langle\overline{\Lambda}_0|$. В итоге суммарная вероятность отсчетов в информационных и контрольном временном окне равна $1-\zeta+\zeta = 1$.

Подчеркнем, что утечка информации к подслушивателю определяется не только ошибкой в информационных временных окнах, но и вероятностью отсчета в контрольном временном окне (см. подробности в [10,11]. Для вычисления утечки информации к Еве требуется знать (измерять) вероятность отсчетов в контрольном временном окне 3.

Поскольку ключ получается только из отсчетов в информационных окнах, для дальнейшего удобно перейти к редуцированной матрице плотности — нормированной на вероятность отсчетов в информационных временных окнах. Получаем (индекс «L» у состояний Боба опускаем)

$$\overline{\rho}_{XYQ} = \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-Q)|0\rangle_{YY}\langle 0| \otimes |\overline{\Phi}_0\rangle_Q \times \\ \times {}_Q\langle\overline{\Phi}_0| + Q|1\rangle_{YY}\langle 1| \otimes |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|] + \\ + \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes [(1-Q)|1\rangle_{YY}\langle 1| \otimes |\overline{\Phi_1}\rangle_{QQ}\langle\overline{\Phi}_1| + \\ + Q|0\rangle_{YY}\langle 0| \otimes |\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|]. \quad (19)$$

Соответственно, для матрицы плотности Алиса–Ева получаем

$$\overline{\rho}_{XQ}=\frac{1}{2}|0\rangle_{XX}\langle 0|\otimes[(1-Q)|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0|+ +Q|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|]+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[(1-Q)|\overline{\Phi_1}\rangle_Q\times \times{}_Q\langle\overline{\Phi}_1|+Q|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|]. \quad (20)$$

Матрица плотности Алиса–Боб имеет вид

$$\overline{\rho}_{XY}=\frac{1}{2}|0\rangle_{XX}\langle 0|\otimes[(1-Q)|0\rangle_{YY}\langle 0|+Q|1\rangle_Y\times \times{}_Y\langle 1|]+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[(1-Q)|1\rangle_{YY}\langle 1|+Q|0\rangle_Y\times \times{}_Y\langle 0|]. \quad (21)$$

Матрица плотности, которую видит Ева, есть

$$\overline{\rho}_Q=\frac{1}{2}(1-Q)[|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0|+|\overline{\Phi_1}\rangle_{QQ}\langle\overline{\Phi}_1|]+ +\frac{1}{2}Q[|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|+|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|]. \quad (22)$$

Аналогично матрица плотности, которую видит Боб, есть

$$\overline{\rho}_Y=\frac{1}{2}\left[|0\rangle_{YY}\langle 0|+|1\rangle_{YY}\langle 1|\right]. \quad (23)$$

Оценка длины секретного ключа в асимптотическом пределе при коррекции ошибок случайными шенновскими кодами имеет вид (см. детали в [2])

$$\ell=H(\overline{\rho}_{XQ}|\overline{\rho}_Q)-H(\overline{\rho}_{XY}|\overline{\rho}_Y), \quad (24)$$

где условные энтропии фон Неймана

$$\begin{aligned}H(\overline{\rho}_{XQ}|\overline{\rho}_Q)&=H(\overline{\rho}_{XQ})-H(\overline{\rho}_Q),\\ H(\overline{\rho}_{XY}|\overline{\rho}_Y)&=H(\overline{\rho}_{XY})-H(\overline{\rho}_Y).\end{aligned} \quad (25)$$

С учетом (19)–(25) получаем

$$\begin{aligned}H(\overline{\rho}_{XQ})&=1+h(Q),\\ H(\overline{\rho}_Q)&=h\left(\frac{\zeta}{1-\zeta}\right)+h(Q),\\ H(\overline{\rho}_{XQ}|\overline{\rho}_Q)&=1-h\left(\frac{\zeta}{1-\zeta}\right),\end{aligned} \quad (26)$$

$$H(\overline{\rho}_{XY})=1+h(Q),\quad H(\overline{\rho}_Y)=1,\quad H(\overline{\rho}_{XY}|\overline{\rho}_Y)=h(Q). \quad (27)$$

С учетом (24) для оценки длины секретного ключа получаем

$$\ell=\left[1-h\left(\frac{\zeta}{1-\zeta}\right)\right]-h(Q). \quad (28)$$

Если коррекция ошибок происходит конструктивными кодами, то последнее слагаемое в (28) надо заменить на $\mathrm{leak}(Q)$:

$$\ell=\left[1-h\left(\frac{\zeta}{1-\zeta}\right)\right]-\mathrm{leak}(Q)= =[1-\chi_{Hol}(\zeta)]-\mathrm{leak}(Q), \quad (29)$$

где $\mathrm{leak}(Q)$ — утечка информации при коррекции ошибок, которая зависит от полной ошибки.

Формула (29) имеет интуитивно прозрачную интерпретацию. Из (29) следует, что протокол является двухпараметрическим, длина секретного ключа зависит не только от наблюдаемой ошибки Q в информационных временных окнах, но и от вероятности отсчетов в контрольных временных окнах ζ. Данную причину несложно понять на примере простейшей атаки прием–перепосыл. Состояния из разных базисов L и R являются неортогональными, они перекрываются во временном окне 2 (см. рисунок). Еве базис неизвестен, поэтому перепосыл состояний в неправильном базисе неизбежно приведет к отсчетам в контрольном временном окне, где их не должно быть. Например, если базис Алисы и Боба есть L, а Ева перепосылает состояния в базисе R, то это приведет к отсчетам в контрольном временном окне 3. Аналогично для базиса измерений Алисы и Боба R перепосыл состояний в базисе L приведет к отсчетам в контрольном временном окне 1, где их не должно быть. Разумеется, атака прием–перепосыл не является самой общей. Наиболее общей атакой на однофотонные состояния является унитарная атака (9)–(11).

3. ДЕТЕКТИРОВАНИЕ ПОБОЧНОГО ИЗЛУЧЕНИЯ ПЕРЕДАЮЩЕЙ АППАРАТУРЫ

Подслушиватель может получать информацию о передаваемом ключе не только из квантового канала связи, но и используя побочные каналы утечки информации. При этом получение информации из этих каналов не приводит к искажению информационных состояний и ошибкам на приемной стороне. Побочные каналы утечки являются информационным «бесплатным бонусом». Одним из таких каналов является побочное электромагнитное излучение передающей аппаратуры. При приготовлении аппаратурой состояния $|0\rangle_{XX}\langle 0|$ вне передающей станции Алисы возникает квантовое состояние $|e_0\rangle_{SS}\langle e_0|$. Если аппаратура приготавливает состояние $|1\rangle_{XX}\langle 1|$, то это приводит к излуче-

нию вне состояния $|e_0\rangle_{SS}\langle e_0|$. Состояния, отвечающие 0 и 1 в побочном канале, можно считать ортогональными, а их неразличимость учесть в вероятности различения p. Эффективно подслушиватель видит в побочном канале матрицу плотности $(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_{SS}\langle e_1|$, которая интерпретируется следующим образом: с вероятностью $1-p$ подслушиватель видит состояние $|0\rangle_{X\,X}\langle 0|$ и считает, что Алиса приготовила бит 0. В этом случае Ева в результате измерения побочного излучения узнает бит ключа. С вероятностью p Ева детектирует состояние $|1\rangle_{X\,X}\langle 1|$ и считает, что Алиса приготовила бит 1, т. е. с вероятностью p Ева ошибается. Аналогично, если Алиса приготавливала бит 1. С учетом сказанного матрица плотности Алиса–Боб–Ева может быть записана в виде

$$\begin{aligned}\rho_{XYQS} = \frac{1}{2}|0\rangle_{X\,X}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_S \times \\ \times {}_S\langle e_1|] \otimes [(1-\zeta)(1-Q)|0\rangle_{YY}\langle 0| \otimes |\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + \\ + (1-\zeta)Q|1\rangle_{YY}\langle 1| \otimes |\overline{\Theta}_0\rangle_Q \times \\ \times {}_Q\langle\overline{\Theta}_0| + \zeta|c\rangle_{YY}\langle c| \otimes |\overline{\Lambda}_0\rangle_{QQ}\langle\overline{\Lambda}_0|] + \\ + \frac{1}{2}|1\rangle_{X\,X}\langle 1| \otimes [(1-p)|e_1\rangle_{SS}\langle e_1| + p|e_0\rangle_{SS}\langle e_0|] \otimes \\ \otimes [(1-\zeta)(1-Q)|1\rangle_{YY}\langle 1| \otimes |\overline{\Phi}_1\rangle_{QQ} \times \\ \times \langle\overline{\Phi}_1| + (1-\zeta)Q|0\rangle_{YY}\langle 0| \otimes |\overline{\Theta}_1\rangle_{QQ} \times \\ \times \langle\overline{\Theta}_1| + \zeta|c\rangle_{YY}\langle c| \otimes |\overline{\Lambda}_1\rangle_{QQ}\langle\overline{\Lambda}_1|]. \quad (30)\end{aligned}$$

Для того чтобы не усложнять выкладки, в (30) побочный канал утечки информации считается симметричным для приготовления 0 и 1. Обобщение на несимметричный случай делается аналогично. При переходе к редуцированной матрице плотности имеем

$$\begin{aligned}\overline{\rho}_{XYQS} = \frac{1}{2}|0\rangle_{X\,X}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_S \times \\ \times {}_S\langle e_1|] \otimes [(1-Q)|0\rangle_{YY}\langle 0| \otimes |\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + Q|1\rangle_Y \times \\ \times {}_Y\langle 1| \otimes |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|] + \frac{1}{2}|1\rangle_{X\,X}\langle 1| \otimes [(1-p)|e_1\rangle_{SS}\langle e_1| + \\ + p|e_0\rangle_{SS}\langle e_0|] \otimes [(1-Q)|1\rangle_{YY}\langle 1| \otimes |\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1| + Q|0\rangle_Y \times \\ \times {}_Y\langle 0| \otimes |\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|], \quad (31)\end{aligned}$$

$$\begin{aligned}\overline{\rho}_{XY} = \frac{1}{2}|0\rangle_{X\,X}\langle 0| \otimes [(1-Q)|0\rangle_{YY}\langle 0| + \\ + Q|1\rangle_{YY}] + \frac{1}{2}|1\rangle_{X\,X}\langle 1| \otimes [(1-Q)|1\rangle_Y \times \\ \times {}_Y\langle 1| + Q|0\rangle_{YY}\langle 0|]. \quad (32)\end{aligned}$$

Матрица плотности Боба записывается как

$$\overline{\rho}_Y = \frac{1}{2}|0\rangle_{YY}\langle 0| + \frac{1}{2}|1\rangle_{YY}\langle 1|. \quad (33)$$

Условная энтропия имеет вид

$$H(\overline{\rho}_{XY}|\overline{\rho}_Y) = H(\overline{\rho}_{XY}) - H(\overline{\rho}_Y) = h(Q), \quad (34)$$

где $h(x) = -x\log(x) - (1-x)\log(1-x)$, $\log \equiv \log_2$.

Вычислим матрицу плотности Алиса–Ева:

$$\begin{aligned}\overline{\rho}_{XQS} = \frac{1}{2}|0\rangle_{X\,X}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_S \times \\ \times {}_S\langle e_1|] \otimes [(1-Q)|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + Q|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|] + \\ + \frac{1}{2}|1\rangle_{X\,X}\langle 1| \otimes [(1-p)|e_1\rangle_{SS}\langle e_1| + p|e_0\rangle_{SS}\langle e_0|] \otimes \\ \otimes [(1-Q)|\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1| + Q|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|]. \quad (35)\end{aligned}$$

Матрица плотности Евы записывается как

$$\begin{aligned}\overline{\rho}_{QS} = \frac{1}{2}(1-Q)[(1-p)|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + p|\overline{\Phi}_1\rangle_{QQ} \times \\ \times \langle\overline{\Phi}_1|] \otimes |e_0\rangle_{SS}\langle e_0| + \frac{1}{2}(1-Q)[p|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + \\ + (1-p)|\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1|] \otimes |e_1\rangle_{SS}\langle e_1| + \\ + \frac{1}{2}Q[(1-p)|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0| + p|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|] \otimes |e_0\rangle_{SS} \times \\ \times \langle e_0| + \frac{1}{2}Q[p|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0| + (1-p)|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|] \otimes \\ \otimes |e_1\rangle_{SS}\langle e_1|. \quad (36)\end{aligned}$$

Собственные числа $\overline{\rho}_{XQS}$ равны

$$\frac{1}{2}(1-p)(1-Q), \quad \frac{1}{2}(1-p)Q, \quad \frac{1}{2}p(1-Q), \quad \frac{1}{2}pQ \quad (37)$$

и дважды вырождены. Энтропия $H(\overline{\rho}_{XQS})$ равна

$$H(\overline{\rho}_{XQS}) = 1 + h(p) + h(Q). \quad (38)$$

Матрица плотности Евы принимает вид

$$\begin{aligned}\overline{\rho}_{QS} = \frac{1}{2}(1-Q)[(1-p)|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + p|\overline{\Phi}_1\rangle_Q \times \\ \times {}_Q\langle\overline{\Phi}_1|] \otimes |e_0\rangle_{SS}\langle e_0| + \frac{1}{2}(1-Q)[p|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + \\ + (1-p)|\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1|] \otimes |e_1\rangle_{SS}\langle e_1| + \\ + \frac{1}{2}(1-Q)[(1-p)|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0| + p|\overline{\Theta}_1\rangle_Q \times \\ \times {}_Q\langle\overline{\Theta}_1|] \otimes |e_0\rangle_{SS}\langle e_0| + \frac{1}{2}(1-Q)[p|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0| + \\ + (1-p)|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|] \otimes |e_1\rangle_{SS}\langle e_1|. \quad (39)\end{aligned}$$

С учетом того, что (см. подробности в [10, 11])

$$\begin{aligned}{}_Q\langle\overline{\Theta}_{0,1}|\overline{\Theta}_{0,1}\rangle_Q = {}_Q\langle\overline{\Phi}_{0,1}|\overline{\Phi}_{0,1}\rangle_Q = \varepsilon(\zeta), \\ \varepsilon(\zeta) = 1 - 2\kappa(\zeta), \quad \kappa(\zeta) = \frac{\zeta}{1-\zeta},\end{aligned} \quad (40)$$

достаточно привести к диагональному виду слагаемые в каждых отдельных квадратных скобках. Для первых скобок задача на собственные значения дает

$$[(1-p)|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + p|\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1|] - \lambda I = 0, \quad (41)$$

где I — единичный оператор в подпространстве, натянутом на $\{|\overline{\Phi}_0\rangle_Q, |\overline{\Phi}_1\rangle_Q\}$, в базисе этих векторов детерминант секулярного уравнения имеет вид

$$\mathrm{Det}\begin{pmatrix} (1-p)+p\varepsilon(\zeta)^2-\lambda & (1-p)\varepsilon(\zeta)+p\varepsilon(\zeta)-\lambda\varepsilon(\zeta) \\ (1-p)\varepsilon(\zeta)+p\varepsilon(\zeta)-\lambda\varepsilon(\zeta) & (1-p)\varepsilon(\zeta)^2+p-\lambda \end{pmatrix} = 0. \quad (42)$$

Корни (42) имеют вид

$$\lambda_\pm(\zeta,p) = \frac{1\pm\varepsilon(\zeta,p)}{2},$$
$$\varepsilon(\zeta,p) = \sqrt{1-4\frac{[(1-p)+p\varepsilon(\zeta)^2][(1-p)\varepsilon(\zeta)^2+p]-\varepsilon(\zeta)^2}{1-\varepsilon(\zeta)^2}}. \quad (43)$$

Проводя аналогичные вычисления для других слагаемых, получаем полный набор собственных чисел:

$$\frac{1}{2}(1-Q)\,\frac{1+\varepsilon(\zeta,p)}{2},$$
$$\frac{1}{2}(1-Q)\,\frac{1-\varepsilon(\zeta,p)}{2}, \quad (44)$$
$$\frac{1}{2}Q\,\frac{1+\varepsilon(\zeta,p)}{2}, \quad \frac{1}{2}Q\,\frac{1-\varepsilon(\zeta,p)}{2},$$

которые двукратно вырождены. Энтропия фон Неймана $\overline{\rho}_{QS}$ равна

$$H(\overline{\rho}_{QS}) = 1 + h(Q) + \chi\left(\frac{1\pm\varepsilon(\zeta,p)}{2}\right), \quad (45)$$

где χ — информация Холево [12–14],

$$\chi\left(\frac{1\pm\varepsilon(\zeta,p)}{2}\right) = -\frac{1+\varepsilon(\zeta,p)}{2}\times \log\left(\frac{1+\varepsilon(\zeta,p)}{2}\right) - \frac{1-\varepsilon(\zeta,p)}{2}\times \log\left(\frac{1-\varepsilon(\zeta,p)}{2}\right). \quad (46)$$

Окончательно для условной энтропии с учетом (40)–(46) находим

$$H(\overline{\rho}_{XQS}|\overline{\rho}_{QS}) = h(p) - \chi\left(\frac{1\pm\varepsilon(\zeta,p)}{2}\right). \quad (47)$$

Соответственно для длины ключа получаем

$$\ell = H(\overline{\rho}_{XQS}|\overline{\rho}_{QS}) - H(\overline{\rho}_{XY}|\overline{\rho}_Y) = h(p) - \chi\left(\frac{1\pm\varepsilon(\zeta,p)}{2}\right) - h(Q) = [1-\chi_{Hol}(\zeta,p)] - h(Q). \quad (48)$$

Отметим, что утечка информации в (48) при коррекции ошибок отвечает шенноновскому пределу. При коррекции ошибок конструктивными кодами последнее слагаемое в (48) надо заменить на leak — число битов в пересчете на посылку, расходуемое при коррекции ошибок.

Важно отметить, что в формуле (48) нижняя граница нехватки информации Евы, допустимая фундаментальными законами квантовой теории, выражается через условную энтропию. Данная нижняя граница достигается на коллективных совместных измерениях Евы, что подразумевает совместные коллективные измерения Евы над квантовыми состояниями в побочном канале и искаженными состояниями ancilla в квантовом канале связи.

Формула (48) имеет простую интерпретацию. Если вероятность различения состояний 0 и 1 в побочном канале равна $p = 1/2$, то $h(p) = 1$ и выражение (48) переходит в выражение (28) для длины ключа без учета побочного канала утечки информации. Если $p = 0$, то Ева достоверно различает состояния 0 и 1 в побочном канале, знает передаваемые биты ключа, даже не вторгаясь в квантовый канал связи и не производя ошибок $Q = 0$ на приемной стороне. В этом случае $h(p) = 0$ и длина секретного ключа оказывается формально отрицательной, т. е. секретный ключ распределить нельзя. Таким образом, утечка информации по побочному каналу связи уменьшает длину секретного ключа. Для уменьшения утечки информации по данному побочному каналу следует эффективно экранировать передающую станцию. Параметры различения состояния p должны определяться экспериментально для каждой конкретной реализации системы квантовой криптографии.

4. АКТИВНОЕ ЗОНДИРОВАНИЕ СОСТОЯНИЯ ФАЗОВОГО МОДУЛЯТОРА НА ПЕРЕДАЮЩЕЙ СТАНЦИИ

Подслушиватель может зондировать состояние фазового модулятора на передающей станции через

волоконную линию связи. Состояние фазового модулятора однозначно связано с передаваемым Алисой битом ключа. В своем распоряжении Ева будет иметь дополнительное квантовое состояние, коррелированное с состоянием фазового модулятора. В пользу Евы можно считать, что отраженные состояния чистые, а это увеличивает их различимость. Наш метод позволяет учесть не только чистые отраженные состояния, но и матрицы плотности. Чистые состояния выбраны для того, чтобы не загромождать выкладки несущественными техническими деталями.

Интенсивность отраженных зондирующих состояний точно неизвестна, но можно ограничить интенсивность входных зондирующих состояний входными волоконными оптическими изоляторами, у которых известно обратное пропускание. Входная интенсивность зондирующего излучения ограничена, поскольку не может быть больше критической интенсивности, при которой происходит плавление волокна. Подбирая нужный коэффициент обратного пропускания оптического изолятора, можно ограничить выходную интенсивность отраженных состояний требуемой величиной.

При атаке с активным зондированием состояния аппаратуры внешним излучением следует ввести в рассмотрение еще один побочный канал. Формально это сводится к введению квантовых состояний, коррелированных с состоянием Алисы. Получаем

$$|0\rangle_X \to |0\rangle_X \otimes |\lambda_0\rangle_T, \quad |1\rangle_X \to |1\rangle_X \otimes |\lambda_1\rangle_T. \tag{49}$$

Для матрицы плотности вместо (30) получаем

$$\begin{aligned}\overline{\rho}_{XYQT} = {}& \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes [|0\rangle_Y \times \\ & \times {}_Y\langle 0| \otimes |\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + |1\rangle_{YY}\langle 1| \otimes |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|] + \\ & + \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes [|1\rangle_{YY}\langle 1| \otimes |\overline{\Phi}_1\rangle_Q \times \\ & \times {}_Q\langle\overline{\Phi}_1| + |0\rangle_{YY}\langle 0| \otimes |\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|]. \end{aligned} \tag{50}$$

Матрица плотности Алиса–Ева приобретает вид

$$\begin{aligned}\overline{\rho}_{XQT} = {}& \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes [|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + \\ & + |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|] + \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes [|\overline{\Phi}_1\rangle_Q \times \\ & \times {}_Q\langle\overline{\Phi}_1| + |\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|]. \end{aligned} \tag{51}$$

Собственные числа с учетом нормировки (13), (40) принимают вид

$$\frac{1}{2}(1-Q), \quad \frac{1}{2}Q, \quad \frac{1}{2}(1-Q), \quad \frac{1}{2}Q. \tag{52}$$

Для энтропии находим

$$H(\overline{\rho}_{XQT}) = 1 + h(Q). \tag{53}$$

Для вычисления собственных чисел требуется диагонализация матрицы плотности $\overline{\rho}_{QT}$, получаем

$$\begin{aligned}\overline{\rho}_{QT} = {}& \frac{1}{2}(1-Q)[\lambda_0\rangle_{TT}\langle\lambda_0| \otimes |\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + \\ & + |\lambda_1\rangle_{TT}\langle\lambda_1| \otimes |\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1|] + \frac{1}{2}Q[\lambda_0\rangle_T \times \\ & \times {}_T\langle\lambda_0| \otimes |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0| + |\lambda_1\rangle_{TT}\langle\lambda_1| \otimes \\ & \otimes |\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|]. \end{aligned} \tag{54}$$

Если зондирование происходит когерентными состояниями, фаза которых, консервативно в пользу Евы, однозначно привязана к состоянию фазового модулятора, т. е. равна либо 0 ($|\lambda_0\rangle_T = |\sqrt{\mu_T}\rangle_T$), либо π ($|\lambda_1\rangle_T = |-\sqrt{\mu_T}\rangle_T$) в зависимости от передаваемого бита, то для скалярного произведения отраженных состояний получаем $|{}_T\langle\lambda_0|\lambda_1\rangle_T| = \eta = e^{-2\mu_T}$. С учетом сказанного находим секулярное уравнение для первого слагаемого в (54):

$$\operatorname{Det}\begin{pmatrix} \dfrac{1+\eta^2\varepsilon(\zeta)^2}{2} - \lambda & 2\eta\varepsilon(\zeta) - \lambda\eta\varepsilon(\zeta) \\ 2\eta\varepsilon(\zeta) - \lambda\eta\varepsilon(\zeta) & \dfrac{1+\eta^2\varepsilon(\zeta)^2}{2} - \lambda \end{pmatrix} = 0. \tag{55}$$

Собственные числа матрицы плотности с учетом секулярного уравнения имеют вид

$$\begin{gathered}(1-Q)\,\frac{1+\eta\varepsilon(\zeta)}{2}, \quad (1-Q)\,\frac{1-\eta\varepsilon(\zeta)}{2}, \\ Q\,\frac{1+\eta\varepsilon(\zeta)}{2}, \quad Q\,\frac{1-\eta\varepsilon(\zeta)}{2}. \end{gathered} \tag{56}$$

Для энтропии $H(\overline{\rho}_{QT})$ получаем

$$H(\overline{\rho}_{QT}) = h(Q) + \chi\left(\frac{1 \pm \eta\varepsilon(\zeta)}{2}\right), \tag{57}$$

где информация Холево [12–14]

$$\begin{aligned}\chi\left(\frac{1 \pm \eta\varepsilon(\zeta)}{2}\right) = {}& -\frac{1+\eta\varepsilon(\zeta)}{2})\log\left(\frac{1+\eta\varepsilon(\zeta)}{2}\right) - \\ & - \frac{1-\eta\varepsilon(\zeta)}{2}\log\left(\frac{1-\eta\varepsilon(\zeta)}{2}\right). \end{aligned} \tag{58}$$

Окончательно для длины секретного ключа находим с учетом (53), (57)

$$\begin{aligned}\ell = {}& H(\overline{\rho}_{XQT}|\overline{\rho}_{QT}) - H(\overline{\rho}_{XY}|\overline{\rho}_Y) = \\ & = 1 - \chi\left(\frac{1 \pm \eta\varepsilon(\zeta)}{2}\right) - h(Q) = \\ & = [1 - \chi_{Hol}(\zeta,\eta)] - h(Q). \end{aligned} \tag{59}$$

Чем меньше среднее число фотонов μ_T в отраженных состояниях, тем скалярное произведение η больше — состояния сильнее слипаются, поэтому отраженные состояния менее различимы. При $\eta \to 1$ ($\mu_T \to 0$) состояния полностью слипаются и полностью неразличимы. При малых μ_T длина секретного ключа уменьшается и становится равной

$$\ell = 1 - h(\varepsilon(\zeta) + O(\mu_T)) - h(Q) = \\ = 1 - h\left(\frac{\zeta}{1-\zeta} + O(\mu_T)\right) - h(Q) < \\ < 1 - h\left(\frac{\zeta}{1-\zeta}\right) - h(Q), \quad (60)$$

что меньше, чем без зондирования фазового модулятора. Отметим также, что нижняя граница нехватки информации подслушивателя, которая выражается через условную энтропию, достигается на совместных коллективных измерениях отраженных квантовых состояний и квантовых состояний ancilla при атаке на информационные квантовые состояния в канале связи.

5. СОВМЕСТНОЕ ДЕТЕКТИРОВАНИЕ ПОБОЧНОГО ИЗЛУЧЕНИЯ И АКТИВНОЕ ЗОНДИРОВАНИЕ СОСТОЯНИЯ ФАЗОВОГО МОДУЛЯТОРА ПЕРЕДАЮЩЕЙ СТАНЦИИ

Рассмотрим комбинированную атаку с детектированием побочного излучения передающей станции и активного зондирования фазового модулятора. Для этого необходимо включить в матрицу плотности квантовые состояния в обоих побочных каналах утечки информации. С учетом формул (30) и (50) матрица плотности Алиса–Ева для комбинированной атаки имеет вид

$$\overline{\rho}_{XQST} = \frac{1}{2}|0\rangle_{X\,X}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_S \times \\ \times {}_S\langle e_1|] \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes [|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|] + \\ + \frac{1}{2}|1\rangle_{X\,X}\langle 1| \otimes [p|e_0\rangle_{SS}\langle e_0| + (1-p)|e_1\rangle_{SS}\langle e_1|] \otimes |\lambda_1\rangle_T \times \\ \times {}_T\langle\lambda_1| \otimes [|\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1| + |\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|]. \quad (61)$$

Вычисление энтропии для матрицы плотности (61) дает

$$H(\overline{\rho}_{XQST}) = 1 + h(p) + h(Q). \quad (62)$$

Далее, частичная матрица плотности, которую имеет в своем распоряжении Ева, с учетом (61) равна

$$\overline{\rho}_{QST} = \frac{1}{2}(1-Q)[(1-p)|\lambda_0\rangle_{TT}\langle\lambda_0| \otimes |\overline{\Phi}_0\rangle_Q \times \\ \times {}_Q\langle\overline{\Phi}_0| + p|\lambda_1\rangle_{TT}\langle\lambda_1| \otimes |\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1|] \otimes |e_0\rangle_{SS}\langle e_0| + \\ + \frac{1}{2}(1-Q)[p|\lambda_0\rangle_{TT}\langle\lambda_0| \otimes |\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| + (1-p)|\lambda_1\rangle_T \times \\ \times {}_T\langle\lambda_1| \otimes |\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1|] \otimes |e_1\rangle_{SS}\langle e_1| + \\ + \frac{1}{2}Q[(1-p)|\lambda_0\rangle_{TT}\langle\lambda_0| \otimes |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0| + p|\lambda_1\rangle_T \times \\ \times {}_T\langle\lambda_1| \otimes |\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|] \otimes |e_0\rangle_{SS}\langle e_0| + \\ + \frac{1}{2}Q[p|\lambda_0\rangle_{TT}\langle\lambda_0| \otimes |\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0| + (1-p)|\lambda_1\rangle_T \times \\ \times {}_T\langle\lambda_1| \otimes |\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|] \otimes |e_1\rangle_{SS}\langle e_1|. \quad (63)$$

Аналогично предыдущему (см. (42), (55)) секулярное уравнение, определяющее собственные числа матрицы плотности (63), записывается как

$$\mathrm{Det}\begin{pmatrix} (1-p) + p\eta^2\varepsilon(\zeta)^2 - \lambda & (1-p)\eta\varepsilon(\zeta) + p\eta\varepsilon(\zeta) - \lambda\eta\varepsilon(\zeta) \\ (1-p)\eta\varepsilon(\zeta) + p\eta\varepsilon(\zeta) - \lambda\eta\varepsilon(\zeta) & (1-p)\eta^2\varepsilon(\zeta)^2 + p - \lambda \end{pmatrix} = 0. \quad (64)$$

Собственные числа (63) с учетом секулярного уравнения (64) имеют вид

$$\frac{1}{2}(1-Q)\left(\frac{1+\varepsilon(\zeta,\eta,p)}{2}\right), \\ \frac{1}{2}(1-Q)\left(\frac{1-\varepsilon(\zeta,\eta,p)}{2}\right), \quad (65) \\ \frac{1}{2}Q\left(\frac{1+\varepsilon(\zeta,\eta,p)}{2}\right), \quad \frac{1}{2}Q\left(\frac{1-\varepsilon(\zeta,\eta,p)}{2}\right),$$

где

$$\varepsilon(\zeta,\eta,p) = \sqrt{1 - 4\frac{[(1-p) + p\eta^2\varepsilon(\zeta)^2][(1-p)\eta^2\varepsilon(\zeta)^2 + p] - \eta^2\varepsilon(\zeta)^2}{1 - \eta^2\varepsilon(\zeta)^2}}. \quad (66)$$

Принимая во внимание (65), для энтропии $H(\overline{\rho}_{QST})$ получаем

$$H(\overline{\rho}_{QST}) = 1 + h(Q) + \chi\left(\frac{1 \pm \varepsilon(\zeta,\eta,p)}{2}\right), \quad (67)$$

где информация Холево [12–14]

$$\chi\left(\frac{1 \pm \varepsilon(\zeta,\eta,p)}{2}\right) = -\frac{1+\varepsilon(\zeta,\eta,p)}{2} \times \\ \times \log\left(\frac{1+\varepsilon(\zeta,\eta,p)}{2}\right) - \frac{1-\varepsilon(\zeta,\eta,p)}{2} \times \\ \times \log\left(\frac{1-\varepsilon(\zeta,\eta,p)}{2}\right). \quad (68)$$

Собирая вместе формулы (62) и (67), окончательно для длины секретного ключа получаем

$$\ell = H(\overline{\rho}_{XQST}|\overline{\rho}_{QST}) - H(\overline{\rho}_{XY}|\overline{\rho}_{Y}) = \\ = h(p) - \chi\left(\frac{1 \pm \varepsilon(\zeta,\eta,p)}{2}\right) - h(Q) = \\ = [1 - \chi_{Hol}(\zeta,p,\eta)] - h(Q). \quad (69)$$

6. СОВМЕСТНОЕ ДЕТЕКТИРОВАНИЕ ПОБОЧНОГО ИЗЛУЧЕНИЯ, АКТИВНОЕ ЗОНДИРОВАНИЕ ФАЗОВОГО МОДУЛЯТОРА ПЕРЕДАЮЩЕЙ СТАНЦИИ И ДЕТЕКТИРОВАНИЕ ПЕРЕИЗЛУЧЕНИЯ ЛАВИННЫХ ДЕТЕКТОРОВ НА ПРИЕМНОЙ СТОРОНЕ

Матрица плотности Алиса–Боб–Ева с учетом упомянутых побочных каналов утечки информации может быть представлена в виде

$$\rho_{XYSQTD} = \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_S \times \\ \times {}_S\langle e_1|] \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes \left\{(1-Q)|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0| \otimes \right. \\ \otimes [(1-d)|d_0\rangle_{DD}\langle d_0| + d|d_1\rangle_{DD}\langle d_1|] \otimes |0\rangle_{YY}\langle 0| + \\ + Q|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0| \otimes [(1-d)|d_1\rangle_{DD}\langle d_1| + d|d_0\rangle_D \times \\ \times {}_D\langle d_0|] \otimes |1\rangle_{YY}\langle 1|\} + \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes [(1-p)|e_1\rangle_S \times \\ \times {}_S\langle e_1| + p|e_0\rangle_{SS}\langle e_0|] \otimes |\lambda_1\rangle_{TT}\langle\lambda_1| \otimes \left\{(1-Q)|\overline{\Phi}_1\rangle_Q \times \right. \\ \times {}_Q\langle\overline{\Phi}_1| \otimes [(1-d)|d_1\rangle_{DD}\langle d_1| + d|d_0\rangle_{DD}\langle d_0|] \otimes |1\rangle_Y \times \\ \times {}_Y\langle 1| + Q|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1| \otimes [(1-d)|d_0\rangle_{DD}\langle d_0| + d|d_1\rangle_D \times \\ \times {}_D\langle d_1|] \otimes |0\rangle_{YY}\langle 0|\}. \quad (70)$$

Матрица плотности имеет простую интерпретацию. Детектирование состояний $|0\rangle_{YY}\langle 0|$ или $|1\rangle_{YY}\langle 1|$ на приемной стороне проводится двумя лавинными детекторами (см. рисунок). При срабатывании детектора образуется лавина носителей, при их рекомбинации может происходить обратное переизлучение в волоконный канал связи, которое может детектироваться Евой. Для учета такого переизлучения требуется ввести в рассмотрение еще один побочный канал утечки, точнее, квантовое состояние, связанное с переизлучением.

Если, например, зарегистрировано состояние $|0\rangle_{YY}\langle 0|$, то это приведет к появлению в побочном канале состояния $[(1-d)|d_0\rangle_{DD}\langle d_0| + d|d_1\rangle_{DD}\langle d_1|]$ — матрицы плотности. Неформально это означает, что с вероятностью $1-d$ Ева будет иметь в своем распоряжении состояние $|d_0\rangle_{DD}\langle d_0|$ и с вероятностью d — состояние $|d_1\rangle_{DD}\langle d_1|$. Состояния $|d_0\rangle_{DD}\langle d_0|$ и $|d_1\rangle_{DD}\langle d_1|$ можно считать ортогональными (чтобы не загромождать выкладки несущественными деталями), тогда с вероятностью $1-d$ Ева, детектируя обратное переизлучение, правильно узнает регистрируемый бит ключа, а с вероятностью d — ошибается. Вероятность различения включена в вероятность d. Аналогично учитываются состояния в побочном канале при регистрации 1. Отметим, что мы рассматриваем симметричную ситуацию в побочном канале. Это сделано исключительно для экономии математических выкладок. Не составляет труда обобщить выкладки на случай, когда состояния и вероятности при регистрации 0 и 1 оказываются разными.

Реализация протокола с фазово-временным кодированием (см. рисунок) не использует фазового модулятора на приемной стороне, поэтому побочный канал утечки информации, связанный с зондированием фазового модулятора на приемной стороне, отсутствует. Отсутствие фазового модулятора достигается за счет использования протокола с фазово-временным кодированием, что делает систему устойчивой к такой атаке по сравнению с другими системами.

При регистрации 0 и 1 состояние электронного оборудования приемной станции является разным, поэтому побочное электромагнитное излучение, связанное с работой электроники, также является разным. Электромагнитное излучение может регистрироваться Евой. Побочный канал, связанный с электромагнитным излучением электронного оборудования приемной станции при регистрации 0 и 1 может быть включен в состояния $|d_0\rangle_{DD}\langle d_0|$ и $|d_1\rangle_{DD}\langle d_1|$, соответствующие вероятностям $d-1$ и d. С учетом (70) матрица плотности Алиса–Ева дается частичным следом по пространству состояний Боба, получаем

$$\rho_{XSQTD}=\frac{1}{2}|0\rangle_{XX}\langle 0|\otimes[(1-p)|e_0\rangle_{SS}\langle e_0|+p|e_1\rangle_S\times$$
$$\times\,{}_S\langle e_1|]\otimes|\lambda_0\rangle_{TT}\langle\lambda_0|\otimes\big\{(1-Q)|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0|\otimes$$
$$\otimes\,[(1-d)|d_0\rangle_{DD}\langle d_0|+d|d_1\rangle_{DD}\langle d_1|]+$$
$$+Q|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|\otimes[(1-d)|d_1\rangle_{DD}\langle d_1|+d|d_0\rangle_{DD}\langle d_0|]\big\}+$$
$$+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[(1-p)|e_1\rangle_{SS}\langle e_1|+p|e_0\rangle_{SS}\langle e_0|]\otimes|\lambda_1\rangle_T\times$$
$$\times\,{}_T\langle\lambda_1|\otimes\big\{(1-Q)|\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1|\otimes[(1-d)|d_1\rangle_D\times$$
$$\times\,{}_D\langle d_1|+d|d_0\rangle_{DD}\langle d_0|]+Q|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|\otimes[(1-d)|d_0\rangle_D\times$$
$$\times\,{}_D\langle d_0|+d|d_1\rangle_{DD}\langle d_1|]\big\}. \quad (71)$$

Собственные числа (71) равны

$$\frac{1}{2}(1-Q)(1-p)(1-d),\quad \frac{1}{2}Q(1-p)(1-d),$$
$$\frac{1}{2}(1-Q)p(1-d),\quad \frac{1}{2}Qp(1-d), \quad (72)$$

$$\frac{1}{2}(1-Q)(1-p)d,\quad \frac{1}{2}Q(1-p)d,$$
$$\frac{1}{2}(1-Q)pd,\quad \frac{1}{2}Qpd, \quad (73)$$

собственные числа двукратно вырождены. С учетом (72), (73) получаем выражение для энтропии:

$$H(\rho_{XSQTDD})=1+h(p)+h(d)+h(Q). \quad (74)$$

Перейдем к вычислению $H(\rho_{SQTD})$. Для матрицы плотности ρ_{SQTD} находим

$$\rho_{SQTD}=\frac{1}{2}[(1-p)|e_0\rangle_{SS}\langle e_0|+p|e_1\rangle_{SS}\langle e_1|]\otimes|\lambda_0\rangle_Q\times$$
$$\times\,{}_Q\langle\lambda_0|\otimes\big[(1-Q)|\overline{\Phi}_0\rangle_{QQ}\langle\overline{\Phi}_0|\otimes[(1-d)|d_0\rangle_D\times$$
$$\times\,{}_D\langle d_0|+d|d_1\rangle_{DD}\langle d_1|]+Q|\overline{\Theta}_0\rangle_{QQ}\langle\overline{\Theta}_0|\otimes$$
$$\otimes\,[(1-d)|d_1\rangle_{DD}\langle d_1|+d|d_0\rangle_{DD}\langle d_0|]]+$$
$$+\frac{1}{2}[(1-p)|e_1\rangle_{SS}\langle e_1|+p|e_0\rangle_{SS}\langle e_0|]\otimes|\lambda_1\rangle_{TT}\langle\lambda_1|\otimes$$
$$\otimes\big[(1-Q)|\overline{\Phi}_1\rangle_{QQ}\langle\overline{\Phi}_1|\otimes[(1-d)|d_1\rangle_D\times$$
$$\times\,{}_D\langle d_1|+d|d_0\rangle_{DD}\langle d_0|]+Q|\overline{\Theta}_1\rangle_{QQ}\langle\overline{\Theta}_1|\otimes$$
$$\otimes\,[(1-d)|d_0\rangle_{DD}\langle d_0|+d|d_1\rangle_{DD}\langle d_1|]]. \quad (75)$$

Собственные числа ρ_{SQTD} определяются корнями секулярных уравнений

$$\mathrm{Det}\begin{pmatrix} A_i-\lambda & \varepsilon(\zeta)\eta(C_i-\lambda)\\ \varepsilon(\zeta)\eta(C_i-\lambda) & B_i-\lambda\end{pmatrix}=0, \quad (76)$$

где

$$A_1=(1-p)(1-d)+pd\varepsilon(\zeta)^2\eta^2,$$
$$B_1=(1-p)(1-d)\varepsilon(\zeta)^2\eta^2+pd, \quad (77)$$
$$C_1=(1-p)(1-d)+pd,$$

$$A_2=(1-p)d+p(1-d)\varepsilon(\zeta)^2\eta^2,$$
$$B_2=(1-p)d\varepsilon(\zeta)^2\eta^2+p(1-d), \quad (78)$$
$$C_2=(1-p)d+p(1-d),$$

$$A_3=p(1-d)+(1-p)d\varepsilon(\zeta)^2\eta^2,$$
$$B_3=p(1-d)\varepsilon(\zeta)^2\eta^2+(1-p)d, \quad (79)$$
$$C_3=p(1-d)+(1-p)d,$$

$$A_4=pd+(1-p)(1-d)\varepsilon(\zeta)^2\eta^2,$$
$$B_4=pd\varepsilon(\zeta)^2\eta^2+(1-p)(1-d), \quad (80)$$
$$C_4=pd+(1-p)(1-d).$$

Корни (76)–(80) равны

$$\lambda_{i\pm}=\frac{1}{2(1-\varepsilon(\zeta)^2\eta^2)}\times$$
$$\times\left[A_i+B_i-2\varepsilon(\zeta)^2\eta^2C_i\pm\sqrt{[A_i+B_i-2\varepsilon(\zeta)^2\eta^2C_i]^2-4[A_iB_i-\varepsilon(\zeta)^2\eta^2C_i^2](1-\varepsilon(\zeta)^2\eta^2)}\right]. \quad (81)$$

Собственные числа (76)–(80) равны

$$\frac{1}{2}(1-Q)\lambda_{i\pm},\quad \frac{1}{2}Q\lambda_{i\pm},,\quad i=1,2,3,4. \quad (82)$$

Введем обозначение

$$\chi_i(\zeta,p,d,\eta)=-\lambda_{i+}\log(\lambda_{i+})-\lambda_{i-}\log(\lambda_{i-}),$$
$$\chi(\zeta,p,\eta,d)=\frac{1}{2}\sum_{i=1}^{4}\chi_i(\zeta,p,d,\eta). \quad (83)$$

Для условной энтропии получаем

$$H(\rho_{XSQTD}|\rho_{SQTD})=h(p)+h(d)-\chi(\zeta,p,d,\eta). \quad (84)$$

В итоге для оценки длины секретного ключа в строго однофотонном случае с учетом (74), (83) имеем

$$\ell = \lim_{n\to\infty} \frac{\ell_n}{n} = h(p) + h(d) - \chi(\zeta, p, d, \eta) - h(Q) = \\ = [1 - \chi_{Hol}(\zeta, p, d, \eta)] - h(Q), \quad (85)$$

где утечка информации при коррекции ошибок взята в шенноновском пределе. При коррекции конструктивными кодами последнее слагаемое в правой части (85) нужно заменить на реальное число битов в пересчете на одну позицию, раскрытое при коррекции ошибок, $h(Q) \to \text{leak}$.

Еще раз отметим, что выражение для длины секретного ключа (85) учитывает совместные коллективные измерения Евы над квантовыми состояниями в побочных каналах и квантовом канале связи.

7. АКТИВНОЕ ЗОНДИРОВАНИЕ СОСТОЯНИЯ МОДУЛЯТОРА ИНТЕНСИВНОСТИ НА ПЕРЕДАЮЩЕЙ СТАНЦИИ

Выше были получены формулы для длины секретного ключа с учетом побочных каналов утечки информации, когда состояния являются строго одофотонными. В реальной ситуации информационные состояния в квантовом канале связи представляют собой статистическую смесь состояний с разным фоковским числом фотонов. Подчеркнем, что реализация системы, использующей импульсный лазер, который включается и выключается в каждой посылке на передающей стороне (см. рисунок), приводит к рандомизации фаз информационных когерентных состояний в разных посылках. Именно по этой причине в квантовом канале связи присутствуют не чистые когерентные состояния, а статистическая смесь фоковских состояний с пуассоновской статистикой по числу фотонов.

Секретный ключ набирается только из однофотонной компоненты статистической смеси состояний. Консервативно в пользу подслушивателя считается, что информация, заключенная в многофотонных компонентах состояний, известна подслушивателю. Поэтому для оценки доли однофотонной компоненты состояний, достигающей приемной стороны, используется Decoy State-метод. В этом методе случайно посылаются в квантовый канал связи состояния с разным средним числом фотонов. Состояние с фоковским числом фотонов k может происходить из состояния с любым средним числом фотонов. Принципиальным моментом для Decoy State-метода является то обстоятельство, что, обнаружив данное фоковское число фотонов в квантовом канале связи, подслушиватель не может знать, из какого состояния и с каким средним числом фотонов происходит данная компонента состояний.

При активном зондировании состояния модулятора интенсивности это условие нарушается. Подслушиватель, пусть с некоторой вероятностью, знает, из какого состояния произошла компонента состояний с данным фоковским числом фотонов. По этой причине при активном зондировании модулятора интенсивности стандартный Decoy State-метод не работает. Ниже явно покажем, на каком этапе это происходит.

Побочный канал утечки информации, связанный с активным зондированием модулятора интенсивности на передающей станции, обладает принципиальным отличием от других побочных каналов. Отраженные от модулятора интенсивности зондирующие состояния не несут прямой информации о передаваемом бите ключа, а лишь об интенсивности состояния — среднем числе фотонов. Поэтому отраженные квантовые состояния не могут непосредственно быть включены в матрицу плотности Алиса–Боб–Ева, через которую вычисляется условная энтропия и утечка информации к подслушивателю.

В предыдущих разделах состояния в побочных каналах утечки информации мы «привязывали» к однофотонной компоненте состояний. Естественно, побочные каналы утечки имеют место и в том случае, когда в квантовом канале присутствуют неоднофотонные компоненты состояний. Но поскольку информация о битах ключа, содержащаяся в этих компонентах и так консервативно в пользу подслушивателя, считается известной Еве, не нужно «привязывать» состояния в побочных каналах к многофотонным компонентам информационных состояний.

Зондирование состояния модулятора интенсивности в отличие от зондирования состояния фазового модулятора не дает прямой информации о передаваемом бите ключа, а дает лишь информацию об интенсивности передаваемого состояния. Доля однофотонной компоненты состояний и вероятность ошибки в ней в посылках, в которых посылались информационные состояния, оценивается через изменение статистики фотоотсчетов в посылках, в которых посылались состояния «ловушки». Имея дополнительную информацию о том, какое состояние передается в конкретной посылке — информационное или состояние «ловушка», подслушиватель может менять свою стратегию при данном обнаруженном числе фотонов k. Например, если известно, что

послано состояние «ловушка», то подслушиватель ничего не делает (ведет себя пассивно) и не искажается статистику фотоотсчетов состояний ловушек.

Ниже мы модифицируем Decoy State-метод на случай активного зондирования модулятора интенсивности, неформально, когда подслушиватель имеет дополнительно в своем распоряжении отраженное квантовое состояние, которое несет информацию о состоянии модулятора интенсивности, соответственно о среднем числе фотонов.

Обозначим отраженное от модулятора интенсивности зондирующее квантовое состояние как $|\psi(\xi)\rangle_{S_M}$. Примем, что данное состояние зависит только от состояния модулятора интенсивности, т. е. от того, какое состояние со средним числом фотонов $\xi \in \mathcal{I} = \{\mu, \nu_1, \nu_2\}$ посылается в канал связи. Возможно обобщение на случай, когда данное состояние зависит также от состояния фазового модулятора. Но чтобы не загромождать выкладки, приведем вывод только для упомянутого случая.

При измерении числа фотонов в канале связи вместо состояния $|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|$, которое не зависит от среднего числа фотонов ξ, Ева имеет в своем распоряжении состояние $|\Psi_k^x(\xi)\rangle_{BSBS}\langle\Psi_k^x(\xi)|$. Данное состояние содержит информацию о среднем числе фотонов, что дается присутствием отраженного зондирующего состояния $|\psi(\xi)\rangle_{S_M}$. Данное состояние дает Еве дополнительную информацию об интенсивности передаваемого состояния. Информационное квантовое состояние вместе с зондирующим отраженным состоянием, доступное Еве, имеет вид

$$\rho^x(\xi) = e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}|\Psi_k^x(\xi)\rangle_{BS_MBS_M}\langle\Psi_k^x(\xi)| = \\ = \sum_{k=0}^{\infty}P^{(k)}(\xi)|\Psi_k^x(\xi)\rangle_{BS_MBS_M}\langle\Psi_k^x(\xi)|, \quad (86)$$

$$P^{(k)}(\xi) = e^{-2\xi}\frac{(2\xi)^k}{k!},$$

$$|\Psi_k^x(\xi)\rangle_{BS_M} = |\Psi_k^x)\rangle_B \otimes |\psi(\xi)\rangle_{S_M}, \quad \xi = \mu, \nu_1, \nu_2,$$

где отраженное от модулятора интенсивности состояние $|\psi(\xi)\rangle_{S_M}$ не зависит от информационного состояния.

Ева имеет в своем распоряжении отраженное от модулятора интенсивности квантовое состояние, поэтому действия Евы после обнаружения фоковского состояния с данным числом фотонов будут зависеть еще от дополнительной информации, которую подслушиватель может получить из отраженного состояния. Действия Евы определяются результатом измерения на ходу над отраженным состоянием. Цель измерений Евы — узнать, из состояния с каким средним числом фотонов ξ произошла компонента с данным числом фотонов k. Фактически цель подслушивателя состоит в различении одного из состояний $|\psi(\mu)\rangle_{S_M}$, $|\psi(\nu_1)\rangle_{S_M}$, $|\psi(\nu_2)\rangle_{S_M}$.

Полное измерение Евы и Боба ($\mathcal{I} = \{\mu, \nu_1, \nu_2\}$) дается разложением единицы:

$$I_{BS_M} = I_B \otimes I_{S_M} = \left(\sum_{\xi'\in\mathcal{I}}\mathcal{F}_{\xi'}\right)\otimes \\ \otimes\left(\sum_{y\in\mathcal{Y}}\mathcal{M}_y\right), \quad \xi' \in \{\mu, \nu_1, \nu_2\}. \quad (87)$$

Измерение подслушивателя над отраженным состоянием дается положительно-значными мерами $\mathcal{F}_{\xi'}$. Естественно, подслушиватель выбирает оптимальное измерение, которое минимизирует ошибку различения отраженных состояний, отвечающих состояниям с разным средним числом фотонов. Для конструирования оптимального измерения необходимо знать структуру отраженного состояния, что должно определяться экспериментально для конкретной реализации системы криптографии.

Далее нам не потребуются явно сами отраженные состояния, нужно лишь знать вероятности различения разных состояний, которые считаем известными из экспериментальных измерений. С учетом (86), (87) получаем

$$P_{J|I}(\xi'|I = \xi) = \mathrm{Tr}_S\{\mathcal{F}_{\xi'}|\psi(\xi)\rangle_{SS}\langle\psi(\xi)|\}, \\ \mathcal{J} = \{\mu, \nu_1, \nu_2\}, \quad (88)$$

где $P_{J|I}(\xi'|I = \xi)$ — условная вероятность того, что в канал было послано состояние со средним числом фотонов ξ, а подслушиватель в результате измерений (87), (88) получил исход ξ' — Ева приняла решение, что в канале присутствует состояние со средним числом фотонов ξ'.

С учетом сказанного действие супероператора Евы может быть представлено в виде

$$\mathcal{T}_{BS_M}[|\Psi_k^x)\rangle_B \otimes |\psi(\xi)\rangle_{S_MS_M}\langle\psi(\xi)| \otimes {}_B\langle\Psi_k^x)|] = \\ = \sum_{\xi'\in\mathcal{J}}P_{J|I}(\xi'|I = \xi)\rho^x_{k,\xi',B}. \quad (89)$$

Дадим интерпретацию формулы (89). После обнаружения в канале числа фотонов k Ева в зависимости от исхода измерений над отраженным квантовым состоянием осуществляет преобразование фоковского информационного состояния. Это означает, что преобразованная матрица плотности $\rho^x_{k,\xi',B}$, в отличие от ситуации без побочного канала, зависит от исходного состояния — от среднего числа фотонов ξ

в нем. Эта зависимость выражается через переходные вероятности $P_{J|I}(\xi'|I=\xi)$, которые определяются различимостью отраженных состояний.

Фактически по этой причине стандартный Decoy State-метод не работает при атаке активного зондирования модулятора интенсивности.

Вероятность исходов измерений на приемной стороне Боба выражается через матрицу плотности в (89), с учетом (88) находим

$$P^{(k)}_{X|Y}(y,\xi'|X=x)=\mathrm{Tr}_B\{\mathcal{M}_y\rho^x_{k,\xi',B}\}, \quad x=0,1, \quad y=0,1,c. \tag{90}$$

Для парциального темпа отсчетов в информационных временных окнах на приемной стороне получаем

$$P^{inf}_{\xi}(y|X=x)=\sum_{k=0}^{\infty}P^{(k)}(\xi)\times \times\sum_{\xi'\in\mathcal{J}}P_{J|I}(\xi'|I=\xi)P^{(k)}_{X|Y}(y,\xi'|X=x), \quad y=0,1. \tag{91}$$

Аналогично для парциального темпа отсчетов в контрольном временном окне на приемной стороне получаем

$$P^{contr}_{\xi}(y|X=x)=\sum_{k=0}^{\infty}P^{(k)}(\xi)\times \times\sum_{\xi'\in\mathcal{J}}P_{J|I}(\xi'|I=\xi)P^{(k)}_{X|Y}(y,\xi'|X=x), \quad y=c. \tag{92}$$

Для полного темпа отсчетов в информационных временных окнах $y=0,1$ с учетом (91) находим

$$P^{inf,tot}_{\xi}=\sum_{x\in\{0,1\}}\sum_{y\in\{0,1\}}P_X(x)P^{inf}_{\xi}(y|X=x)= =\sum_{k=0}^{\infty}P^{(k)}(\xi)\sum_{\xi'\in\mathcal{J}}P_{J|I}(\xi'|I=\xi)\times \times\sum_{x\in\{0,1\}}\sum_{y\in\{0,1\}}P_X(x)P^{(k)}_{X|Y}(y,\xi'|X=x). \tag{93}$$

Для полного темпа отсчетов в контрольном окне (индекс c) 3 в базисе L и окне 1 в базисе R с учетом (92) находим

$$P^{contr,tot}_{\xi}=\sum_{x\in\{0,1\}}\sum_{y\in\{C\}}P_X(x)P^{contr}_{\xi}(y|X=x)= =\sum_{k=0}^{\infty}P^{(k)}(\xi)\sum_{\xi'\in\mathcal{J}}P_{J|I}(\xi'|I=\xi)\times \times\sum_{x\in\{0,1\}}\sum_{y\in\{C\}}P_X(x)P^{(k)}_{X|Y}(y,\xi'|X=x). \tag{94}$$

Перейдем к более компактным обозначениям, для вероятности отсчетов в информационных временных окон получаем

$$Y^{inf}_k(\xi')= =\sum_{x\in\{0,1\}}\sum_{y\in\{0,1\}}P_X(x)P^{(k)}_{X|Y}(y,\xi'|X=x). \tag{95}$$

Во избежание недоразумений необходимо интерпретировать величины $P^{(k)}_{X|Y}(y,\xi'|X=x)$ и пояснить обозначения. Хотя обозначение и выглядит как вероятность, но не является нормированной на единицу величиной. Рассмотрим посылки, в которых базисы Алисы и Боба совпадали, и Алиса посылала состояния со средним числом фотонов ξ. Выделим посылки, в которых Алиса посылала состояния, отвечающие биту x с вероятностью $P_X(x)$. Пусть таких посылок было $N(x)$. Рассмотрим отсчеты у Боба в информационных временных окнах. Действия Евы зависят от исхода измерений над отраженными состояниями от модулятора интенсивности. Пусть Ева решила, что k-фотонная компонента состояний произошла от состояний со средним числом фотонов ξ' при заданном (реальном) ξ (см. формулу (91)). На приемной стороне для k-фотонной компоненты состояний при условии, что Ева решила, что в канале состояния со средним числом фотонов ξ' и информационный бит есть x, будет зарегистрировано $N^{(k)}(\xi',y)$ отсчетов и результат регистрации бита будет интерпретирован Бобом как y. При больших $N(\xi,x)$ доля отсчетов $\frac{N^{(k)}(\xi',y)}{N(x)}$ будет стремиться к $P^{(k)}_{X|Y}(y,\xi'|X=x)$ (см. формулу (95)).

Для вероятности отсчетов в контрольных временных окнах получаем

$$Y^{contr}_k(\xi')= =\sum_{x\in\{0,1\}}\sum_{y\in\{C\}}P_X(x)P^{(k)}_{X|Y}(y,\xi'|X=x). \tag{96}$$

Далее, обозначив для краткости $P(\xi'|\mu)= =P_{J|I}(\xi'|I=\mu)$ для (88), находим

$$P^{inf,tot}_{\mu}=\sum_{k=0}^{\infty}P^{(k)}(\mu)\sum_{\xi'\in\mathcal{J}}P(\xi'|\mu)Y^{inf}_k(\xi'), \tag{97}$$

$$P_{\mu}^{contr,tot}=\sum_{k=0}^{\infty}P^{(k)}(\mu)\sum_{\xi'\in\mathcal{J}}P(\xi'|\mu)Y_k^{contr}(\xi'). \quad (98)$$

Получим выражение для парциальной ошибки в информационных состояниях:

$$e_k(\xi')=\frac{\sum\limits_{x=0,1,y=0,1,x\neq y}P_X(i)P_{X|Y}^{(k)}(y,\xi'|X=x)}{\sum\limits_{x=0,1,y=0,1}P_X(i)P_{X|Y}^{(k)}(y,\xi'|X=x)}. \quad (99)$$

Используя (91), (93), (96), получаем выражение для полной ошибки в информационных состояниях:

$$\mathrm{Err}_{\mu}^{tot}=\sum_{k=0}^{\infty}P^{(k)}(\mu)\sum_{\xi'\in\mathcal{J}}P(\xi'|\mu)e_k(\xi')Y_k^{inf}(\xi'). \quad (100)$$

8. ОЦЕНКА ПАРАМЕТРОВ ОДНОФОТОННОЙ КОМПОНЕНТЫ ИНФОРМАЦИОННЫХ СОСТОЯНИЙ НА ПРИЕМНОЙ СТАНЦИИ

Нашей дальнейшей целью будет оценка вероятности однофотонной компоненты и ошибки в однофотонной компоненте для определения длины секретного ключа. Для вычисления длины секретного ключа необходимо знать по отдельности величины $Y_1(\mu)$, $Y_1(\nu_1)$, $Y_1(\nu_2)$, аналогично для вероятности ошибки нужны отдельные значения $e_1(\mu)$, $e_1(\nu_1)$, $e_1(\nu_2)$.

Decoy State-метод не позволяет получить выражения для отдельных долей однофотонных компонент и ошибок. Decoy State-метод позволяет получить лишь их комбинации (сумму всех величин, см. ниже). Тем не менее, можно будет получить оценку длины ключа, используя только сумму величин.

Перейдем к получению необходимых комбинаций однофотонных компонент. Для дальнейшего введем новые обозначения:

$$\overline{P}_{\xi}^{inf,tot}=e^{2\xi}P_{\xi}^{inf,tot}=\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}\sum_{\xi'\in\mathcal{J}}P(\xi'|\xi)Y_k^{inf}(\xi), \quad (101)$$

$$\overline{P}_{\xi}^{contr,tot}=e^{2\xi}P_{\xi}^{contr,tot}=\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}\sum_{\xi'\in\mathcal{J}}P(\xi'|\xi)Y_k^{contr}(\xi). \quad (102)$$

Отметим, что в отличие от стандартного Decoy State-метода в выражение для темпа отсчетов состояний с разным средним числом фотонов входят различные величины $Y_k^{inf,contr}$ и с разными весовыми коэффициентами — условными вероятностями, зависящими от отраженных состояний от модулятора интенсивности.

Введем новые более удобные обозначения для вероятности ошибки:

$$\overline{\mathrm{Err}}_{\xi}^{tot}=e^{2\xi}\mathrm{Err}_{\xi}^{tot}=\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}\sum_{\xi'\in\mathcal{J}}P(\xi'|\xi)e_k(\xi)Y_k^{inf}(\xi). \quad (103)$$

Далее обозначим

$$\begin{aligned}p^{min}(\xi)&=\min_{\xi'\in\{\mu,\nu_1,\nu_2\}}P(\xi'|\xi),\\ p^{max}(\xi)&=\max_{\xi'\in\{\mu,\nu_1,\nu_2\}}P(\xi'|\xi).\end{aligned} \quad (104)$$

С использованием (101)–(104) получаем следующую цепочку неравенств:

$$\overline{P}_{\mu}^{inf,tot}\geq p^{min}(\mu)Y_0^{inf,\Sigma}+p^{min}(\mu)\times\left[2\mu Y_1^{inf,\Sigma}+\sum_{k=2}^{\infty}\frac{(2\mu)^k}{k!}Y_k^{inf,\Sigma}\right], \quad (105)$$

$$\begin{aligned}Y_k^{inf,\Sigma}&=Y_k^{inf}(\mu)+Y_k^{inf}(\nu_1)+Y_k^{inf}(\nu_2),\\ Y_0^{inf,\Sigma}&=\sum_{\xi\in\{\mu,\nu_1,\nu_2\}}Y_0^{inf}(\xi).\end{aligned} \quad (106)$$

Далее имеем

$$\overline{P}_{\nu_1}^{inf,tot}\leq p^{max}(\nu_1)Y_0^{inf,\Sigma}+p^{max}(\nu_1)\times\left[2\nu_1 Y_1^{inf,\Sigma}+\sum_{k=2}^{\infty}\frac{(2\nu_1)^k}{k!}Y_k^{inf,\Sigma}\right], \quad (107)$$

$$\overline{P}_{\nu_2}^{inf,tot}\geq p^{min}(\nu_2)Y_0^{inf,\Sigma}+p^{min}(\nu_2)\times\left[2\nu_2 Y_1^{inf,\Sigma}+\sum_{k=2}^{\infty}\frac{(2\nu_2)^k}{k!}Y_k^{\Sigma}\right]. \quad (108)$$

Введены обозначения

$$\begin{aligned}\overline{P}_{\mu}^{inf,tot,min}&=\frac{P_{\mu}^{inf,tot}}{p^{min}(\mu)},\\ \overline{P}_{\nu_1}^{inf,tot,max}&=\frac{P_{\nu_1}^{inf,tot}}{p^{max}(\nu_1)}.\end{aligned} \quad (109)$$

Комбинируя (105)–(109), находим

$$(2\nu_1-2\nu_2)Y_1^{inf,\Sigma}\geq\left[\overline{P}_{\nu_1}^{inf,tot,max}-\overline{P}_{\nu_2}^{inf,tot,min}\right]-\\-\sum_{k=2}^{\infty}\frac{(2\nu_1)^k-(2\nu_2)^k}{k!}Y_k^{inf,\Sigma}. \quad (110)$$

Учитывая, что

$$\frac{(2\nu_1)^2-(2\nu_2)^2}{(2\mu)^2}\sum_{k=2}^{\infty}\frac{(2\mu)^k}{k!}Y_k^{inf,\Sigma}\geq\\\geq\sum_{k=2}^{\infty}\frac{(2\nu_1)^k-(2\nu_2)^k}{k!}Y_k^{inf,\Sigma}, \quad (111)$$

а также (110), (111), получаем

$$\overline{P}_{\mu}^{inf,tot,min}-Y_0^{inf,\Sigma}-2\mu Y_1^{inf,\Sigma}\geq\\\geq\sum_{k=2}^{\infty}\frac{(2\mu)^k}{k!}Y_k^{inf,\Sigma}. \quad (112)$$

Окончательно находим

$$Y_1^{inf,\Sigma}\geq\frac{1}{(2\nu_1-2\nu_2)-\dfrac{(2\nu_1)^2-(2\nu_2)^2}{2\mu}}\times\\\times\left\{\left[\overline{P}_{\nu_1}^{inf,tot,max}-\overline{P}_{\nu_2}^{inf,tot,min}\right]-\frac{(2\nu_1)^2-(2\nu_2)^2}{(2\mu)^2}\times\right.\\\left.\times\left[\overline{P}_{\mu}^{inf,tot,min}-Y_0^{inf,\Sigma}\right]\right\}. \quad (113)$$

Как было упомянуто выше и как видно из (106), (113), удается получить лишь оценку для суммы однофотонных компонент Y_1^{Σ}, а не оценку для отдельных компонент. В то же время в оценку для длины секретного ключа (см. ниже формулу (129)) входят значения отдельных компонент. Ниже увидим, что эту проблему удается обойти, используя свойство выпуклости условных энтропий (см. ниже).

Для оценки суммарной доли вакуумной компоненты Y_0^{Σ} получаем

$$Y_0^{inf,\Sigma}\geq\\\geq\max\left\{\frac{2\nu_1\overline{P}_{\nu_2}^{inf,tot,max}-2\nu_2\overline{P}_{\nu_1}^{inf,tot,min}}{2\nu_1-2\nu_2},0\right\}, \quad (114)$$

где

$$\overline{P}_{\nu_{1,2}}^{inf,tot,min}=\frac{P_{\nu_{1,2}}^{inf,tot}}{p^{min}(\nu_{1,2})},\\\overline{P}_{\nu_{1,2}}^{inf,tot,max}=\frac{P_{\nu_{1,2}}^{inf,tot}}{p^{max}(\nu_{1,2})}. \quad (115)$$

Как следует из формул (28), (40), в длину секретного ключа для однофотонной компоненты входит отношение вероятностей отсчетов в контрольных временных окнах и информационных временных окнах $\zeta/(1-\zeta)$ (см. детали в [10,11]). Нехватка информации Евы о ключе выражается через данное отношение.

Получим оценку для вероятности ошибки в однофотонной компоненте состояний:

$$\overline{\mathrm{Err}}_{\nu_1}^{tot}\geq p^{min}(\nu_1)\left\{\sum_{k=0}^{\infty}\frac{(2\nu_1)^k}{k!}(eY)_k^{\Sigma}\right\}. \quad (116)$$

Аналогично предыдущему находим

$$\overline{\mathrm{Err}}_{\nu_2}^{tot}\leq p^{max}(\nu_2)\left\{\sum_{k=0}^{\infty}\frac{(2\nu_2)^k}{k!}(eY)_k^{\Sigma}\right\}, \quad (117)$$

где введено обозначение

$$(eY)_k^{\Sigma}=e_k(\mu)Y_k^{inf}(\mu)+e_k(\nu_1)Y_k^{inf}(\nu_1)+\\+e_k(\nu_2)Y_k^{inf}(\nu_2). \quad (118)$$

Комбинируя неравенства (116) и (117), получаем

$$(eY)_1^{\Sigma}\leq\frac{\overline{\mathrm{Err}}_{\nu_1}^{tot,min}-\overline{\mathrm{Err}}_{\nu_2}^{tot,max}}{2\nu_1-2\nu_2}, \quad (119)$$

где введены обозначения

$$\overline{\mathrm{Err}}_{\nu_1}^{tot,min}=\frac{\overline{\mathrm{Err}}_{\nu_1}^{tot}}{p^{min}(\nu_1)},\\\overline{\mathrm{Err}}_{\nu_2}^{tot,max}=\frac{\overline{\mathrm{Err}}_{\nu_2}^{tot}}{p^{max}(\nu_2)}. \quad (120)$$

Получим оценку вероятности однофотонной компоненты состояний в контрольных временных окнах:

$$\overline{P}_{\nu_1}^{contr,tot}\geq p^{min}(\nu_1)\left\{\sum_{k=0}^{\infty}\frac{(2\nu_1)^k}{k!}Y_k^{contr,\Sigma}\right\}. \quad (121)$$

Аналогично предыдущему находим

$$\overline{P}_{\nu_2}^{contr,tot}\leq p^{max}(\nu_2)\left\{\sum_{k=0}^{\infty}\frac{(2\nu_2)^k}{k!}Y_k^{contr,\Sigma}\right\}. \quad (122)$$

Комбинируя неравенства (121) и (122), получаем

$$Y_1^{contr,\Sigma}\leq\frac{\overline{P}_{\nu_1}^{contr,tot,min}-\overline{P}_{\nu_2}^{contr,tot,max}}{2\nu_1-2\nu_2}, \quad (123)$$

где введены обозначения

$$\overline{P}_{\nu_1}^{contr,tot,min}=\frac{\overline{P}_{\nu_1}^{contr,tot}}{p^{min}(\nu_1)},\\\overline{P}_{\nu_2}^{contr,tot,max}=\frac{\overline{P}_{\nu_2}^{tot}}{p^{max}(\nu_2)}. \quad (124)$$

Для дальнейшего потребуется отношение, которое входит в нехватку информации Евы о ключе в однофотонной компоненте. Для k-фотонной компоненты имеем

$$\frac{Y_k^{contr}(\xi)}{Y_k^{inf}(\xi)} = \frac{\zeta_k(\xi)}{1-\zeta_k(\xi)}. \tag{125}$$

Далее обозначим для краткости

$$Y_1^{inf,\Sigma} = Y_1^{inf}(\mu) + Y_1^{inf}(\nu_1) + Y_1^{inf}(\nu_2), \tag{126}$$

$$Y_k^{inf,\Sigma} = Y_k^{inf}(\mu) + Y_k^{inf}(\nu_1) + Y_k^{inf}(\nu_2). \tag{127}$$

Модифицированный Decoy State-метод не позволяет получить отдельно парциальные отношения. Он позволяет лишь получить интегральные отношения

$$(\zeta Y)_1^{inf,\Sigma} = \frac{Y_1^{contr,\Sigma}}{Y_1^{inf,\Sigma}}, \tag{128}$$

которых вместе с учетом свойств выпуклости энтропии будет достаточно для вычисления длины секретного ключа.

9. ОЦЕНКА ДЛИНЫ СЕКРЕТНОГО КЛЮЧА С УЧЕТОМ ПОБОЧНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ И НЕОДНОФОТОННОСТИ ИНФОРМАЦИОННЫХ СОСТОЯНИЙ

Выше были получены оценки длины секретного ключа для строго однофотонной компоненты. При этом параметры, описывающие побочное излучение (p,d,η), следует относить к посылкам, в которых передавались информационные состояния со средним числом фотонов μ. Выражения для длины секретного ключа имеют следующую структуру:

$$\ell = P_\mu^{inf,tot}\left\{\frac{e^{-2\mu}(2\mu)}{P_\mu^{inf,tot}} \times \right.$$
$$\times \left(\sum_{\xi=\mu,\nu_1,\nu_2} P(\xi|\mu)Y_1^{inf}(\xi)[1-\chi_{Hol}(\zeta_1(\xi),p,\eta,d)]\right) -$$
$$\left. - \operatorname{leak}(\mathrm{Err}_\mu^{tot})\right\} = P_\mu^{inf,tot} \times$$
$$\times\left\{\frac{e^{-2\mu}(2\mu)}{P_\mu^{inf,tot}}\left(\sum_{\xi'} P(\xi'|\mu)Y_1^{inf}(\xi')\right)\times\right.$$
$$\times\left(\sum_{\xi=\mu,\nu_1,\nu_2}\frac{P(\xi|\mu)Y_1^{inf}(\xi)}{\sum_{\xi'}P(\xi'|\mu)Y_1^{inf}(\xi')}\times\right.$$
$$\left.\left.\times\ [1-\chi_{Hol}(\zeta_1(\xi),p,\eta,d)]\right) - \operatorname{leak}(\mathrm{Err}_\mu^{tot})\right\}. \tag{129}$$

Неформально говоря, после обнаружения в канале состояния с числом фотонов k Ева проводит измерения над отраженным зондирующим состоянием с целью выяснить, из какого состояния, информационного или состояния «ловушки», произошло обнаруженное состояние. После измерения вероятность исхода дается условной вероятностью $P(\xi'|\xi)$ и Ева делает вывод о дальнейших действиях. Другими словами, вероятности отсчетов в контрольных окнах $\zeta_1(\xi)$ и доли однофотонной компоненты $Y_1^{inf}(\xi)$ зависят от исхода измерений над отраженным состоянием. Условные вероятности $P(\xi'|\xi)$ являются известными. Отметим, что в длину секретного ключа (129) входят парциальные величины $\zeta_1(\xi)$ $\left(\frac{\zeta_1(\xi)}{1-\zeta_1(\xi)}\right)$, которые являются разными в посылках для состояний с разной интенсивностью ξ.

Функции $\chi_{Hol}(\zeta_1(\xi),p,\eta,d)$ в (129) являются выпуклыми функциями аргументов. Для выпуклой функции $f(x)$ по определению

$$\sum_i \lambda_i f(x_i) \le f\left(\sum_i \lambda_i x_i\right),$$
$$0 \le \lambda_i \le 1, \quad \sum_i \lambda_1 = 1. \tag{130}$$

Поскольку

$$\sum_{\xi'} P(\xi'|\mu)Y_1^{inf}(\xi') \ge p^{min}(\mu)Y_1^{inf,\Sigma}, \tag{131}$$

с учетом (130) получаем следующую цепочку неравенств:

$$\sum_{\xi=\mu,\nu_1,\nu_2}\frac{P(\xi|\mu)Y_1^{inf}(\mu)}{\sum_{\xi'}P(\xi'|\mu)Y_1^{inf}(\xi')}\chi_{Hol}(\zeta_1(\xi),p,\eta,d) \le$$
$$\le \frac{p^{max}(\mu)}{p^{min}(\mu)}\sum_{\xi=\mu,\nu_1,\nu_2}\frac{Y_1^{inf}(\xi)}{Y_1^{inf,\Sigma}}\chi_{Hol}(\zeta_1(\xi),p,\eta,d) \le$$
$$\le \frac{p^{max}(\mu)}{p^{min}(\mu)}\chi_{Hol}\left(\sum_{\xi=\mu,\nu_1,\nu_2}\frac{Y_1^{inf}(\xi)\zeta_1(\xi)}{Y_1^{inf,\Sigma}},p,\eta,d\right) =$$
$$= \frac{p^{max}(\mu)}{p^{min}(\mu)}\chi_{Hol}\left(\sum_{\xi=\mu,\nu_1,\nu_2}\frac{Y_1^{contr}(\xi)}{Y_1^{inf,\Sigma}},p,\eta,d\right) =$$
$$= \frac{p^{max}(\mu)}{p^{min}(\mu)}\chi_{Hol}\left(\frac{Y_1^{contr,\Sigma}}{Y_1^{inf,\Sigma}},p,\eta,d\right) =$$
$$= \frac{p^{max}(\mu)}{p^{min}(\mu)}\chi_{Hol}\left((\zeta Y)_1^{inf,\Sigma},p,\eta,d\right). \tag{132}$$

В (132) учтено, что

$$\zeta_1(\xi) = \frac{Y_1^{contr}(\xi)}{Y_1^{inf}(\xi)}, \quad (\zeta Y)_1^{inf,\Sigma} = \frac{Y_1^{contr,\Sigma}}{Y_1^{inf,\Sigma}}. \tag{133}$$

В итоге, используя (132), а также для краткости обозначение (133), для доли секретных битов получаем

$$\sum_{\xi=\mu,\nu_1,\nu_2} \frac{P(\xi|\mu)Y_1^{inf}(\xi)}{\sum\limits_{\xi'} P(\xi'|\mu)Y_1^{inf}(\xi')} \times \\ \times [1-\chi_{Hol}(\zeta_1(\xi),p,\eta,d)] \geq \\ \geq 1-\frac{p^{max}(\mu)}{p^{min}(\mu)}\chi_{Hol}\left((\zeta Y)_1^{inf,\Sigma},p,\eta,d\right). \quad (134)$$

С учетом (134) находим

$$\ell = P_\mu^{inf,tot}\left\{\frac{e^{-2\mu}(2\mu)p^{min}(\mu)Y_1^{inf,\Sigma}}{P_\mu^{inf,tot}} \times \right. \\ \times \left(1-\frac{p^{max}(\mu)}{p^{min}(\mu)}\chi_{Hol}\left((\zeta Y)_1^{inf,\Sigma},p,\eta,d\right)\right) - \\ \left. - \text{leak}(\text{Err}_\mu^{tot})\right\}. \quad (135)$$

В формулу (135) входят интегральная доля однофотонной компоненты $Y_1^{inf,\Sigma}$ и интегральное отношение $(\zeta Y)_1^{inf,\Sigma}$. Фактически это означает, что в формулах (134), (135) в аргументе $\chi_{Hol}(\zeta_1,p,d,\eta)$ нужно заменить парциальные отношения на средние значения:

$$\zeta_1 \to (\zeta Y)_1^{inf,\Sigma}. \quad (136)$$

Данные величины выражаются в модифицированном Decoy State-методе через наблюдаемые величины — темп отсчетов на приемной стороне для состояний с разным средним числом фотонов. Напомним, что это длина секретного ключа в одном базисе. Для того чтобы получить длину ключа по всем базисам, придется еще раз воспользоваться свойством выпуклости функций в (135).

10. ОЦЕНКА ДЛИНЫ СЕКРЕТНОГО КЛЮЧА ПО ВСЕМ БАЗИСАМ

Перейдем к оценке длины секретного ключа по всем базисам. Теперь величины в (135) необходимо снабдить индексом базиса $b = L, R$, получаем

$$\ell^\Sigma = \sum_{b=L,R}\ell(b) = \\ = \sum_{b=L,R}\left\{p^{min}(\mu)e^{-2\mu}(2\mu)Y_1^{inf,\Sigma}(b) \times \right. \\ \times \left.\left(1-\frac{p^{max}(\mu)}{p^{min}(\mu)}\chi_{Hol}\left((\zeta Y)_1^{inf,\Sigma}(b),p,\eta,d\right)\right)\right\} - \\ - P_\mu^{inf,\Sigma tot}\sum_{b=L,R}\frac{P_\mu^{inf,tot}(b)}{P_\mu^{inf,\Sigma tot}}\text{leak}(\text{Err}_\mu^{tot}(b)), \quad (137)$$

где

$$P_\mu^{inf,\Sigma tot} = \sum_{b=L,R} P_\mu^{inf,tot}(b).$$

Используя свойство выпуклости функций $\text{leak}(\text{Err}_\mu^{tot}(b))$ и $\chi_{Hol}(\zeta,p,\eta,d)$, находим

$$\text{leak}\left(\sum_{b=L,R}\frac{P_\mu^{inf,tot}(b)}{P_\mu^{inf,\Sigma tot}}\text{Err}_\mu^{tot}(b)\right) \geq \\ \geq \sum_{b=L,R}\frac{P_\mu^{inf,tot}(b)}{P_\mu^{inf,\Sigma tot}}\text{leak}(\text{Err}_\mu^{tot}(b)), \quad (138)$$

$$\text{Err}_\mu^{\Sigma tot} = \sum_{b=L,R}\frac{P_\mu^{inf,tot}(b)}{P_\mu^{inf,\Sigma tot}}\,\text{Err}_\mu^{tot}(b),$$

$$\chi_{Hol}\left(\sum_{b=L,R}(\zeta Y)_1^{inf,\Sigma}(b),p,\eta,d\right) \geq \\ \geq \sum_{b=L,R}\frac{Y_1^{inf,\Sigma}(b)}{Y_1^{inf,\Sigma tot}}\chi_{Hol}\left((\zeta Y)_1^{inf,\Sigma}(b),p,\eta,d\right).$$

Окончательно получаем

$$\ell^\Sigma = P_\mu^{inf,\Sigma tot}\left\{\frac{e^{-2\mu}(2\mu)p^{min}(\mu)Y_1^{inf,\Sigma tot}}{P_\mu^{inf,\Sigma tot}} \times \right. \\ \times \left(1-\frac{p^{max}(\mu)}{p^{min}(\mu)}\chi_{Hol}\left((\zeta Y)_1^{inf,\Sigma tot},p,\eta,d\right)\right) - \\ \left. - \text{leak}(\text{Err}_\mu^{\Sigma tot})\right\}, \quad (139)$$

где

$$(\zeta Y)_1^{inf,\Sigma tot} = \sum_{b=L,R}\frac{Y_1^{inf,\Sigma}(b)(\zeta Y)_1^{inf,\Sigma}(b)}{Y_1^{inf,\Sigma tot}},$$

$$Y_1^{inf,\Sigma tot} = \sum_{b=L,R} Y_1^{inf,\Sigma}(b).$$

11. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Формула (139) дает длину секретного ключа в битах в пересчете на одну зарегистрированную посылку по всем базисам. Длина ключа в пересчете на одну зарегистрированную посылку по всем базисам выражается через средние значения наблюдаемых параметров на приемной стороне. Такими параметрами являются следующие.

1. Средняя по всем базисам полная вероятность ошибок $\mathrm{Err}_{\mu}^{\Sigma tot}$ в информационных временных окнах. Данная величина может определяться как путем раскрытия части последовательности зарегистрированных посылок, так и по факту, если исправление ошибок происходит сразу без предварительной оценки вероятности ошибок. При этом доля исправленных позиций в асимптотическом пределе сразу дает величину $\mathrm{Err}_{\mu}^{\Sigma tot}$.

2. Полная вероятность зарегистрированных посылок $P_{\mu}^{inf,\Sigma tot}$ по всем базисам.

3. Полная вероятность регистрации в информационных временных окнах однофотонной компоненты состояний $Y_1^{inf,\Sigma tot}$ по всем базисам. Данная величина оценивается через наблюдаемые на приемной стороне величины для информационных посылок и посылок с состояниями ловушками.

4. Полная усредненная вероятность регистрации в контрольных временных окнах однофотонной компоненты состояний $(\zeta Y)_1^{inf,\Sigma tot}$ по всем базисам. Данная величина оценивается через наблюдаемые величины для информационных посылок и посылок с состояниями ловушками.

5. Величины $p^{max}(\mu)$ и $p^{min}(\mu)$, определяющие максимальную и минимальную вероятности различения отраженных зондирующих состояний от модулятора интенсивности, зависят от конкретной экспериментальной реализации системы квантовой криптографии и должны определяться/вычисляться путем специальных исследований.

6. Величина η, определяющая минимальное перекрытие (максимальную различимость) отраженных зондирующих состояний от фазового модулятора на приемной стороне, также должна измеряться/вычисляться путем специальных исследований и определяться для конкретной реализации системы.

7. Величины p, d, описывающие вероятность различений квантовых состояний в побочных каналах, связанных с пассивным детектированием электромагнитного излучения и переизлучения лавинных детекторов, должны определяться экспериментально, и также зависят от конкретной реализации системы.

Верхняя граница утечки информации к подслушивателю при атаке на информационные состояния в квантовом канале связи, по крайней мере для однофотонных состояний, можно получить, не прибегая к каким-либо модельным соображениям, а опираясь только на фундаментальные ограничения квантовой теории, например, на энтропийные соотношения неопределенностей [3], поскольку известен вид информационных состояний, направляемых в канал связи. Ситуация с состояниями в побочных каналах принципиально иная. Введение в рассмотрение побочных каналов утечки информации и квантовых состояний в них не может быть сделано без каких-то модельных соображений. Структура квантовых состояний в побочных каналах точно неизвестна. Умозрительно структура квантовых состояний в побочных каналах при каждой конкретной реализации системы квантовой криптографии может быть определена квантовой томографией. Но это только умозрительно. Практически это сделать невозможно из-за огромного числа степеней свободы системы. Например, точный вид побочного электромагнитного излучения электронной аппаратуры из-за макроскопически большого числа степеней свободы неизвестен. Поэтому требуются модельные соображения. Выше были рассмотрены модели бинарных квантовых каналов для побочного излучения. Предложенный метод позволяет включить в рассмотрение регулярным образом любые другие виды побочных каналов. Более того, как показывает рассмотрение выше, не требуется точный вид самих состояний, достаточно только знать верхнюю границу различимости состояний, что является более простой экспериментальной задачей.

Выше был рассмотрен асимптотический предел длинных передаваемых последовательностей. Учет конечной длины передаваемых последовательностей представляет собой более или менее обычную задачу по учету флуктуаций наблюдаемых величин за счет конечной длины последовательностей, что представляет собой стандартную задачу классической теории вероятностей.

Благодарности. Автор выражает благодарность коллегам по Академии криптографии Российской Федерации за обсуждения и поддержку, а также И. М. Арбекову и С. П. Кулику за многочисленные интересные обсуждения и замечания, позволившие улучшить изложение.

Финансирование. Работа выполнена при поддержке Российского научного фонда (проект № 16-12-00015 (продолжение)).

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, pp. 175–179, Bangalore, India (1984).

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

3. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, arXiv:1103.4130 v2 (2011); Nature Commun. **3**, 1 (2012).

4. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

5. Won-Young Hwang, arXiv[quant-ph]:0211153.

6. Xiang-Bin Wang, Phys. Rev. Lett. **94**, 230503 (2005).

7. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Phys. Rev. Lett. **94**, 230504 (2005).

8. Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, arXiv[quant-ph]: 0503005.

9. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).

10. С. Н. Молотков, ЖЭТФ **133**, 5 (2008).

11. S. N. Molotkov, Laser Phys. Lett. **16**, 035203 (2019).

12. A. S. Holevo, Probl. Inf. Transmission **9**, 177 (1973).

13. А. С. Холево, УМН **53**, 193 (1998).

14. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, Москва (2010).