Письма в ЖЭТФ, том 118, вып. 1, с. 62 – 70 10 июля

MDI – Measurement Device Independent квантового распределения ключей

С. П. Кулик[+], *С. Н. Молотков*[*×1)]

[+]*Центр квантовых технологий МГУ,* [*]*Академия криптографии Российской Федерации, 119331 Москва, Россия*

[×]*Институт физики твердого тела имени Ю. А. Осипьяна РАН, 142432 Черноголовка, Россия*

Поступила в редакцию 2 июня 2023 г.
После переработки 2 июня 2023 г.
Принята к публикации 4 июня 2023 г.

Приведено прямое доказательство стойкости MDI протокола квантового распределения ключей через недоверенные узлы, которое базируется на фундаментальных энтропийных соотношениях неопределенностей. Проясняются причины удивительного совпадения выражений для длины секретного ключа для протокола BB84 и MDI протокола.

DOI: 10.31857/S1234567823130128, EDN: gdblmf

1. Введение. Квантовая криптография решает центральную проблему симметричной криптографии – распределение общего секрета – криптографического ключа между пространственно удаленными пользователями через открытые квантовый и классический аутентичный каналы связи, которые доступны для прослушивания [1].

Базовой конфигурацией квантового распределения ключей (КРК) является конфигурация точка–точка, в которой ключ распределяется между двумя узлами. В существующих на сегодняшний день телекоммуникационных сетях требуется наличие общего ключа между любой парой узлов, которые не связаны непосредственно квантовым каналом связи. На сегодняшний день данная проблема решается посредством использования доверенных узлов, через которые происходит согласование ключей (см., например, [2–4]). Такое решение принято в китайской национальной сети [5] и российской университетской сети [6].

Доверенные узлы требуют полной криптографической защиты аппаратуры, поскольку на доверенном узле имеются квантовые ключи от соседних сегментов сети, соединенных с данным узлом. Иначе говоря, работа аппаратуры должна быть недоступна нарушителю. Требуется также обеспечить защиту от несанкционированной модификации работы аппаратуры.

В большинстве систем КРК ключ формируется в результате обработки фотоотсчетов в паре однофотонных детекторов. Отсчет в одном детекторе означает бит 0 в ключе, отсчет во втором детекторе означает бит 1. *По этой причине результаты работы детекторов не должны быть доступны нарушителю.*

Имеются модификации КРК, которые позволяют сделать результаты работы детекторов доступными нарушителю – так называемое КРК с недоверенными детекторами [7]. Однако такая модификация не позволяет сделать недоверенным сам узел сети, а лишь решает задачу выноса детекторов в неконтролируемую зону.

В последнее десятилетие активно исследуются системы КРК с недоверенным промежуточным узлом. Такие системы КРК позволяют получить общий ключ между двумя узлами сети, которые соединены через промежуточный недоверенный узел, который не требует защиты аппаратуры на нем – нарушитель видит всю работу аппаратуры, включая результаты работы фотодетекторов. Данная идея была предложена в работе [8, 9], протокол КРК был назван MDI-Measurement Device Independent.

В работах [8, 9] были приведены лишь соображения, почему такая система КРК обеспечивает секретность распределяемых ключей, со ссылкой на то, что доказательство стойкости MDI протокола, которое не было приведено, аналогично доказательству секретности КРК для базового протокола BB84 [1].

Хотя протоколы совершенно разные, формула для длины секретного ключа для MDI протокола КРК совпадает со знаменитой формулой для протокола BB84, которая в асимптотическом пределе длинных последовательностей в прямом базисе + [11] (см. также ниже) имеет вид

$$\ell_+ \geq 1 - h(Q^{\times}) - \mathrm{leak}(Q^{+}), \qquad (1)$$

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

здесь $1 - h(Q^{\times})$ – утечка информации к подслушивателю при атаках на квантовый канал связи в базисе $\times$, $Q^{\times}$ – ошибка на приемной стороне Боба в этом базисе, $\mathrm{leak}(Q^{+})$ – утечка информации к подслушивателю при коррекции ошибок через классический канал связи в базисе $+$, Q^{+} – ошибка в базисе $+$ (в шенноновском пределе $\mathrm{leak}(Q^{+}) = h(Q^{+})$), $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ – бинарная энтропийная функция Шеннона, и формула (1) переходит в $\ell_{+} \geq 1 - h(Q^{\times}) - h(Q^{+})$.

Цель работы – прояснить причину столь удивительного совпадения выражений для длины секретного ключа для протокола BB84 и MDI протокола, а также привести явное доказательство стойкости MDI протокола КРК, основанное на фундаментальных энтропийных соотношениях неопределеностей [12, 13].

Различные подходы к доказательству стойкости протокола КРК BB84. Ниже при доказательстве стойкости MDI КРК и прояснении связи с базовым протоколом BB84 потребуются более подробные комментарии. Чтобы их сделать, необходимо напомнить различные подходы к доказательству секретности протокола BB84.

По-видимому, первое и достаточно сложное для понимания доказательство секретности протокола BB84 было дано в работе [14].

Далее в работе [15] доказательство стойкости BB84 было сведено к так называемой, ЭПР ((ЭПР от Эйнштейн–Подольский–Розен) версии протокола. Идея доказательства сводилась к тому, что Алиса и Боб используя "очищение" запутанности [16], получают некоторое количество чистых (идеальных) запутанных ЭПР пар, которые содержат идеальные корреляции состояний Алисы и Боба. Идеальные корреляции позволяют получить общий секретный ключ. Однако при очищении ЭПР пар требуется квантовая память. Второй момент – запутанность обладает свойством *моногамии [17]*, т.е. если пара пользователей имеют распределенную идеальную ЭПР пару, то данное запутанное состояние не может быть коррелировано с другим квантовым состоянием нарушителя.

Следующий важный шаг был сделан в работе [10]. В данном доказательстве использовались квантовые коды коррекции ошибок. Было показано, что утечка информации к Еве в одном из базисов, связана с ошибкой в канале Алиса-Боб в сопряженном базисе. В этой работе была получена знаменитая формула (1) для длины ключа.

Важный шаг был сделан в работе [18], где доказательство секретности было дано в терминах близости в смысле следового расстояния между трехчастичными квантовыми состояниями Алиса-Боб-Ева, отвечающих реальной ситуации со вторжением Евы в квантовый канал связи и идеальным состоянием, когда состояние Евы не коррелировано с состоянием Алисы-Боба.

Существенное продвижение в понимании секретности протокола BB84 [19] было достигнуто с использованием фундаментальных энтропийных соотношений неопределенностей [12, 13] (см. также историю вопроса в [20], где имеется большое число ссылок и вариантов соотношений неопределенностей). *Однако, энтропийные соотношения неопределенностей сами по себе не дают знание о явном виде квантовых состояний участников протокола.*

В работе [21] была построена явная атака Евы на передаваемые состояния в протоколе BB84, которая достигает теоретического предела по критической ошибке $Q_c \approx 11\,\%$. *Учет побочных каналов утечки информации требует знания явного вида квантовых состояний всех участников протокола.* Явное построение квантовых состояний всех участников протокола позволило в дальнейшем позволило доказать секретность протокола не для идеальных ситуаций, а для реальных условий работы систем [22, 23]: в случае не строго однофотонных состояний, разных квантовых эффективностях детекторов, побочных каналов утечки информации к Еве, включая пассивное и активное зондирование элементов системы – фазовых модуляторов, модуляторов интенсивности, обратного переизлучения однофотонных детекторов (back flash), а также в случае конечных передаваемых последовательностей с учетом побочных каналов утечки информации.

2. MDI квантовое распределение ключей. Прежде чем приступить к доказательству, для самодостаточности изложения приведем описание MDI протокола КРК с поляризационным кодированием в однофотонном случае [8].

Алиса и Боб случайно, равновероятно независимо друг от друга выбирают один из базисов $+$ – прямой или $\times$ – диагональный, аналогично протоколу BB84 [1]. Внутри базиса Алиса и Боб равновероятно выбирают одно из ортогональных состояний, отвечающих 0 и 1,

$$\mathrm{basis}+\begin{cases} 0 \to |0^{+}\rangle_{A',B'} \\ 1 \to |1^{+}\rangle_{A',B'} \end{cases}, \quad \mathrm{basis}\times\begin{cases} 0 \to |0^{\times}\rangle_{A',B'} \\ 1 \to |1^{\times}\rangle_{A',B'} \end{cases}, \tag{2}$$

$$|0^{\times}\rangle_{A',B'} = \frac{1}{\sqrt{2}}(|0^{+}\rangle_{A',B'} + |1^{+}\rangle_{A',B'},$$

$$|1^{\times}\rangle_{A',B'} = \frac{1}{\sqrt{2}}(|0^{+}\rangle_{A',B'} - |1^{+}\rangle_{A',B'},$$

где состояния $|0^{+}\rangle_{A',B'}$, $|1^{+}\rangle_{A',B'}$ отвечают горизонтальной и вертикальной поляризациям в прямом базисе, соответственно, состояния $|0^{\times}\rangle_{A',B'}$, $|1^{\times}\rangle_{A',B'}$ отвечают ортогональным поляризациям в диагональном базисе, повернутом на $\pi/4$ относительно прямого базиса

Состояния (2) поступают на недоверенный узел, на котором происходят измерения – более формально, реализуются проекции состояний на запутанные состояния – измерения в неполном белловском базисе. В базисе + запутанные состояния имеют вид: $|\Psi^{\pm}\rangle_{A'B'} = \frac{1}{\sqrt{2}}(|0^{+}\rangle_{A'} \otimes |1^{+}\rangle_{B'} \pm |1^{+}\rangle_{A'} \otimes |0^{+}\rangle_{B'})$.

Измерения в неполном белловском базисе реализуются оптической схемой с линейными элементами [8, 24].

Измерения в полном белловском базисе $|\Psi^{\pm}\rangle_{A'B'}$, $|\Phi^{\pm}\rangle_{A'B'} = \frac{1}{\sqrt{2}}(|0^{+}\rangle_{A'} \otimes |0^{+}\rangle_{B'} \pm |1^{+}\rangle_{A'} \otimes |1^{+}\rangle_{B'})$ *требуют нелинейных оптических элементов, поэтому гораздо более сложны в экспериментальной реализации.*

Отметим, что впервые измерения в полном белловском базисе в экспериментах по телепортации были сделаны в работе [25].

Результаты измерений на недоверенном узле доступны всем, включая нарушителя. После серии измерений, посылки, в которых Алиса и Боб использовали разные базисы, отбрасываются.

В базисе + после отсчета в каналах измерений $|\Psi^{\pm}\rangle_{A'B'}$ Боб инвертирует бит, который он посылал. В этом случае привязка происходит к биту Алисы. Это связано со следующим. Если не было вторжений в квантовый канал связи, то отсчет в каналах измерений $|\Psi^{\pm}\rangle_{A'B'}$ будет иметь место только в том случае, когда Алиса посылала 0, а Боб посылал 1 (и наоборот, Алиса посылала 1, Боб 0). Для получения общего одинакового бита, Боб инвертирует свой посланный бит. Происходит синхронизация битов Алисы и Боба. Вторжение в квантовый канал связи будет приводить к ошибкам.

При посылке Алисой 0 и Бобом 0, без вторжения в квантовый канал связи, отсчета на недоверенном узле не будет. При вторжении в квантовый канал будут отсчеты, приводящие к ошибкам в битовой последовательности Боба.

Состояние $|\Psi^{+}\rangle_{A'B'}$ в базисе +, переходит в состояние $|\Phi^{-}\rangle_{A'B'} = \frac{1}{\sqrt{2}}(|0^{\times}\rangle_{A'} \otimes |0^{\times}\rangle_{B'} - |1^{\times}\rangle_{A'} \otimes |1^{\times}\rangle_{B'})$ в базисе $\times$, которое содержит компоненты 00 и 11, что не требует инверсии бита Боба при отсчете в этом канале измерения. Состояние $|\Psi^{-}\rangle_{A'B'}$ инвариантно к смене базисов; оно переходит в состояние $|\Psi^{-}\rangle_{A'B'} = \frac{1}{\sqrt{2}}(|0^{\times}\rangle_{A'} \otimes |1^{\times}\rangle_{B'} - |1^{\times}\rangle_{A'} \otimes |0^{\times}\rangle_{B'})$. Поэтому при отсчете в канале $|\Psi^{-}\rangle_{A'B'}$ также как и в базисе +, Боб инвертирует свой бит. При отсчете в канале $|\Psi^{+}\rangle_{A'B'}$ в базисе $\times$ Боб свой бит не инвертирует.

Далее часть посылок раскрывается для оценки вероятности ошибки. Оценка вероятности требуется для вычисления величины утечки информации к Еве, с учетом того, что ей известны отсчеты на недоверенном узле.

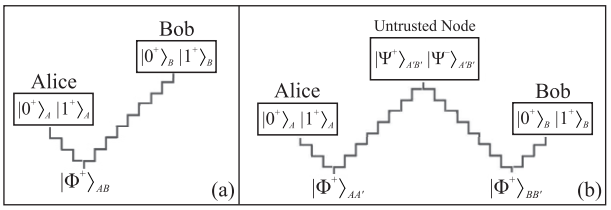

Рис. 1. (a) – Схематическое изображение запутанных состояний для ЭПР версии протокола BB84. (b) – Схематическое изображение запутанных состояний для ЭПР версии протокола MDI

3. Доказательство стойкости протокола, версия MDI протокола на запутанных состояниях. Алиса и Боб в каждой посылке посылают однофотонные состояния, отвечающие 0 или 1 в одном из базисов. Для использования энтропийных соотношений неопределенностей, а также прояснения связи с BB84 протоколом, удобно воспользоваться эквивалентной версией протокола на ЭПР состояниях.

ЭПР версия протокола BB84 сводится к следующему. Алиса готовит ЭПР пару (рис. 1a) $|\Phi^{+}\rangle_{AB}$. Подсистему A Алиса оставляет у себя как эталонную, подсистему B направляет к Бобу. Данная подсистема подвержена атакам Евы в квантовом канале. Затем Алиса производит измерение над своей подсистемой в одном из случайно выбранных базисов. В результате измерений подсистема A случайно и равновероятно оказывается в одном из состояний 0 или 1. Из-за идеальных корреляций в ЭПР состоянии, подсистема B оказывается в том же состоянии, что и подсистема Алисы. Такая процедура эквивалентна приготовлению равновероятно одного из состояний в базисе и посылке его в канал связи. ЭПР версия позволяет иметь общее прародительское состояние в любом базисе, и получить трехчастичную матрицу плотности Алиса-Боб-Ева, которая фигурирует в дальнейшем в энтропийных соотношениях неопределенностей.

В MDI протоколе кроме Алисы-Боба-Евы имеется еще одна подсистема – недоверенный узел, который является информационным бонусом для Евы.

ЭПР версия MDI протокола выглядит следующим образом. Алиса и Боб готовят свои ЭПР пары $|\Phi^+\rangle_{AA'}$ и $|\Phi^+\rangle_{BB'}$. Подсистемы A' и B' направляются на недоверенный узел, а подсистемы A и B остаются в распоряжении Алисы и Боба как эталонные. Подсистемы $A'B'$ подвержены атакам Евы в квантовом канале связи.

Далее Алиса и Боб производят измерения над своими эталонными подсистемами в одном из базисов. Если бы не было вторжений в квантовый канал связи, то имели бы место идеальные корреляции битов Алисы и Боба после измерений на недоверенном узле над подсистемой $A'B'$.

Рассмотрим теперь ситуацию более формально. ЭПР состояния Алисы и Боба имеют вид

$$|\Phi^+\rangle_{AA'}\otimes|\Phi^+\rangle_{BB'}= \tag{3}$$

$$=\frac{1}{\sqrt{2}}\left(|0^+\rangle_A\otimes|0^+\rangle_{A'}+|1^+\rangle_A\otimes|1^+\rangle_{A'}\right)\otimes$$

$$\otimes\frac{1}{\sqrt{2}}\left(|0^+\rangle_B\otimes|0^+\rangle_{B'}+|1^+\rangle_B\otimes|1^+\rangle_{B'}\right)=$$

$$=\frac{1}{2}\left((|0^+\rangle_A\otimes|0^+\rangle_B)\otimes(|0^+\rangle_{A'}\otimes|0^+\rangle_{B'})+\right.$$

$$+(|0^+\rangle_A\otimes|1^+\rangle_B)\otimes(|0^+\rangle_{A'}\otimes|1^+\rangle_{B'})+$$

$$+(|1^+\rangle_A\otimes|0^+\rangle_B)\otimes(|1^+\rangle_{A'}\otimes|0^+\rangle_{B'})+$$

$$\left.+(|1^+\rangle_A\otimes|1^+\rangle_B)\otimes(|1^+\rangle_{A'}\otimes|1^+\rangle_{B'})\right).$$

Из (3) видно, что измерения на недоверенном узле над подсистемой $A'B'$ в базисе $|i^+\rangle_{A'}\otimes|j^+\rangle_{B'}$, $(i^+,j^+=0,1)$ приводят к корреляциям между подсистемами A и B. Например, пусть произошел отсчет в канале $|0^+\rangle_{A'}\otimes|1^+\rangle_{B'}$, тогда в канале A и B возникнет отсчет в канале $|0^+\rangle_A\otimes|1^+\rangle_B$.

Таким образом, Алиса и Боб, зная результат отсчета на недоверенном узле, могут знать какой бит получил партнер.

Если Ева вторгается в квантовый канал связи, то такие идеальные корреляции между битами Алисы и Боба будут нарушаться – возникнут ошибки в битовых последовательностях.

3.1. Атака нарушителя на состояния в квантовом канале связи. Действие Евы задается супероператором, любой супероператор (вполне положительное отображение – CPM – Completely Positive Map) унитарно представим [26, 27], т.е. может быть представлен как унитарное преобразование $U_{A'B'E}\otimes I_{AB}$ над исходным состоянием и вспомогательным состоянием $|E\rangle_E$ нарушителя.

Рассмотрим атаку Евы на состояния подсистемы $A'B'$. В базисе + имеем (рассмотрение в базисе $\times$ аналогично, и сводится к замене индекса $+\to\times$ в формулах ниже)

$$|\Psi\rangle_{ABA'B'E}=(U_{A'B'E}\otimes I_{AB})\times \tag{4}$$

$$\times\left(\left(|\Phi^+\rangle_{AA'}\otimes|\Phi^+\rangle_{BB'}\right)\otimes|E\rangle_E\right)=$$

$$=(U_{A'B'E}\otimes I_{AB})\,\frac{1}{2}\left(\left((|0^+\rangle_A\otimes|0^+\rangle_B)\otimes(|0^+\rangle_{A'}\otimes\right.\right.$$

$$\otimes|0^+\rangle_{B'})+(|0^+\rangle_A\otimes|1^+\rangle_B)\otimes(|0^+\rangle_{A'}\otimes|1^+\rangle_{B'})+$$

$$+(|1^+\rangle_A\otimes|0^+\rangle_B)\otimes(|1^+\rangle_{A'}\otimes|0^+\rangle_{B'})+$$

$$\left.\left.+(|1^+\rangle_A\otimes|1^+\rangle_B)\otimes(|1^+\rangle_{A'}\otimes|1^+\rangle_{B'})\right)\otimes|E\rangle_E\right).$$

Получим действие унитарного преобразования подслушивателя на отдельные компоненты состояния (4), которые потребуются для дальнейшей интерпретации исходов измерений,

$$(U_{A'B'E}\otimes I_{AB})\left(\left((|0^+\rangle_A\otimes|0^+\rangle_B)\otimes\right.\right. \tag{5}$$

$$\left.\left.\otimes(|0^+\rangle_{A'}\otimes|0^+\rangle_{B'})\right)\otimes|E\rangle_E\right)=$$

$$=\left(|0^+\rangle_A\otimes|0^+\rangle_B\otimes\right)\Big(|\Phi^+\rangle_{A'B'}\otimes|E^{0^+0^+}_{\Phi^+}\rangle_E+$$

$$+|\Phi^-\rangle_{A'B'}\otimes|E^{0^+0^+}_{\Phi^-}\rangle_E+|\Psi^+\rangle_{A'B'}\otimes$$

$$\otimes\Big|E^{0^+0^+}_{\Psi^+}\rangle_E+|\Psi^-\rangle_{A'B'}\otimes|E^{0^+0^+}_{\Psi^-}\rangle_E\Big),$$

$$(U_{A'B'E}\otimes I_{AB})\left(\left((|0^+\rangle_A\otimes|1^+\rangle_B)\otimes(|0^+\rangle_{A'}\otimes\right.\right. \tag{6}$$

$$\left.\left.\otimes\ |1^+\rangle_{B'})\right)\otimes|E\rangle_E\right)=$$

$$=\left(|0^+\rangle_A\otimes|1^+\rangle_B\otimes\right)\Big(|\Phi^+\rangle_{A'B'}\otimes|E^{0^+1^+}_{\Phi^+}\rangle_E+$$

$$+|\Phi^-\rangle_{A'B'}\otimes|E^{0^+1^+}_{\Phi^-}\rangle_E+|\Psi^+\rangle_{A'B'}\otimes|E^{0^+1^+}_{\Psi^+}\rangle_E+$$

$$+|\Psi^-\rangle_{A'B'}\otimes|E^{0^+1^+}_{\Psi^-}\rangle_E\Big),$$

$$(U_{A'B'E}\otimes I_{AB})\left(\left((|1^+\rangle_A\otimes|0^+\rangle_B)\otimes(|1^+\rangle_{A'}\otimes\right.\right. \tag{7}$$

$$\left.\left.\otimes|0^+\rangle_{B'})\right)\otimes|E\rangle_E\right)=$$

$$=\left(|1^+\rangle_A\otimes|0^+\rangle_B\otimes\right)\Big(|\Phi^+\rangle_{A'B'}\otimes|E^{1^+0^+}_{\Phi^+}\rangle_E+$$

$$+|\Phi^-\rangle_{A'B'}\otimes|E^{1^+0^+}_{\Phi^-}\rangle_E+$$

$$+|\Psi^+\rangle_{A'B'}\otimes|E^{1^+0^+}_{\Psi^+}\rangle_E+|\Psi^-\rangle_{A'B'}\otimes|E^{1^+0^+}_{\Psi^-}\rangle_E\Big),$$

$$(U_{A'B'E}\otimes I_{AB})\left(\left((|1^+\rangle_A\otimes|1^+\rangle_B)\otimes\right.\right. \tag{8}$$

$$\left.\left.\otimes(|1^+\rangle_{A'}\otimes|1^+\rangle_{B'})\right)\otimes|E\rangle_E\right)=$$

$$=(|1\rangle_A\otimes|1\rangle_B\otimes)\Big(|\Phi^+\rangle_{A'B'}\otimes|E^{1^+1^+}_{\Phi^+}\rangle_E+$$

$$+|\Phi^-\rangle_{A'B'}\otimes|E^{1^+1^+}_{\Phi^-}\rangle_E+|\Psi^+\rangle_{A'B'}\otimes|E^{1^+1^+}_{\Psi^+}\rangle_E+$$

$$+|\Psi^-\rangle_{A'B'}\otimes|E^{1^+1^+}_{\Psi^-}\rangle_E\Big).$$

Разложение состояния чистого состояния (4) в виде (5)–(8) представляет разложение состояния по базисным векторам состояний в пространстве $A'B'E$. В качестве базисных векторов в этом пространстве выбраны 4-е белловских состояния, и состояния Евы $|E^{i^+j^+}_{\Psi^\pm}\rangle_E$, $|E^{i^+j^+}_{\Phi^\pm}\rangle_E$ $(i,j=0,1)$. Конкретный вид состояний Евы в данной работе не потребуется, однако может быть явно получен из условий унитарности $U_{A'B'E}$.

3.2. Измерения на недоверенном узле и измерения Алисы и Боба. Обсудим измерения над подсистемами A и B и измерения на недоверенном узле. Измерения Алисы и Боба в базисах $+$ и $\times$ даются разложением единицы и независимы друг от друга. Для измерений Алисы имеем

$$I_A = |0^+\rangle_{AA}\langle 0^+| + |1^+\rangle_{AA}\langle 1^+| = \\ = |0^\times\rangle_{AA}\langle 0^\times| + |1^\times\rangle_{AA}\langle 1^\times|, \tag{9}$$

аналогично для измерений Боба

$$I_B = |0^+\rangle_{BB}\langle 0^+| + |1^+\rangle_{BB}\langle 1^+| = \\ = |0^\times\rangle_{BB}\langle 0^\times| + |1^\times\rangle_{BB}\langle 1^\times|. \tag{10}$$

Измерение на недоверенном узле дается частичным разложением единицы в подпространстве $(A'B')$, натянутом на векторы $|0\rangle_{A'}\otimes|1\rangle_{B'}$ и $|1\rangle_{A'}\otimes|0\rangle_{B'}$, находим

$$\overline{I}_{A'B'} = |\Psi^+\rangle_{A'B'A'B'}\langle\Psi^+| + |\Psi^-\rangle_{A'B'A'B'}\langle\Psi^-|. \tag{11}$$

Совместная трехчастичная матрица плотности всех участников, определяющая совместную вероятность исходов измерений на недоверенном узле в канале измерений $|\Psi^\pm\rangle_{A'B'A'B'}\langle\Psi^\pm|$ и в каналах измерений Алисы и Боба $|0^+\rangle_{AA}\langle 0^+|, |1^+\rangle_{AA}\langle 1^+|$ $|0^+\rangle_{BB}\langle 0^+|, |1^+\rangle_{BB}\langle 1^+|$, после измерений над общим квантовым состоянием (4) $\rho_{ABA'B'E} = |\Psi\rangle_{ABA'B'E\ ABA'B'E}\langle\Psi|$, имеет вид

$$\rho_{X^+Y^+\Psi^+\Psi^-E^+} = \tag{12}$$

$$= \sigma_B^X \Bigg\{ \mathrm{Tr}_{ABA'B'} \Bigg\{ \Bigg\{ \sum_{i,j=0,1} \sum_{m=+,-} \Big(\big(|i^+\rangle_{AA}\langle i^+| \otimes \\ \otimes |j^+\rangle_{BB}\langle j^+|\big) \otimes \big(|\Psi^m\rangle_{A'B'A'B'}\langle\Psi^m|\big) \Big) \Bigg\} \\ \rho_{ABA'B'E} \\ \Bigg\{ \sum_{i,j=0,1} \sum_{m=+,-} \Big(\big(|i^+\rangle_{AA}\langle i^+| \otimes |j^+\rangle_{BB}\langle j^+|\big) \otimes \\ \otimes \big(|\Psi^m\rangle_{A'B'A'B'}\langle\Psi^m|\big) \Big) \Bigg\} \Bigg\} \Bigg\} \sigma_B^X.$$

Поскольку после измерений Алиса и Боб получают битовые строки, и которые обычно обозначаются x, y, и которым сопоставлены ортогональные квантовые состояния, то в формуле (12) и ниже произведена замена индексов $A \to X$, $B \to Y$, $x \in \mathcal{X} = \{0,1\}$, $y \in \mathcal{Y} = \{0,1\}$.

После измерений в базисе $+$ Боб инвертирует свой бит, что задается действием оператора σ_B^X – оператор Паули. После измерений над $\rho_{ABA'B'E}$ и инвертированием своего бита Бобом, в базисе $+$ с учетом (5)–(8), получаем

$$\rho_{X^+Y^+\Psi^+\Psi^-E} = \rho_{X^+Y^+\pm E^+} = \rho_{X^+Y^+\overline{E}} = \tag{13}$$

$$= |0^+1^+\rangle_{X^+Y^+X^+Y^+}\langle 0^+1^+| \otimes \Big(|\Psi^+\rangle_{A'B'A'B'}\langle\Psi^+| \otimes \\ \otimes |E^{0^+0^+}_{\Psi^+}\rangle_{EE}\langle E^{0^+0^+}_{\Psi^+}| + |\Psi^-\rangle_{A'B'A'B'}\langle\Psi^-| \otimes \\ \otimes |E^{0^+0^+}_{\Psi^-}\rangle_{EE}\langle E^{0^+0^+}_{\Psi^-}| \Big) + |0^+0^+\rangle_{X^+Y^+X^+Y^+}\langle 0^+0^+| \times \\ \times \Big(|\Psi^+\rangle_{A'B'A'B'}\langle\Psi^+| \otimes |E^{0^+1^+}_{\Psi^+}\rangle_{EE}\langle E^{0^+1^+}_{\Psi^+}| + \\ + |\Psi^-\rangle_{A'B'A'B'}\langle\Psi^-| \otimes |E^{0^+1^+}_{\Psi^-}\rangle_{EE}\langle E^{0^+1^+}_{\Psi^-}| \Big) + \\ + |1^+1^+\rangle_{X^+Y^+X^+Y^+}\langle 1^+1^+| \times \Big(|\Psi^+\rangle_{A'B'A'B'}\langle\Psi^+| \otimes \\ \otimes |E^{1^+0^+}_{\Psi^+}\rangle_{EE}\langle E^{1^+0^+}_{\Psi^+}| + |\Psi^-\rangle_{A'B'A'B'}\langle\Psi^-| \otimes \\ \otimes |E^{1^+0^+}_{\Psi^-}\rangle_{EE}\langle E^{1^+0^+}_{\Psi^-}| \Big) + |1^+0^+\rangle_{X^+Y^+X^+Y^+}\langle 1^+0^+| \times \\ \times \Big(|\Psi^+\rangle_{A'B'A'B'}\langle\Psi^+| \otimes |E^{11}_{\Psi^+}\rangle_{EE}\langle E^{1^+1^+}_{\Psi^+}| + \\ + |\Psi^-\rangle_{A'B'A'B'}\langle\Psi^-| \otimes |E^{1^+1^+}_{\Psi^-}\rangle_{EE}\langle E^{1^+1^+}_{\Psi^-}| \Big).$$

В (13) введено обозначение $\Psi^+\Psi^-E = \overline{E}$, т.к. Еве доступен недоверенный узел, то состояние $\overline{E}$ "полной" Евы включает в себя состояние Евы в квантовом канале и состояние не недоверенном узле.

Поскольку измерения (11) производятся в неполном белловском базисе, то требуется нормировка матрицы плотности (12), (13) на единицу, считаем, для экономии обозначений, что состояния Евы нормированы так (см. ниже), чтобы след матрицы плотности (13) был равен единице.

Для частичной матрицы плотности Алиса-Боб в базисе $+$ с учетом (13) находим

$$\rho_{X^+Y^+} = \mathrm{Tr}_{\overline{E}}\{\rho_{X^+Y^+\overline{E}}\} = \tag{14}$$

$$= |0^+\rangle_{X^+X^+}\langle 0^+| \otimes \big(p_{00}|0^+\rangle_{Y^+Y^+}\langle 0^+| + \\ + p_{01}|1^+\rangle_{Y^+Y^+}\langle 1^+| \big) + |1^+\rangle_{X^+X^+}\langle 1^+| \otimes \\ \otimes \big(p_{11}|1^+\rangle_{Y^+Y^+}\langle 1^+| + p_{10}|0^+\rangle_{Y^+Y^+}\langle 0^+| \big) = \\ = \overline{p}_0^+ |0^+\rangle_{X^+X^+}\langle 0^+| \otimes \big((1-Q_0^+)|0^+\rangle_{Y^+Y^+}\langle 0^+| +$$

$$+ Q_0^+ |1^+\rangle_{Y^+Y^+}\langle 1^+| \big) + \overline{p}_1^+ |1^+\rangle_{X^+X^+}\langle 1^+| \otimes$$
$$\otimes \big((1 - Q_1^+) |1^+\rangle_{Y^+Y^+}\langle 1^+| + Q_1^+ |0^+\rangle_{Y^+Y^+}\langle 0^+| \big),$$

где нормировка состояний Евы

$$\overline{p}_0^+ = \frac{p_0}{p_0 + p_1}, \quad p_0 = p_{00} + p_{01}, \qquad 1 - Q_0^+ = \frac{p_{00}}{p_0}, \quad Q_0^+ = \frac{p_{01}}{p_0}, \tag{15}$$

$$\overline{p}_1^+ = \frac{p_1}{p_0 + p_1}, \quad p_1 = p_{11} + p_{10}, \qquad 1 - Q_1^+ = \frac{p_{11}}{p_1}, \quad Q_1^+ = \frac{p_{10}}{p_1}. \tag{16}$$

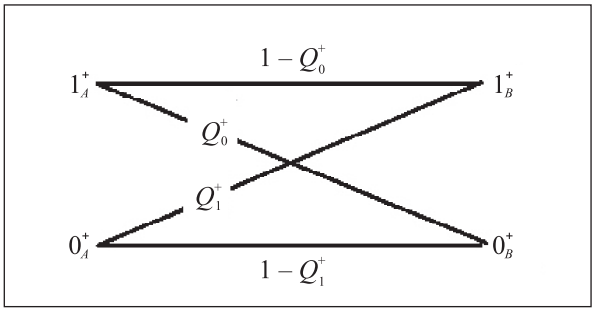

Рис. 2. Представление классического канала Алиса-Боб в базисе + вместе с обозначением переходных вероятностей

Вероятность ошибок в битах Боба относительно битов Алисы зависит от действий Евы в кантовом канале связи, далее, введены обозначения

$$p_{01} = {}_E\langle E_{\Psi^+}^{0^+0^+} | E_{\Psi^+}^{0^+0^+} \rangle_E + {}_E\langle E_{\Psi^-}^{0^+0^+} | E_{\Psi^-}^{0^+0^+} \rangle_E, \tag{17}$$

$$p_{10} = {}_E\langle E_{\Psi^+}^{1^+1^+} | E_{\Psi^+}^{1^+1^+} \rangle_E + {}_E\langle E_{\Psi^-}^{1^+1^+} | E_{\Psi^-}^{1^+1^+} \rangle_E, \tag{18}$$

$$p_{00} = {}_E\langle E_{\Psi^+}^{0^+1^+} | E_{\Psi^+}^{0^+1^+} \rangle_E + {}_E\langle E_{\Psi^-}^{0^+1^+} | E_{\Psi^-}^{0^+1^+} \rangle_E, \tag{19}$$

$$p_{11} = {}_E\langle E_{\Psi^+}^{1^+0^+} | E_{\Psi^+}^{1^+0^+} \rangle_E + {}_E\langle E_{\Psi^-}^{1^+0^+} | E_{\Psi^-}^{1^+0^+} \rangle_E. \tag{20}$$

Величины (15)–(20) имеют смысл условных (переходных) вероятностей для классического канала Алиса-Боб (рис. 2) и зависят от действий нарушителя. Матрица плотности Ева-недоверенный узел имеет вид

$$\rho_{\overline{E}} = \mathrm{Tr}_{X^+Y^+} \{ \rho_{X^+Y^+\overline{E}} \} = \tag{21}$$
$$= |\Psi^+\rangle_{A'B'A'B'}\langle\Psi^+| \otimes \Big(|E_{\Psi^+}^{0^+0^+}\rangle_{EE}\langle E_{\Psi^+}^{0^+0^+}| +$$
$$+ |E_{\Psi^+}^{0^+1^+}\rangle_{EE}\langle E_{\Psi^+}^{0^+1^+}| + |E_{\Psi^+}^{1^+0^+}\rangle_{EE}\langle E_{\Psi^+}^{1^+0^+}| +$$
$$+ |E_{\Psi^+}^{1^+1^+}\rangle_{EE}\langle E_{\Psi^+}^{1^+1^+}| \Big) + |\Psi^-\rangle_{A'B'A'B'}\langle\Psi^-| \otimes$$
$$\otimes \Big(|E_{\Psi^-}^{0^+0^+}\rangle_{EE}\langle E_{\Psi^-}^{0^+0^+}| + |E_{\Psi^-}^{0^+1^+}\rangle_{EE}\langle E_{\Psi^-}^{0^+1^+}| +$$
$$+ |E_{\Psi^-}^{1^+0^+}\rangle_{EE}\langle E_{\Psi^-}^{1^+0^+}| + |E_{\Psi^-}^{1^+1^+}\rangle_{EE}\langle E_{\Psi^-}^{1^+1^+}| \Big).$$

3.3. Интерпретация исходов измерений, перенос корреляций между состояниями Алисы и Боба через недоверенный узел. Пусть Алиса посылала состояние 0, а Боб 1 в базисе +. В этом случае, если произошел отсчет в канале ± на недоверенном узле, то это означает, что имеют место корреляции – состояние $|0^+\rangle_{A'} \otimes |1^+\rangle_{B'}$ с определенной вероятностью достигло недоверенного узла неискаженным – второе слагаемое в (13), что дало отсчет в каналах $|\Psi^\pm\rangle_{A'B'A'B'}$, которые включают в себя такое состояние. Для согласования битов Алисы и Боба (привязка идет к биту Алисы), Боб инвертирует свой бит $1 \to 0$. В этом случае с вероятностью (15), (16) имеет место согласование битов Алисы и Боба.

Пусть теперь Алиса и Боб посылали состояние $|0^+\rangle_{A'} \otimes |0^+\rangle_{B'}$. Если бы не было вторжений в квантовый канал связи нарушителем, то данные состояния не дали бы отсчет в каналах $|\Psi^\pm\rangle_{A'B'A'B'}$ на недоверенном узле, поскольку $|\Psi^\pm\rangle_{A'B'A'B'}$ не содержат таких состояний.

В случае вторжения в канал связи возникнет возмущение данных состояний – появятся компоненты $|0^+\rangle_{A'} \otimes |1^+\rangle_{B'}$, которые дадут отсчет на недоверенном узле. После отсчета Боб инвертирует свой бит $0 \to 1$. В итоге биты Алиса (0) и Боба (1) будут рассогласованы – возникнет ошибка с вероятностью (15), (16).

Аналогично рассматриваются другие состояния.

Вероятность ошибок оценивается раскрытием Алисой и Бобом части последовательности, которая затем отбрасывается.

Здесь уместно напомнить ситуацию в протоколе BB84. В этом протоколе идеальные корреляции между состояниями Алисы и Боба исходно заложены в ЭПР пару Алисы $|\Phi^+\rangle_{AB}$ (рис. 1a)). Идеальные корреляции нарушаются – нарушается идеальная исходная "чистота" ЭПР пары после вторжений в канал нарушителя – после атак на подсистему B.

В MDI протоколе идеальные корреляции между состоянием Алисы и состоянием, посланным на недоверенный узел, заключены в ЭПР паре $|\Phi^+\rangle_{AA'}$. Аналогично для состояний Боба – корреляции исходно заложены в ЭПР пару $|\Phi^+\rangle_{BB''}$.

Без вторжения в квантовый канал нарушителя, измерения на недоверенном узле переносят идеальные корреляции внутри каждой ЭПР пары на идеальные корреляции между состояниями Алисы (подсистема A) и Боба (подсистема B). Иначе говоря, без вторжений в канал связи, чистота каждой ЭПР пары после измерений переносится на чистоту новой ЭПР пары Алисы и Боба.

Вторжение в канал связи нарушают идеальные корреляции новой ЭПР пары с некоторой вероятностью, неидеальность новой ЭПР пары приводит к рассогласованию битов Алисы и Боба – ошибкам битов Алисы и Боба.

Неформально говоря, чистоту (идеальность) новой ЭПР пары, которая имеет место с определенной вероятностью (см. (15), (16)), Алиса и Боб выясняют через результаты измерений на недоверенном узле и раскрытием части своих битовых последовательностей.

Напомним также, что инверсия бита Боба после факта измерений на недоверенном узле связана с тем, что измерения производятся в каналах $|\Psi^{\pm}\rangle_{A'B'}$ – измерения реализуют проекцию на данные состояния, которые содержат состояния $|0^+\rangle_{A'} \otimes |1^+\rangle_{B'}$ и $|1^+\rangle_{A'} \otimes |0^+\rangle_{B'}$. Выбор измеряющих состояний $|\Psi^{\pm}\rangle_{A'B'}$ связан с простотой экспериментальной реализации таких измерений по схеме совпадений с помощью только линейных оптических элементов [8].

При посылке и измерении состояний в базисе $\times$ инверсия бита Боба требуется только при отсчетах в канале измерений $|\Psi^-\rangle_{A'B'}$. При отсчетах в канале $|\Psi^+\rangle_{A'B'A'B'}$ инверсия бита Боба не требуется. Это связано с тем, что в базисе $\times$ состояние $|\Psi^+\rangle_{A'B'A'B'}$ содержит компоненты состояний $|0^\times\rangle_{A'} \otimes |1^\times\rangle_{B'}$ и $|1^\times\rangle_{A'} \otimes |1^\times\rangle_{B'}$ (см. связь состояний в разных базисах (2)).

3.4. Вычисление условной энтропии Алиса-Боб. Таким образом, после измерений на недоверенном узле, Алиса и Боб оказываются в ситуации классического бинарного канала связи (необязательно симметричного, рис. 2). Данный канал описывается частичными матрицами плотности $\rho_{X^+Y^+}$ и ρ_{Y^+}, которые имеют диагональный вид. Для дальнейшего нам потребуются условные энтропии фон Неймана, с учетом (14) находим

$$H(\rho_{X^+Y^+}) = h(\overline{p}_0^+) + \overline{p}_0^+ h(Q_0^+) + (1-\overline{p}_0^+) h(Q_1^+). \quad (22)$$

$$H(\rho_{Y^+}) = h(\overline{p}^+),\ \ \overline{p}^+ = \overline{p}_0^+(1-Q_0^+) + (1-\overline{p}_0^+)Q_1^+, \quad (23)$$

$$H(\rho_{X^+Y^+}|\rho_{Y^+}) = \\ = h(\overline{p}_0^+) - h(\overline{p}^+) + \overline{p}_0^+ h(Q_0^+) + (1-\overline{p}_0^+) h(Q_1^+). \quad (24)$$

В симметричном случае $Q_0^+ = Q_1^+ = Q$, $\overline{p}_0^+ = \frac{1}{2}$, получаем

$$H(\rho_{X^+Y^+}|\rho_{Y^+}) = h(Q). \quad (25)$$

Неформальная интерпретация (25) сводится к тому, что $h(Q)$ – минимальное число бит в пересчете на посылку, которое требуется для исправления ошибок у Боба в асимптотическом пределе длинных последовательностей – шенноновский предел.

4. Энтропийные соотношения неопределенностей, длина секретного ключа. Энтропийные соотношения неопределенностей являются теоретико-информационной переформулировкой соотношений неопределенностей для пары некоммутирующих наблюдаемых [28, 29] (см. также историю вопроса в обзоре [20]).

Пусть квантовое состояние, описывающее состояние трех участников протокола Алиса-Боб-Ева-недоверенный узел задается матрицей плотности в базисе $+$ $\rho_{X^+Y^+\overline{E}}$, соответственно в базисе $\times$ $\rho_{X^\times Y^\times \overline{E}}$.

Энтропийные соотношения неопределенностей [20, 28, 29] для сглаженных энтропий min и max энтропий были доказаны в работе [12, 13]. Поскольку рассматриваем асимптотический предел длинных последовательностей, то сглаженные min и max энтропии переходят в энтропии фон Неймана, имеем

$$H(\rho_{X^\times \overline{E}}|\rho_{\overline{E}}) + H(\rho_{X^+B}|\rho_B) \geq \log\left(\frac{1}{c}\right), \quad (26)$$

$$c = \max_{x^+,x^\times} ||\sqrt{\mathcal{M}_{x^+}}\sqrt{\mathcal{M}_{x^\times}}||^2_\infty.$$

Пусть над матрицей плотности над подсистемой A проводится измерение, которое задается операторно-значными мерами $\{\mathcal{M}_{x^+}\}$ в базисе $+$, и $\{\mathcal{M}_{x^\times}\}$ в базисе $\times$. В нашем случае операторно-значные меры являются проекторами. Матрицы плотности после измерений над подсистемой A в базисе $+$ и базисе $\times$ с учетом (14) имеют вид

$$\rho_{X^\times \overline{E}} = \sum_{x^\times} \sqrt{\mathcal{M}_{x^\times}}\rho_{A\overline{E}}\sqrt{\mathcal{M}_{x^\times}}, \quad \rho_{A\overline{E}} = \mathrm{Tr}_B\{\rho_{AB\overline{E}}\}, \quad (27)$$

$$\rho_{X^+B} = \sum_{x^+} \sqrt{\mathcal{M}_{x^+}}\rho_{AB}\sqrt{\mathcal{M}_{x^+}}, \quad \rho_{AB} = \mathrm{Tr}_{\overline{E}}\{\rho_{AB\overline{E}}\}. \quad (28)$$

Пусть над подсистемой B проводится измерение в базисах $+$ и $\times$, которое задается аналогичными операторно-значными мерами $\{\mathcal{M}_{y^+}\}$ в базисе $+$, и $\{\mathcal{M}_{y^\times}\}$ в базисе $\times$, что дает матрицы плотности

$$\rho_{X^+Y^+} = \sum_{y^+} \sqrt{\mathcal{M}_{y^+}}\rho_{X^+B}\sqrt{\mathcal{M}_{y^+}}, \quad (29)$$

аналогчно в базисе $\times$

$$\rho_{X^\times Y^\times} = \sum_{y^\times} \sqrt{\mathcal{M}_{y^\times}}\rho_{X^\times B}\sqrt{\mathcal{M}_{y^\times}}. \quad (30)$$

Учитывая, что $H(\rho_{X^+Y^+}|\rho_{Y^+}) \geq H(\rho_{X^+B}|\rho_B)$ (см., например, [18]), получаем

$$H(\rho_{X^\times\overline{E}}|\rho_{\overline{E}}) + H(\rho_{X^+Y^+}|\rho_{Y^+}) \geq \log\left(\frac{1}{c}\right), \quad c = |{}_{X^+}\langle i^+|j^\times\rangle_{X^\times}|^2 = \frac{1}{2}, \quad i^+, j^\times = 0,1, \tag{31}$$

и аналогично в базисе $\times$. Для длины ключа в базисе $\times$ находим

$$\begin{aligned}\ell_\times &\geq H(\rho_{X^\times\overline{E}}|\rho_{\overline{E}}) - H(\rho_{X^\times\overline{E}}|\rho_{\overline{E}}) \geq \\ &\geq 1 - H(\rho_{X^+\overline{E}}|\rho_{\overline{E}}) - H(\rho_{X^\times\overline{E}}|\rho_{\overline{E}}) \geq \\ &\geq \big\{1 - \big(h(\overline{p}_0^+) - h(\overline{p}^+) + \overline{p}_0^+ h(Q_0^+) + \\ &+ (1-\overline{p}_0^+)h(Q_1^+)\big)\big\} - \big\{h(\overline{p}_0^\times) - h(\overline{p}^\times) + \\ &+ \overline{p}_0^\times h(Q_0^\times) + (1-\overline{p}_0^\times)h(Q_1^\times)\big\}.\end{aligned} \tag{32}$$

В формуле (32) величины $\overline{p}_0^\times$, $\overline{p}^\times$, $Q_{0,1}^\times$ имеют такой же смысл как и величины в (14)–(16), но при измерениях в базисе $\times$.

Энтропийные соотношения неопределенностей связывают нехватку информации $H(\rho_{X^\times\overline{E}}|\rho_{\overline{E}})$ о битовой строке Алисы в базисе $\times$ при условии, что нарушитель имеет в своем распоряжении квантовую систему (Ева-недоверенный узел) с нехваткой информации Боба $H(\rho_{X^+Y^+}|\rho_{Y^+})$ о битовой строке Алисы в базисе $+$ при условии, что Боб имеет в своем распоряжении битовую строку Y^+, коррелированную со строкой Алисы X^+. Сумма двух дефицитов информаций не может быть меньше одного бита. Неформально говоря, нехватка информации Боба представляет собой минимальное число бит, которые требуются Бобу для коррекции ошибок через классический аутентичный канал связи.

Энтропийные соотношения неопределенностей позволяют не перебирать всевозможные атаки Евы, но при этом позволяют получить утечку информации к Еве через наблюдаемые ошибки на приемной стороне – нехватку информации Боба. В симметричном случае находим

$$\ell_\times \geq 1 - 2h(Q), \tag{33}$$

что совпадает со знаменитой формулой для длины секретного ключа протокола BB84 [10].

5. Заключение. Обсудим неформальные причины секретности ключей в MDI протоколе. Алиса и Боб в каждой посылке посылают на недоверенный узел по одному биту информации. Измерения на недоверенном узле в базисе запутанных состояний раскрывают один бит – фактически бит четности Алисы и Боба. Остается один неизвестный бит.

При атаке на квантовый канал Ева производит ошибки между битами Алисы и Боба и получает дополнительную информацию, кроме бита четности.

При отсутствии ошибок между Алисой и Бобом, в отсутствии вторжения в квантовый канал Евой, имеют место идеальные корреляции между Алисой и Бобом в любом базисе. Данные корреляции между Алисой и Бобом переносятся через измерения на недоверенном узле. Идеальные корреляции в любом базисе означают идеальность ЭПР пары AB. При вторжении в квантовый канал связи идеальные корреляции между Алисой и Бобом нарушаются – идеальность ЭПР пары имеет место лишь с некоторой вероятностью, зависящей от вероятности ошибок.

После измерений на недоверенном узле в канале измерений, в котором не появляются ошибки у Боба, возникает неидеальная ЭПР пара между Алисой и Бобом, как это имеет место в протоколе BB84. Например, Алиса посылала 0, Боб посылал 1, и если с определенной вероятностью возник отсчет в канале измерений $|\Psi^+\rangle_{A'B'}$, то между Алисой и Бобом возникает идеальная ЭПР пара.

Энтропийные соотношения неопределенностей позволяют вычислить утечку информации к Еве через нехватку информации Боба по отношению к информации Алисы. Алиса и Боб связаны классическим бинарным каналом связи, аналогично тому, как это имеет место в протоколе BB84 (см., например, [30]). По этой причине утечка информации к Еве имеет такой же функциональный вид как в протоколе BB84.

Утечка информации к Еве при коррекции ошибок через классический канал определяется свойствами аналогичного классического канала между Алисой и Бобом, поэтому утечка имеет такой же вид, как в протоколе BB84.

Выражаем благодарность И. М. Арбекову, А. В. Уривскому за обсуждения и замечания, а также коллегам по Академии криптографии Российской Федерации.

С. П. Кулик благодарит ОАО РЖД за поддержку работы.

1. C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, In *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, Bangalore, India (1984), p. 175.
2. Д. Д. Сукачев, Успехи физических наук **191**(10), 1077 (2021), раздел **6.2** *"Доверенные узлы"*.
3. И. М. Арбеков, С. Н. Молотков, Математические вопросы крипографии **14**(4) (2022), в печати.
4. С.Н.Молотков, Письма в ЖЭТФ **117**, 470 (2023).

5. Q. Zhang, F. Xu, Y.-A. Chen, C.-Zh. Peng, and J. Pan, Opt. Express **26**, 24260 (2018).
6. https://www.youtube.com/watch?v=0WAuDcYhKbo.
7. К. А. Балыгин, С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **116**, 128 (2022).
8. H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
9. H.-K. Lo, M. Curty, and B. Qi, Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.108.130503.
10. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
11. H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
12. M. Tomamichel and R.Renner, Phys. Rev. Lett. **106**, 110506 (2011).
13. M. Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, PhD thesis, ETH Zürich (2012); arXiv/quant-ph:1203.2142.
14. D. Mayers, J. ACM, **48**, 351 (2001).
15. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
16. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, arxiv/quant-ph:9604024.
17. M. Koashi and A. Winter, Phys. Rev. A **69**, 022309 (2004).
18. R. Renner, *Security of Quantum Key Distribution*, PhD thesis, ETH Zürich (2005); arXiv/quant-ph:0512258.
19. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 1 (2012).
20. P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002-1 (2017).
21. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ, **85**, 632 (2007).
22. S. N. Molotkov, Laser Phys. Lett. **18**, 045202 (2021).
23. С. Н. Молотков, ЖЭТФ **160**, 327 (2021).
24. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).
25. Y.-H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).
26. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, М. (2010).
27. K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory*, Springer, Berlin, Heidelberg (1983).
28. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
29. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
30. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).