Письма в ЖЭТФ, том 120, вып. 1, с. 17 – 25

Интерференция Hong-Ou-Mandel в квантовой оптике, моногамия запутанности, неортогональность, недоверенные узлы

С. П. Кулик[+], *С. Н. Молотков*[*1)]

[+]*Центр квантовых технологий, МГУ имени М. В. Ломоносова, 119991 Москва, Россия*

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

Поступила в редакцию 5 июня 2024 г.
После переработки 6 июня 2024 г.
Принята к публикации 5 июня 2024 г.

В последнее десятилетие активно исследуются системы квантового распределения ключей с недоверенным промежуточным узлом, протокол квантового распределения ключей был назван MDI (Measurement Device Independent). В ранних работах были приведены лишь соображения, почему такая система квантового распределения ключей 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. *По этой причине, несмотря на имеющиеся экспериментальные реализации системы квантового распределения ключей MDI, продолжают возникать вопросы о физических причинах стойкости такого протокола.* Такие системы квантового распределения ключей 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. В работе приведен анализ MDI протокола, показаны физические причины стойкости протокола, которые основаны на таких фундаментальных свойствах, как интерференция фотонов из разных источников, моногамия запутанности, неортогональность состояний. *Приведен простой и явный вывод, показывающий эквивалентность MDI и BB84 протоколов и физические причины совпадения выражений для длины финального ключа.*

DOI: 10.31857/S1234567824130044, EDN: HMMNJY

Введение. Идея MDI (Measurement Device Independent) квантового распределения ключей (КРК) была предложена в работе [1, дополнительный материал], в работах [1,доп.материал] 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 [2–9].

В квантовой оптике существует замечательный эффект, который называют интерференцией Hong-Ou-Mandel (HOM) [10] и, который связан с *различимостью/неразличимостью фотонов при преобразовании на светоделителе.* Следующий эффект, который получил название *моногамии квантовой запутанности* и, связан с тем, что *пара частиц, находящихся в максимально запутанном состоянии, не может быть запутана – коррелирована с третьей квантовой системой [11].* Еще одно свойство квантовых состояний, которое играет принципиальную роль в квантовой криптографии и, которое гарантирует на уровне фундаментальных законов квантовой механики, детектирование вторжений в квантовый канал связи, это *свойство неортогональности [12].*

В последнее десятилетие в связи с развитием сетей с квантовым распределением ключей (КРК) появились новые протоколы [1, дополнительный материал]. В сетях возможно распределение ключей через доверенные узлы [13–17], на которых работа аппаратуры недоступна нарушителю. Однако квантовая теория позволяет распределять ключи через недоверенные узлы, т.е. узлы, на которых работа аппаратуры известна нарушителю [1, дополнительный материал], что представляетя далеко не очевидным. Такой протокол был предложен 10 лет назад [1, дополнительный материал], однако детального исследования причин стойкости такого протокола приведено не было [1, дополнительный материал]. Фактически для анализа протокола были приведены формулы, которые ранее использовались для протокола КРК BB84 в конфигурации точка-точка [1, дополнительный материал, 2–9]. Впоследствии появились экспериментальные реализации таких систем.

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

Несмотря на это, до сих пор высказываются сомнения и недопонимание причин, которые гарантируют стойкость протокола. По-видимому, это связано с тем, что анализ стойкости протокола не был доведен до фундаментальных первопричин.

В работе [18] был приведен анализ протокола и получен точный результат, который использует фундаментальные энтропийные соотношения неопределенностей [19–23]. Данные соотношения позволяет не перебирать различные атаки на передаваемые состояния, поэтому точное решение является неявным. Энтропийные соотношения неопределенностей связывают утечку информации с возмущением квантовых состояний и ошибками на приемной стороне. Утечка информации через побочные каналы связи часто не приводит к возмущению информационных квантовых состояний, поэтому учет утечки информации через побочные каналы связи находится за пределами энтропийных соотношений неопределенностей [23]. По этой причине для учета побочных каналов утечки информации в системах КРК требуется уметь строить явные атаки нарушителя на состояния в квантовом канале связи [24].

Ниже мы приведем анализ протокола и продемонстрируем явные физические причины стойкости протокола, которые базируются на упомянутых выше фундаментальных явлениях – интерференции HOM, моногамии запутанности и неортогональности квантовых состояний. Будет также приведено явное сведение протокола распределения ключей через недоверенные узлы к классическому протоколу BB84 – распределению ключей в конфигурации точка-точка.

Интерференция HOM из двух источников. Пусть имеются два независимых источника квантовых однофотонных состояний Алисы и Боба (рис. 1). Пусть источники порождают фоковские состояния, которым отвечают операторы рождения a_i^+ и b_j^+, индексы i, j отвечают различным состояниям поляризации $i = h, v$ $j = h, v$, которое могут принимать состояния. Состояния подвергаются следующим преобразованиям.

Преобразование на поляризационно-независимом симметричном светоделителе.

Преобразование операторов имеет вид

$$a_i^+ \to \frac{1}{\sqrt{2}}\left(c_i^+ + d_i^+\right), \quad b_j^+ \to \frac{1}{\sqrt{2}}\left(c_j^+ - d_j^+\right). \qquad (1)$$

Для состояний в двух каналах светоделителя c, d получаем

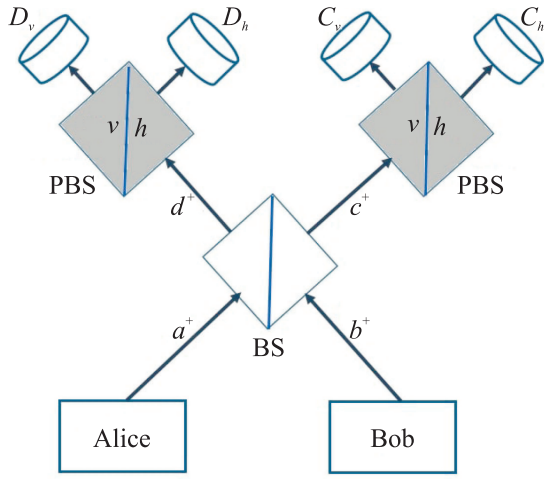

Рис. 1. (Цветной онлайн) Схема детектирования состояний на недоверенном узле. Обозначения: BS – поляризационно-нечувствительный симметричный 50/50 светоделитель, PBS – поляризационный светоделитель, D_v, D_y, C_V, C_h – детекторы

$$|\psi^{\text{out}}\rangle_{CD} = U_{BS}|\Psi_{\text{in}}\rangle_{ab} = U_{BS}\left(a_i^+ b_j^+ |\text{vac}\rangle_{ab}\right) = \\ = \frac{1}{2}\left(c_i^+ c_j^+ + c_j^+ d_i^+ - c_i^+ d_j^+ - d_i^+ d_j^+\right)|\text{vac}\rangle_{cd}, \qquad (2)$$

Состояния на выходе светоделителя BS (рис. 1) зависят от поляризаций фотонов.

1) Фотоны имеют различные поляризации – различимые по поляризациям фотоны $i \neq j$, пусть $i = h$, $j = v$. В этом случае на выходах c, d светоделителя будет *общее заутанное состояние*

$$|\psi^{\text{out}}\rangle_{CD} = \qquad (3)$$

$$= \frac{1}{2}\left(c_h^+ c_v^+ + c_v^+ d_h^+ - c_h^+ d_v^+ - d_h^+ d_v^+\right)|\text{vac}\rangle_{cd} =$$

$$= \frac{1}{2}\left(|h\rangle_c|v\rangle_c + |v\rangle_c|h\rangle_d - |h\rangle_c|v\rangle_d - |h\rangle_d|v\rangle_d\right).$$

После прохождения состояний из канала D через поляризационный светоделитель PBS (рис. 1), поляризационные компоненты состояния (1), (2) h и v направляются на выходы D_h и D_v, соответственно. Аналогично для компонент поляризации состояния в канале C.

Таким образом, при различных поляризациях фотонов будут иметь место *совпадение отсчетов одновременно в двух детекторах с одинаковой вероятностью.* Детекторы, в которых будет совпадение отсчетов при $i \neq j$ приведены в строках 1 и 2 табл. 1. Например, состояния Алисы $|v\rangle_A$, и Боба $|h\rangle_B$, тогда будут отсчеты в одном из 4-х вариантов двух детекторов: C_vC_h, C_vD_h, C_hD_v, D_hD_v (см. табл. 1).

Таблица 1. Детекторы, в которых будет регистрация в зависимости от входной поляризации состояний Алисы и Боба в прямом и сопряженном базисах. Приведены также вероятности отсчетов в различных детекторах, и соответствующие значения логических битов, для различных квантовых состояний

N	Состояние Алисы	Состояние Боба	Отсчет детектора	Вероятность отсчета	Значение бита Алисы–Боба
1	$\|v\rangle_A$	$\|h\rangle_B$	$C_vC_h,\ C_hD_v,\ C_vD_h,\ D_vD_h$	$\frac{1}{4}4=1$	1
2	$\|h\rangle_A$	$\|v\rangle_B$	$C_vC_h,\ C_hD_v,\ C_vD_h,\ D_vD_h$	$\frac{1}{4}4=1$	0
)	$\|h\rangle_A$	$\|h\rangle_B$	$C_hC_h,\ D_hD_h$	$\frac{1}{2}2=1$	–
4	$\|v\rangle_A$	$\|v\rangle_B$	$C_vC_v,\ D_vD_v$	$\frac{1}{2}2=1$	–
5	$\|ad\rangle_A$	$\|ad\rangle_B$	$C_hC_v,\ D_hD_v$	$\frac{1}{4}2=\frac{1}{2}$	0
6	$\|d\rangle_A$	$\|d\rangle_B$	$C_hC_h,\ C_vC_v,\ D_hD_h,\ D_vD_v$	$\frac{1}{4}2=\frac{1}{2}$	–
7	$\|ad\rangle_A$	$\|d\rangle_B$	$C_hD_v,\ C_vD_h$	$\frac{1}{4}2=\frac{1}{2}$	1
8	$\|d\rangle_A$	$\|ad\rangle_B$	$C_hC_h,\ C_vC_v,\ D_hD_h,\ D_vD_v$	$\frac{1}{4}2=\frac{1}{2}$	–

Такие же парные отсчеты в детекторах будут, если состояние Алисы $|h\rangle_A$, а Боба $|v\rangle_B$. Данное обстоятельство принципиально для протокола распределения ключей с недоверенным узлом. Это означает, что нарушитель, зная отсчеты в паре детекторов не знает какие состояния посылали Алиса и Боб, поскольку отсчеты от состояний $|h\rangle_A$, $|v\rangle_B$ или $|v\rangle_A$, $|h\rangle_B$ Алисы и Боба одинаковые (см. ниже).

2) Фотоны имеют одинаковые поляризации – неразличимые фотоны, $i=j$, $i=j=h$ или $i=j=v$. На выходах c,d светоделителя будет общее запутанное состояние

$$|\psi^{\rm out}\rangle_{CD} = \tag{4}$$

$$= \frac{1}{2}\left(c_i^+c_i^+ + c_i^+d_i^+ - c_i^+d_i^+ - d_i^+d_i^+\right)|{\rm vac}\rangle_{cd} =$$

$$= \frac{1}{2}\left(|i\rangle_c|i\rangle_c - |i\rangle_d|i\rangle_d\right),$$

оба фотона синхронно "идут" в каналы c и d, что является проявлением неразличимости частиц – статистики Бозе–Эйнштейна. В этом и состоит эффект интерференция HOM [10].

После прохождения состояний из канала D через поляризационный светоделитель PBS (рис. 1), обе одинаковые поляризационные компонеты состояния (2) – *оба фотона* направляются на выход D_h при поляризации h, и *оба фотона* на выход D_v при поляризации v.

Таким образом, при одинаковых поляризациях фотонов, будут *отсчеты от обоих фотонов только в одном из детекторов*, т.е *совпадения отсчетов одновременно в двух разных детекторах не будет* (см. табл. 1, строки 3 и 4).

Состояния с одинаковой поляризацией не дают вклада в ключ – не используются в протоколе КРК, двойные отсчеты в одном из детекторов отбрасываются, поскольку по отсчету в детекторе с h или с v можно достоверно сказать какие состояния, соответственно, какие логические биты, посылались Алисой и Бобом.

Выше были приведены преобразования состояний в прямом базисе. В сопряженном базисе диагональные d и антидиагональные ad входные состояния Алисы и Боб имеют вид

$$|d\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|h\rangle_{A,B} + |v\rangle_{A,B}\right),$$
$$|ad\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|h\rangle_{A,B} - |v\rangle_{A,B}\right). \tag{5}$$

Анализ преобразования состояний в сопряженном базисе аналогичен анализу в прямом базисе. *Для дальнейшего важно, что отсчеты в детекторах в сопряженном базисе такие же, как прямом (см. табл. 1, строки 5–8).*

Преобразование информационных состояний, свойство моногамии парной запутанности. Прежде, чем рассмотреть атаку Евы на передаваемые состояния, рассмотрим преобразование состояний без нарушителя. Для дальнейшего удобнее ввести более привычные для квантовой криптографии обозначения информационных состояний. В прямом базисе + обозначим состояния как

$$|v\rangle \to |0\rangle, \quad |h\rangle \to |1\rangle, \tag{6}$$

соответственно обозначим информационные состояния в сопряженном базисе $\times$

$$|d\rangle \to |0^\times\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$
$$|ad\rangle \to |1^\times\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{7}$$

Рассмотрим, какие отсчеты будут при посылке состояний Алисой и Бобом в отсутствии Евы.

Посылка состояний на недоверенный узел в базисе +:

$|0\rangle_A|0\rangle_B$ и $|1\rangle_A|1\rangle_B$ – парные отсчеты только в одном детекторе (4), такие отсчеты отбрасываются.

$|0\rangle_A|1\rangle_B$, $|1\rangle_A|0\rangle_B$ – удобно представить такие состояния как $|\Psi^+\rangle_{AB}$, $|\Psi^-\rangle_{AB}$, как обычно $|\Psi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}\,(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B)$, что будет отвечать отсчетам по совпадению в каналах (3), что отвечает *проекциям на запутанные состояния за счет перепутывания входных состояний светоделителями.*

В отсутствии возмущения состояний имеются идеальные корреляции между битами Алисы и Боба. При вторжении Евы в канал связи – атака на состояния $|0\rangle_A|1\rangle_B$ или $|1\rangle_A|0\rangle_B$ приводит к нарушению идеальных корреляций. Самая общая атака Евы сводится к запутыванию вспомогательного состояния Евы (ancilla) с состояниями Алисы и Боба. Свойство моногамии парной запутанности [11] гарантирует, что любое запутывание пары состояний с третьим, приводит к нарушению идеальной запутанности, а значит и к нарушению идеальных корреляций между битом Алисы и Боба, т.е. к ошибкам. Фактически свойство парной запутанности на недоверенном узле является физической причиной, гарантирующей обнаружение любых вторжений в квантовый канал. Важно еще раз отметить, что без вторжения в канал связи, даже знание в каких детекторах произошел отсчет не дают Еве никакой информации о передаваемых битах. Действительно, состояния $|0\rangle_A|0\rangle_B$ и $|1\rangle_A|1\rangle_B$ дают одинаковые отсчеты (3). При этом Алиса и Боб, зная отсчеты детекторов и зная, что они посылали, могут достоверно сказать, какой бит посылал партнер, и привязаться к одному из битов, например, к биту Алисы.

$|0^\times\rangle_A|0^\times\rangle_B = \frac{1}{2}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}\,(|\Phi^+\rangle_{AB} + |\Psi^+\rangle_{AB})$, – отсчеты будут в канале $|\Psi^+\rangle_{AB}$.
$|1^\times\rangle_A|1^\times\rangle_B = \frac{1}{2}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B - |0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}\,(|\Phi^+\rangle_{AB} - |\Psi^+\rangle_{AB})$, – отсчеты будут в канале $|\Psi^+\rangle_{AB}$.

Посылка состояний на недоверенный узел в сопряженном базисе ×:

Состояния в базисе × также можно представить как суперпозицию пар запутанных состояний. $|\Phi^+\rangle_{AB}$, $|\Phi^-\rangle_{AB}$, где $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\,(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B)$.

$|0^\times\rangle_A|1^\times\rangle_B = \frac{1}{2}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B - |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}\,(|\Phi^-\rangle_{AB} - |\Psi^-\rangle_{AB})$. Канал $|\Phi^+\rangle_{AB}$ – отсчеты будут только в одном детекторе (4), такие отсчеты отбрасываются. Канал $|\Psi^+\rangle_{AB}$ – отсчеты будут по совпадению двух детекторах (3).

$|1^\times\rangle_A|0^\times\rangle_B = \frac{1}{2}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B + |0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}\,(|\Phi^-\rangle_{AB} + |\Psi^-\rangle_{AB})$. Отсчеты аналогичны ситуации с посылкой состояний $|0^\times\rangle_A|1^\times\rangle_B$. Так же, как и в базиисе +, доступ к отсчетам в дух детекторах в базисе × по схеме совпадения (3) без вторжения в квантовый канал, не дает Еве никакой информации о передаваемых битах Алисы и Боба, поскольку отсчеты для состояний $|0^\times\rangle_A|1^\times\rangle_B$ и $|1^\times\rangle_A|0^\times\rangle_B$ одинаковые.

Согласование битов Алисы и Боба. Пусть привязка общего бита идет к биту Алисы.

Базис +.

При посылке состояний $|0\rangle_A|0\rangle_B$ в базисе + без вторжения Евы в квантовый канал отсчеты в детекторах отсутствуют. Вторжение в канал связи приводит к отсчетам в каналах $|\Psi^\pm\rangle_{AB}$ – отсчеты в двух детекторах. В этом случае такие отсчеты являются ошибочными. При наличии отсчета Боб инвертирует свой бит $0 \to 1$. В итоге для такой посылки Алиса имеет бит 0, а Боб ошибочный бит 1. Аналогично при посылке состояний $|1\rangle_A|1\rangle_B$ в базисе +.

Иначе говоря, отсчет в каналах $|\Psi^\pm\rangle_{AB}$ при передаче состояний $|1\rangle_A|1\rangle_B$ или $|0\rangle_A|0\rangle_B$ будет ошибочным. Зная этот факт, нарушителю нет никакого смысла производить ошибки в тех посылках, когда Алиса и Боб посылали $|1\rangle_A|1\rangle_B$ или $|0\rangle_A|0\rangle$. Посылки, в которых посылались Алиса и Боб посылали одинаковые состояния, Ева может узнать, используя невозмущающие (nondemolishing) измерения (см. ниже). После обнаружения в канале состояний $|1\rangle_A|1\rangle_B$ или $|0\rangle_A|0\rangle$ Ева перепосылает их на недоверенный узел, состояния дают отсчеты только в одном из детекторов, которые отбрасываются и не участвуют в формировании ключа. Неформально говоря, в таких посылках Ева действует на состояния "прозрачно".

При посылке состояний $|0\rangle_A|1\rangle_B$ или $|1\rangle_A|0\rangle_B$ в базисе + в отсутствии нарушителя отсчеты в двух детекторах будут происходить равновероятно как в канале $|\Psi^-\rangle_{AB}$, так и в канале $|\Psi^+\rangle_{AB}$. При наличии отсчетов в двух детекторах Боб инвертирует свой бит $0 \to 1$. В итоге в такой посылке Алиса имеет бит 0, а Боб – правильный бит 0, что аналогично посылке состояний $|1\rangle_A|1\rangle_B$ в базисе +.

Таким образом, происходит согласование битов Алисы и Боба для получения общего бита в базисе +.

Базис ×.

При посылке состояний $|0^\times\rangle_A|0^\times\rangle_B$ в базисе × в отсутствии нарушителя отсчеты в детекторах будут

только в канале $|\Psi^+\rangle_{AB}$ – правильный отсчет. У Алисы бит 0, у Боба также бит 0. *Инвертировать свой бит Боб не должен при отсчете в канале* $|\Psi^+\rangle_{AB}$. Аналогично при посылке состояний $|1^\times\rangle_A|1^\times\rangle_B$ в базисе $\times$.

При посылке состояний $|0^\times\rangle_A|1^\times\rangle_B$ в базисе $\times$ в отсутствии нарушителя отсчеты в детекторах будут только в канале $|\Psi^-\rangle_{AB}$ – правильный отсчет. У Алисы бит 0, у Боба после инверсии также бит 1. *Боб инвертирует свой бит при отсчете в канале* $|\Psi^-\rangle_{AB}$. *При отсчете в канале* $|\Psi^+\rangle_{AB}$ *Боб свой бит не инвертирует.*

Аналогично при посылке состояний $|1^\times\rangle_A|0^\times\rangle_B$ в базисе $\times$.

При вторжении в канал связи приводят к отсчетам в каналах $|\Psi^+\rangle_{AB}$, которые будут ошибочными.

Таким образом, происходит согласование битов Алисы и Боба для получения общего бита в базисе $\times$.

Стратегия нарушителя при атаке на передаваемые состояния.

Прежде чем перейти к финальному доказательству эквивалентности протоколов MDI и BB84, обсудим стратегию атаки на квантовые состояния в канале связи. *Напомним, тот факт, что Ева видит отсчеты детекторов на недоверенном узле, без вторжения в квантовый канал связи не дает Еве никакой информации о передаваемых битах Алисы и Боба (см. обсуждение выше).*

Поскольку измерения устроены таким образом, что реализуют только проекции на состояния $|\Psi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B)$ – отсчеты по совпадению в двух детекторах, а двойной отсчеты только в одном детекторе, которые отвечают проекциям на состояния $|\Phi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B)$, отбрасываются, то Ева *предварительно может спроектировать передаваемые состояния на запутанные состояния – сделать неразрушающие измерения состояния пары фотонов.*

Поясним более детально, что имеется в виду.

Пусть Алиса и Боб посылают состояния $|0\rangle_A|0\rangle_B$ или $|1\rangle_A|1\rangle_B$ в базисе $+$. Такие состояния не дадут отсчетов, поскольку измерения сводятся к проекциям на состояния $|\Psi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B)$, и которые не содержат компонент состояний $|0\rangle_A|0\rangle_B$ или $|1\rangle_A|1\rangle_B$.

Отсчеты будут возникать только при посылке Алисой и Бобом состояний $|0\rangle_A|1\rangle_B$ или $|1\rangle_A|0\rangle_B$ в базисе $+$.

По этой причине, если нарушитель сделает *предварительно неразрушающие измерения*, которые задаются разложением единицы $I_{AB} = \mathcal{P}_{\Phi^+} + \mathcal{P}_{\Phi^-} + \mathcal{P}_{\Psi^+} + \mathcal{P}_{\Psi^-}$, и которые имеют два исхода, отвечающие проекциям на $\mathcal{P}_{\Phi^\pm} = |\Phi^\pm\rangle_{AB\,AB}\langle\Phi^\pm|$ и проекциям на $\mathcal{P}_{\Psi^\pm} = |\Psi^\pm\rangle_{AB\,AB}\langle\Psi^\pm|$.

Такие измерения по сути являются неразрушающими (nondemolishing measurements) – измерения не возмущают передаваемых состояний Алисы и Боба.

Если произошел исход в канале $\mathcal{P}_{\Phi^\pm}$, то нарушитель посылает одно из состояний $|\Phi^\pm\rangle_{AB}$, которые не дают ошибочных исходов. Такой перепосыл состояний является *прозрачным, состояния Алисы и Боба (00 или 11) Еве неизвестны, но эти состояния дадут отсчет в только одном детекторе, и будут отброшены.*

Если произошел исход в канале $\mathcal{P}_{\Psi^\pm}$, то Ева также не знает состояния Алисы и Боба (01 или 10), а само измерение их не возмущает.

Поскольку неразрушающие измерения и знание отсчетов детекторов после них не дают Еве никакой информации о передаваемых состояниях, то для того, чтобы получить информацию о передаваемых состояниях, Ева должна производить измерения, которые будут возмущать состояния – производить унитарную атаку (см. ниже).

Разберем теперь, что происходит, когда в канал посылаются состояния в базисе $\times$. *Важно только отметить, что предварительные измерения Евы с проектированием на запутанные состояния, являются невозмущающими, с точки зрения отсчетов детекторов, в любом базисе.*

Если произошел исход в канале $\mathcal{P}_{\Psi^\pm}$, то нарушитель посылает одно из состояний $|\Psi^\pm\rangle$, при этом Ева знает, что это могли быть состояния

$$|0\rangle_A|1\rangle_B,\ \text{либо}\ |1\rangle_A|0\rangle_B,\ \text{либо}\ |0^\times\rangle_A|1^\times\rangle_B, \qquad (8)$$
$$\text{либо}\ |1^\times\rangle_A|0^\times\rangle_B,\ \text{либо}\ |0^\times\rangle_A|0^\times\rangle_B,\ \text{либо}\ |1^\times\rangle_A|1^\times\rangle_B.$$

Если произошел исход в канале $\mathcal{P}_{\Phi^\pm}$, то нарушитель посылает одно из состояний $|\Phi^\pm\rangle$, то Ева знает, что это могли быть состояния

$$|0\rangle_A|0\rangle_B,\ \text{либо}\ |1\rangle_A|1\rangle_B,\ \text{либо}\ |0^\times\rangle_A|1^\times\rangle_B, \qquad (9)$$
$$\text{либо}\ |1^\times\rangle_A|0^\times\rangle_B,\ \text{либо}\ |0^\times\rangle_A|0^\times\rangle_B,\ \text{либо}\ |1^\times\rangle_A|1^\times\rangle_B.$$

Рассмотренные выше предварительные измерения Евы являются невозмущающими и не дают никакой информации о передаваемых битах, но позволяют Еве решить, проводить или нет атаку, уже с возмущением состояний. При исходах в канале $\mathcal{P}_{\Phi^\pm}$, Ева только перепосылает состояния. При исходе в канале $\mathcal{P}_{\Psi^\pm}$ Ева производит атаку на состояния с целью узнать передаваемые бит.

Эквивалентность Measurement Device Independent протокола и протокола Bennett-Brassard 84 (BB84). *Теперь все готово, чтобы*

Таблица 2. Соответствие информационных состояний для протокола BB84 и MDI протокола

Протокол BB84	Протокол MDI
Базис +, $\|0\rangle$, $\|1\rangle$ Базис ×, $\|0^{\times}\rangle = \frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$, $\|1^{\times}\rangle = \frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	Базис +, $\|\overline{0}\rangle_{AB}$, $\|\overline{1}\rangle_{AB}$ Базис ×, $\|\overline{\overline{0^{\times}}}\rangle_{AB} = \frac{\|\overline{0}\rangle_{AB}+\|\overline{1}\rangle_{AB}}{\sqrt{2}}$, $\|\overline{\overline{1^{\times}}}\rangle = \frac{\|\overline{0}\rangle_{AB}-\|\overline{1}\rangle_{AB}}{\sqrt{2}}$

показать формальную эквивалентность MDI протокола и протокола BB84. В отличие от более раннего и неявного доказательства эквивалентности протоколов [18], основанного на фундаментальных энтропийных соотношениях неопределенностей [19–23], ниже приведем доказательство прямым построением, что позволит в дальнейшем включать в рассмотрение побочные каналы утечки информации, которые требуют знания явной атаки Евы (см., например, [24]).

После проектирования имеем следующие состояния:

Базис + – состояния в канале связи:

$|\overline{0}\rangle_{AB} = |01\rangle_{AB}$ логический бит 0,

$|\overline{1}\rangle_{AB} = |10\rangle_{AB}$ логический бит 1,

Состояния $|\overline{0}\rangle_{AB}$ и $|\overline{1}\rangle_{AB}$ *внутри базиса ортогональны* и дают отсчет в канале $|\Psi^{\pm}\rangle_{AB}$.

Боб инвертирует свой бит при отсчете как в канале $|\Psi^{+}\rangle_{AB}$, так и $|\Psi^{+}\rangle_{AB}$. В итоге возникает общий бит. Напомним, что привязка идет к биту Алисы.

Базис × – состояния в канале связи:

Логический бит 0 возникает от состояний $|0^{\times}\rangle_A|0^{\times}\rangle_B$, состояния в канале, которые видит подслушиватель

$$|0^{\times}\rangle_A|0^{\times}\rangle_B \to |\overline{\overline{0}}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\overline{0}\rangle_{AB} + |\overline{1}\rangle_{AB}\right) = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} + |10\rangle_{AB}\right),$$

а логический бит 1 возникает от состояний $|1^{\times}\rangle_A|1^{\times}\rangle_B$, состояния в канале, которые видит подслушиватель

$$|1^{\times}\rangle_A|1^{\times}\rangle_B \to |\overline{\overline{0}}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\overline{0}\rangle_{AB} + |\overline{1}\rangle_{AB}\right) = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} + |10\rangle_{AB}\right).$$

Это то самое место, которое гарантирует секретность ключей в MDI протоколе даже при условии, что Ева видит отсчеты в детекторах. Общий бит 0 или 1 у Алисы и Боба возникает из одних и тех же состояний, которые Ева "видит" в канале связи. Состояния для логического 0 и для логической 1 в канале связи для Евы неразличимы.

При отсчете в канале $|\Psi^{+}\rangle_{AB}$ Боб свой бит не инвертирует, в итоге возникает общий бит с привязкой к биту Алисы.

Состояния для 0 и 1 в канале связи выглядят для подслушивателя одинаково, поэтому зная результат отсчета на недоверенном узле, нарушитель не знает передаваемого бита в отличии от Алисы и Боба, которые знают, какие состояния они посылали.

Логический бит 0 также возникает от состояний $|0^{\times}\rangle_A|1^{\times}\rangle_B$, состояния в канале, которые видит подслушиватель

$$|0^{\times}\rangle_A|1^{\times}\rangle_B \to |\overline{\overline{1}}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\overline{0}\rangle_{AB} - |\overline{1}\rangle_{AB}\right) = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right).$$

Логический бит 1 возникает от состояний $|1^{\times}\rangle_A|0^{\times}\rangle_B$, состояния в канале, которые видит подслушиватель

$$|1^{\times}\rangle_A|0^{\times}\rangle_B \to |\overline{\overline{1}}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\overline{0}\rangle_{AB} - |\overline{1}\rangle_{AB}\right) = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right).$$

Состояния для 0 и для 1 неразличимы для Евы, ситуация аналогична выше рассмотренному случаю.

При отсчете в канале $|\Psi^{-}\rangle_{AB}$ Боб свой бит инвертирует, в итоге возникает общий бит с привязкой к биту Алисы.

Фактически для нарушителя ситуация выглядит как, если бы Алиса и Боб посылали равновероятно одно из 4-х состояний в двух базисах, а именно, состояния: $|\overline{0^{+}}\rangle_{AB}$, $|\overline{1^{+}}\rangle_{AB}$ – базис +; $|\overline{\overline{0^{\times}}}\rangle_{AB}$, $|\overline{\overline{1^{\times}}}\rangle_{AB}$ – базис ×.

Состояния $|\overline{0^{+}}\rangle_{AB}$ и $|\overline{1^{+}}\rangle_{AB}$ ортогональны внутри базиса +, состояния $|\overline{\overline{0^{\times}}}\rangle_{AB}$ и $|\overline{\overline{1^{\times}}}\rangle_{AB}$ ортогональны внутри базиса ×. Состояния из разных базисов попарно неортогональны в полной аналогии с протоколом BB84.

Соответствие состояний для MDI и BB84 протоколов приведены в табл. 2.

Таким образом, имеется формальное один в один соответствие между MDI и BB84 протоколами,

поэтому можно воспользоваться результатами для BB84 при явном построении атаки на протокол MDI.

Любое преобразование квантовых состояний в квантовые состояния является супероператором – вполне положительным отображением (CPM – Completely Positive Map) [25, 26]. Любой супероператор унитарно представим, т.е может быть реализован как исходное состояние с дополнительным вспомогательным состоянием (ancilla) и запутывающим преобразованием, которое *задается унитарным оператором, реализующим унитарную атаку.*

Поскольку *после предварительных невозмущающих измерений* протоколы BB84 и MDI эквивалентны с точностью до изменения обозначений для информационных состояний (см. табл. 2), то для построения явной атаки на протокол MDI можно воспользоваться результатами для протокола BB84 [8]. Пусть Алиса и Боб имеют эталонные состояния (далее индекс $A'B'$), которые они оставляют у себя, а их копии (далее индекс AB) посылают в канал связи на недоверенный узел. Для состояний в базисе + получаем (см. детали в [8, 9])

$$|\overline{0}\rangle_{A'B'}U_{ABE}\left(|\overline{0}\rangle_{AB}|E\rangle\right) = \tag{10}$$
$$= |\overline{0}\rangle_{A'B'}\left\{\sqrt{1-Q}|\overline{0}\rangle_{AB}|\Phi_0\rangle + \sqrt{Q}|\overline{1}\rangle_{AB}|\Theta_0\rangle\right\},$$

$$|\overline{1}\rangle_{A'B'}U_{ABE}\left(|\overline{1}\rangle_{AB}|E\rangle\right) = \tag{11}$$
$$= |\overline{1}\rangle_{A'B'}\left\{\sqrt{1-Q}|\overline{1}\rangle_{AB}|\Phi_1\rangle + \sqrt{Q}|\overline{0}\rangle_{AB}|\Theta_1\rangle\right\},$$

где величина Q имеет смысл вероятности ошибки между битами Алисы и Боба.

В сопряженном базисе $\times$ состояния получаются линейной комбинацией уравнений (6), (7) (см. также табл. 2).

Здесь, во избежании недоразумений, нужно сделать принципиально важный комментарий. Несмотря на формальное соответствие протоколов BB84 и MDI, имеются отличия. В протоколе BB84 состояния $|0,1\rangle_B$, которые направляются от Алисы к Бобу, после атаки Евы и измерений на приемной стороне, доступны Бобу и недоступны Еве.

В (10), (11) также считаем, что состояния в правой части (10), (11) $|\overline{0}\rangle_{AB}$ и $|\overline{1}\rangle_{AB}$ после измерений на недоверенном узле недоступны Еве, хотя Ева и видит отсчеты детекторов. Естественно возникает вопрос – нет ли здесь противоречия, поскольку измерения в MDI протоколе проводятся на недоверенном узле и известны Еве, в отличие от протокола BB84.

Противоречия нет, поскольку, как детально обсуждалось в предыдущих разделах, знание результата измерения – отсчет в канале $|\Psi^{\pm}\rangle$ не дает Еве никакой информации о передаваемой паре бит (0,1) или (1,0) Алисой и Бобом. Информацию о передаваемых битах Ева может получить только из своих вспомогательных состояний $|\Phi_{0,1}\rangle$ и $|\Theta_{0,1}\rangle$. По этой причине, так же как и в протоколе BB84, нужно считать, что состояния $|\overline{0,1}\rangle_{AB}$ недоступны Еве. *Фактически, это связано с тем, что логический бит 0 и 1 в каждом базисе ассоциируется с одним и тем же квантовым состоянием, которое "видит" Ева в канале связи (см. обсуждение выше).*

Данное обстоятельство можно пояснить на теоретико-информационном языке. В известном базисе исходно от Алисы в канал поступает один бит информации 0 или 1, от Боба также один бит 0 или 1. В итоге в канал и на недоверенный узел от Алисы и Боба поступают два бита информации. Измерения на недоверенном узле дают Еве один бит информации, фактически, это бит четности передаваемых битов от Алисы и Боба, так как отсчеты от состояний для битов $(0_A, 1_B)$ и $(1_A, 0_B)$ одинаковые для Евы. Известность результата отсчета дает Еве один бит информации. Один бит остается для Евы неизвестным, неформально говоря, из данного бита формируется общий секретный бит Алисы и Боба, с привязкой общего бита к биту Алисы.

Матрица плотности в базисе + после измерений на недоверенном узле принимает вид

$$\rho_{A'B'ABE} = \tag{12}$$
$$= \frac{1}{2}|\overline{0}\rangle_{A'B'A'B'}\langle\overline{0}\{(1-Q)|\overline{0}\rangle_{ABAB}\langle\overline{0}||\Phi_0\rangle\langle\Phi_0| +$$
$$+ Q|\overline{1}\rangle_{ABAB}\langle\overline{1}||\Theta_0\rangle\langle\Theta_0|\} +$$
$$+ \frac{1}{2}|\overline{1}\rangle_{A'B'A'B'}\langle\overline{1}|\{(1-Q)|\overline{1}\rangle_{ABAB}\langle\overline{1}||\Phi_1\rangle\langle\Phi_1| +$$
$$+ Q|\overline{0}\rangle_{ABAB}\langle\overline{0}||\Theta_1\rangle\langle\Theta_1|\}.$$

Длина ключа определяется через условные квантовые энтропии фон Неймана, последние выражаются через частичные матрицы плотности. Для длины ключа ℓ в асимптотическом пределе длинных последовательностей, аналогично протоколу BB84, находим (см. подробности, например, в [8, 9])

$$\ell = H(\rho_{A'B'E}|\rho_E) - H(\rho_{A'B'AB}|\rho_{AB}), \tag{13}$$
$$H(\rho_{A'B'E}|\rho_E) = H(\rho_{A'B'E}) - H(\rho_E),$$
$$H(\rho_{A'B'AB}|\rho_{AB}) = H(\rho_{A'B'AB}) - H(\rho_{AB}).$$

Частичные матрицы плотности имеют вид

$$\rho_{A'B'E} = \mathrm{Tr}_{AB}\{\rho_{A'B'ABE}\}, \quad \rho_E = \mathrm{Tr}_{A'B'}\{\rho_{A'B'E}\},$$
$$\rho_{A'B'AB} = \mathrm{Tr}_{E}\{\rho_{A'B'ABE}\}, \quad \rho_{AB} = \mathrm{Tr}_{A'B'E}\{\rho_{A'B'ABE}\}.$$

Далее, считаем для экономии места, что детекторы на недоверенном узле имеют одинаковую квантовую эффективность. Решение может быть обобщено для детекторов с разной квантовой эффективностью, например, методом работы [24, 27], что требует большего места. При одинаковых квантовых эффективностях детекторов оптимальным, в смысле – максимальная утечка информации к Еве при данной вероятности ошибки Q, достигается при [5, 8]

$$\langle\Phi_0|\Phi_1\rangle = 1-2Q,\ \langle\Theta_0|\Theta_1\rangle = 1-2Q,\ \langle\Phi_{0,1}|\Theta_{0,1}\rangle = 0, \tag{14}$$

т.е. состояния $|\Phi_{0,1}\rangle$ и $|\Theta_{0,1}\rangle$ лежат в ортогональных подпространствах.

Вычисление длины ключа, в пересчете на одну посылку, с использованием формул (10)–(14), приводят к знаменитой формуле для длины ключа для протокола BB84, которая была получена в нескольких работах разными методами (см. [5–9])

$$\begin{gathered}\ell = (1-h(Q)) - h(Q),\\ h(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q),\end{gathered} \tag{15}$$

где первое слагаемое представляет собой нехватку информации Евы о бите ключа Алисы, второе – нехватку информации Боба о бите Алисы.

Заключение. Таким образом, несмотря на существенно разную структуру протоколов MDI и BB84, явным образом показана формальная эквивалентность MDI и BB84 протоколов, а также детально обсуждены физические причины совпадения выражений для длины финального ключа.

Отметим в заключение, одной из главных мотиваций для MDI протокола служил тот факт, что при недоверенном узле – недоверенных детекторах, и доступности для нарушителя знания отсчетов детекторов, не нужно защищать работу детекторов от внешних вторжений через линию связи, которые могут изменить их штатную работу. Кроме MDI протокола [1, дополнительный материал], существует более простой способ реализовать недоверенные – открытые для нарушителя детекторы [28], который не требует сложных эксперментальных методов достижения интерференции из разных источников.

Наконец, MDI протокол использует на недоверенном узле только элементы линейной оптики. Известно, что в рамках линейной оптики можно реализовать проекции только на пару белловских состояний, такие неполные беллвовские измерения используются также в квантовой телепортации [29]. Для реализаии полных белловских измерений приходится использовать нелинейные оптические элементы, что впервые в экспериментах по телепортации было реализвано в [30].

Выражаем благодарность И. М. Арбекову, В. Л. Елисееву, А. В. Уривскому за интерес к работе, обсуждения и замечания, коллегам по Академии криптографии Российской Федерации и сотрудникам ИнфоТекс и СФБ Лаборатории, которые фактически инициировали данную работу для поддержки экспериментальных исследований.

Финансирование работы. Работа выполнялась в рамках госзадания. Никаких дополнительных грантов на проведение или руководство данным конкретным исследованием получено не было.

Конфликт интересов. Авторы данной работы заявляют, что у них нет конфликта интересов.

1. H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012); Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.108.130503.
2. 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.
3. D. Mayers, J. ACM, **48**, 351 (2001).
4. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
5. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
6. R. Renner, arXiv/quant-ph:0512258 (2005).
7. M. Tomamichel, Ch. C. W. Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 1 (2012).
8. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
9. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).
10. C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
11. M. Koashi and A. Winter, Phys. Rev. A **69**, 022309 (2004).
12. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
13. Д. Д. Сукачев, Успехи физических наук **191**(10), 1077 (2021), раздел **6.2** *Доверенные узлы*.
14. И. М. Арбеков, С. Н. Молотков, Математические вопросы крипографии **14**(3), 9 (2023).
15. С. Н. Молотков, Письма в ЖЭТФ **117**, 470 (2023).
16. Q. Zhang, F. Xu, Y.-A. Chen, C.-Zh. Peng, and J. Pan, Opt. Express **26**, 24260 (2018).
17. https://www.youtube.com/watch?v=0WAuDcYhKbo
18. С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **118**, 62 (2023).
19. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
20. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

21. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
22. M. Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, PhD thesis, ETH Zürich (2012); arXiv/quant-ph:1203.2142.
23. P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002-1 (20017).
24. С. Н. Молотков, ЖЭТФ **160**, 327 (2021).
25. K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory*, Springer Verlag, Berlin (1983).
26. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, М. (2010).
27. S. N. Molotkov, Laser Phys. Lett. **18**, 045202 (2021).
28. К. А. Балыгин, С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **116**, 128 (2022).
29. D. Bouwmeester, J-W. Pan, K.Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).
30. Y.-H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).