ЖЭТФ, 2010, том 138, вып. 1 (7), стр. 33–66

КВАНТОВАЯ СХЕМА ДЛЯ ОПТИМАЛЬНОГО ПОДСЛУШИВАНИЯ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ФАЗОВО-ВРЕМЕННЫ́М КОДИРОВАНИЕМ

Д. А. Кронберг [c]***, С. Н. Молотков*** [a,b,c*]

[a] *Институт физики твердого тела Российской академии наук*
142432, Черноголовка, Московская обл., Россия

[b] *Академия криптографии Российской Федерации*
121552, Москва, Россия

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

Поступила в редакцию 28 декабря 2009 г.

Построена квантовая схема и предложена ее физическая реализация на основе линейных и нелинейных волоконно-оптических элементов для оптимальной атаки на ключ, передаваемый через квантовый канал связи, в протоколе квантового распределения ключей с фазово-временны́м кодированием.

1. ВВЕДЕНИЕ

Системы квантовой криптографии — квантового распределения ключей — предназначены для передачи секретных ключей по открытым и доступным для любой модификации каналам связи. В отличие от систем распределения ключей, которые используют классические сигналы и секретность которых основана на вычислительной сложности (например, как в системах с открытым ключом типа RSA [1]) или на технических ограничениях возможностей подслушивателя, в квантовой криптографии детектирование любых попыток подслушивания и секретность финальных ключей (при условии, что поток ошибок на приемной стороне не превышает некоторую критическую величину) гарантируется фундаментальными законами квантовой механики [2–4]. Любое получение информации о передаваемых квантовых состояниях неизбежно ведет к их возмущению, которое детектируется на приемной стороне. Поэтому цель подслушивателя состоит в том, чтобы при данном уровне возмущения (потоке ошибок на приемной стороне) получить максимум информации о квантовых состояниях, который допускается принципиальными ограничениями квантовой механики.

В последние годы было осознано и строго доказано (см., например, работу [5] и ссылки в ней), что для систем квантового распределения ключей, в которых квантовые состояния в каждой посылке посылаются в канал связи независимо друг от друга, наиболее общей атакой непосредственно на передаваемые квантовые состояния[1)] является так называемая коллективная атака [5, 7, 8]. Данная атака сводится к следующему[2)]. В каждой посылке подслушиватель (Ева) готовит свое вспомогательное квантовое состояние $|A\rangle_E$ (см. рис. 1). Данное квантовое состояние описывает исходное состояние измерительного прибора Евы. Прибор (квантовое состояние) приводится на некоторое время во взаимодей-

*E-mail: molotkov@issp.ac.ru

[1)] Возможны также атаки на ключ с использованием так называемых побочных каналов утечки информации (side channel leakage) [6], например, непосредственно на передающую и приемную аппаратуру Алисы и Боба. В этом случае модификации и возмущения передаваемых квантовых состояний не происходит.

[2)] Формально это является следствием того, что общее, вообще говоря, запутанное состояние подслушивателя и легитимных пользователей $\rho_{A^N B^N E^N}$ после N посылок представимо как линейная комбинация тензорного произведения состояний $\rho_{A^N B^N E^N} \approx \sigma_{ABE}^{\otimes N}$, относящихся к каждой посылке.

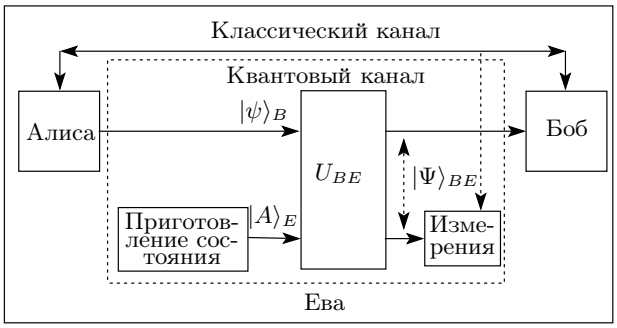

Рис. 1. Общая схема атаки через квантовый канал связи непосредственно на передаваемые квантовые состояния

ствие с передаваемым Алисой (передающая сторона) состоянием $|\psi\rangle_B$ по квантовому каналу связи к Бобу (приемная сторона). В квантовой механике эволюция полной системы (прибор Евы + передаваемое квантовое состояние Алисы) описывается унитарным оператором U_{BE}:

$$U_{BE}(|\psi\rangle_B \otimes |A\rangle_E) = |\Psi\rangle_{BE}. \qquad (1)$$

В результате взаимодействия обе подсистемы — прибор и передаваемое квантовое состояние — оказываются в общем запутанном состоянии $|\Psi\rangle_{BE}$ (1) ($|\Psi\rangle_{BE} \neq |\psi\rangle_B \otimes |A\rangle_E$, рис. 1). Модифицированное квантовое состояние Ева направляет к Бобу, а свое оставляет у себя в квантовой памяти[3)]. После передачи всей последовательности квантовых состояний и измерений на приемной стороне Алиса и Боб проводят согласование базисов, коррекцию ошибок и сжатие (усиление секретности) «очищенного» ключа, обмениваясь информацией через открытый и доступный для прослушивания классический канал связи (рис. 1). Ева использует информацию из открытого классического канала связи для своих измерений, которые она проводит в самом конце протокола. Максимум информации может быть получен, если Ева использует коллективные измерения над всеми состояниями в своей квантовой памяти, т. е. когда Ева минимизирует ошибку различения не отдельных квантовых состояний, а ошибку различения целых кодовых последовательностей [9]. При таких измерениях достигается фундаментальная граница Холево [9], которая дает достижимую верхнюю границу классической информации, которая может быть получена из ансамбля квантовых состояний.

Протокол с фазово-временны́м кодированием был предложен в работе [10]. На формальном уровне оптимальная атака для протокола квантового распределения ключей с фазово-временным кодированием была построена в работе [11]. Позднее в статье [12] была также проанализирована стойкость комбинированного протокола с фазово-временны́м кодированием и неортогональными состояниями внутри базиса. В однофотонном режиме данный протокол обеспечивает секретность ключей при наибольшем потоке ошибок Q на приемной стороне, вплоть до теоретического предела $Q \to 50\,\%$. В случае не строго однофотонного источника, неидеальных фотодетекторов и потерях в квантовой линии связи из всех известных протоколов [13, 14] данный протокол обеспечивает максимальную дальность передачи ключей, при которой гарантируется их секретность.

Унитарный оператор U_{BE} является формальным описанием взаимодействия физического прибора с передаваемыми квантовыми состояниями. Цель Евы сконструировать такой унитарный оператор U_{BE} (подобрать такое взаимодействие), который в итоге позволит ей устроить оптимальную атаку на передаваемые квантовые состояния. Оптимальность понимается в том смысле, что данная атака позволяет Еве получить максимум информации о ключе при заданном потоке ошибок на приемной стороне Боба.

Построение полной оптоволоконной физической реализации схемы для оптимального подслушивания, на наш взгляд, является вполне интересной и осмысленной задачей. Кроме того, как будет видно ниже, подслушивание квантовых каналов связи является гораздо более сложной и деликатной задачей, чем подслушивание оптоволоконных линий связи с классическими сигналами.

На сегодняшний день известна лишь одна попытка лабораторного модельного эксперимента (proof of principles) [15] по подслушиванию квантовых состояний, которая не реализует полную схему подслушивания. Кроме того, из-за технических ограничений при проведении эксперимента требуется прямой доступ Евы к передающей и приемной станциям, что очевидно не имеет места в реальной ситуации. При этом в нем используется поляризационное кодирование, которое не приемлемо для реальных оптоволоконных линий квантовой связи, поскольку оптоволокно, как известно, не сохраняет поляризацию.

Далее будет удобно рассматривать атаку на передаваемые квантовые состояния как некоторое одношаговое квантовое вычисление.

Любое квантовое вычисление является специально подобранной унитарной эволюцией квантовой системы с последующим измерением над ней с целью

[3)] В реальной ситуации достаточно использовать оптоволоконную линию задержки.

получения классических данных (результата вычислений) [16]. На формальном уровне квантовое вычисление сводится к построению соответствующего унитарного оператора. На физическом уровне квантовое вычисление сводится к выбору физической системы и взаимодействий, которые реализуют заданную эволюцию. Любое квантовое вычисление (унитарный оператор) может быть реализовано в виде квантовой схемы, которая может быть представлена как последовательность элементарных квантовых преобразований [16] над одним кубитом (в нашем случае фотоном) и двумя кубитами (двумя фотонами). Данные преобразования всегда могут быть сведены к последовательному применению двух универсальных квантовых вентилей, отвечающих унитарным поворотам отдельных кубитов и управляемого NOT (control NOT) над двумя, вообще говоря, любыми парами кубитов [16].

Данная работа посвящена построению физической реализации (на основе линейных и нелинейных оптических элементов) квантовой схемы, позволяющей реализовать экспериментально оптимальную атаку на передаваемый ключ.

Структура работы следующая. В разд. 2 построена квантовая схема и ее физическая реализация для оптимального подслушивания для протокола распределения ключей BB84. В разд. 3 приведена аналогичная схема для протокола с фазово-временным кодированием. В Заключении обсуждаются полученные результаты.

2. КВАНТОВАЯ СХЕМА ДЛЯ ОПТИМАЛЬНОЙ АТАКИ НА ПРОТОКОЛ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ BB84

2.1. Построение квантовой схемы в вычислительном базисе

Для целостности и самодостаточности изложения удобно сначала построить квантовую схему и физическую реализацию основных вентилей для квантового протокола распределения ключей BB84 [2], поскольку данный протокол как базовый используется практически во всех реализациях оптоволоконных систем квантовой криптографии (см., например, [17–37]). Затем основные квантовые вентили как составные блоки войдут в квантовую схему для оптимального подслушивания протокола с фазово-временны́м кодированием [11], которая является технически существенно более сложной.

Кроме того, сначала будет удобнее и короче построить квантовую схему в вычислительном (логическом) базисе, не конкретизируя внутреннюю физическую структуру квантовых состояний, а затем сделать преобразование элементов квантовой схемы для физического базиса, имея в виду, что физические состояния представляют собой суперпозицию однофотонных состояний, локализованных в различных временны́х окнах.

В протоколе BB84 [2] используются два базиса, в каждом из которых имеется пара информационных ортогональных состояний, отвечающих 0 и 1. Состояния из разных базисов попарно неортогональны.

Далее, чтобы отличать физические состояния от формальных вычислительных базисных состояний, которые не привязаны к конкретной физической структуре, будем снабжать вычислительные базисные состояния чертой сверху. Информационные квантовые состояния в прямом базисе обозначим как

$$|\overline{0^+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |\overline{1^+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \qquad \langle\overline{0^+}|\overline{1^+}\rangle = 0. \tag{2}$$

Состояния в сопряженном базисе получаются из состояний (2) поворотом в комплексной плоскости:

$$|\overline{0^\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |\overline{1^\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle), \qquad \langle\overline{0^\times}|\overline{1^\times}\rangle = 0. \tag{3}$$

Здесь $|1\rangle$ и $|2\rangle$ — однофотонные состояния, локализованные во временны́х окнах 1 и 2 (см. рис. 2)[4)].

Атака Евы описывается унитарным оператором U_{BE}, действие которого на информационные состояния в базисах + и × может быть представлено в виде (см. детали в работах [11, 12])

$$\begin{gathered} |\Psi_{0^+}\rangle_{BE} = U_{BE}(|\overline{0^+}\rangle \otimes |A\rangle) = \\ = \sqrt{1-Q}|\overline{0^+}\rangle \otimes |\psi_{0^+}\rangle + \sqrt{Q}|\overline{1^+}\rangle \otimes |\theta_{0^+}\rangle, \\ |\Psi_{1^+}\rangle_{BE} = U_{BE}(|\overline{1^+}\rangle \otimes |A\rangle) = \\ = \sqrt{Q}|\overline{0^+}\rangle \otimes |\theta_{1^+}\rangle + \sqrt{1-Q}|\overline{1^+}\rangle \otimes |\psi_{1^+}\rangle, \end{gathered} \tag{4}$$

и соответственно в сопряженном базисе

$$\begin{gathered} |\Psi_{0^\times}\rangle_{BE} = U_{BE}(|\overline{0^\times}\rangle \otimes |A\rangle) = \\ = \sqrt{1-Q}|\overline{0^\times}\rangle \otimes |\psi_{0^\times}\rangle + \sqrt{Q}|\overline{1^\times}\rangle \otimes |\theta_{0^\times}\rangle, \\ |\Psi_{1^\times}\rangle_{BE} = U_{BE}(|\overline{1^\times}\rangle \otimes |A\rangle) = \\ = \sqrt{Q}|\overline{0^\times}\rangle \otimes |\theta_{1^\times}\rangle + \sqrt{1-Q}|\overline{1^\times}\rangle \otimes |\psi_{1^\times}\rangle. \end{gathered} \tag{5}$$

Параметр Q является вероятностью ошибки на приемной стороне Боба (см. детали, например, в работах [11, 12]) и находится в руках подслушивателя.

[4)] Строго говоря, состояния получаются квазиоднофотонные.

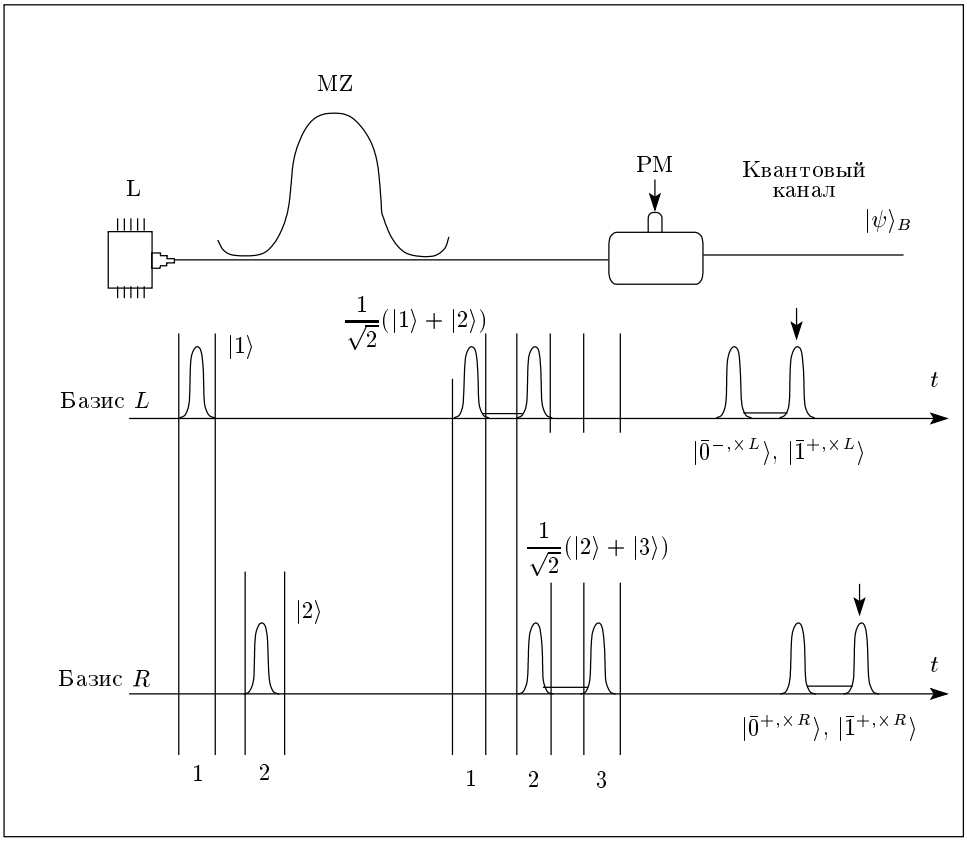

Рис. 2. Передающая станция — Алиса. L — лазер, формирующий локализованные во времени состояния (квазиоднофотонные), MZ — оптоволоконный интерферометр Маха – Цандера, PM — фазовый модулятор, к которому прикладывается напряжение в момент прохождения заднего фронта («половинки» $|2\rangle$ состояния из суперпозиции $(|1\rangle + |2\rangle)/\sqrt{2}$), что приводит к появлению относительной разности фаз между $|2\rangle$ и $|1\rangle$ и формированию одного из состояний $|\psi\rangle_B = \{\{|\overline{0^+L}\rangle, \{|\overline{1^+L}\rangle, |\overline{0^{\times L}}\rangle, |\overline{1^{\times L}}\rangle\}$, которые Алиса выбирает равновероятно. В случае протокола BB84 используются состояния только в базисе L (верхняя временна́я диаграмма). В протоколе с фазово-временны́м кодированием состояния в базисе R аналогичны состояниям в базисе L с той лишь разницей, что их моменты приготовления сдвинуты по времени на величину, равную разности оптического пути по верхнему и нижнему плечам интерферометра Маха – Цандера (верхняя и нижняя временны́е диаграммы). Вертикальными линиями отмечены временны́е окна 1, 2 и 3

Ниже мы увидим, что Q напрямую связан с коэффициентами прохождения и отражения оптоволоконных светоделителей.

Из условия унитарности преобразования (4), (5) с учетом (2), (3) следует, что $\{|\psi_{0\times}\rangle$, $|\theta_{0\times}\rangle$, $|\psi_{1\times}\rangle$, $|\theta_{1\times}\rangle\}$ выражаются линейным образом через $\{|\psi_{0^+}\rangle$, $|\theta_{0^+}\rangle$, $|\psi_{1^+}\rangle$, $|\theta_{1^+}\rangle\}$ [11, 12]. Кроме того, унитарность преобразования подслушивателя требует, чтобы выполнялись равенства

$$\langle\psi_{0^+}|\theta_{0^+}\rangle = \langle\psi_{0\times}|\theta_{1\times}\rangle = \\ = \langle\psi_{1^+}|\theta_{0^+}\rangle = \langle\psi_{1^+}|\theta_{1^+}\rangle = 0. \quad (6)$$

Оптимальность атаки, в смысле максимизации информации Евы при заданной наблюдаемой вероятности ошибки Q на приемной стороне Боба, приводит к условию (см. детали в работах [11, 12])

$$\langle\psi_{0^+}|\psi_{1^+}\rangle = \langle\theta_{0^+}|\theta_{1^+}\rangle = \cos\alpha, \quad (7)$$

где

$$Q = \frac{1-\cos\alpha}{2}. \quad (8)$$

Фиксируем исходное состояние Евы в виде $|A\rangle_E = |\overline{00}\rangle_E = |\overline{0}\rangle_E \otimes |\overline{0}\rangle_E$. Данные состояния являются элементами формального вычислительного базиса у Евы и описывают исходное состояние прибора Евы. Забегая вперед, отметим, что далее этим состояниям будут сопоставлены реальные физические состояния, представляющие собой состояния, которые Ева посылает по двум вспомогательным оптоволокнам и которые локализованы во временны́х окнах, привязанных к моменту посылки состояний Алисы в квантовый канал связи.

Соотношениям (6), (7) удовлетворяют следующие векторы состояний для возмущенного вспомогательного квантового состояния Евы:

$$\begin{aligned}
|\psi_{0^+}\rangle &= \cos\frac{\alpha}{2}|\overline{00}\rangle + \sin\frac{\alpha}{2}|\overline{10}\rangle,\\
|\psi_{1^+}\rangle &= \cos\frac{\alpha}{2}|\overline{00}\rangle - \sin\frac{\alpha}{2}|\overline{10}\rangle,\\
|\theta_{0^+}\rangle &= \cos\frac{\alpha}{2}|\overline{01}\rangle - \sin\frac{\alpha}{2}|\overline{11}\rangle,\\
|\theta_{1^+}\rangle &= \cos\frac{\alpha}{2}|\overline{01}\rangle + \sin\frac{\alpha}{2}|\overline{11}\rangle.
\end{aligned} \tag{9}$$

Далее, опять же для краткости, будем обозначать состояния, опуская индексы базисов + и ×, что возможно в силу линейности унитарного оператора. Первый символ в состоянии относится к состоянию Алисы (Боба), остальные два к состоянию Евы, т. е. $|\overline{0}\rangle_B \otimes |\overline{00}\rangle_E \equiv |\overline{000}\rangle$. В новых обозначениях действие унитарного оператора на состояния в прямом базисе сводится к следующему:

$$\begin{aligned}
U_{BE}(|\overline{000}\rangle) &= \sqrt{1-Q}\left(\cos\frac{\alpha}{2}|\overline{000}\rangle + \right.\\
&\left. + \sin\frac{\alpha}{2}|\overline{010}\rangle\right) + \sqrt{Q}\left(\cos\frac{\alpha}{2}|\overline{101}\rangle - \right.\\
&\left. - \sin\frac{\alpha}{2}|\overline{111}\rangle\right),\\
U_{BE}\left(|\overline{100}\rangle\right) &= \sqrt{Q}\left(\cos\frac{\alpha}{2}|\overline{001}\rangle + \right.\\
&\left. + \sin\frac{\alpha}{2}|\overline{011}\rangle\right) + \sqrt{1-Q}\left(\cos\frac{\alpha}{2}|\overline{100}\rangle - \right.\\
&\left. - \sin\frac{\alpha}{2}|\overline{110}\rangle\right).
\end{aligned} \tag{10}$$

Аналогичные выражения с учетом (2), (3) имеют место в сопряженном базисе. Матричное представление унитарного оператора в вычислительном базисе, упорядоченном в лексиграфическом порядке, с учетом (4) имеет вид

$$\begin{pmatrix}
\tilde{Q}c_\alpha & 0 & -\tilde{Q}s_\alpha & 0 & 0 & \sqrt{Q}c_\alpha & 0 & -\sqrt{Q}s_\alpha\\
0 & \tilde{Q}c_\alpha & 0 & -\tilde{Q}s_\alpha & \sqrt{Q}c_\alpha & 0 & -\sqrt{Q}s_\alpha & 0\\
\tilde{Q}s_\alpha & 0 & \tilde{Q}c_\alpha & 0 & 0 & \sqrt{Q}s_\alpha & 0 & \sqrt{Q}c_\alpha\\
0 & \tilde{Q}s_\alpha & 0 & \tilde{Q}c_\alpha & \sqrt{Q}s_\alpha & 0 & \sqrt{Q}c_\alpha & 0\\
0 & -\sqrt{Q}c_\alpha & 0 & \sqrt{Q}s_\alpha & -\tilde{Q}c_\alpha & 0 & -\tilde{Q}s_\alpha & 0\\
\sqrt{Q} & 0 & -\sqrt{Q}s_\alpha & 0 & 0 & -\tilde{Q}c_\alpha & 0 & \tilde{Q}s_\alpha\\
0 & -\sqrt{Q}s_\alpha & 0 & -\sqrt{Q}c_\alpha & -\tilde{Q}s_\alpha & 0 & -\tilde{Q}c_\alpha & 0\\
-\sqrt{Q}s_\alpha & 0 & -\sqrt{Q}c_\alpha & 0 & 0 & \tilde{Q}s_\alpha & 0 & \tilde{Q}c_\alpha
\end{pmatrix}. \tag{11}$$

Здесь для краткости введены обозначения $c_\alpha = \cos(\alpha/2)$, $s_\alpha = \sin(\alpha/2)$, $\tilde{Q} = \sqrt{1-Q}$.

Унитарный оператор U_{BE} может быть представлен как действие однокубитных и двухкубитных квантовых преобразований CNOT, действующих на избранную пару кубитов.

Займемся теперь разложением оператора на элементарные вентили. С учетом (11) имеем следующее разложение:

$$U_{BE} = U^{(1)} \cdot U^{(2)} \cdot U^{(3)}, \tag{12}$$

где

$$U^{(1)} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1
\end{pmatrix},$$

$$U^{(2)} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}, \tag{13}$$

$$U^{(3)} = \mathrm{CNOT}_{13} \cdot Q_{13} \cdot \mathrm{CNOT}_{13}^{*} \otimes R_2 = \\ = \begin{pmatrix} \sqrt{1-Q} & 0 & 0 & \sqrt{Q} \\ 0 & \sqrt{1-Q} & \sqrt{Q} & 0 \\ 0 & \sqrt{Q} & -\sqrt{1-Q} & 0 \\ \sqrt{Q} & 0 & 0 & -\sqrt{1-Q} \end{pmatrix}_{13} \otimes \\ \otimes \begin{pmatrix} c_\alpha & -s_\alpha \\ s_\alpha & c_\alpha \end{pmatrix}_2, \quad (14)$$

где введено обозначение

$$Q_{13} = \begin{pmatrix} \sqrt{1-Q} & \sqrt{Q} \\ \sqrt{Q} & -\sqrt{1-Q} \end{pmatrix}. \quad (15)$$

Индексы у операторов отвечают за номера кубитов, на которые они действуют. Всего имеется три кубита (один у Боба — номер 1, и два у Евы — номера 2, 3). Например, CNOT_{13} означает, что оператор действует на кубит Боба и второй кубит Евы. Одиночные индексы у операторов указывают их действие на кубиты с соответствующими номерами. Операторы стандартных однокубитных поворотов имеют вид

$$R^{+}(a) = \begin{pmatrix} c_\alpha & s_\alpha \\ -s_\alpha & c_\alpha \end{pmatrix}, \\ R^{-}(a) = \begin{pmatrix} c_\alpha & -s_\alpha \\ s_\alpha & c_\alpha \end{pmatrix}. \quad (16)$$

Операторы Z и Z^T имеют вид

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad Z^T = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}. \quad (17)$$

Недостающая пара операторов $U^{(1)}$ и $U^{(2)}$ в формуле (12) реализуется следующим образом:

$$U^{(1)} = \left(Z_{(1)}^{\dagger} \cdot \mathrm{CNOT}_{(1,2)} \cdot Z_{(2)} \cdot \mathrm{CNOT}_{(1,2)} \cdot Z_{(2)}^{\dagger} \right) \otimes \\ \otimes I_{(3)}, \quad (18)$$

$$U^{(2)} = \left(Z_{(1)} \cdot \mathrm{CNOT}_{(1,3)} \cdot Z_{(3)} \cdot \mathrm{CNOT}_{(1,3)} \cdot Z_{(3)}^{\dagger} \right) \otimes \\ \otimes I_{(2)}. \quad (19)$$

Нижние индексы в скобках означают позиции, к которым применяются преобразования, т. е. первый из операторов получается последовательностью одночастичных операций и CNOT над первыми двумя кубитами, а второй — над первым и третьим кубитами.

Теперь можно собрать все элементы в единую квантовую схему, реализующую действие унитарного оператора Евы, на передаваемые информационные квантовые состояния и вспомогательное квантовое состояние подслушивателя. Квантовая схема после всех упрощений приведена на рис. 3.

2.2. Переход к временно́му базису

В предыдущих разделах был избран наиболее короткий и экономный способ построения квантовой схемы, которая была построена в абстрактном (вычислительном) базисе $|\overline{0}^{+}\rangle$ и $|\overline{1}^{+}\rangle$ (соответственно в сопряженном базисе $|\overline{0}^{\times}\rangle$ и $|\overline{1}^{\times}\rangle$). В реальности данные абстрактные состояния имеют внутреннюю структуру и представляют собой суперпозицию состояний, локализованных во временны́х окнах 1 и 2 ($|1\rangle$ и $|2\rangle$) (2), (3) (см. также рис. 2).

Дальнейший наиболее экономный ход действий следующий. Сначала формально нужно переобозначить вычислительные базисные состояния $|\overline{0}\rangle$ и $|\overline{1}\rangle$ в формулах (4), (5) на временны́е базисные $|1\rangle$ и $|2\rangle$. Данные состояния являются пока формальными новыми базисными состояниями. Однако этим состояниям можно уже напрямую сопоставить физические базисные состояния — однофотонные лазерные импульсы (пакеты), локализованные в различных временны́х окнах. Формальное переобозначение позволяет использовать уже полученную квантовую схему при условии, что будет введен оператор, описывающий переход между этими базисами. Имеем

$$|\overline{0}^{+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \to |1\rangle, \\ |\overline{1}^{+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \to |2\rangle, \quad (20)$$

и в сопряженном базисе

$$|\overline{0}^{\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle) \to \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \\ |\overline{1}^{\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle) \to \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle). \quad (21)$$

Таким оператором является следующий

$$U_c = U_z \cdot U_y = \begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix} \times \\ \times \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}. \quad (22)$$

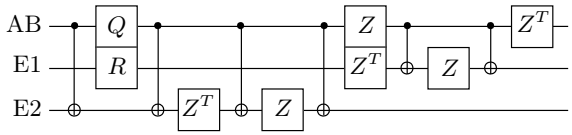

Рис. 3. Квантовая схема для оптимальной атаки в вычислительном базисе

Его действие в прямом базисе записывается как

$$U_c\left[\frac{1}{\sqrt{2}}(|1\rangle+|2\rangle)\right]=\frac{1+i}{\sqrt{2}}|1\rangle,$$
$$U_c\left[\frac{1}{\sqrt{2}}(|1\rangle-|2\rangle)\right]=\frac{i-1}{\sqrt{2}}|2\rangle, \tag{23}$$

соответственно в сопряженном —

$$U_c\left[\frac{1}{\sqrt{2}}(|1\rangle+i|2\rangle)\right]=\frac{i}{\sqrt{2}}(|1\rangle+|2\rangle),$$
$$U_c\left[\frac{1}{\sqrt{2}}(|1\rangle-i|2\rangle)\right]=\frac{1}{\sqrt{2}}(|1\rangle-|2\rangle). \tag{24}$$

Общие фазовые множители не важны для дальнейшего.

Таким образом, из формул (20)–(24) следует, что для того, чтобы наиболее просто перейти к временно́му базису, достаточно сделать формальное переобозначение — заменить $\overline{0}$, $\overline{1}$ на временны́е базисные состояния 1, 2. Имеем

$$U_{BE}(|1\rangle\otimes|A\rangle)=\sqrt{1-Q}|1\rangle\otimes|\psi_1\rangle+ \\ +\sqrt{Q}|2\rangle\otimes|\theta_1\rangle, \tag{25}$$

$$U_{BE}(|2\rangle\otimes|A\rangle)=\sqrt{Q}|1\rangle\otimes|\theta_2\rangle+ \\ +\sqrt{1-Q}|2\rangle\otimes|\psi_2\rangle, \tag{26}$$

где

$$|\psi_1\rangle=\cos\frac{\alpha}{2}|11\rangle+\sin\frac{\alpha}{2}|21\rangle,$$
$$|\psi_2\rangle=\cos\frac{\alpha}{2}|11\rangle-\sin\frac{\alpha}{2}|21\rangle,$$
$$|\theta_1\rangle=\cos\frac{\alpha}{2}|12\rangle-\sin\frac{\alpha}{2}|22\rangle, \tag{27}$$
$$|\theta_2\rangle=\cos\frac{\alpha}{2}|12\rangle+\sin\frac{\alpha}{2}|22\rangle.$$

Затем надо сделать преобразование унитарного оператора Евы, который в физическом базисе принимает вид

$$U_{BE}^{phys}=U_c^{\dagger}U_{BE}\cdot U_c. \tag{28}$$

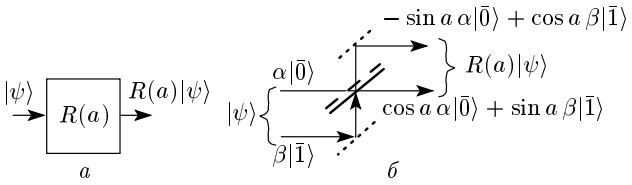

Рис. 4. Пример преобразования квантовых состояний. *а* — формальное обозначение квантового вентиля поворота, *б* — физическая реализация квантового вентиля

Абстрактные базисные состояния Евы в (4), (5) переобозначены на временны́е базисные состояния, локализованные в окнах 1 и 2. Имеем $|\overline{0}\rangle\to|1\rangle$ и $|\overline{1}\rangle\to|2\rangle$. В дальнейшем базисные состояния Евы и Боба, локализованные во временны́х окнах 1 и 2 будут разнесены по двум пространственным каналам (по двум разным оптоволокнам).

2.3. Построение квантовой схемы в физическом базисе

Квантовая схема была получена в базисе вычислительных состояний. При физической реализации формальным квантовым вентилям должны быть сопоставлены реальные физические элементы, которые выполняют требуемую функциональность — преобразование физических квантовых состояний во временно́м базисе. Поясним более подробно, что это означает. Например, формальный однокубитный квантовый вентиль унитарного поворота изображен на рис. 4*а*. Линии отвечают однокубитному квантовому состоянию. Входное состояние есть

$$|\psi\rangle=\alpha|\overline{0}\rangle+\beta|\overline{1}\rangle, \tag{29}$$

где $|\overline{0}\rangle, |\overline{1}\rangle$ — ортогональные состояния в вычислительном базисе. Повороту отвечает оператор, который в базисе $|\overline{0}\rangle, |\overline{1}\rangle$, имеет вид (30). Действие на состояние $|\psi\rangle$ дает преобразованное состояние, которое в компонентах, отвечающих вычислительному базису, имеет вид

$$R(a)|\psi\rangle\to\begin{pmatrix}\cos a & \sin a\\ -\sin a & \cos a\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}= \\ =\begin{pmatrix}\alpha\cos a+\beta\sin a\\ -\alpha\sin a+\beta\cos a\end{pmatrix}. \tag{30}$$

Матричные элементы оператора $R(a)$ в вычислительном базисе представляются как

$$\langle\overline{0}|R(a)|\overline{0}\rangle = \cos a, \quad \langle\overline{0}|R(a)|\overline{1}\rangle = \sin a,$$

$$\langle\overline{1}|R(a)|\overline{0}\rangle = -\sin a, \quad \langle\overline{1}|R(a)|\overline{1}\rangle = \cos a.$$

Верхний элемент вектор-столбца является коэффициентом перед вычислительным базисным состоянием $|\overline{0}\rangle$, а нижний — коэффициентом перед базисным состоянием $|\overline{1}\rangle$. Таким образом, преобразованное выходное состояние в вычислительном базисе с учетом (29), (30) принимает вид

$$R(a)|\overline{0}\rangle = \cos a|\overline{0}\rangle - \sin a|\overline{1}\rangle,$$

$$R(a)|\overline{1}\rangle = \cos a|\overline{1}\rangle + \sin a|\overline{0}\rangle,$$

где

$$R(a)|\psi\rangle = \alpha R(a)|\overline{0}\rangle + \beta R(a)|\overline{1}\rangle = \\ = (\alpha\cos a + \beta\sin a)|\overline{0}\rangle + \\ + (-\alpha\sin a + \beta\cos a)|\overline{1}\rangle. \quad (31)$$

На физическом уровне унитарный поворот реализуется при помощи асимметричного светоделителя (рис. 4*б*).

Из рис. 4*б* следует рецепт реализации квантового вентиля унитарного поворота.

1. Надо «развести» компоненты квантового состояния перед базисными вычислительными векторами на два физических пространственно разделенных канала (два входа светоделителя). Это всегда можно сделать из-за ортогональности базисных векторов. Амплитуды состояний в двух пространственно разделенных каналах будут соответствовать амплитудам (коэффициентам) перед базисными векторами.

2. Для того чтобы получить правильное значение амплитуды в каждом канале (см. рис. 4*б*), нужно привести базисные состояния в каждом пространственном канале к одному состоянию. Состояния $|\overline{0}\rangle$ и $|\overline{1}\rangle$ должны быть преобразованы в одно физическое состояние, например, локализованное во временно́м окне 2, т. е. в состояние $|2\rangle$. Это необходимо для «сбивки» (интерференции) амплитуд из разных пространственных каналов. Входное состояние в верхнем канале $|\overline{0}\rangle \to |2\rangle$ отвечает нулю, а в нижнем $|\overline{1}\rangle \to |2\rangle$ — единице.

Приведение состояний в верхнем и нижнем каналах к одному временно́му окну необходимо для достижения интерференции амплитуд в двух каналах при дальнейших преобразованиях состояния.

Действительно, после данных процедур амплитуда состояния в разных каналах становится следующей (см. рис. 4*б*): в нижнем $(\alpha\cos a + \beta\sin a)|2\rangle$, в верхнем $(-\alpha\sin a + \beta\cos a)|2\rangle$. Это как раз те амплитуды, которые возникают при действии оператора и являются коэффициентами при вычислительных базисных состояниях в выражении (31).

В этом случае матричное представление оператора остается таким же, как и в вычислительном базисе, но строки отвечают теперь двум (верхнему и нижнему) физическим каналам[5)].

Другими словами, каждый элемент в матрице представляет собой оператор, действующий на состояния во временны́х окнах $1, 2, 3, \ldots$ Например, единичный оператор $I = |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| + \ldots$ (однако актуальными для нас будут состояния только в трех временны́х окнах).

Отметим, что приведение состояний в верхнем и нижнем каналах может быть сделано к любому временно́му окну 1, 2 и т. д., но обязательно общему для обеспечения интерференции. Как следует из рис. 2, состояния в верхнем и нижнем каналах (до их разделения это состояния, локализованные в разных временны́х окнах) происходят из одного и того же исходного состояния, которое было разделено на светоделителе.

2.4. Реализация оператора U_{BE} в физическом базисе

Теперь необходимо учесть конкретную физическую структуру квантовых состояний. Фактически это будет сводиться к сопоставлению базисным состояниям $|1\rangle$ и $|2\rangle$ однофотонных пакетов в двух пространственно разделенных каналах (оптоволокнах).

Вычислительные квантовые состояния в нашем случае фазового кодирования для протокола BB84 представляют собой суперпозицию базисных состояний $|1\rangle$ и $|2\rangle$ (рис. 2), локализованных во временны́х окнах 1 и 2 (2, 3), и далее для фазово-временно́го кодирования — суперпозицию состояния во временны́х окнах 1 и 2 в базисе L, 2 и 3 в базисе R.

Отметим, что во всех системах оптоволоконной квантовой криптографии используются интенсивные (классические) оптические сигналы синхронизации, которые также передаются по открытой волоконной линии связи. Это делается для того, чтобы стробировать лавинные фотодетекторы только в момент прихода информационных состояний, и тем

[5)] Само квантовое состояние присутствует одновременно в обоих каналах аналогично тому, как имеет место при интерференции на двух щелях. Измерение в одном из каналов приведет к разрушению квантового состояния. Для однофотонного пакета регистрация фотодетектором даст отсчеты только в одном из каналов с соответствующими вероятностями $|\alpha\cos a + \beta\sin a)|^2$ и $|-\alpha\sin a + \beta\cos a)|^2$.

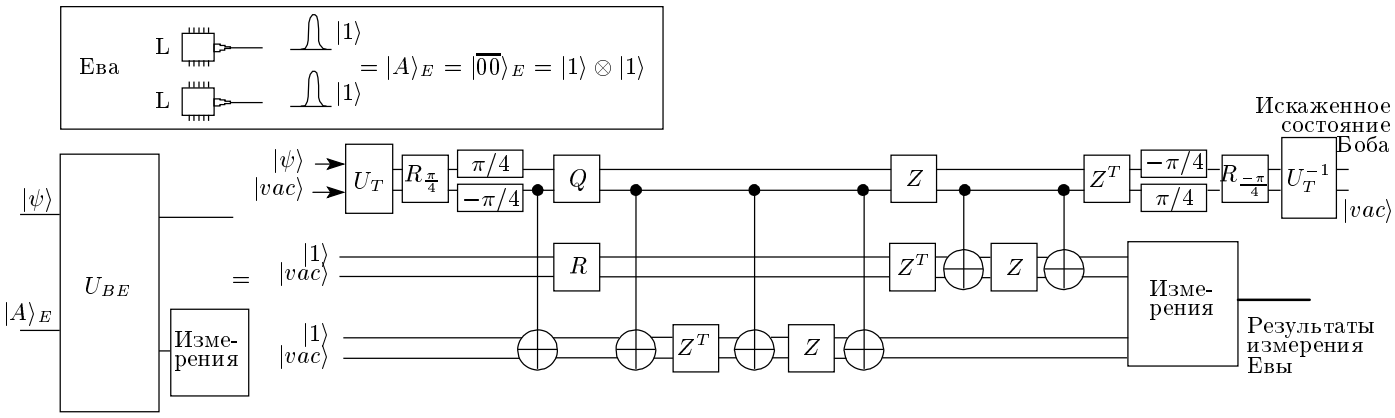

Рис. 5. Квантовая схема для подслушивания в физическом базисе. На вставке схематично показано приготовление исходного вспомогательного состояния Евы — двух независимых однофотонных состояний

самым уменьшить вероятность темновых отсчетов. Технически это осуществляется при помощи лазера на другой длине волны. Информационные квантовые состояния в каждой посылке привязаны по времени к импульсам синхронизации. Ева также имеет доступ к сигналам синхронизации, поэтому она может сделать вставку в оба канала. Иными словами, протокол квантового распределения ключей не содержит времени в том смысле, что Ева может удлинить обе линии связи на ту длину, которая ей требуется для вставки своей аппаратуры. Важно лишь сохранить привязку (относительное положение по времени) квантовых состояний к импульсам синхронизации в каждой посылке.

Для приготовления своего исходного состояния Ева может использовать пару лазеров, аналогичных лазеру на передающей стороне Алисы, которые формируют в двух каналах пару квазиоднофотонных состояний локализованных во временно́м окне 1 (см. вставку на рис. 5). Использование Евой двух разных источников для приготовления исходного квантового состояния возможно, поскольку, как видно из схемы рис. 5, не требуется суперпозиция состояний, принадлежащих разным кубитам (фотонам из разных каналов — 2 и 3).

Таким образом, приготовление исходного вспомогательного состояния Евы сводится к приготовлению двух однофотонных состояний, поступающих по двум оптоволоконным линиям Евы в каналы 2 и 3. Моменты приготовления этих состояний по времени привязаны к приходу к Еве информационных состояний Алисы. Эта привязка осуществляется Евой с использованием оптических импульсов синхронизации. Соответствие абстрактных состояний Евы в вычислительном базисе $|\overline{0}\rangle_E$ и $|\overline{1}\rangle_E$ явствует из рис. 5. Каждому вспомогательному кубиту Евы отвечает пара оптоволоконных каналов на рис. 5. Присутствие амплитуды состояния в верхней волоконной линии для каждой пары отвечает базисным состояниям $|\overline{0}\rangle_E|\overline{0}\rangle_E \to |1\rangle_E|1\rangle_E$ кубита, а вычислительным базисным состояниям $|\overline{1}\rangle_E|\overline{1}\rangle_E \to |1\rangle_E|1\rangle_E$ — присутствие амплитуд состояний в нижних волоконных линиях для каждой пары. Здесь под $|1\rangle_E|1\rangle_E$ понимается квантовое состояние, локализованное во временно́м окне 1, либо в верхних, либо нижних оптоволокнах Евы в каналах 2 и 3 (см. рис. 5).

Далее, в результате взаимодействия на квантовой схеме возникает состояние, которое является суперпозицией состояний в верхних и нижних каналах у Евы. Кроме того, модифицированное состояние Евы и модифицированное состояние Алисы (Боба) оказываются в общем запутанном (нефакторизуемом) состоянии. В дальнейшем это приводит к тому, что результат измерения Евы над своими квантовыми состояниями зависит от результата измерений Боба (см. разделы ниже). Фактически квантовая схема приводит к появлению эффекта Эйнштейна–Подольского–Розена [38] (ЭПР-корреляций) для двух однофотонных пакетов Евы и однофотонного пакета Боба.

Дополнительные блоки на схеме рис. 5 (U_T, U_T^{-1}, $R(\pm\pi/4)$, $\pm\pi/4$) служат, соответственно, для преобразования состояний из одной волоконной линии в две и переходу от формального вычислительного базиса к временно́му (см. формулы (20)–(24)). К описанию этих блоков мы переходим в следующем разделе.

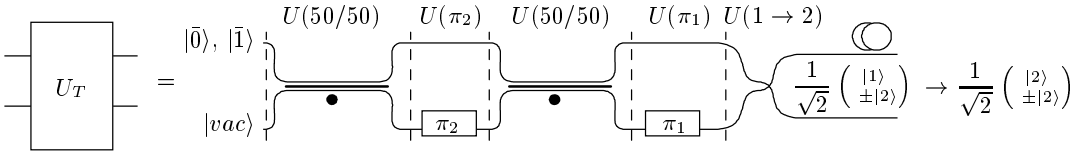

Рис. 6. Физическая реализация оператора преобразования квантового состояния Алисы–Боба из одной оптоволоконной линии связи (квантового канала) на два разных оптоволокна

2.4.1. Реализация оператора U_T преобразования к физическому базису

Дальнейшие действия будут сводиться к следующему. Квантовые состояния поступают к Еве по одной оптоволоконной линии (рис. 5). При физической реализации унитарных преобразований требуется «разведение» состояний на разные каналы, в каждом из которых присутствуют ортогональные компоненты. Займемся конструированием оператора преобразования U_T, разделяющего на разные физические каналы компоненты, фигурирующие перед базисными состояниями, локализованными во временных окнах 1 и 2.

Отметим во избежание путаницы, что ниже в этом разделе матрицы операторов записаны в представлении номеров двух пространственных каналов, а не базисных вычислительных квантовых состояний, поэтому матричные элементы операторов действуют на сами квантовые состояния в разных пространственных каналах, а не на их амплитуды (коэффициенты), как это имеет место в формулах (30), (31).

Оператор преобразования состояний может быть записан в виде

$$U_T = U(\pi_1)U(50/50)U(\pi_2)U(50/50), \qquad (32)$$

где действие оператора поворота, который реализуется при помощи оптоволоконного симметричного светоделителя, например, на квантовые состояния 0 и 1 в базисе + ($|\bar{0}\rangle = (|1\rangle + |2\rangle)/\sqrt{2}$ и $|\bar{1}\rangle = (|1\rangle - |2\rangle)/\sqrt{2}$), поступающее по верхнему каналу от Алисы, сводится к следующему[6]:

$$U(50/50)\{|\bar{0}\rangle, |\bar{1}\rangle\} = \frac{1}{\sqrt{2}}\begin{pmatrix} I & I \\ -I & I \end{pmatrix} \times \times \frac{1}{\sqrt{2}}\begin{pmatrix} |1\rangle \pm |2\rangle \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} |1\rangle \pm |2\rangle \\ -|1\rangle \mp |2\rangle \end{pmatrix}. \qquad (33)$$

Здесь $I = |1\rangle\langle 1| + |2\rangle\langle 2|$ — единичный оператор в канале. Верхний знак в формуле (33) отвечает преобразованию нуля $|\bar{0}\rangle$, нижний знак — состоянию $|\bar{1}\rangle$, отвечающему единице в вычислительном базисе.

Далее во втором временно́м окне (нижнем канале, см. рис. 6) действует оператор, изменяющий относительную фазу в суперпозиции состояний. Такой оператор относительного сдвига фазы в суперпозиции в нижнем канале реализуется при помощи фазового модулятора, аналогичного модулятору на передающей стороне Алисы, на который подается напряжение на короткое время только в момент прохождения через него состояния во втором временном окне. Напряжение изменяет оптическую длину и, соответственно, относительную фазу состояния, локализованного во временном окне 2 (см. рис. 6) относительно состояния в окне 1 (т. е. относительную фазу между передней и задней «половинками», находящимися в суперпозиции — общем квантовом состоянии). Формально действие такого оператора может быть описано как

$$U(\pi_2)U(50/50)\{|\bar{0}\rangle, |\bar{1}\rangle\} = = \begin{pmatrix} |1\rangle\langle 1| + |2\rangle\langle 2| & 0 \\ 0 & |1\rangle\langle 1| + e^{i\pi}|2\rangle\langle 2| \end{pmatrix} \times \times \frac{1}{2}\begin{pmatrix} |1\rangle \pm |2\rangle \\ -|1\rangle \mp |2\rangle \end{pmatrix} = \frac{1}{2}\begin{pmatrix} |1\rangle \pm |2\rangle \\ -|1\rangle \pm |2\rangle \end{pmatrix}. \qquad (34)$$

Действие следующего светоделителя сводится к выражению

[6] Из-за линейности квантовой схемы аналогично будут преобразовываться информационные состояния в сопряженном базисе с сохранением исходных фазовых соотношений между временными базисными состояниями $|1\rangle$ и $|2\rangle$.

$$U(50/50)U(\pi_2)U(50/50)\{|\overline{0}\rangle, |\overline{1}\rangle\} =$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ -I & I \end{pmatrix} \frac{1}{2} \begin{pmatrix} |1\rangle \pm |2\rangle \\ -|1\rangle \pm |2\rangle \end{pmatrix} =$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} \pm|2\rangle \\ -|1\rangle \end{pmatrix}. \quad (35)$$

Следующее изменение относительной фазы (оператор $U(\pi_1)$) аналогично изменению фазы (оператор $U(\pi_2)$) с той лишь разницей, что он действует на относительную фазу между состояниями в нижнем канале относительно друг друга и активируется лишь в момент прохождения состояния, локализованного во временном окне 1. Поскольку в нижнем канале присутствует лишь состояние, локализованное во временно́м окне 1, то по сути его действие сводится к устранению знака минус у состояния $|1\rangle$ (изменение относительной фазы на π) в суперпозиции состояний $|1\rangle$ и $|2\rangle$. Имеем

$$U(\pi_1)U(50/50)U(\pi_2)U(50/50)\{|\overline{0}\rangle, |\overline{1}\rangle\} =$$

$$= \begin{pmatrix} |1\rangle\langle 1| + |2\rangle\langle 2| & 0 \\ 0 & e^{i\pi}|1\rangle\langle 1| + |2\rangle\langle 2| \end{pmatrix} \times$$

$$\times \frac{1}{\sqrt{2}} \begin{pmatrix} \pm|2\rangle \\ -|1\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \pm|2\rangle \\ |1\rangle \end{pmatrix}. \quad (36)$$

Последний оператор $U(1 \leftrightarrow 2)$ просто меняет местами каналы 1 и 2, что реализуется перестановкой оптоволокон в двух каналах (рис. 6):

$$U(1 \leftrightarrow 2)\frac{1}{\sqrt{2}} \begin{pmatrix} \pm|2\rangle \\ |1\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |1\rangle \\ \pm|2\rangle \end{pmatrix}. \quad (37)$$

Наконец, для дальнейшей реализации однокубитных операторов необходимо обеспечить интерференцию состояний в верхнем и нижнем каналах, для этого требуется привести состояния к одному временно́му окну — сделать задержку состояния в окне 1, $|1\rangle \to |2\rangle$[7)].

В итоге состояние, поступающее от Алисы по одной линии «разводится» на два пространственных канала, причем все амплитудные и фазовые соотношения коэффициентов перед новыми пространственно-временны́ми базисными векторами состояний сохраняются как в исходных состояниях.

Подчеркнем, что такое состояние в двух пространственных каналах (оптоволокнах) это единое квантовое состояние с нормировкой на единицу. Например, измерение в одном из каналов приведет к разрушению состояния. Вероятность отсчета в каждом из каналов пропорциональна квадрату амплитуды.

2.4.2. Реализация операторов H, Q, Z, $R^{\pm}(a)$

Приведем реализацию недостающих операторов, фигурирующих в квантовой схеме. В следующем разделе нам потребуются операторы Адамара H и несимметричного Адамара Q (см. (14), (15)):

$$H = \begin{pmatrix} I & I \\ I & -I \end{pmatrix},$$
$$Q = \begin{pmatrix} \sqrt{1-Q}I & \sqrt{Q}I \\ \sqrt{Q}I & -\sqrt{1-Q}I \end{pmatrix}. \quad (38)$$

Физическая реализация представлена на рис. 7.

Реализация оператора Адамара H представляет собой симметричный оптоволоконный светоделитель и фазовый модулятор в нижнем плече, который изменяет фазу амплитуды состояния на π в нижнем плече относительно амплитуды в верхнем плече.

Реализация несимметричного оператора Адамара Q аналогична предыдущему с той лишь разницей, что используется несимметричный светоделитель с коэффициентами прохождения/отражения $\sqrt{1-Q}/\sqrt{Q}$.

Операторы Z и Z^T обеспечивают относительный сдвиг фазы между верхним и нижним каналами соответственно на $\pm\pi/4$ и реализуются при помощи фазового модулятора в нижнем оптоволокне.

Операторы поворота $R^{\pm}$ представляют собой асимметричные светоделители, которые уже обсуждались выше.

2.4.3. Оператор CNOT

Наиболее сложным в реализации является двухкубитный квантовый вентиль CNOT. Действие данного вентиля на базисные состояния в вычислительном базисе сводится к следующему:

[7)] Напомним, что из-за наличия синхронизации состояния в разных каналах должны быть приведены лишь к общему временно́му окну. Номер его 1 или 2 не важен, поскольку на выходе квантовой схемы Ева всегда может привести временно́е положение информационных состояний Боба к исходному положению относительно классического синхроимпульса. Поэтому ниже без дополнительных оговорок мы будем приводить квантовые состояния в разных пространственных каналах внутри схемы к тому общему временно́му окну (1 или 2), которое более удобно в соответствующем месте схемы.

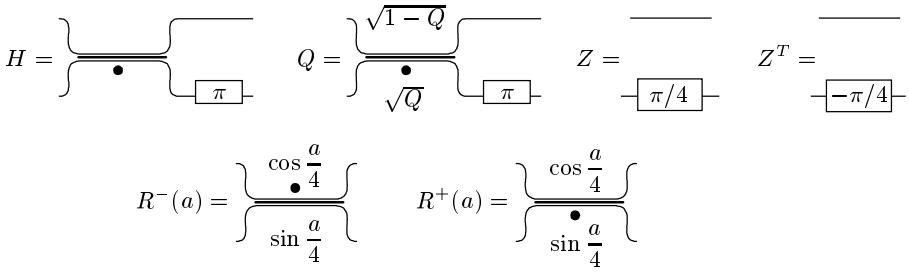

Рис. 7. Физическая реализация основных однокубитных вентилей

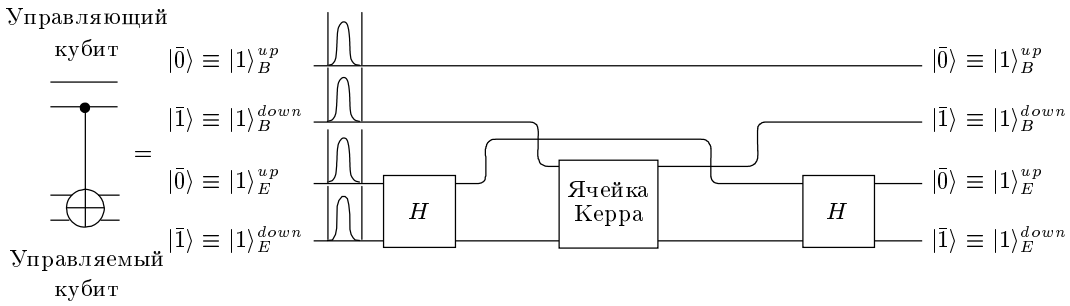

Рис. 8. Реализация оператора CNOT при помощи ячейки Керра и двух квантовых вентилей Адамара

$$\begin{aligned} \mathrm{CNOT}|\overline{00}\rangle = |\overline{00}\rangle, \quad \mathrm{CNOT}|\overline{01}\rangle = |\overline{01}\rangle, \\ \mathrm{CNOT}|\overline{10}\rangle = |\overline{11}\rangle, \quad \mathrm{CNOT}|\overline{11}\rangle = |\overline{10}\rangle, \end{aligned} \tag{39}$$

где первый кубит является управляющим (control), а второй управляемым (target). Удобнее получить действие CNOT сразу в физическом (временно́м) базисе состояний, локализованных во временных окнах 1 и 2. Состояния представляют собой однофотонные пакеты $|1\rangle$ и $|2\rangle$. Введем для удобства индексы для контрольного (состояние Алисы–Боба) и управляемого кубита (состояние Евы). Действие CNOT должно сводиться к следующему (см. рис. 8):

$$\begin{aligned} \mathrm{CNOT}|0\rangle_B \otimes |0\rangle_E = |0\rangle_B \otimes |0\rangle_E, \\ \mathrm{CNOT}|1\rangle_B \otimes |0\rangle_E = |1\rangle_B \otimes |1\rangle_E, \\ \mathrm{CNOT}|0\rangle_B \otimes |1\rangle_E = |0\rangle_B \otimes |1\rangle_E, \\ \mathrm{CNOT}|1\rangle_B \otimes |1\rangle_E = |1\rangle_B \otimes |0\rangle_E, \\ |\overline{0}\rangle \to |0\rangle_{B,E} \to |1\rangle_{B,E}^{up}, \\ |\overline{1}\rangle \to |1\rangle_{B,E} \to |1\rangle_{B,E}^{down}. \end{aligned} \tag{40}$$

Для получения необходимого результата удобно разбить действие CNOT на действие двух операторов Адамара и нелинейной ячейки Керра (рис. 8). Поскольку для действия операторов Адамара требуется суперпозиция состояний из верхнего и нижнего каналов, состояния в верхнем и нижнем каналах должны поступать в одном и том же временно́м окне (см. рис. 8).

Рассмотрим теперь оператор на основе ячейки Керра. Введем операторы рождения однофотонных пакетов в верхнем $|0\rangle$ и нижнем $|1\rangle$ каналах для состояний Боба a_{0B}^+, a_{1B}^+ и Евы a_{0E}^+, a_{1E}^+. Введем гамильтониан, описывающий кубическую нелинейность, $\mathcal{H} = \chi^{(3)} n_{1B} n_{1E}$. Здесь $n_{0B,E} = a_{0B,E}^+ a_{0B,E}$ — операторы числа пакетов фотонов в верхнем канале, $n_{1B,E} = a_{1B,E}^+ a_{1B,E}$ — в нижнем, L — длина кристалла.

Действие гамильтониана на базисные состояния дает

$$\begin{aligned} \mathcal{H}|0\rangle_B \otimes |0\rangle_E = 0, \quad \mathcal{H}|0\rangle_B \otimes |1\rangle_E = 0, \\ \mathcal{H}|1\rangle_B \otimes |0\rangle_E = 0, \\ \mathcal{H}|1\rangle_B \otimes |1\rangle_E = \chi^{(3)}|1\rangle_B \otimes |1\rangle_E. \end{aligned} \tag{41}$$

Соответствующий оператор эволюции, описывающий преобразование квантовых состояний при прохождении через квантовый вентиль имеет вид $U_{\mathrm{CNOT}} = e^{-iL\mathcal{H}}$. Если параметры гамильтониана выбраны такими, что набег фазы $L\chi^{(3)} = \pi$, то преобразование состояний имеет вид

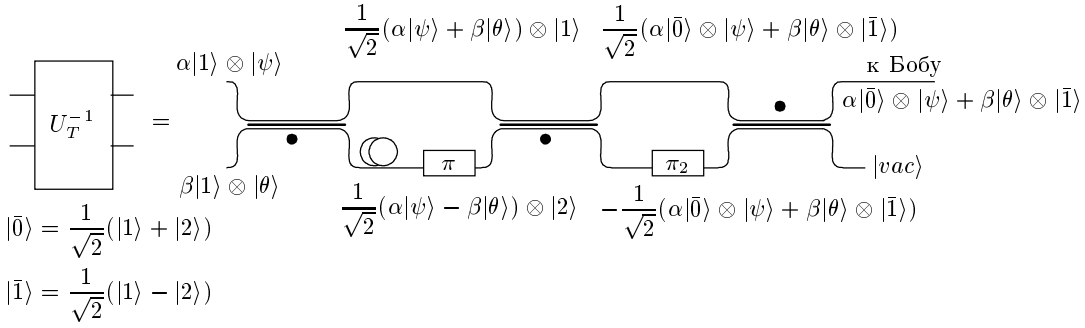

Рис. 9. Физическая реализация схемы преобразования квантового состояния из разных каналов в одну волоконно-оптическую линию

$$\begin{aligned} U_{\mathrm{CNOT}}|0\rangle_B\otimes|0\rangle_E &= |0\rangle_B\otimes|0\rangle_E,\\ U_{\mathrm{CNOT}}|0\rangle_B\otimes|1\rangle_E &= |0\rangle_B\otimes|1\rangle_E,\\ U_{\mathrm{CNOT}}|1\rangle_B\otimes|0\rangle_E &= |1\rangle_B\otimes|0\rangle_E,\\ U_{\mathrm{CNOT}}|1\rangle_B\otimes|1\rangle_E &= -|1\rangle_B\otimes|1\rangle_E. \end{aligned} \tag{42}$$

Требуемое действие CNOT получается «обкладыванием» оператора эволюции U_{CNOT} операторами Адамара, которые уже рассматривались выше. Имеем

$$\mathrm{CNOT} = (I_B\otimes H_E)U_{\mathrm{CNOT}}(I_B\otimes H_E). \tag{43}$$

Здесь нужно оговорить следующее. Реализация CNOT требует специфического гамильтониана. В требуемом виде гамильтонианов, которые действуют, как требуется в формуле (41), не бывает, кроме кубичной нелинейности всегда присутствуют другие слагаемые — линейное и, возможно, квадратичное. Данные слагаемые будут играть роль нежелательных. Поэтому действие CNOT не будет детерминистическим, оно будет вероятностным в том смысле, что требуемое действие CNOT будет иметь место не с вероятностью единица (детерминистическое действие), а лишь с некоторой вероятностью (вероятностное действие). Вторая проблема состоит в том, что необходимо иметь достаточно большую кубичную нелинейность (при разумной длине L кристалла), чтобы обеспечить необходимый набег фазы π. Существуют оценки для резонансного случая, которые показывают на достижимость сдвига фазы π (см. детали, например, в работах [39–45]).

Отметим также, что известны предложения по реализации вероятностного (с вероятностью правильного результата 1/9) оператора CNOT, которые используют только линейные оптические компоненты (асимметричные светоделители) [46–49]. Действие такого CNOT продемонстрировано в модельных экспериментах [49]. Однако для наших целей такая реализация не подходит, поскольку требует суперпозиции состояний, полученных из разных и независимых источников (Евы и Боба). В модельных экспериментах [49] для состояний управляющего (control) и управляемого (target) кубитов, используется один источник оптических состояний. Поэтому использование ячейки Керра, по-видимому, является единственно возможным вариантом реализации CNOT для подслушивания в квантовой криптографии. Фактически данная проблема (а вовсе не проблема декогерентности) в значительной степени лимитирует создание крупномасштабного квантового компьютера.

2.4.4. Обратное преобразование модифицированных состояний Боба

После взаимодействия система оказывается в общем запутанном состоянии, которое описывается формулами (4), (5). После модификации состояний Боба Ева осуществляет обратное преобразование, сводящее состояния в одно оптоволокно. Такое преобразование осуществляется локально, т. е. затрагивает только степени свободы, относящиеся к состоянию Боба. Но поскольку система находится в общем запутанном состоянии, преобразование состояний Боба косвенно затрагивает и степени свободы состояния Евы.

Физическая реализация схемы приведена на рис. 9. Для экономии места мы не записываем матричное представление физической реализации схемы, поскольку выкладки аналогичны вычислениям, приведенным в предыдущих разделах при описании преобразования состояний из одной волоконно-оптической линии в разные каналы.

Единственное существенное отличие данной схемы от предыдущей состоит в том, что входное со-

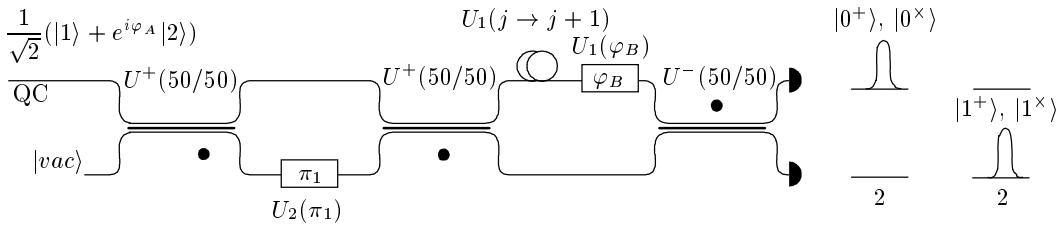

Рис. 10. Физическая реализация схемы волоконно-оптической схемы для детерминистического детектирования состояний на приемной стороне Боба

стояние является запутанным (см. рис. 9). Входное состояние присутствует в двух каналах (оптоволокнах):

$$\begin{pmatrix} \alpha|1\rangle \otimes |\psi\rangle \\ \beta|1\rangle \otimes |\theta\rangle \end{pmatrix}.$$

На выходе схемы запутанное квантовое состояние поступает в одну линию $\alpha|1\rangle \otimes |\psi\rangle + \beta|2\rangle \otimes |\theta\rangle$. Степени свободы Евы «присутствуют» в оптоволокнах у Евы. Свойство квантово-механической запутанности в отличие от суперпозиции, которая возможна и для классических систем, не имеет классического аналога. Дальнейшие измерения Боба над своим модифицированным состоянием будет приводить к редукции общего запутанного состояния. Поэтому состояние, которое оказывается в распоряжении Евы, будет зависеть от исхода измерений Боба.

2.5. Измерение квантовых состояний на приемной стороне

При измерениях Боб случайно и независимо от Алисы выбирает базис измерений. Затем через открытый канал Алиса раскрывает базис, в котором она посылала состояния, но не сами состояния. Те посылки, где базисы не совпадали, отбрасываются. Ева также отбрасывает данные посылки. Информацию из открытого канала связи Ева использует при проведении своих измерений. Цель Евы минимизировать ошибку различения квантовых состояний.

Выбор информационных состояний (2), (3) осуществляется Алисой при помощи выбора фазы (φ_A). Аналогично, при детектировании состояний Боб выбирает базис (фазу φ_B). Соответствие между фазами и информационными состояниями следующее:

Базис	Бит	Алиса, φ_A	Боб, φ_B
$+$	0	$\varphi_A = 0$	$\varphi_B = 0$
	1	$\varphi_A = \pi$	
$\times$	0	$\varphi_A = \frac{\pi}{2}$	$\varphi_B = \frac{\pi}{2}$
	1	$\varphi_A = \frac{3\pi}{2}$	

(44)

Измерения Боба описываются ортогональными проекторами, которые суммируются в единичный оператор. Измерения в прямом и сопряженном базисах описываются следующими разложениями единицы:

$$I_B = |\overline{0^+}\rangle\langle\overline{0^+}| + |\overline{1^+}\rangle\langle\overline{1^+}|, \tag{45}$$

$$I_B = |\overline{0^\times}\rangle\langle\overline{0^\times}| + |\overline{1^\times}\rangle\langle\overline{1^\times}|. \tag{46}$$

Формальные измерения, описываемые разложениями единицы (45), (46), реализуются при помощи оптоволоконной схемы, показанной на рис. 10. Данная схема, в отличие от всех известных оптоволоконных систем квантовой криптографии [17–37], осуществляет детерминистическое детектирование квантовых состояний. Под детерминистическим понимается такое измерение, которое дает исход с вероятностью единица (при совпадающих базисах). Все остальные реализованные схемы, идея реализации которых восходит к работе [3] (см. также патент [3]), дают результат лишь с вероятностью $1/2$.

Входным является одно из состояний (2), (3). Для выходного состояния перед детекторами находим, что

$$U^{Measure}_{Determ}(\varphi_B)\frac{1}{\sqrt{2}}\begin{pmatrix} (|1\rangle + e^{i\varphi_A}|2\rangle) \\ |vac\rangle \end{pmatrix} = \\ = \frac{1}{2}\begin{pmatrix} (e^{i\varphi_A} + e^{i\varphi_B})|2\rangle \\ -(e^{i\varphi_A} - e^{i\varphi_B})|2\rangle \end{pmatrix}. \tag{47}$$

Оператор $U_{Determ}^{Measure}(\varphi_B)$ описывает работу схемы на рис. 10, его более детальное представление через элементарные вентили очевидно из рис. 10, поэтому из-за экономии места не приводится.

Дополнительный светоделитель и управляемый переменный фазовый модулятор в нижнем плече позволяют избавиться от нежелательных не информационных компонент состояния перед детекторами во временны́х окнах 1 и 3. Все выходные состояния локализованы только во втором временно́м окне, причем с нужными фазовыми соотношениями. Таким образом, если после согласования базисов произошел отсчет в верхнем детекторе, то это событие однозначно и с вероятностью единица интерпретируется Бобом как логический 0. Срабатывание нижнего детектора также во временно́м окне 2 так же однозначно интерпретируется как логическая 1.

Вероятность детектирования по верхнему каналу в информационном временно́м окне 2 есть

$$\Pr(2,\mathrm{up}) = \frac{1}{4}|e^{i\varphi_A} + e^{i\varphi_B}|^2, \qquad (48)$$

соответственно, по нижнему каналу во втором окне —

$$\Pr(2,\mathrm{down}) = \frac{1}{4}|e^{i\varphi_A} - e^{i\varphi_B}|^2. \qquad (49)$$

Как следует из формул (47)–(49), при совпадающих базисах информационные состояния различаются с вероятностью единица. Кстати отметим, что использование детерминистической схемы регистрации повышает скорость передачи ключей в два раза при прочих равных условиях[8)].

2.6. Преобразование состояний подслушивателя перед измерением

Цель данного раздела — построить физическую схему измерений Евы. Единственной реальной возможностью является регистрация фотонов детекторами. Вероятность регистрации (при идеальной квантовой эффективности детектора) равна амплитуде квантового состояния в канале регистрации. Поэтому перед посылкой состояния на детектор требуется определенное преобразование состояния к такому виду, который обеспечивал бы минимальную ошибку Евы при различении пары неортогональных состояний.

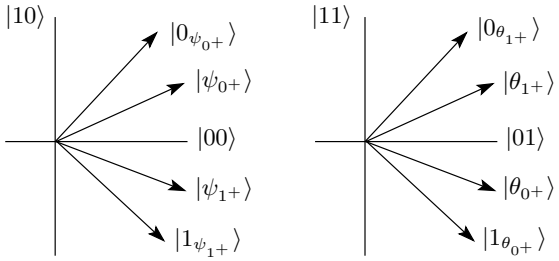

Рис. 11. Геометрия состояний у Евы после измерений Боба

Совместное состояние Боба и Евы является запутанным, поэтому состояние, которое оказывается в распоряжении Евы, зависит от исхода измерений Боба. Например, если Алиса посылала 0 в базисе +, то измерения Боба над состоянием $|\Psi_{0+}\rangle_{BE}$ (см. формулы (4), (5)) могут дать как правильный результат $|\overline{0+}\rangle$ (0), так и ошибочный $|\overline{1+}\rangle$ (1). Если Боб получил правильный результат, то из-за запутанности совместного состояния в распоряжении Евы окажется состояние $|\psi_{0+}\rangle$. Если же Боб получил неправильный исход, у Евы окажется состояние $|\theta_{0+}\rangle$.

Аналогичная ситуация имеет место, если Алиса посылала 1 в базисе +. При правильном исходе у Боба (1) состояние Евы есть $|\psi_{1+}\rangle$, соответственно, при неправильном исходе у Боба (0) у Евы будет состояние $|\theta_{1+}\rangle$.

Кроме того, как будет видно непосредственно из квантовой схемы, Ева достоверно различает ситуации, когда Боб получил правильный или неправильный результат. Но, естественно, при этом она не может достоверно отличить, что получил Боб, 0 или 1. Это связано с тем, что состояния, которые оказываются у Евы и отвечают 0 и 1 (при правильном исходе у Боба это, соответственно, состояния $|\psi_{0+}\rangle$ — 0 и $|\psi_{1+}\rangle$ — 1), являются неортогональными, т. е. принципиально достоверно неразличимыми.

Аналогичная ситуация имеет место, если Боб получил неверный исход. В этом случае в распоряжении Евы будут состояния $|\theta_{0+}\rangle$ и $|\theta_{1+}\rangle$, которые также неортогональны и достоверно неразличимы.

Таким образом, Ева должна построить такую схему измерений, которая минимизирует ошибку различения пары неортогональных состояний, либо $|\psi_{0+}\rangle$ и $|\psi_{1+}\rangle$, либо $|\theta_{0+}\rangle$ и $|\theta_{1+}\rangle$. Такие измерения формально известны [51] и сводятся к измерению в базисах, показанных на рис. 11. Неформально, базисные векторы при измерении расположены симметрично

[8)] Отметим, что может быть предъявлена оптическая схема для детерминистического приготовления квантовых состояний на передающей стороне Алисы (см. [50]), что в совокупности позволяет в четыре раза увеличить скорость передачи ключей по сравнению со всеми существующими оптоволоконными реализациями систем квантовой криптографии [17–37].

между векторами $|\psi_{0^+}\rangle$ и $|\psi_{1^+}\rangle$, и аналогично для векторов $|\theta_{0^+}\rangle$ и $|\theta_{1^+}\rangle$ (рис. 11). Напомним также, что пары векторов $|\psi_{0^+}\rangle$, $|\psi_{1^+}\rangle$ и $|\theta_{0^+}\rangle$, $|\theta_{1^+}\rangle$ (см. формулу (8), где приведены явные выражения для этих векторов) лежат в ортогональных подпространствах. Именно это обстоятельство позволяет Еве достоверно различать, правильный или неправильный исход был у Боба, но не установить сам исход, 0 или 1, так как для этого требуется различать векторы состояний внутри каждой пары.

Наконец, перейдем к конструированию самой схемы.

Условная вероятность того, что Алисой был послан 0, например, в прямом базисе, и Боб получил правильный результат 0 в том же базисе, равна

$$\Pr(0_B|0_A) = \mathrm{Tr}_{BE}\{|\Psi^{0^+}\rangle_{BEBE}\langle\Psi^{0^+}||\overline{0^+}\rangle\langle\overline{0^+}|\}. \quad (50)$$

Соответственно, условная вероятность того, что Алисой был послан 0 и Боб получил неверный результат, т. е. в результате измерений получена 1, равна

$$\Pr(1_B|0_A) = \mathrm{Tr}_{BE}\{|\Psi^{0^+}\rangle_{BEBE}\langle\Psi^{0^+}||\overline{1^+}\rangle\langle\overline{1^+}|\}. \quad (51)$$

Ошибка на приемной стороне Боба имеет вид

$$Q = \frac{\Pr(1_B|0_A)}{\Pr(0_B|0_A) + \Pr(1_B|0_A)}. \quad (52)$$

Аналогичные выражения получаются для условных вероятностей, если Алисой была послана 1. Имеем в прямом базисе

$$\Pr(1_B|1_A) = \mathrm{Tr}_{BE}\{|\Psi^{1^+}\rangle_{BEBE}\langle\Psi^{1^+}||\overline{1^+}\rangle\langle\overline{1^+}|\}. \quad (53)$$

Соответственно

$$\Pr(0_B|1_A) = \mathrm{Tr}_{BE}\{|\Psi^{1^+}\rangle_{BEBE}\langle\Psi^{1^+}||\overline{0^+}\rangle\langle\overline{0^+}|\}. \quad (54)$$

Аналогичные выражения имеют место для условных вероятностей в сопряженном базисе, которые получаются из формул (50)–(54) заменой индекса «+» на «×»:

$$\Pr(0_B|0_A) = \mathrm{Tr}_{BE}\{|\Psi^{0^\times}\rangle_{BEBE}\langle\Psi^{0^\times}||\overline{0^\times}\rangle\langle\overline{0^\times}|\}, \quad (55)$$

$$\Pr(1_B|0_A) = \mathrm{Tr}_{BE}\{|\Psi^{0^\times}\rangle_{BEBE}\langle\Psi^{0^\times}||\overline{1^\times}\rangle\langle\overline{1^\times}|\}, \quad (56)$$

$$\Pr(1_B|1_A) = \mathrm{Tr}_{BE}\{|\Psi^{1^\times}\rangle_{BEBE}\langle\Psi^{1^\times}||\overline{1^\times}\rangle\langle\overline{1^\times}|\}, \quad (57)$$

$$\Pr(0_B|1_A) = \mathrm{Tr}_{BE}\{|\Psi^{1^\times}\rangle_{BEBE}\langle\Psi^{1^\times}||\overline{0^\times}\rangle\langle\overline{0^\times}|\}. \quad (58)$$

Если Боб получил правильный результат (50), то состояние Евы описывается матрицей плотности (пока ненормированной)

$$\sigma_E^{0^+,0^+} = \mathrm{Tr}_B\{|\Psi^{0^+}\rangle_{BEBE}\langle\Psi^{0^+}||\overline{0^+}\rangle\langle\overline{0^+}|\} = \\ = (1-Q)|\psi_{0^+}\rangle\langle\psi_{0^+}|. \quad (59)$$

Если Бобом был получен неверный исход (51), то состояние Евы оказывается равным

$$\sigma_E^{1^+,0^+} = \mathrm{Tr}_B\{|\Psi^{0^+}\rangle_{BEBE}\langle\Psi^{0^+}||\overline{1^+}\rangle\langle\overline{1^+}|\} = \\ = Q|\theta_{0^+}\rangle\langle\theta_{0^+}|. \quad (60)$$

Соответственно для исходов измерений (57), (58) частичные матрицы плотности Евы имеют вид

$$\sigma_E^{1^+,1^+} = \mathrm{Tr}_B\{|\Psi^{1^+}\rangle_{BEBE}\langle\Psi^{1^+}||\overline{1^+}\rangle\langle\overline{1^+}|\} = \\ = (1-Q)|\psi_{1^+}\rangle\langle\psi_{1^+}|, \quad (61)$$

$$\sigma_E^{0^+,1^+} = \mathrm{Tr}_B\{|\Psi^{1^+}\rangle_{BEBE}\langle\Psi^{1^+}||\overline{0^+}\rangle\langle\overline{0^+}|\} = \\ = Q|\theta_{1^+}\rangle\langle\theta_{1^+}|. \quad (62)$$

Аналогично в сопряженном базисе

$$\sigma_E^{0^\times,0^\times} = \mathrm{Tr}_B\{|\Psi^{0^\times}\rangle_{BEBE}\langle\Psi^{0^\times}||\overline{0^\times}\rangle\langle\overline{0^\times}|\} = \\ = (1-Q)|\psi_{0^\times}\rangle\langle\psi_{0^\times}|, \quad (63)$$

$$\sigma_E^{1^\times,0^\times} = \mathrm{Tr}_B\{|\Psi^{0^\times}\rangle_{BEBE}\langle\Psi^{0^\times}||\overline{1^\times}\rangle\langle\overline{1^\times}|\} = \\ = Q|\theta_{0^\times}\rangle\langle\theta_{0^\times}|, \quad (64)$$

$$\sigma_E^{1^\times,1^\times} = \mathrm{Tr}_B\{|\Psi^{1^\times}\rangle_{BEBE}\langle\Psi^{1^\times}||\overline{1^\times}\rangle\langle\overline{1^\times}|\} = \\ = (1-Q)|\psi_{1^\times}\rangle\langle\psi_{1^\times}|, \quad (65)$$

$$\sigma_E^{0^\times,1^\times} = \mathrm{Tr}_B\{|\Psi^{1^\times}\rangle_{BEBE}\langle\Psi^{1^\times}||\overline{0^\times}\rangle\langle\overline{0^\times}|\} = \\ = Q|\theta_{1^\times}\rangle\langle\theta_{1^\times}|. \quad (66)$$

Далее ограничимся оптимальными индивидуальными измерениями Евы, поскольку коллективные измерения, хотя формально могут быть построены и дают больше информации о ключе, на сегодняшний день находятся далеко за пределами технологических возможностей.

После раскрытия базисов Алисой и Бобом задача Евы сводится к различению состояний 0 и 1 внутри известного базиса, т. е. различению одной из четырех частичных матриц плотности Евы, например, в базисе + это следующие состояния $\sigma_E^{0^+,0^+}$, $\sigma_E^{1^+,0^+}$,

$\sigma_E^{1^+,1^+}$, $\sigma_E^{0^+,1^+}$. Аналогично в сопряженном базисе задача сводится к различению состояний $\sigma_E^{0^\times,0^\times}$, $\sigma_E^{1^\times,0^\times}$, $\sigma_E^{1^\times,1^\times}$, $\sigma_E^{0^\times,1^\times}$. Далее, так как состояния $|\psi_{0^+,1^+}\rangle$ и $|\theta_{0^+,1^+}\rangle$ лежат в ортогональных подпространствах (см. формулы (6), (9)) и поэтому достоверны (безошибочно различимы), то задача Евы фактически сводится лишь к различению состояний внутри каждой пары, т. е. отдельно к различению $|\psi_{0^+}\rangle$ и $|\psi_{1^+}\rangle$, а также к различению $|\theta_{0^+}\rangle$ и $|\theta_{1^+}\rangle$. Аналогично, в сопряженном базисе — к различению $|\psi_{0^\times}\rangle$ и $|\psi_{1^\times}\rangle$ и отдельно к различению $|\theta_{0^\times}\rangle$ и $|\theta_{1^\times}\rangle$.

Построим следующие состояния: $\{|0_{\psi_{0^+}}\rangle, |1_{\psi_{1^+}}\rangle, |0_{\theta_{0^+}}\rangle, |1_{\theta_{1^+}}\rangle\}$ (соответственно $\{|0_{\psi_{0^\times}}\rangle, |1_{\psi_{1^\times}}\rangle, |0_{\theta_{1^\times}}\rangle, |1_{\theta_{1^\times}}\rangle\}$). При этом пара ортогональных состояний $|0_{\psi_{0^+}}\rangle$, $|1_{\psi_{1^+}}\rangle$ лежит в плоскости, натянутой на векторы $|\psi_{0^+}\rangle$, $|\psi_{1^+}\rangle$, которые расположены симметрично относительно них (рис. 11), аналогично для второй пары ортогональных векторов $|0_{\theta_{0^+}}\rangle$, $|1_{\theta_{1^+}}\rangle$ (рис. 11). Аналогичная ситуация имеет место для вектора в сопряженном базисе. Фактически при таком измерении имеется четыре элементарные исхода, каждому из которых сопоставляется ортогональный проектор.

Пара ортогональных векторов, на которые происходит проектирование состояний Евы, может быть записана как (см. рис. 11)

$$\begin{aligned} |0_{\psi_{0^+}}\rangle &= \frac{1}{\sqrt{2}}(|\overline{00}\rangle + |\overline{10}\rangle), \\ |1_{\psi_{1^+}}\rangle &= \frac{1}{\sqrt{2}}(|\overline{00}\rangle - |\overline{10}\rangle), \end{aligned} \tag{67}$$

векторы были между собой ортогональны. Аналогично для измеряющих векторов в подпространстве θ

$$\begin{aligned} |1_{\theta_{0^+}}\rangle &= \frac{1}{\sqrt{2}}(|\overline{01}\rangle - |\overline{11}\rangle), \\ |0_{\theta_{1^+}}\rangle &= \frac{1}{\sqrt{2}}(|\overline{01}\rangle + |\overline{11}\rangle). \end{aligned} \tag{68}$$

Аналогично для измерений в сопряженном базисе.

Боб получает правильный результат (50) с вероятностью $1-Q$, соответственно для Евы вероятность получить правильный результат равна (переходная вероятность того, что состояние, посланное Алисой, есть 0 и Ева получит результат 0)

$$\begin{aligned} \Pr_E(0_E, 0_B|0_A) &= \mathrm{Tr}_E\{\overline{\sigma}_E^{0^+,0^+}|0_{\psi_{0^+}}\rangle\langle 0_{\psi_{0^+}}|\} = \\ &= \frac{1}{2}\left|\cos\frac{\alpha}{2} + \sin\frac{\alpha}{2}\right|^2 = \frac{1+\sqrt{1-(1-2Q)^2}}{2}, \end{aligned} \tag{69}$$

соответственно, вероятность неправильного исхода у Евы при условии, что Боб получил правильный результат,

$$\begin{aligned} \Pr_E(1_E, 0_B|0_A) &= \mathrm{Tr}_E\{\overline{\sigma}_E^{0^+,0^+}|1_{\psi_{0^+}}\rangle\langle 1_{\psi_{0^+}}|\} = \\ &= \frac{1}{2}\left|\cos\frac{\alpha}{2} - \sin\frac{\alpha}{2}\right|^2 = \frac{1-\sqrt{1-(1-2Q)^2}}{2}. \end{aligned} \tag{70}$$

Вероятность неправильного исхода у Евы при условии, что Боб тоже получил неправильный результат,

$$\begin{aligned} \Pr_E(1_E, 1_B|0_A) &= \mathrm{Tr}_E\{\overline{\sigma}_E^{1^+,0^+}|1_{\theta_{0^+}}\rangle\langle 1_{\theta_{0^+}}|\} = \\ &= \frac{1}{2}\left|\cos\frac{\alpha}{2} - \sin\frac{\alpha}{2}\right|^2 = \frac{1-\sqrt{1-(1-2Q)^2}}{2}, \end{aligned} \tag{71}$$

соответственно вероятность правильного исхода у Евы при условии, что Боб получил неправильный результат

$$\begin{aligned} \Pr_E(0_E, 1_B|0_A) &= \mathrm{Tr}_E\{\overline{\sigma}_E^{1^+,0^+}|0_{\theta_{1^+}}\rangle\langle 0_{\theta_{1^+}}|\} = \\ &= \frac{1}{2}\left|\cos\frac{\alpha}{2} + \sin\frac{\alpha}{2}\right|^2 = \frac{1+\sqrt{1-(1-2Q)^2}}{2}. \end{aligned} \tag{72}$$

Аналогичные соотношения имеют место в сопряженном базисе. В формулах (69)–(72) чертой сверху обозначены уже нормированные матрицы плотности Евы.

После измерений Евы они связаны бинарным классическим каналом связи с вероятностью ошибки, которая с учетом соотношений (59)–(62) равна

$$\begin{aligned} Q_E = {} & [\Pr_E(1_E, 0_B|0_A) + \Pr_E(1_E, 1_B|0_A)] \times \\ & \times [\Pr_E(0_E, 0_B|0_A) + \Pr_E(1_E, 0_B|0_A) + \\ & + \Pr_E(1_E, 1_B|0_A) + \Pr_E(0_E, 1_B|0_A)]^{-1} = \\ & = \frac{1-\sqrt{1-(1-2Q)^2}}{2}. \end{aligned} \tag{73}$$

Соответствующая ошибка в классическом канале Алиса–Боб после измерений Боба есть Q. Секретное распределение ключей возможно, если $Q < Q_E$. Соответственно, критическая ошибка, до которой возможна передача секретных ключей, определяется из уравнения

$$\begin{aligned} Q_c &= \frac{1-\sqrt{1-(1-2Q_c)^2}}{2}, \\ Q_c &= \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) \approx 14.6\,\%. \end{aligned} \tag{74}$$

На рис. 12 приведена квантовая схема, реализующая оптимальные (в смысле минимизации ошибки различения) измерения Евы. Верхняя половина

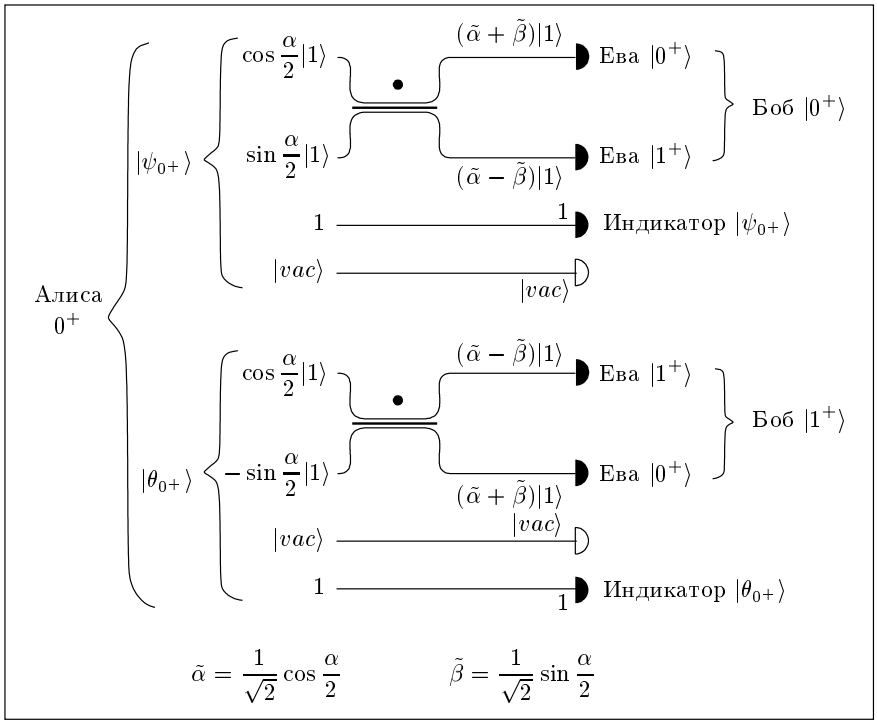

Рис. 12. Квантовая схема для оптимальных измерений Евы

схемы относится к случаю, когда Бобом был получен правильный исход (Алиса посылала 0 в базисе +). В этом случае из-за неортогональности состояний Евой может быть получен также правильный исход (верхний детектор), либо неправильный (нижний). Данные исходы происходят независимо от Евы (случайно) с вероятностями (69) и (71). Напомним, что вероятность срабатывания детектора пропорциональна квадрату модуля амплитуды квантового состояния в соответствующем канале.

Нижняя половина рис. 12 относится к случаю, когда Боб получил неверный исход. В этом случае Ева также может случайно с вероятностями (72) и (70) получить как правильный (нижний детектор), так и неправильный (верхний детектор) исходы.

Пара нижних детекторов служит для того, чтобы Ева смогла идентифицировать, в каком подпространстве у Боба был результат. Фактически по срабатыванию этих двух детекторов Ева может различить достоверно с вероятностью единица, правильный или не правильный результат получил Боб, но при этом Ева не может достоверно узнать, какой именно результат, 0 или 1, получил Боб (за это отвечают отсчеты в верхних детекторах, которые не дают Еве достоверной информации о передаваемом Алисой состоянии).

Сделаем дополнительные неформальные пояснения относительно детектирования состояний Евой. Состояние $|\psi_{0^+}\rangle$ оказывается в распоряжении Евы, когда Боб получил правильный результат (0). Данное состояние имеет структуру (см. формулу (9))

$$|\psi_{0^+}\rangle = \Big(\cos\frac{\alpha}{2}|0\rangle + \sin\frac{\alpha}{2}|1\rangle\Big)\otimes|0\rangle.$$

Второй кубит независим от первого и находится в базисном состоянии $|0\rangle$. На физическом уровне в оптоволоконной реализации это означает присутствие однофотонного состояния в верхнем канале оптоволокна, относящегося ко второму кубиту (см. рис. 12, верхняя половина).

Если же Боб получил неверный отсчет — 1, то у Евы будет состояние $|\theta_{0^+}\rangle$. Структура этого состояния (9) имеет вид

$$|\theta_{0^+}\rangle = \Big(\cos\frac{\alpha}{2}|0\rangle - \sin\frac{\alpha}{2}|1\rangle\Big)\otimes|1\rangle.$$

При этом второй кубит также независим от первого и находится в базисном состоянии $|1\rangle$, что означает присутствие однофотонного состояния в нижнем канале оптоволокна, относящегося ко второму кубиту (см. рис. 12, верхняя половина). Таким образом, состояние второго кубита является индикатором для Евы того, какой отсчет получил Боб — правильный

или ошибочный. Однако ничего не говорит о значении самого результата, для этого служит состояние первого кубита, которое также из-за неортогональности не дает Еве достоверного ответа о передаваемом состоянии.

Аналогичная ситуация имеет место, когда Алиса посылала 1 в базисе +.

Информацию о базисе Ева получает из открытого классического канала на стадии согласования базисов Алисой и Бобом. Если состояния посылались в сопряженном базисе ×, то имеет место ситуация, аналогичная рассмотренной выше.

3. КВАНТОВАЯ СХЕМА ДЛЯ ОПТИМАЛЬНОЙ АТАКИ НА ПРОТОКОЛ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ФАЗОВО-ВРЕМЕННЫ́М КОДИРОВАНИЕМ

В следующих разделах будет построена квантовая схема и ее физическая реализация для оптимального подслушивания протокола распределения ключей с фазово-временны́м кодированием. Общий алгоритм действий аналогичен предыдущему. Сначала приведем информационные состояния, затем формальную квантовую схему, а затем ее физическую реализацию.

3.1. Информационные состояния

В данном протоколе в отличие от протокола BB84 используются не два, а четыре базиса, пара из которых отличается друг от друга только смещением по времени квантовых состояний (см. детали в работах [10–12], а также рис. 2). Пару дополнительных временны́х базисов условно будем называть левым и правым базисами (см. рис. 2). Внутри левого и правого базисов состояния аналогичны рассмотренным в предыдущих разделах. Принципиальное преимущество данного метода кодирования состоит в том, что он является двухпараметрическим, т. е. присутствие подслушивателя детектируется не только по ошибкам в информационных последовательностях, но также и по отсчетам в контрольных временны́х окнах. Данный протокол обеспечивает самую большую критическую ошибку (вплоть до теоретического предела в 50 %), до которой гарантируется секретное распределение ключей [10–12]. Напомним, что предельная критическая ошибка для протокола BB84 при использовании Евой коллективных измерений составляет приблизительно 11 % [7]. При оптимальных индивидуальных измерениях допустимая ошибка, как мы видели в разд. 2.6, оказывается несколько больше — приблизительно 14.6 %. Кроме того, оказывается [8], что существует бесконечный набор атак Евы с коллективными измерениями разного типа, которые дают допустимые ошибки в интервале $11\,\% < Q < 14.6\,\%$.

Информационные квантовые состояния в левом базисе обозначим как

$$|\overline{0_L^+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |\overline{1_L^+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle). \quad (75)$$

Состояния в сопряженном базисе получаются из состояний поворотом:

$$|\overline{0_L^\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |\overline{1_L^\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle).$$

Соответственно, в правом базисе имеем

$$|\overline{0_R^+}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle), \quad |\overline{1_R^+}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle), \quad (76)$$

и, наконец, для состояний в сопряженном правом базисе —

$$|\overline{0_R^\times}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + i|3\rangle), \quad |\overline{1_R^\times}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - i|3\rangle).$$

3.2. Случай ортогональных состояний внутри базиса

Требуется построить квантовую схему, реализующую унитарный оператор U_{BE}. Достаточно выяснить действие оператора на временны́е базисные векторы, действие на информационные состояния (75), (76) можно получить, учитывая линейность U_{BE}. Преобразование Евы, которое действует на векторы из $\mathcal{H}_{AB}$ и анциллу из $\mathcal{H}_E$, имеет вид (см. детали в работах [11, 12])

$$\begin{aligned}
U_E(|1\rangle \otimes |A\rangle) &= \sqrt{1-2\delta}|1\rangle \otimes |\psi_1^1\rangle + \\
&+ \sqrt{\delta}|2\rangle \otimes |\psi_2^1\rangle + \sqrt{\delta}|3\rangle \otimes |\psi_3^1\rangle, \\
U_E(|2\rangle \otimes |A\rangle) &= \sqrt{\delta}|1\rangle \otimes |\psi_1^2\rangle + \\
&+ \sqrt{1-2\delta}|2\rangle \otimes |\psi_2^2\rangle + \sqrt{\delta}|3\rangle \otimes |\psi_3^2\rangle, \\
U_E(|3\rangle \otimes |A\rangle) &= \sqrt{\delta}|1\rangle \otimes |\psi_1^3\rangle + \\
&+ \sqrt{\delta}|2\rangle \otimes |\psi_2^3\rangle + \sqrt{1-2\delta}|3\rangle \otimes |\psi_3^3\rangle,
\end{aligned} \quad (77)$$

где справедливы следующие соотношения между состояниями $|\psi_i^j\rangle \in \mathcal{H}_E$:

$$\begin{aligned}
&\langle\psi_i^j|\psi_i^k\rangle = \langle\psi_j^i|\psi_k^i\rangle = 0, \\
&\langle\psi_1^1|\psi_2^2\rangle = \langle\psi_2^2|\psi_3^3\rangle = \cos\alpha, \\
&\langle\psi_1^2|\psi_2^1\rangle = \langle\psi_2^3|\psi_3^2\rangle = \cos\alpha.
\end{aligned} \quad (78)$$

Достаточно использовать вспомогательное состояние Евы, состоящее из трех кубитов (фотонов). Этого достаточно для построения состояний, удовлетворяющих приведенным соотношениям (78). Возьмем состояния следующего вида, записанные в вычислительном базисе:

$$|\psi_1^1\rangle = |\overline{000}\rangle, \quad |\psi_2^1\rangle = \cos\alpha|\overline{110}\rangle - \sin\alpha|\overline{111}\rangle,$$
$$|\psi_3^1\rangle = |\overline{010}\rangle,$$

$$|\psi_1^2\rangle = |\overline{110}\rangle, \quad |\psi_2^2\rangle = \cos\alpha|\overline{000}\rangle - \sin\alpha|\overline{001}\rangle, \quad |\psi_3^2\rangle = |\overline{100}\rangle, \tag{79}$$

$$|\psi_1^3\rangle = |\overline{010}\rangle, \quad |\psi_2^3\rangle = \cos\alpha|\overline{100}\rangle - \sin\alpha|\overline{101}\rangle, \quad |\psi_3^3\rangle = |\overline{000}\rangle. \tag{80}$$

Далее, базисным вычислительным состояниям будут сопоставлены базисные состояния во временны́х окнах, т. е. будет иметь место сопоставление $|\overline{0}\rangle \to |1\rangle$, где $|1\rangle$ — «часть» состояния в верхнем пространственном канале, $|\overline{1}\rangle \to |1\rangle$ — в нижнем пространственном канале.

Теперь покажем, как можно представить преобразование Евы, пользуясь операторами простой структуры.

Основу составляют операторы в пространстве Алисы и Боба, имеющем размерность 3, поскольку любое однофотонное состояние Алисы и Боба может быть представлено как линейная комбинация состояний, локализованных в трех временны́х окнах 1, 2 и 3. Далее для краткости будем называть такие состояния кутритами. Помимо единичного оператора в этом пространстве понадобятся также следующие преобразования, затрагивающие состояния отдельных фотонов.

1. Оператор «размазывания» по временны́м окнам $|1\rangle$ и $|3\rangle$ кутрита — он действует на подпространстве размерности 2 —

$$Q_{13} = \begin{pmatrix} \sqrt{1-2\delta} & 0 & \sqrt{2\delta} \\ 0 & 1 & 0 \\ \sqrt{2\delta} & 0 & -\sqrt{1-2\delta} \end{pmatrix}. \tag{81}$$

2. Оператор сдвига фазы на $\pi/4$ в определенном пространственном канале. В зависимости от знака угла он имеет в качестве верхнего индекса «+» или «−». Нижний индекс относится к номеру кубита, для которого проводится относительный сдвиг фазы между базисными состояниями. Например, положительный сдвиг фазы для первого кубита выглядит как

$$P_1^+ = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{82}$$

3. Оператор отрицания (NOT)

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{83}$$

4. Введем ряд операторов, реализующих «разложение» оператора отрицания F: A, B и C. Данные операторы удовлетворяют равенству $ABC = I$, но такие $PAFBFCF = F$, где P — необходимый сдвиг фазы. Нетрудно получить (см., например, [16]), что эти операторы имеют вид

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1-i & 0 \\ 0 & 1+i \end{pmatrix} \begin{pmatrix} \cos\dfrac{\pi}{8} & \sin\dfrac{\pi}{8} \\ -\sin\dfrac{\pi}{8} & \cos\dfrac{\pi}{8} \end{pmatrix}, \tag{84}$$

$$B = \begin{pmatrix} \cos\dfrac{\pi}{8} & -\sin\dfrac{\pi}{8} \\ \sin\dfrac{\pi}{8} & \cos\dfrac{\pi}{8} \end{pmatrix}, \tag{85}$$

$$C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix}. \tag{86}$$

5. Оператор отрицания для кутрита имеет вид (индексы относятся к базисным состояниям, для которых проводится отрицание)

$$F_{12} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{87}$$

6. Оператор поворота для кутрита. Обычно будет использоваться угол $\pm\pi/16$. Индексом обозначается то временно́е базисное состояние, которое не затрагивается данным преобразованием. Например,

$$R_{\pi/16}^{3+} = \begin{pmatrix} \cos\dfrac{\pi}{16} & \sin\dfrac{\pi}{16} & 0 \\ -\sin\dfrac{\pi}{16} & \cos\dfrac{\pi}{16} & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{88}$$

7. Операторы A, B и C, аналогичные введенным выше, но действующие на кутрит. Индексы обозначают временны́е базисные состояния кутрита, на которые действует оператор. Например,

$$B_{12} = \begin{pmatrix} \cos\dfrac{\pi}{8} & \sin\dfrac{\pi}{8} & 0 \\ -\sin\dfrac{\pi}{8} & \cos\dfrac{\pi}{8} & 0 \\ 0 & 0 & 1 \end{pmatrix}. \qquad (89)$$

Предыдущие преобразования затрагивают состояния либо отдельного кубита, либо кутрита. Рассмотрим теперь необходимые преобразования, которые запутывают состояния кутрита с отдельными кубитами. Матричное представление операторов в данном разделе записано в следующем базисе кутрит–кубит: $\{|10\rangle, |11\rangle, |20\rangle, |21\rangle, |30\rangle, |31\rangle\}$ (первый индекс относится к временны́м базисным состояниям кутрита, второй — к базисным состояниям кубита).

8. Оператор условного «размазывания» вспомогательного кубита анциллы при условии нахождения контрольного кутрита в базисном временно́м состоянии 2:

$$Q_2^c = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{1-2\delta} & \sqrt{2\delta} & 0 & 0 \\ 0 & 0 & \sqrt{2q} & -\sqrt{1-2\delta} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (90)$$

9. Несколько запутывающих операций для связки кутрит – два кубита, действующих только на двух наборах базисных состояний. Нам потребуются операторы двух типов: условное изменение бита и условный поворот на угол $\pi/4$. Для каждого из этих операторов будем обозначать индексами номера затрагиваемых базисных состояний при их лексикографическом упорядочении.

Запишем разложение оператора «несимметричного размазывания» Q_2^c и оператора условного поворота на связке «кутрит–кубит» R_α.

Оператор Q_2^c можно представить как условный поворот с последующей условной сменой фазы на π, т. е.

$$Q_2^c = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{1-2\delta} & \sqrt{2\delta} & 0 & 0 \\ 0 & 0 & \sqrt{2\delta} & -\sqrt{1-2\delta} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{1-2\delta} & \sqrt{2\delta} & 0 & 0 \\ 0 & 0 & -\sqrt{2\delta} & \sqrt{1-2\delta} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (91)$$

Оператор условного изменения фазы считаем уже реализованным (были перечислены такие операторы для угла $\pi/4$), поэтому осталось реализовать условный поворот на угол $\arcsin\sqrt{2\delta}$. Это сделать несложно, и этот оператор представляется как

$$CN^2R^{(2)}\left(-\frac{\arcsin\sqrt{2\delta}}{2}\right) \times$$

$$\times\, CN^2R^{(2)}\left(\frac{\arcsin\sqrt{2\delta}}{2}\right). \qquad (92)$$

Второй оператор условного поворота на угол α, реализуется аналогично:

$$R_\alpha = CN^2R^{(2)}\left(-\frac{\alpha}{2}\right) CN^2R^{(2)}\left(\frac{\alpha}{2}\right). \qquad (93)$$

Присутствующие в выражениях операторы имеют вид

$$R\left(\frac{\arcsin\sqrt{2\delta}}{2}\right) =$$

$$= \begin{pmatrix} \cos\dfrac{\arcsin\sqrt{2\delta}}{2} & \sin\dfrac{\arcsin\sqrt{2\delta}}{2} \\ -\sin\dfrac{\arcsin\sqrt{2\delta}}{2} & \cos\dfrac{\arcsin\sqrt{2\delta}}{2} \end{pmatrix}, \qquad (94)$$

$$R\left(\frac{\alpha}{2}\right) = \begin{pmatrix} \cos\dfrac{\alpha}{2} & \sin\dfrac{\alpha}{2} \\ -\sin\dfrac{\alpha}{2} & \cos\dfrac{\alpha}{2} \end{pmatrix}. \qquad (95)$$

Так, условное изменение бита, действующее на 2-й ($|101\rangle$) и 6-й ($|201\rangle$) по счету базисные векторы записывается как

$$F_{26} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1 \end{pmatrix}. \tag{96}$$

Условные повороты на $\pi/4$ обозначаются подобным же образом (верхний индекс отвечает за знак поворота):

$$C_{39}^{+} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&\frac{1}{\sqrt{2}}&0&0&0&0&0&\frac{1}{\sqrt{2}}&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&-\frac{1}{\sqrt{2}}&0&0&0&0&0&\frac{1}{\sqrt{2}}&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1 \end{pmatrix}, \tag{97}$$

$$C_{39}^{-} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&\frac{1}{\sqrt{2}}&0&0&0&0&0&-\frac{1}{\sqrt{2}}&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&\frac{1}{\sqrt{2}}&0&0&0&0&0&\frac{1}{\sqrt{2}}&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1 \end{pmatrix}. \tag{98}$$

Операторы такого вида несложно получить из элементарных операций и ниже будет показан явный способ получения указанных операторов. Матрицы операторов $C_{ij}^{\pm}$ и F_{ij} для связки записаны в базисе соответствующих векторов, упорядоченных следующим образом: {$|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$, $|200\rangle$, $|201\rangle$, $|210\rangle$, $|211\rangle$, $|300\rangle$, $|301\rangle$, $|310\rangle$, $|311\rangle$}.

10. Условный поворот на угол α кубита анциллы при контрольном кутрите в состоянии $|2\rangle$:

$$R_\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \cos\alpha & \sin\alpha & 0 & 0 \\ 0 & 0 & -\sin\alpha & \cos\alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (99)$$

11. Хорошо известный оператор «условное НЕ» (control NOT)

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (100)$$

12. Аналог оператора «условное НЕ» для связки кутрит–кубит, меняющий состояние кубита только при условии нахождения кутрита в определенном состоянии. Для условного изменения состояния кубита, при значении 2 кутрита, матрица оператора выглядит как

$$CN^2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (101)$$

13. Оператор для связки кутрит–кубит, аналогичный предыдущему, но изменяющий состояние кутрита при условии единичного состояния кубита. Числа в индексах обозначают временны́е базисные состояния кутрита, меняющиеся между собой местами, при состоянии кубита в единице. Например, условная смена местами амплитуд состояний во временны́х окнах 2 и 3 кутрита выглядит следующим образом:

$$CN_{23} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}. \qquad (102)$$

14. Условный сдвиг фазы на $\pi/4$ в связке кутрит–кубит. Индексы таких операторов означают сигнальное и преобразуемое значения связки. Так, перемена фазы у элемента, где значение кутрита равно 2, а значение кубита равно 1, обозначается как P_1^2. Оператор этого преобразования выглядит как

$$P_1^{2+} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{i\pi/4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (103)$$

Будем по очереди присоединять кубиты анциллы к исходному состоянию. За основу возьмем оператор Q_{13}. Присоединим теперь анциллу в состоянии $|0\rangle$. Имеем

$$U_1 = Q_2^c(Q_{13}\otimes I) = \begin{pmatrix} \sqrt{1-2\delta} & 0 & 0 & 0 & \sqrt{2\delta} & 0 \\ 0 & \sqrt{1-2\delta} & 0 & 0 & 0 & \sqrt{2\delta} \\ 0 & 0 & \sqrt{1-2\delta} & \sqrt{2\delta} & 0 & 0 \\ 0 & 0 & \sqrt{2\delta} & -\sqrt{1-2\delta} & 0 & 0 \\ \sqrt{2\delta} & 0 & 0 & 0 & -\sqrt{1-2\delta} & 0 \\ 0 & \sqrt{2\delta} & 0 & 0 & 0 & -\sqrt{1-2\delta} \end{pmatrix}. \qquad (104)$$

Если применить указанное преобразование к состоянию $|10\rangle$, получится

$$U_1|10\rangle = \sqrt{1-2\delta}|10\rangle + \sqrt{2\delta}|30\rangle = \\ = \left(\sqrt{1-2\delta}|1\rangle + \sqrt{2\delta}|3\rangle\right)|0\rangle. \quad (105)$$

Для полной реализации U_{BE} понадобится еще один кубит анциллы. Имеем

$$U_2 = F_{12}F_{35}F_{26}(U_1 \otimes I)F_{26}F_{35}F_{12} = \quad (106)$$

$$= \begin{pmatrix} \tilde{\delta} & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{2\delta} & 0 & 0 & 0 & 0 \\ 0 & \tilde{\delta} & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{2\delta} & 0 & 0 & 0 \\ 0 & 0 & \tilde{\delta} & 0 & 0 & 0 & \sqrt{2\delta} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\delta} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{2\delta} \\ 0 & 0 & 0 & 0 & \tilde{\delta} & 0 & 0 & 0 & 0 & 0 & \sqrt{2\delta} & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\delta} & 0 & 0 & 0 & \sqrt{2\delta} & 0 & 0 \\ 0 & 0 & \sqrt{2\delta} & 0 & 0 & 0 & -\tilde{\delta} & 0 & 0 & 0 & 0 & 0 \\ \sqrt{2\delta} & 0 & 0 & 0 & 0 & 0 & 0 & -\tilde{\delta} & 0 & 0 & 0 & 0 \\ 0 & \sqrt{2\delta} & 0 & 0 & 0 & 0 & 0 & 0 & -\tilde{\delta} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{2\delta} & 0 & 0 & 0 & -\tilde{\delta} & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2\delta} & 0 & 0 & 0 & 0 & 0 & -\tilde{\delta} & 0 \\ 0 & 0 & 0 & \sqrt{2\delta} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\tilde{\delta} \end{pmatrix}, \quad (107)$$

где $\tilde{\delta} = \sqrt{1-2\delta}$. Как видно, преобразование U_2 приводит к следующему:

$$U_2|100\rangle = \sqrt{1-2\delta}\,|100\rangle + \sqrt{2\delta}|211\rangle, \\ U_2|200\rangle = \sqrt{1-2\delta}\,|200\rangle + \sqrt{2\delta}|310\rangle, \quad (108) \\ U_2|300\rangle = -\sqrt{1-2\delta}\,|300\rangle + \sqrt{2\delta}|101\rangle,$$

однако для выполнения (108) нужно сделать также «размазывание» по остальным контрольным состояниям и добавить параметр α. «Размазывание» по остальным кубитам выглядит как последовательность условных операторов Адамара (здесь потребовались также 3 условных изменения бита, чтобы сохранить коэффициент $\sqrt{1-2\delta}$ на главной диагонали):

$$U_3 = F_{16}F_{39}C_{39}^{\dagger}C_{512}^{\dagger}C_{16}U_2C_{16}C_{512}^{\dagger}C_{39}^{\dagger}F_{39} =$$

$$= \begin{pmatrix} \tilde{\delta} & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{\delta} & 0 & \sqrt{\delta} & 0 & 0 \\ 0 & \tilde{\delta} & \sqrt{\delta} & 0 & 0 & 0 & 0 & 0 & \sqrt{\delta} & 0 & 0 & 0 \\ 0 & \sqrt{\delta} & -\tilde{\delta} & 0 & 0 & 0 & \sqrt{\delta} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\delta} & \sqrt{\delta} & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{\delta} \\ 0 & 0 & 0 & -\sqrt{\delta} & \tilde{\delta} & 0 & 0 & 0 & 0 & 0 & \sqrt{\delta} & 0 \\ 0 & 0 & 0 & 0 & 0 & -\tilde{\delta} & 0 & -\sqrt{\delta} & 0 & \sqrt{\delta} & 0 & 0 \\ 0 & 0 & -\sqrt{\delta} & 0 & 0 & 0 & -\tilde{\delta} & 0 & \sqrt{\delta} & 0 & 0 & 0 \\ \sqrt{\delta} & 0 & 0 & 0 & 0 & \sqrt{\delta} & 0 & -\tilde{\delta} & 0 & 0 & 0 & 0 \\ 0 & -\sqrt{\delta} & 0 & 0 & 0 & 0 & \sqrt{\delta} & 0 & \tilde{\delta} & 0 & 0 & 0 \\ \sqrt{\delta} & 0 & 0 & 0 & 0 & -\sqrt{\delta} & 0 & 0 & 0 & -\tilde{\delta} & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{\delta} & 0 & 0 & 0 & 0 & 0 & -\tilde{\delta} & -\sqrt{\delta} \\ 0 & 0 & 0 & \sqrt{\delta} & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{\delta} & -\tilde{\delta} \end{pmatrix}.$$

Наконец, чтобы добиться получения соотношений (77), осталось добавить третий кубит к анцилле и применить к нему и контрольному кутриту условный поворот R:

$$U_E = (R)_{1,4}(U_3 \otimes I). \tag{109}$$

Для экономии места матрица данного преобразования (размера 24×24) приводиться не будет, однако несложно убедиться, что при исходном состоянии анциллы $|\overline{000}\rangle$ его действие будет иметь вид (77), где состояния Евы определяются формулами (79), (80).

3.3. Построение операций кутрит–кубит

Осталось показать, каким образом из перечисленных операторов можно построить двухуровневые операции, описанные выше. Начнем с операторов условного отрицания F_{ij}. В схемах присутствуют операторы F_{16}, F_{39}, F_{12}, F_{35}, F_{26}. Заметим, что их можно получить следующим образом:

$$F_{16} = F_{12}F_{26}F_{12}, \tag{110}$$

$$F_{39} = F_{19}F_{13}F_{19}, \tag{111}$$

$$F_{35} = F_{13}F_{15}F_{13}. \tag{112}$$

В то же время

$$F_{12} = F^{(2)}F_{34}F^{(2)}, \tag{113}$$

$$F_{26} = F^{(2)}F_{48}F^{(2)}, \tag{114}$$

$$F_{19} = F^{(3)}F^{(2)}F_{12}^{(1)}F_{48}F_{12}^{(1)}F^{(2)}F^{(3)}, \tag{115}$$

$$F_{13} = F^{(3)}F_{24}F^{(3)}, \tag{116}$$

$$F_{15} = F^{(3)}F^{(2)}F_{48}F^{(2)}F^{(3)}, \tag{117}$$

где $F^{(2)}$ — оператор F, действующий на второй базисный вектор кубита, $F_{12}^{(1)}$ — оператор F_{12}, действующий на первый базисный вектор кутрита и т. д.

В результате оказывается, что достаточно реализовать только три оператора: F_{24}, F_{34} и F_{48}, остальные же можно получить их комбинациями между собой и с однокубитными преобразованиями. Схемы для этих трех операторов приведены на рис. 13.

Аналогичные рассуждения можно использовать и для построения остальных двухкубитных поворотов. Оказывается достаточным один поворот, а именно C_{48}^{+}. Действительно, можно видеть, что

$$C_{16}^{+} = F_{12}C_{26}^{+}F_{12}, \tag{118}$$

$$C_{26}^{+} = F^{(2)}C_{48}^{+}F^{(2)} \tag{119}$$

и т. д.

Квантовая схема верхнего уровня для оптимального подслушивания приведена на рис. 13 (верхняя часть). Ниже на рис. 14 приведены квантовые схемы более низких по уровню блоков (F_{48}, F_{34}, F_{24}, C_{48}^{+}). Остальные блоки получаются с учетом формул (110)–(119) и из-за экономии места не приводятся.

3.4. Преобразование состояний к физическому (временно́му) базису

Квантовая схема для фазово-временно́го кодирования (рис. 13) получена в базисе состояний, локализованных во временных окнах $|1\rangle$, $|2\rangle$, $|3\rangle$. Состояния же поступают к Еве в вычислительном базисе (75), (76) по одной оптоволоконной линии квантового канала связи. Для манипуляции этими состояниями при помощи квантовой схемы рис. 13 необходимо развести их на три разных пространственных канала. Физическая реализация схемы приведена на рис. 14. Кратко поясним работу схемы.

На вход поступают состояния $|0,1_L^{+}\rangle = (|1\rangle \pm |2\rangle)/\sqrt{2}$ (соответственно в сопряженном «левом» базисе $|0,1_L^{\times}\rangle = (|1\rangle \pm i|2\rangle)/\sqrt{2}$). Состояния в «правом» базисе имеют аналогичный вид $|0,1_R^{+}\rangle = (|2\rangle \pm |3\rangle)/\sqrt{2}$ (соответственно в сопряженном «правом» базисе $|0,1_R^{\times}\rangle = (|2\rangle \pm i|3\rangle)/\sqrt{2}$).

Преобразования для состояний в прямом левом и правом базисах проводятся аналогично рассмотренному ранее преобразованию состояний для протокола BB84. Единственное отличие составляет оператор фазовой модуляции. Приведем их явный вид (см. рис. 14). Имеем

$$U(\pi_1) = \begin{pmatrix} |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| & 0 \\ 0 & e^{i\pi}|1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| \end{pmatrix}, \tag{120}$$

$$U(\pi_3) = \begin{pmatrix} |1\rangle\langle 1| + |2\rangle\langle 2| + e^{i\pi}|3\rangle\langle 3| & 0 \\ 0 & |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| \end{pmatrix}, \tag{121}$$

$$U(\pi_2) = \begin{pmatrix} |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| & 0 \\ 0 & |1\rangle\langle 1| + e^{i\pi}|2\rangle\langle 2| + |3\rangle\langle 3| \end{pmatrix}. \tag{122}$$

Наконец, осуществляется приведение состояний по всем каналам к одному временно́му окну для получения интерференции, аналогично тому как это происходило для протокола BB84. Формально сдвиг состояния на k позиций вправо описывается оператором

$$U(\to k) = \left(\begin{array}{cc} \sum\limits_{i=-\infty}^{\infty} |i+k\rangle\langle i| & 0 \\ 0 & \sum\limits_{i=-\infty}^{\infty} |i+k\rangle\langle i| \end{array} \right). \quad (123)$$

Поскольку актуальными являются только три соседних временны́х окна, то в суммах (118) присутствуют только три слагаемых.

3.5. Физическая реализация элементарных вентилей

Приведем физическую реализацию квантовых вентилей, которые еще не встречались в предыдущих разделах для протокола BB84.

Оператор P реализуется при помощи фазового модулятора в нижнем оптоволокне, сдвигающем относительную фазу между состояниями в верхнем и нижнем каналах.

Оператор A выполняется при помощи асимметричного светоделителя и фазового модулятора в нижнем канале.

Оператор C реализуется включением двух фазовых модуляторов в верхнем и нижнем каналах, сдвигающих относительную фазу соответственно на $-\pi/4$ и $\pi/4$.

Способ реализации операторов CN^2 и N_{23} ясен из рис. 15 и осуществляется при помощи ячейки Керра, аналогичной той, которая представлена на рис. 8.

Действие оператора F на произвольное однокубитное состояние в физическом временно́м базисе сводится к перестановке каналов (рис. 15)[9)]

$$F|\psi\rangle = \left(\begin{array}{cc} 0 & I \\ I & 0 \end{array} \right) \left(\begin{array}{c} \alpha|2\rangle \\ \beta|2\rangle \end{array} \right) = \left(\begin{array}{c} \beta|2\rangle \\ \alpha|2\rangle \end{array} \right). \quad (124)$$

И, наконец, последний оператор условного сдвига фазы P_1^+ реализуется при помощи ячейки Керра.

Введем операторы рождения однофотонных пакетов в верхнем $|0\rangle$ и нижнем $|1\rangle$ каналах для состояний Боба a_{2B}^+ и Евы a_{1E}^+.

Введем гамильтониан, описывающий кубическую нелинейность $\mathcal{H} = \chi^{(3)} n_{2B} n_{1E}$ (n_{2B}, n_{1E} — операторы числа пакетов фотонов в верхнем и нижнем каналах, $n_{2B} = a_{2B}^+ a_{2B}$, $n_{1E} = a_{1E}^+ a_{1E}$), L — длина кристалла.

[9)] Напомним, что состояния в верхней и нижней оптоволоконных линиях приведены к общему временно́му окну, например, 2. Выбор окна не существен. Можно сделать приведение к любому общему временно́му окну.

Действие оператора $U_{P_1^+} = e^{-iL\mathcal{H}}$ на состояние $|21\rangle$ дает $U_{P_1^+} = e^{-iL\mathcal{H}}$. Если параметры гамильтониана выбраны такими, что набег фазы $L\chi^{(3)} = \pi/4$, то преобразование состояний имеет вид

$$U_{P_1^+}|2\rangle_B \otimes |1\rangle_E = e^{i\pi/4}|2\rangle_B \otimes |1\rangle_E. \quad (125)$$

На остальные состояния оператор действует как единичный. Реализация операторов приведена на рис. 15.

3.6. Обратное преобразование модифицированных состояний Боба

Цель данного преобразования состоит в том, чтобы любое входное запутанное состояние Евы и Боба

$$|\Psi\rangle_{BE} = \alpha|1\rangle \otimes |\psi\rangle + \beta|1\rangle \otimes |\varphi\rangle + \gamma|1\rangle \otimes |\theta\rangle,$$

присутствующее в трех пространственных каналах (оптоволокнах) свести в одну оптоволоконную линию, осуществляя при этом только локальные преобразования над степенями свободы Боба. Работа схемы ясна из рис. 16.

Перед входом в схему состояния в трех разных каналах присутствовали в одном и том же временно́м окне, например, 1. Для передачи их Бобу осуществляется сдвиг по времени в соответствующих каналах с дальнейшим «гашением» — деструктивной интерференцией по двум выходам и конструктивной интерференцией по третьему выходу. В результате к Бобу направляется модифицированное состояние. На двух оставшихся выходах присутствует лишь вакуумное состояние $|vac\rangle$.

3.7. Преобразование состояний подслушивателя перед измерением для протокола с фазово-временны́м кодированием

Любое измерение в квантовой механике описывается разложением единицы, которое для «левого» (L) прямого базиса, имеет вид

$$I = |\overline{0}_L^+\rangle\langle\overline{0}_L^+| + |\overline{1}_L^+\rangle\langle\overline{1}_L^+| + |3\rangle\langle 3|. \quad (126)$$

Неформально разложение единицы означает следующее. Каждому элементарному событию сопоставляется положительный эрмитов оператор (в данном случае проектор), которые в сумме дают единичный оператор. Последний отражает тот факт, что сумма вероятностей по всем элементарным событиям дает единицу. В нашем случае элементарными событиями являются регистрация либо 0, либо 1, либо отсчет в контрольном временно́м окне 3.

Удобно для подсчета вероятностей исходов у Боба представить первые два уравнения (77) в несколько ином эквивалентном виде:

$$|\Psi^{0^+L}\rangle = U_E(|\overline{0}_L^+\rangle \otimes |A\rangle) = |\overline{0}_L^+\rangle \otimes |\varphi_1^{0La}\rangle + |\overline{1}_L^+\rangle \otimes |\varphi_2^{0La}\rangle + |3\rangle \otimes \frac{|\psi_3^1\rangle + |\psi_3^2\rangle}{\sqrt{2}}, \quad (127)$$

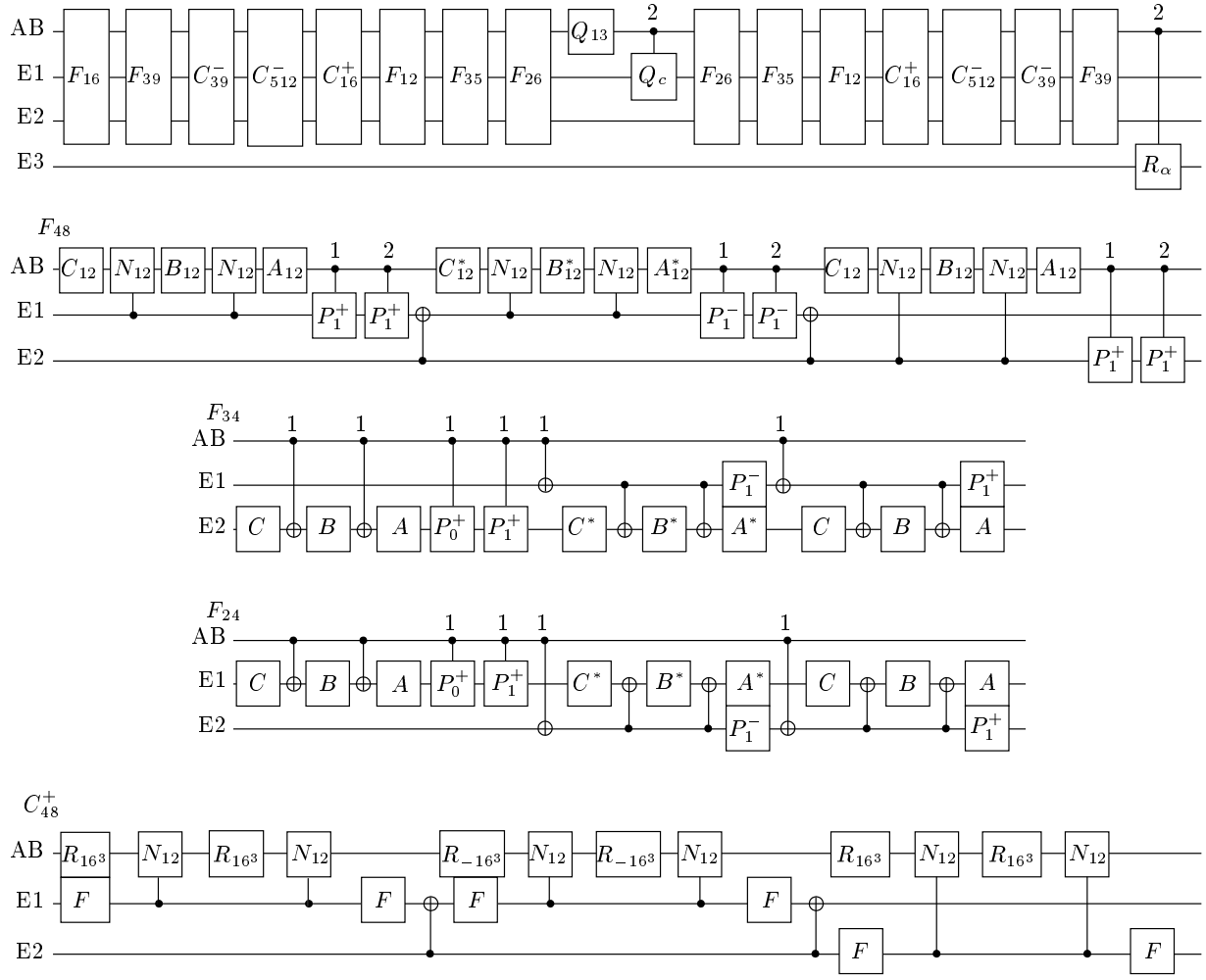

Рис. 13. Квантовая схема для оптимального подслушивания протокола с фазово-временны́м кодированием. Показана схема верхнего уровня с расшифровкой вентилей следующего более нижнего уровня. Остальные вентили получаются аналогично с учетом формул (110)–(119)

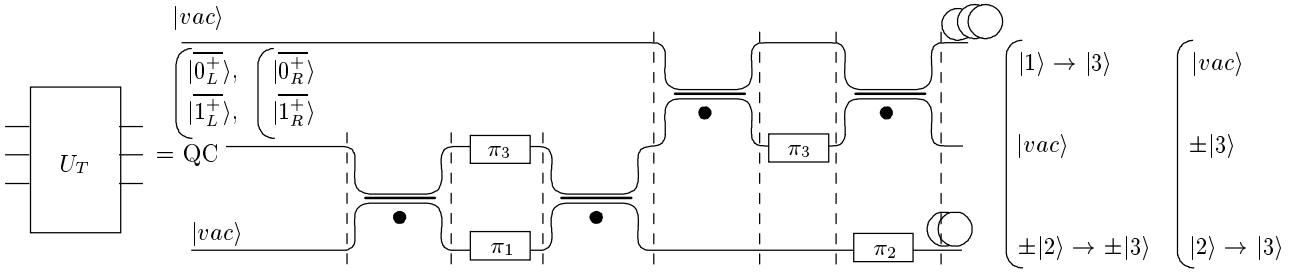

Рис. 14. Физическая реализация схемы преобразования квантовых состояний из одной волоконной линии на три оптоволоконных линии

$$|\Psi^{1^+L}\rangle = U_E(|\overline{1}_L^+\rangle \otimes |A\rangle) = |\overline{0}_L^+\rangle \otimes |\varphi_1^{1La}\rangle + \\ + |\overline{1}_L^+\rangle \otimes |\varphi_2^{1La}\rangle + |3\rangle \otimes \frac{|\psi_3^1\rangle - |\psi_3^2\rangle}{\sqrt{2}}. \quad (128)$$

Вероятность правильного исхода у Боба в случае, когда Алиса посылала 0 в прямом базисе L, равна

$$\Pr(0_B|0_A) = \mathrm{Tr}_{BE}\{|\Psi^{0^+L}\rangle\langle\Psi^{0^+L}||\overline{0}_L^+\rangle\langle\overline{0}_L^+|\} = \\ = (1-\delta)(1-Q), \quad (129)$$

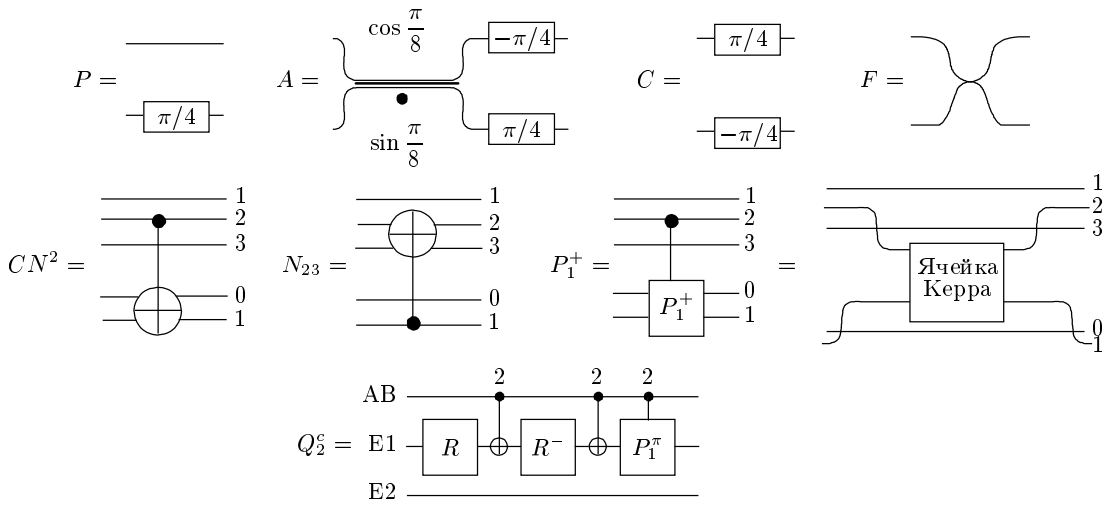

Рис. 15. Физическая реализация элементарных квантовых вентилей для схемы рис. 13

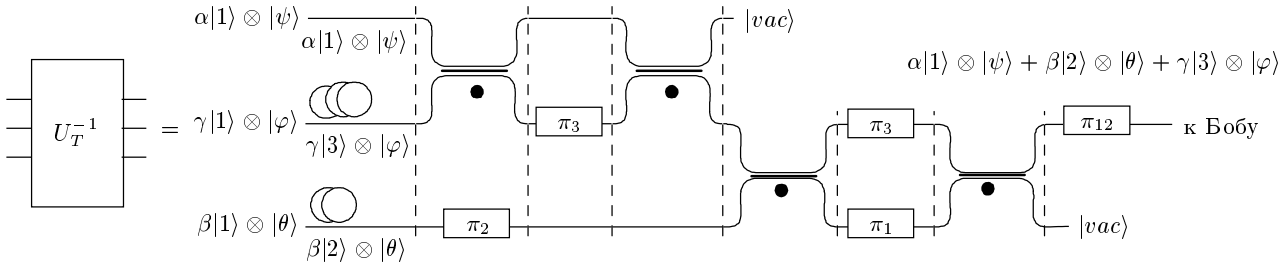

Рис. 16. Физическая реализация схемы преобразования квантовых состояний из трех волоконных линий в одну линию квантового канала связи

соответственно, вероятность неправильного исхода у Боба есть

$$\Pr(1_B|0_A) = \mathrm{Tr}_{BE}\{|\Psi^{0^+L}\rangle\langle\Psi^{0^+L}||\overline{1}_L^+\rangle\langle\overline{1}_L^+|\} = \\ = (1-\delta)Q. \quad (130)$$

Аналогичные выражения имеют место, если Алиса посылала 1. Кроме того, возможен отсчет в контрольном временно́м окне 3 с вероятностью

$$\Pr(3|0_A) = \mathrm{Tr}_{BE}\{|\Psi^{0^+L}\rangle\langle\Psi^{0^+L}||3\rangle\langle 3|\} = \delta. \quad (131)$$

Таким образом, вероятность ошибки на приемной стороне Боба, с учетом нормировки только на вероятность отсчетов в информационных временны́х окнах (0 и 1), имеет вид

$$\frac{\Pr(1_B|0_A)}{\Pr(0_B|0_A)+\Pr(1_B|0_A)} = Q. \quad (132)$$

После согласования базисов Ева стоит перед задачей о различении нескольких неортогональных состояний. Рассмотрим для определенности использование Бобом базиса L. Тогда при посылке состояния 0 возможны два варианта. В случае получения Бобом правильного результата в распоряжении Евы окажется состояние

$$\sigma_{E,OK}^{0L} = \mathrm{Tr}_B\{|\Psi^{0^+L}\rangle\langle\Psi^{0^+L}||\overline{0}_L^+\rangle\langle\overline{0}_L^+|\} = \\ = |\varphi_1^{0L}\rangle\langle\varphi_1^{0L}|, \quad (133)$$

а в случае ошибочного исхода на стороне Боба Ева получит состояние

$$\sigma_{E,Err}^{0L} = \mathrm{Tr}_B\{|\Psi^{0^+L}\rangle\langle\Psi^{0^+L}||\overline{1}_L^+\rangle\langle\overline{1}_L^+|\} = \\ = |\varphi_2^{0L}\rangle\langle\varphi_2^{0L}|. \quad (134)$$

Аналогично для посылаемого состояния 1: состояния Евы будут соответственно равны

$$\sigma_{E,OK}^{1L} = \mathrm{Tr}_B\{|\Psi^{1^+L}\rangle\langle\Psi^{1^+L}||\overline{1}_L^+\rangle\langle\overline{1}_L^+|\} = \\ = |\varphi_1^{1L}\rangle\langle\varphi_1^{1L}|, \quad (135)$$

$$\sigma_{E,Err}^{1L} = \mathrm{Tr}_B\{|\Psi^{1^+L}\rangle\langle\Psi^{1^+L}||\overline{0}_L^+\rangle\langle\overline{0}_L^+|\} = \\ = |\varphi_2^{1L}\rangle\langle\varphi_2^{1L}|. \quad (136)$$

Таким образом, при использовании базиса L Ева стоит перед задачей различения четырех состояний. Заметим, что состояния $|\varphi_1^i\rangle\langle\varphi_1^i|$ и $|\varphi_2^j\rangle\langle\varphi_2^j|$ коммутируют. Это несколько упрощает задачу Евы, так как операторы измерения теперь можно строить по отдельности для верного и ошибочного исходов.

Найдем оптимальные операторы измерения для каждого случая. Сначала выпишем все приведенные состояния в вычислительном базисе:

$$
\begin{aligned}
|\varphi_1^{0L}\rangle &= \frac{1}{2}(|\psi_1^1\rangle + |\psi_2^1\rangle + |\psi_1^2\rangle + |\psi_2^2\rangle),\\
|\varphi_1^{1L}\rangle &= \frac{1}{2}(|\psi_1^1\rangle - |\psi_2^1\rangle - |\psi_1^2\rangle + |\psi_2^2\rangle),\\
|\varphi_2^{0L}\rangle &= \frac{1}{2}(|\psi_1^1\rangle - |\psi_2^1\rangle + |\psi_1^2\rangle - |\psi_2^2\rangle),\\
|\varphi_2^{1L}\rangle &= \frac{1}{2}(|\psi_1^1\rangle + |\psi_2^1\rangle - |\psi_1^2\rangle - |\psi_2^2\rangle),\\
|\psi_1^1\rangle &= \sqrt{1-2\delta}|\overline{000}\rangle,\\
|\psi_2^1\rangle &= \sqrt{\delta}(\cos\alpha|\overline{110}\rangle - \sin\alpha|\overline{111}\rangle),\\
|\psi_1^2\rangle &= \sqrt{\delta}|\overline{110}\rangle,\\
|\psi_2^2\rangle &= \sqrt{1-2\delta}(\cos\alpha|\overline{000}\rangle - \sin\alpha|\overline{001}\rangle).
\end{aligned}
\tag{137}
$$

Векторы состояния Евы в вычислительном базисе будут выглядеть следующим образом:

$$
\begin{aligned}
|\varphi_1^{0L}\rangle = \frac{\sqrt{1-2\delta}}{2}\left[(1+\cos\alpha)|\overline{000}\rangle - \sin\alpha|\overline{001}\rangle\right] +\\
+ \frac{\sqrt{\delta}}{2}\left[(1+\cos\alpha)|\overline{110}\rangle - \sin\alpha|\overline{111}\rangle\right],
\end{aligned}
$$

$$
\begin{aligned}
|\varphi_1^{1L}\rangle = \frac{\sqrt{1-2\delta}}{2}\left[(1+\cos\alpha)|\overline{000}\rangle - \sin\alpha|\overline{001}\rangle\right] -\\
- \frac{\sqrt{\delta}}{2}\left[(1+\cos\alpha)|\overline{110}\rangle - \sin\alpha|\overline{111}\rangle\right],
\end{aligned}
$$

$$
\begin{aligned}
|\varphi_2^{0L}\rangle = \frac{\sqrt{1-2\delta}}{2}\left[(1-\cos\alpha)|\overline{000}\rangle + \sin\alpha|\overline{001}\rangle\right] +\\
+ \frac{\sqrt{\delta}}{2}\left[(1-\cos\alpha)|\overline{110}\rangle + \sin\alpha|\overline{111}\rangle\right],
\end{aligned}
$$

$$
\begin{aligned}
|\varphi_2^{1L}\rangle = \frac{\sqrt{1-2\delta}}{2}\left[(1-\cos\alpha)|\overline{000}\rangle + \sin\alpha|\overline{001}\rangle\right] -\\
- \frac{\sqrt{\delta}}{2}\left[(1-\cos\alpha)|\overline{110}\rangle + \sin\alpha|\overline{111}\rangle\right].
\end{aligned}
$$

Рассмотрим по отдельности измерения Евы для случаев правильного и неправильного исходов у Боба. Оператор Грама системы $|\varphi_1^{0L}\rangle$ и $|\varphi_1^{1L}\rangle$ равен

$$
G = |\varphi_1^{0L}\rangle\langle\varphi_1^{0L}| + |\varphi_1^{1L}\rangle\langle\varphi_1^{1L}|.
$$

Матрица этого оператора в вычислительном базисе имеет вид

$$
G = \begin{pmatrix}
\frac{\tilde\delta}{2}(1+\cos\alpha)^2 & -\frac{\tilde\delta}{2}\sin\alpha(1+\cos\alpha) & 0 & 0\\
-\frac{\tilde\delta}{2}\sin\alpha(1+\cos\alpha) & \frac{\tilde\delta}{2}\sin^2\alpha & 0 & 0\\
0 & 0 & \frac{\sqrt{\delta}}{2}(1+\cos\alpha)^2 & -\frac{\sqrt{\delta}}{2}\sin\alpha(1+\cos\alpha)\\
0 & 0 & -\frac{\sqrt{\delta}}{2}\sin\alpha(1+\cos\alpha) & \frac{\sqrt{\delta}}{2}\sin^2\alpha
\end{pmatrix}.
$$

Его собственные значения равны $(1-2\delta)(1+\cos\alpha)$ и $\delta(1+\cos\alpha)$, а собственные векторы — соответственно $\cos(\alpha/2)|\overline{000}\rangle - \sin(\alpha/2)|\overline{001}\rangle$ и $\cos(\alpha/2)|\overline{110}\rangle - -\sin(\alpha/2)|\overline{111}\rangle$. Тогда оператор $G^{-1/2}$ можно записать в вычислительном базисе следующим образом:

$$
\begin{aligned}
G^{-1/2} = \frac{1}{\sqrt{2}\sqrt{1-2\delta}c}\begin{pmatrix} c^2 & -cs & 0 & 0\\ -cs & s^2 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 \end{pmatrix} +\\
+ \frac{1}{\sqrt{2\delta}c}\begin{pmatrix} 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & c^2 & -cs\\ 0 & 0 & -cs & s^2 \end{pmatrix},
\end{aligned}
$$

где $c = \cos(\alpha/2)$, $s = \sin(\alpha/2)$.

Действуя им на состояния $|\varphi_1^{0L}\rangle$ и $|\varphi_1^{1L}\rangle$, получаем векторы

$$
\begin{aligned}
|f_1^{0L}\rangle = G^{-1/2}|\varphi_1^{0L}\rangle = \frac{1}{\sqrt{2}}\Big(\cos\frac{\alpha}{2}|\overline{000}\rangle -\\
- \sin\frac{\alpha}{2}|\overline{001}\rangle + \cos\frac{\alpha}{2}|\overline{110}\rangle - \sin\frac{\alpha}{2}|\overline{111}\rangle\Big),\\
|f_1^{1L}\rangle = G^{-1/2}|\varphi_1^{1L}\rangle = \frac{1}{\sqrt{2}}\Big(\cos\frac{\alpha}{2}|\overline{000}\rangle -\\
- \sin\frac{\alpha}{2}|\overline{001}\rangle - \cos\frac{\alpha}{2}|\overline{110}\rangle + \sin\frac{\alpha}{2}|\overline{111}\rangle\Big),
\end{aligned}
\tag{138}
$$

и соответственно операторы оптимального измерения равны $|f_1^{0L}\rangle\langle f_1^{0L}|$ и $|f_1^{1L}\rangle\langle f_1^{1L}|$.

Аналогичными вычислениями получаются операторы оптимального измерения при получении Бобом ошибочного результата. Они равны соответственно $|f_2^{0L}\rangle\langle f_2^{0L}|$ и $|f_2^{1L}\rangle\langle f_2^{1L}|$, где

$$|f_2^{0L}\rangle = G^{-1/2}|\varphi_2^{0L}\rangle = \frac{1}{\sqrt{2}}\left(\sin\frac{\alpha}{2}|\overline{000}\rangle + \right.$$
$$\left. + \cos\frac{\alpha}{2}|\overline{001}\rangle + \sin\frac{\alpha}{2}|\overline{110}\rangle + \cos\frac{\alpha}{2}|\overline{111}\rangle\right),$$
$$|f_2^{1L}\rangle = G^{-1/2}|\varphi_2^{1L}\rangle = \frac{1}{\sqrt{2}}\left(\sin\frac{\alpha}{2}|\overline{000}\rangle + \right. \quad (139)$$
$$\left. + \cos\frac{\alpha}{2}|\overline{001}\rangle - \sin\frac{\alpha}{2}|\overline{110}\rangle - \cos\frac{\alpha}{2}|\overline{111}\rangle\right).$$

Для подсчета вероятностей необходимо перейти к нормированным состояниям. Введем нормированные состояния

$$|\overline{\varphi}_1^{0L}\rangle = \frac{|\varphi_1^{0L}\rangle}{\sqrt{1-Q}\sqrt{1-\delta}},$$
$$|\overline{\varphi}_1^{1L}\rangle = \frac{|\varphi_1^{1L}\rangle}{\sqrt{1-Q}\sqrt{1-\delta}},$$
$$|\overline{\varphi}_2^{0L}\rangle = \frac{|\varphi_2^{0L}\rangle}{\sqrt{1-Q}\sqrt{1-\delta}}, \quad (140)$$
$$|\overline{\varphi}_2^{1L}\rangle = \frac{|\varphi_2^{1L}\rangle}{\sqrt{1-Q}\sqrt{1-\delta}},$$

здесь принято во внимание (см. формулу (79)), что

$$\cos^2\frac{\alpha}{2} = 1 - Q. \quad (141)$$

Такая нормировка является следствием того, что после вторжения Евы Боб может получить результат не только в информационных временны́х окнах (1 и 2 в базисе L), но также и в контрольном временно́м окне 3. Полная вероятность по всем временны́м окнам, естественно, равна 1. Но поскольку события, когда были отсчеты в контрольном временно́м окне отбрасываются Бобом через открытый канал, удобнее нормировать состояния Евы только на вероятность отсчетов в информационных окнах.

Таким образом, при условии того, что Боб получил правильный исход, соответствующая вероятность получить правильный исход у Евы равна (переходная вероятность того, что состояние, посланное Алисой есть 0 и Ева получит результат 0)

$$\mathrm{Pr}_E(0_E,0_B|0_A) = \mathrm{Tr}_E\{\overline{\sigma}_{E,OK}^{0L}|f_1^{0L}\rangle\langle f_1^{0L}|\} =$$
$$= \frac{\left(\sqrt{1-2\delta}+\sqrt{\delta}\right)^2}{2(1-\delta)}. \quad (142)$$

Соответственно, вероятность неправильного исхода у Евы при условии, что Боб получил правильный результат равна

$$\mathrm{Pr}_E(1_E,0_B|0_A) = \mathrm{Tr}_E\{\overline{\sigma}_{E,OK}^{0L}|f_1^{1L}\rangle\langle|f_1^{1L}|\} =$$
$$= \frac{\left(\sqrt{1-2\delta}-\sqrt{\delta}\right)^2}{2(1-\delta)}, \quad (143)$$

В случае ошибочного исхода у Боба Ева может получить правильный результат с вероятностью

$$\mathrm{Pr}_E(0_E,1_B|0_A) = \mathrm{Tr}_E\{\overline{\sigma}_{E,Err}^{0L}|f_2^{0L}\rangle\langle f_2^{0L}|\} =$$
$$= \frac{\left(\sqrt{1-2\delta}+\sqrt{\delta}\right)^2}{2(1-\delta)}, \quad (144)$$

соответственно, вероятность неправильного исхода у Евы при условии, что Боб также получил неправильный результат равна

$$\mathrm{Pr}_E(1_E,1_B|0_A) = \mathrm{Tr}_E\{\overline{\sigma}_{E,Err}^{0L}|f_2^{1L}\rangle\langle f_2^{1L}|\} =$$
$$= \frac{\left(\sqrt{1-2\delta}-\sqrt{\delta}\right)^2}{2(1-\delta)}. \quad (145)$$

Аналогично для случая, если Алиса посылала 1. После измерений Боба между ним и Алисой имеет место ситуация, которая описывается классическим бинарным каналом связи с вероятностью ошибки Q. После измерений Евы, ситуация между Алисой и Евой также описывается классическим бинарным каналом связи с вероятностью ошибки Q_E, которая определяется соотношениями (142)–(145):

$$Q_E = [\mathrm{Pr}_E(1_E,0_B|0_A) + \mathrm{Pr}_E(1_E,1_B|0_A)] \times$$
$$\times [\mathrm{Pr}_E(0_E,0_B|0_A) + \mathrm{Pr}_E(1_E,0_B|0_A) +$$
$$+ \mathrm{Pr}_E(0_E,1_B|0_A) + \mathrm{Pr}_E(1_E,1_B|0_A)]^{-1}. \quad (146)$$

Распределение секретных ключей возможно, если $Q < Q_E$ [5, 7, 11, 12]. Таким образом, критическая ошибка на приемной стороне, до которой возможно распределение секретных ключей, определяется с учетом выражений (129)–(132) и (142)–(146) из уравнения

$$Q = \frac{1}{2} - \frac{\sqrt{(1-2\delta)\delta}}{1-\delta}. \quad (147)$$

Зависимость критической ошибки от δ приведена на рис. 17. Параметр δ имеет смысл вероятности отсчетов в контрольном временно́м окне. Протокол квантового распределения ключей с фазово-временны́м кодированием является двухпараметрическим. Критическая ошибка зависит от вероятности отсчетов в контрольных временны́х окнах. Если нет отсчетов в контрольных временны́х окнах, то допустимая критическая ошибка достигает теоретического предела в 50 % (см. подробности в работах [11, 12]).

Квантовая схема, реализующая оптимальные индивидуальные измерения Евы, приведена на рис. 18[10)].

[10)] Теоретически можно построить коллективные измерения Евы, однако последние находятся далеко за пределами современных технических возможностей.

Наиболее доступное на практике измерение для Евы — это подсчет амплитуды в физическом базисе (т. е. ортогональное разложение единицы в нем), поэтому состояния $|\varphi_j^i\rangle$ требуется отобразить таким образом, чтобы операторы оптимального измерения $|f_j^i\rangle$ перешли в диагональные операторы. Из простого соотношения

$$\mathrm{Tr}(M \cdot UXU^\dagger) = \mathrm{Tr}(U^\dagger MU \cdot X)$$

следует, что для этого перехода можно применить преобразование, сопряженное к отображению, переводящему базисные векторы в векторы измерения $|f_j^i\rangle$. Построим это преобразование. Матрица преобразования от вычислительного базиса к измерительному базису,

$$\left.\begin{array}{l} |\overline{000}\rangle \\ |\overline{001}\rangle \\ |\overline{110}\rangle \\ |\overline{111}\rangle \end{array}\right\} \to \left\{\begin{array}{l} |f_1^{0L}\rangle \\ |f_2^{0L}\rangle \\ |f_1^{1L}\rangle \\ |f_2^{1L}\rangle \end{array}\right\},$$

в вычислительном базисе будет иметь следующий вид:

$$U = (\mathrm{CNOT}_{12} \cdot (H_1 \otimes I_2) \cdot \mathrm{CNOT}_{12}) \otimes R_3 =$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} & 0 & 0 & 0 & 0 & \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} \\ -\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} & 0 & 0 & 0 & 0 & -\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \\ 0 & 0 & \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} & 0 & 0 \\ 0 & 0 & -\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} & -\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} & 0 & 0 \\ 0 & 0 & \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} & -\cos\frac{\alpha}{2} & -\sin\frac{\alpha}{2} & 0 & 0 \\ 0 & 0 & -\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} & -\cos\frac{\alpha}{2} & 0 & 0 \\ \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} & 0 & 0 & 0 & 0 & -\cos\frac{\alpha}{2} & -\sin\frac{\alpha}{2} \\ -\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} & 0 & 0 & 0 & 0 & \sin\frac{\alpha}{2} & -\cos\frac{\alpha}{2} \end{pmatrix}, \tag{148}$$

оператор в (148) записан в базисе векторов, упорядоченных лексикографически. Нас интересуют позиции, соответствующие базисным векторам $|000\rangle$, $|001\rangle$, $|110\rangle$ и $|111\rangle$ — это два первых и два последних столбца матрицы в (148). Нетрудно видеть, что преобразование действует на эти векторы нужным образом.

Неформально, оператор (148) и соответствующая оптическая схема осуществляют преобразование входных состояний Евы в базисе $|000\rangle$, $|001\rangle$, $|110\rangle$, $|111\rangle$ к тем же самым векторам, но записанным в базисе $|f_1^{0L}\rangle$, $|f_2^{0L}\rangle$, $|f_1^{1L}\rangle$, $|f_2^{1L}\rangle$.

Имеем с учетом формул (138)–(140)

$$\begin{aligned} |\overline{\varphi}_1^{0L}\rangle &= \frac{1}{\sqrt{1-\delta}} \left[\left(\sqrt{1-2\delta} + \sqrt{\delta} \right) |f_1^{0L}\rangle + \right. \\ &\quad \left. + \left(\sqrt{1-2\delta} - \sqrt{\delta} \right) |f_1^{1L}\rangle \right], \\ |\overline{\varphi}_1^{1L}\rangle &= \frac{1}{\sqrt{1-\delta}} \left[\left(\sqrt{1-2\delta} - \sqrt{\delta} \right) |f_1^{0L}\rangle + \right. \\ &\quad \left. + \left(\sqrt{1-2\delta} + \sqrt{\delta} \right) |f_1^{1L}\rangle \right], \end{aligned}$$

$$\begin{aligned} |\overline{\varphi}_2^{0L}\rangle &= \frac{1}{\sqrt{1-\delta}} \left[\left(\sqrt{1-2\delta} - \sqrt{\delta} \right) |f_2^{0L}\rangle + \right. \\ &\quad \left. + \left(\sqrt{1-2\delta} + \sqrt{\delta} \right) |f_2^{1L}\rangle \right], \\ |\overline{\varphi}_2^{1L}\rangle &= \frac{1}{\sqrt{1-\delta}} \left[\left(\sqrt{1-2\delta} - \sqrt{\delta} \right) |f_2^{0L}\rangle + \right. \\ &\quad \left. + \left(\sqrt{1-2\delta} + \sqrt{\delta} \right) |f_2^{1L}\rangle \right]. \end{aligned} \tag{149}$$

Фактически применение оператора (148) к входным состояниям означает, что амплитуды состояний в соответствующих каналах являются коэффициентами разложения в соотношениях (149). Поэтому вероятность срабатывания детекторов в этих каналах как раз и будет равна квадрату модуля соответствующих коэффициентов разложения. Напомним, что для Евы состояния в вычислительном базисе совпадают с состояниями, локализованными во временны́х окнах, которые приведены для каждого кубита (в верхнем и нижним каналах) к одному временно́му окну.

Поясним еще раз данную ситуацию при измерении. Для этого удобно ввести новые обозначения. Снабдим состояния на выходе квантовой схемы индексами «out». Состояние $|f_1^{0L}\rangle$ в исходном базисе имеет вид

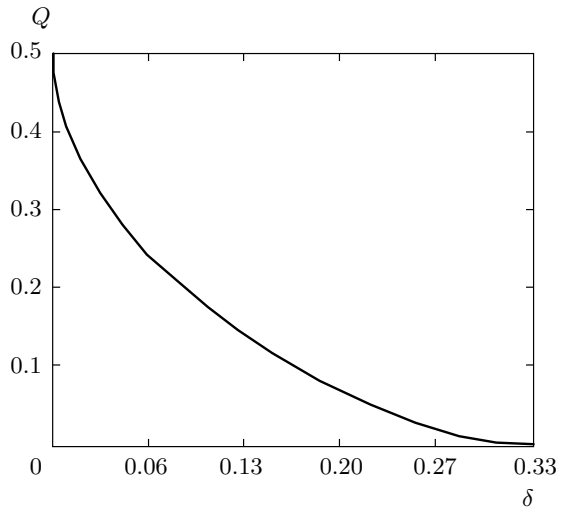

Рис. 17. Критическая ошибка как функция вероятности отсчетов в контрольных временны́х окнах

$$|f_1^{0L}\rangle = c_\alpha(|000\rangle_{in} + |110\rangle_{in}) - s_\alpha(|001\rangle_{in} + |111\rangle_{in}) =$$
$$= (|00\rangle_{in} + |11\rangle_{in}) \otimes (c_\alpha|0\rangle_{in} - s_\alpha|1\rangle_{in}).$$

На выходе квантовой схемы будут состояния (сам вектор состояния $|f_1^{0L}\rangle$ не зависит от выбора базиса)

$$|f_1^{0L}\rangle = |00\rangle_{out} \otimes |0\rangle_{out},$$

порядок новых базисных состояний отвечает номеру выходного канала, т. е. состояние $|00\rangle_{out} \otimes |0\rangle_{out} \otimes |0\rangle_{out}$ отвечает присутствию состояний в верхних каналах для кубитов 1, 2 и 3 (преобразования кубита 3 не затрагивают состояний двух первых). Фактически проекция на состояние $|f_1^{0L}\rangle$ означает реализацию проекции на двухфотонную ЭПР-пару из первых двух кубитов $|00\rangle_{in} + |11\rangle_{in}$ и на состояние кубита 3, который не зависит от первых двух (см. рис. 18). Схема переводит состояние ЭПР-пары для первых двух фотонов в состояние $|00\rangle_{out}$ и третьего независимого от них фотона в состояние $|0\rangle_{out}$. Состояние первых двух кубитов уже можно регистрировать двумя детекторами по схеме совпадения. Срабатывание двух детекторов в первых двух верхних каналах как раз и реализует проективное измерение на ЭПР-пару. Третий детектор является индикатором. Срабатывание третьего детектора в верхнем канале указывает, на какое состояние произошло проектирование в первых двух каналах. Если сработал верхний детектор в третьем канале, то входным состоянием было либо $|\varphi_1^{0L}\rangle$, либо $|\varphi_1^{1L}\rangle$. Отсчет в нижнем детекторе в третьем канале является указанием для Евы на то, какое состояние было входным, $|\varphi_2^{0L}\rangle$ или $|\varphi_2^{1L}\rangle$. В этом случае выходное состояние третьего кубита будет $|1\rangle_{out}$. Состояние же первых двух, как и в предыдущем случае, будет случайным: либо $|00\rangle_{out}$, либо $|11\rangle_{out}$.

4. ЗАКЛЮЧЕНИЕ

В предыдущих разделах были построены квантовые схемы для оптимального подслушивания протоколов квантового распределения ключей BB84 [2] и протокола с фазово-временны́м кодированием [10–12]. Оптимального в том смысле, что при такой стратегии Ева получает максимум информации о передаваемых квантовых состояниях (ключе) при заданной наблюдаемой ошибке на приемной стороне.

В квантовой криптографии при анализе криптографической стойкости протоколов квантового распределения ключей консервативно считается, что подслушиватель не ограничен никакими техническими возможностями. Например, подслушиватель может иметь долговременную квантовую память и делать коллективные измерения сразу над целой последовательностью квантовых состояний. Оказывается, что даже в этом случае, при ошибке на приемной стороне меньше критической, возможна передача секретных ключей.

Предпочтение тому или иному протоколу отдается лишь по одному критерию — допустимой ошибке на приемной стороне, до которой гарантируется секретность передаваемых ключей. Технические сложности при реализации подслушивания через квантовый канал связи не принимаются во внимание.

В реальности ситуация несколько иная. Как было видно из предыдущего анализа, реализация атаки на протокол с фазово-временным кодированием [10–12] по сравнению с широко используемым протоколом BB84 [2] технически оказывается существенно более сложной. При этом данный протокол квантового распределения ключей обеспечивает наибольшую допустимую критическую ошибку при однофотонном источнике. При не строго однофотонном источнике и затухании в квантовом канале связи данный протокол обеспечивает максимальную дальность передачи ключей по сравнению с другими протоколами.

Основной проблемой при реализации квантовой схемы для подслушивания является квантовый вентиль CNOT. Остальные вентили выполняются при помощи стандартных оптоволоконных компонентов — светоделителей и фазовых модуляторов. Хотя нужно понимать, что реализация схемы, даже если бы в ней имелись только «простые» волоконные компоненты, требует обеспечения интерференции состояний из разных пространственных каналов схемы. При таком большом числе оптических элементов даже обеспечение интерференции нулевого порядка[11)] является крайне сложной задачей.

Для элемента CNOT невозможно использовать никакие вероятностные реализации, типа рассмотренных в работах [46–49], поскольку требуется запутывать состояния, полученные из разных источников. Единственная

[11)] Под интерференцией нулевого порядка понимается интерференция состояния, прошедшего по разным оптическим путям, самого с собой (см. разд. 2.3).

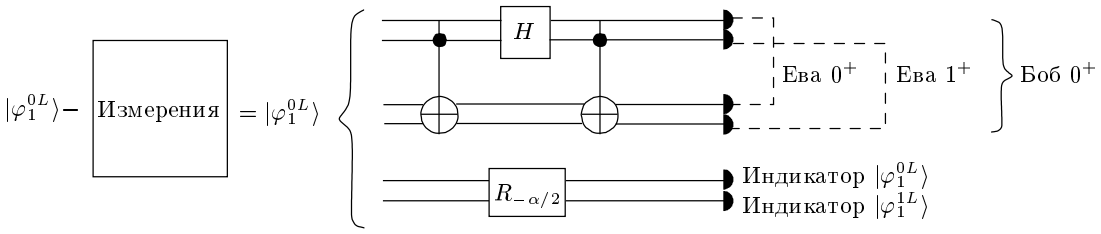

Рис. 18. Квантовая схема, реализующая оптимальные измерения подслушивателя

возможность на сегодняшний день — это использование ячейки Керра. Однако из-за крайне маленькой величины восприимчивости третьего порядка (типичные значения $10^{-18}\ m^2/W$) приходится использовать резонансные схемы типа описанных в работах [39–45]. В этом случае можно увеличить значение восприимчивости до величины $10^{-2}\ m^2/W$, чтобы обеспечить сдвиг фазы на π при разумных длинах кристалла. Но даже в этом случае, поскольку гамильтониан взаимодействия будет содержать кроме нелинейных членов третьего порядка линейные и квадратичные, вентиль CNOT не будет детерминистическим, т. е. не требуемое действие данного вентиля будет осуществляться не в каждой посылке.

Далее, здесь была построена квантовая схема для оптимальных индивидуальных измерений. В принципе можно построить квантовую схему, которая реализует коллективные измерения Евы над всей последовательностью переданных состояний [11, 12]. В этом случае при заданной наблюдаемой ошибке Ева может получить больше информации о передаваемом ключе, т. е. достигнуть фундаментальной границы Холево [9]. Однако такие измерения находятся далеко за пределами современных технологических возможностей.

Резюмируя, можно сказать следующее. Системы квантовой криптографии, секретность которых базируется не на технических ограничениях подслушивателя, а на фундаментальных запретах квантовой механики (фактически на соотношениях неопределенности Гайзенберга), обеспечивают секретность ключей при ошибке меньше некоторой критической и длине линии связи также не превышающей некоторой критической величины[12)]. При этом считается, что подслушиватель может реализовать любую стратегию, не ограничивая себя существующими на сегодняшний день технологиями, а легитимные пользователи используют только аппаратуру, которая имеется на сегодняшний день. Даже в таких неравных условиях квантовая криптография обеспечивает секретную передачу ключей.

В реальности технические возможности легитимных пользователей (Алисы и Боба) и подслушивателя (Евы) практически одинаковы, поэтому требования к системам могут быть смягчены. Пока наиболее реальной атакой остается атака прием–перепосыл. Для такой атаки допустимая критическая ошибка оказывается больше, чем допустимая ошибка с коллективными измерениями.

Более эффективными могут оказаться атаки, связанные не с прямым вторжением в квантовый канал связи, а с детектированием утечек информации по так называемым побочным каналам. Такими атаками являются атаки с активным зондированием состояния фазового модулятора на передающей и приемной сторонах, и детектирование обратного свечения лавинных фотодетекторов. Однако и с учетом этих каналов (см., например, [6]) системы квантовой криптографии обеспечивают секретность ключей.

Один из авторов (С. Н. М.) выражает благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку. Работа выполнена при частичной финансовой поддержке РФФИ (грант № 08-02-00559).

ЛИТЕРАТУРА

1. R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).
2. C. H. Bennett and G. Brassard, Proc. IEEE, Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India (1984), p. 175.
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, *Interferometric Quantum Key Distribution System*, April 26 (1994), Date of Patent, Patent Number 5, 307, 410.
4. W. K. Wooters and W. H. Zurek, Nature **299**, 802 (1982).
5. R. Renner, arXiv:quant-ph/0512258.
6. А. В. Корольков, К. Г. Катамадзе, С. П. Кулик, С. Н. Молотков, ЖЭТФ **137**, 637 (2010).
7. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, arXiv:quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).

[12)] При условии не строго однофотонного источника и затухания. При строго однофотонном источнике и наличии затухания в квантовом канале связи ограничений на длину линии связи для секретной передачи ключей не существует.

8. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).

9. А. С. Холево, *Введение в квантовую теорию информации*, сер. *Совр. матем. физ.*, вып. 5, МЦНМО, Москва (2002); УМН **53**, 193 (1998).

10. С. П. Кулик, С. Н. Молотков, А. П. Маккавеев, Письма в ЖЭТФ **85**, 354 (2007).

11. С. Н. Молотков, ЖЭТФ **133**, 5 (2009).

12. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009).

13. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, arXiv:quant-ph/0802.4155.

14. W. Mauerer, W. Helwig, and C. Silberhorn, arXiv:quant-ph/0712.0517.

15. T. Kim, I. Stork genannt Wersborg, F. N. C. Wong, and J. H. Shapiro, arXiv:quant-ph/0611235.

16. М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, Мир, Москва (2006) [M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2001)].

17. R. J. Hughes, G. L. Morgan, and C. G. Peterson, arXiv:quant-ph/9904038.

18. R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, Contemp. Phys. **36**, 149 (1995).

19. R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. M. Simmons, Proc. Advances in Cryptology — Crypto'96, Springer-Verlag, Berlin (1996), p. 329.

20. A. Muller, J. G. Rarity, P. R. Tapster et al., Electr. Lett. **23**, 634 (1993).

21. A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996).

22. C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).

23. P. D. Townsend, Nature **385**, 47 (1997).

24. P. D. Townsend, Electr. Lett. **30**, 809 (1994).

25. J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994).

26. A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995).

27. H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Electr. Lett. **33**, 586 (1997).

28. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).

29. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zhbinden, New J. Phys. **4**, 41.1 (2002).

30. D. S. Bethune and W. P. Risk, QEC'98 Digest of Postdeadline Papers, Vol. QPD12-2, May (1998).

31. D. S. Bethune and W. P. Risk, IEEE J. Quant. Elecron. **36**, 340 (2000).

32. D. S. Bethune, M. Navarro, and W. P. Risk, arXiv:quant-ph/0104089.

33. C. Elliott, D. Pearson, and G. Troxel, arXiv:quant-ph/ /0307049.

34. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, arXiv:quant-ph/0503058; C. Elliot, New J. Phys. **4**, 46.1 (2002).

35. Y. Nambu, T. Hatanaka, H. Yamazaki, and K. Nakamura, arXiv:quant-ph/0404015.

36. T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, arXiv:quant-ph/ /0603041.

37. Y. Nambu, K. Yoshino, and A. Tomita, arXiv:quant-ph/0403104.

38. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

39. S. Rebi, D. Vitali, C. Ottaviani, P. Tombesi, M. Artoni, F. Cataliotti, and R. Corbal, Phys. Rev. A **70**, 032317 (2004).

40. S. Glancy, J. M. LoSecco, and C. E. Tanner, arXiv:quant-ph/0009110.

41. Hiroshi Ajiki, Wang Yao, and Lu J. Sham, Superlatt. Microstruct. **34**, 213 (2003).

42. C. Ottaviani, S. Rebi, D. Vitali, and P. Tombesi, Preprint, QMJ5 (2006).

43. Amitabh Joshi and Min Xiao, Phys. Rev. A **72**, 062319 (2005).

44. P. M. Leung, T. C. Ralph, W. J. Munro, and Kae Nemoto, arXiv:quant-ph/0810.2828.

45. Amitabh Joshi and Min Xiao, Preprint, JWB100 (2005).

46. T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. **64**, 062311 (2001).

47. T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, Phys. Rev. A **65**, 062324 (2002).

48. H. F. Hofmann and Shigeki Takeuchi, Phys. Rev. A **66**, 024308 (2002).

49. J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Nature **426**, 264 (2003).

50. С. Н. Молотков, Письма в ЖЭТФ **91**, 51 (2010).

51. C. W. Helstrom, *Quantum Detection and Estimation Theory*, Acad. Press, New York, San Francisco, London (1976).