УДК 003.26:621.39+530.145

Василиу Е.В., Мамедов Р.С.
Vasiliu E.V., Mamedov R.S.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ И СТОЙКОСТИ К НЕКОГЕРЕНТНЫМ АТАКАМ КВАНТОВЫХ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ПЕРЕДАЧЕЙ МНОГОМЕРНЫХ КВАНТОВЫХ СИСТЕМ

COMPARATIVE ANALYSIS OF EFFICIENCY AND RESISTANCE AGAINST NOT COHERENT ATTACKS OF QUANTUM KEY DISTRIBUTION PROTOCOLS WITH TRANSFER OF MULTIDIMENSIONAL QUANTUM SYSTEMS

Аннотация. Проведено сравнительное исследование эффективности и стойкости к некогерентным атакам квантовых протоколов распределения ключей с передачей кудитов типа "приготовление – измерение" и протоколов с перепутанными кудитами с целью определения оптимальных протоколов. Показано, что стойкость к полупрозрачной некогерентной атаке протоколов типа "приготовление – измерение" и протоколов с перепутанными кудитами приблизительно одинакова. Оптимальными одновременно по критериям стойкости и эффективности являются протоколы с наибольшей эффективностью – это протоколы типа "приготовление – измерение" с использованием двух взаимно несмещенных базисов.

Summary. Comparative research of efficiency and resistance against not coherent attacks of quantum key distribution protocols with qudits transfer of "preparation – measurement" type and protocols with entangled qudits for the purpose of finding of optimum protocols is carried out. It is shown, that resistance against halftransparent not coherent attack of "preparation – measurement" type protocols and protocols with entangled qudits is approximately identical. Simultaneously by criteria of resistance and efficiency the protocols with the greatest efficiency are optimum – the protocols of "preparation – measurement" type with use of two mutually unbiased bases.

Одной из важнейших проблем криптографии с секретным ключом является разработка процедур распределения ключа между пользователями канала связи (Алисой и Бобом). В настоящее время для распределения секретного ключа широко используют схемы с открытым ключом, например, схему цифрового конверта или алгоритм Диффи-Хеллмана [1], обладающие только вычислительной стойкостью, т.е. использующие ограниченность вычислительных мощностей злоумышленника (Евы). Альтернативой таким схемам распределения ключей на основе ассиметричной криптографии являются системы квантового распределения ключей, стойкость которых основана на законах квантовой физики и при определенных условиях является теоретико – информационной [2].

Для достижения теоретико-информационной стойкости квантовых протоколов распределения ключей (КПРК) необходимы оценки количества информации, которая могла попасть к Еве при реализации протокола [2]. Полный учет всех факторов, влияющих на утечку информации, представляет собой крайне сложную задачу и частично выполнен к настоящему времени только для нескольких наиболее простых протоколов, например, протокола BB84 [3]. Поэтому в качестве приближенной оценки рассматривают шенноновскую взаимную информацию между Алисой и Евой $I_{\mathrm{AE}}(D)$, которая является функцией уровня ошибок D, вносимых подслушиванием Евы [4…7].

Другой главной характеристикой КПРК является эффективность, которая показывает, сколько информации может быть использовано для генерации секретного ключа при передаче по каналу связи одной квантовой системы. Одним из путей увеличения эффективности является использование вместо кубитов многоуровневых квантовых систем, называемых кудитами (qudit = quantum dit). Естественно, что эффективность зависит также и от схемы самого протокола.

Предложенные к настоящему времени КПРК (с конечномерными квантовыми системами) можно разделить на два класса: первый основан на передаче одиночных квантовых состояний, относящихся к неортогональным базисам (этот класс протоколов называют "приготовление – измерение") [4…6], а второй – на распределении перепутанных квантовых состояний между пользователями [7]. Стойкость протоколов обоих классов к некоторым видам атак исследована к настоящему времени. Так, в частности, получены зависимости $I_{\mathrm{AE}}(D)$ для атаки "перехват – повторная отправка" кудита [6] и для оптимальной некогерентной атаки [4, 5, 7]. Однако систематического сравнительного исследования всей совокупности предложенных КПРК с кудитами с целью определения оптимального протокола (или класса протоколов) одновременно по критериям стойкости и эффективности не проводилось. Такое исследование является целью настоящей работы.

1. Стратегии атак на протоколы с передачей кудитов. В данной работе мы ограничимся анализом атак, которые доступны Еве в случае, когда источник излучает строго один кудит. В настоящее время такие источники не созданы, однако работы в этом направлении активно ведутся. Пока же, например, для протоколов с кубитами используют слабые когерентные импульсы, излучаемые лазерными светодиодами [2]. Число кубитов (фотонов) в импульсе определяется распределением Пуассона, т.е. часть передаваемых импульсов содержит два и более фотона. Если импульс содержит более одного фотона, то Ева может отвести один фотон из импульса, не влияя на остальные, которые беспрепятственно проходят к Бобу. Тем самым Ева не создает ошибок у Боба при такой атаке, называемой атакой разделения числа фотонов [8]. Отметим, что детальный анализ этой атаки и способов защиты от нее выполнен пока только для протоколов с кубитами [8]. Кроме того, такая атака станет в принципе невозможной, когда в будущем будут созданы источники, излучающее строго один кудит. Поэтому рассмотрим только атаки, которые может применить Ева в случае однокудитных источников. В этом случае доступные Еве атаки подразделяются на два класса [2].

К первому классу относят *некогерентные* атаки. При таких атаках Ева обрабатывает каждый кудит Алисы отдельно. Простейшим вариантом является атака "перехвата – повторной отправки" (*intercept – resend*) кудита, в дальнейшем будем обозначать эту атаку как *IR-атаку*. Ева перехватывает посылаемые Алисой кудиты, измеряет их состояния в одном из используемых легитимными пользователями базисов, а затем отправляет Бобу новые кудиты, приготовленные в измеренных ею состояниях. Поскольку Ева не пропускает кудиты Алисы по квантовому каналу, а излучает новые, такую стратегию подслушивания называют также *непрозрачной*.

Более сложной некогерентной атакой является перепутывание вспомогательных квантовых систем (проб) Евы с пересылаемыми по каналу кудитами. При этом каждый кудит Алисы перепутывается с отдельной пробой независимо от других, а провзаимодействовавшие с пробами кудиты посылаются Бобу. Затем Ева хранит пробы в квантовой памяти и измеряет их состояния по отдельности после того, как закончится открытый обмен сообщениями между Алисой и Бобом на этапе просеивания ключа. Прослушивание открытых сообщений позволяет Еве узнать базис, который использовала Алиса для каждого кудита, и тем самым выбрать оптимальные измерительные процедуры для своих проб, чтобы получить больше информации. Разумеется, состояния кудитов Алисы, с которыми Ева перепутывает свои пробы, изменяются после перепутывания, однако уровень вносимых Евой ошибок при такой атаке в некоторых случаях может быть сделан меньше, чем при непрозрачной атаке. Эту атаку называют также *полупрозрачной*.

Отметим, что при любой некогерентной атаке Ева может уменьшить уровень вносимых ею ошибок за счет уменьшения получаемой ею информации – она должна перехватывать или перепутывать со своими пробами только некоторую часть кудитов Алисы.

Второй класс атак – так называемые *когерентные* атаки, при которых Ева может любым (унитарным) способом перепутать пробу любой размерности с целой группой передаваемых одиночных кудитов [2]. Далее Ева хранит свою большую пробу до тех пор, пока не закончатся все открытые коммуникации между Алисой и Бобом, а затем производит наиболее общее измерение пробы по своему выбору. Отметим, что такие атаки, кроме большой квантовой памяти, могут требовать наличия у Евы многокубитного квантового компьютера (пока не созданного), т.е. в настоящее время технически неосуществимы.

Полный теоретический анализ стойкости КПРК к когерентной атаке выполнен к настоящему времени только для протоколов с кубитами – BB84 и с шестью состояниями [9]. В настоящей работе когерентная атака на протоколы с кудитами не рассматривается.

2. Анализ стойкости к некогерентным атакам протоколов типа "приготовление – измерение" с многомерными квантовыми системами. Рассмотрим сначала простейшую *IR*-атаку на протоколы типа "приготовление – измерение" с передачей кудитов, являющиеся обобщением на многомерные системы протоколов BB84 и с шестью состояниями [6]. В таких протоколах для обеспечения секретности необходимо использовать как минимум два взаимно несмещенных базиса, как в протоколе BB84. Отметим, что взаимно несмещенными (дополнительными) называют два базиса, любые два базисных вектора которых удовлетворяют соотношению $\langle i | j' \rangle = 1/\sqrt{d}$, где i – базисный вектор первого базиса; j' – второго базиса и d – размерность гильбертового пространства.

Известно, что если d является степенью простого числа, то в d-мерном гильбертовом пространстве существует точно $d + 1$ взаимно несмещенных базисов. Таким образом, максимальное количество базисов, которые могут использовать легитимные пользователи, равно $d + 1$. Так, для

двумерного гильбертового пространства таких базисов три. Соответствующий протокол с использованием кубитов и трех взаимно несмещенных базисов называется протоколом с шестью состояниями. Этот протокол обладает несколько большей стойкостью по сравнению с протоколом BB84 как к некогерентной, так и к когерентной атаке, однако его эффективность значительно меньше ($1/2$ для BB84 и $1/3$ бит/кубит для протокола с шестью состояниями соответственно) [10].

Взаимная информация между Алисой и Бобом как функция уровня ошибок D у Боба для протоколов с кудитами определяется выражением [4, 6]:

$$I_{\mathrm{AB}}(D) = \log_2 d + (1 - D)\log_2(1 - D) + D\log_2(D/2), \tag{1}$$

где, как и в последующих формулах для взаимной информации, единицей информации выбран *бит*.

IR-атака была проанализирована в [6] как для случая использования двух, так и для случая использования $d + 1$ взаимно несмещенных базисов. Получены выражения для взаимной информации между Алисой и Евой для этих случаев:

$$I^{(2)}_{\mathrm{AE}\text{-}IR}(D) = \frac{2D}{1 - \frac{1}{d}} \cdot \frac{\log_2 d}{2}, \tag{2}$$

$$I^{(d+1)}_{\mathrm{AE}\text{-}IR}(D) = \frac{D}{\left(1 - \frac{1}{d+1}\right)\cdot\left(1 - \frac{1}{d}\right)} \cdot \frac{\log_2 d}{d+1}. \tag{3}$$

В табл. 1 представлены максимальные уровни ошибок у легитимных пользователей при *IR*-атаке для случаев двух и $d + 1$ базисов, которые определяются выражениями $D^{(2)}_{IR\,\max} = \frac{1}{2}\cdot\left(1 - \frac{1}{d}\right)$ и $D^{(d+1)}_{IR\,\max} = \left(1 - \frac{1}{d+1}\right)\cdot\left(1 - \frac{1}{d}\right)$ соответственно. Максимальный уровень ошибок при такой атаке Ева создает, если перехватывает все пересылаемые по квантовому каналу кудиты.

Таблица 1 – Максимальные уровни ошибок при *IR*-атаке

Размерность гильбертового пространства кудитов, d	2	3	4	5	7	8	9	11	13	16
Максимальный уровень ошибок при использовании двух базисов, %	25	33,3	37,5	40	42,9	43,8	44,4	45,5	46,2	46,9
Максимальный уровень ошибок при использовании $d + 1$ базисов, %	33,3	50	60	66,7	75	77,8	80	83,3	85,7	88,2

Как видно, при *IR*-атаке максимальный уровень создаваемых перехватом ошибок значительно больше при использовании $d + 1$ базисов, чем при использовании только двух. При $d \to \infty$ максимальный уровень ошибок в первом случае стремится к 100%, а во втором – к 50%. Это означает, что использование всех $d + 1$ базисов в протоколе с d-мерными кудитами повышает стойкость протокола к *IR*-атаке. Однако известно, что для протоколов с кубитами *IR*-атака дает подслушивающему агенту меньше всего информации при всех D, т.е. является наименее мощной. Для протоколов с кудитами сравнение *IR*-атаки и некогерентной полупрозрачной атаки во всем интервале уровня ошибок D ранее не проводилось.

Полупрозрачная некогерентная атака на протоколы типа "приготовление – измерение" с передачей кудитов рассмотрена в [4] для случая, когда легитимные пользователи используют $d + 1$ базис. Выражение для взаимной информации между Алисой и Евой имеет вид [4]:

$$I^{(d+1)}_{\mathrm{AE}}(D) = \log_2 d + (1 - D)\left[f(D)\log_2(D) + (1 - f(D))\log_2\frac{1 - f(D)}{d - 1}\right], \tag{4}$$

где

$$f(D) = \frac{d - 2D + \sqrt{(d - 2D)^2 - d^2(1 - 2D)^2}}{d^2(1 - D)}. \tag{5}$$

Аналогичная полупрозрачная атака при использовании легитимными пользователями двух базисов рассмотрена в [5]. Выражение для $I_{\mathrm{AE}}(D)$ имеет вид:

$$I_{\mathrm{AE}}^{(2)}(D) = \log_2 d + F_{\mathrm{E}}(D)\log_2 F_{\mathrm{E}}(D) + (1 - F_{\mathrm{E}}(D))\log_2 \frac{1 - F_E(D)}{d - 1}, \qquad (6)$$

где

$$F_E(D) = \frac{1 - D}{d} + (d - 1)\frac{D}{d} + \frac{2}{d}\sqrt{(d - 1)D(1 - D)}\,. \qquad (7)$$

На рис. 1 проведено сравнение мощности *IR*-атаки и некогерентной полупрозрачной атаки для $d = 4$ и $d = 32$. Видно, что для *IR*-атаки $I_{\mathrm{AE}\text{-}IR}^{(d+1)}(D)$ лежит гораздо ниже $I_{\mathrm{AE}\text{-}IR}^{(2)}(D)$, как и должно быть: так, например, при $d = 32$ в первом случае Ева угадывает один из 33 базисов, а во втором – только один из двух. Подчеркнем, что и Боб при реализации протокола угадывает в первом случае один из 33 базисов, а во втором – один из двух, т.е. для получения ключа могут быть использованы соответственно $1/33$ часть и половина переданных кудитов.

Что касается мощности полупрозрачной атаки, то из рис. 1,а видно, что при $d = 4$ эта атака мощнее *IR*-атаки во всем диапазоне уровня ошибок D как при использовании $d + 1$ базисов, так и при использовании двух (как и при $d = 2$, см. рис. 1 в [10]). Однако при $d = 32$ (см. рис. 1,б) картина становится иной – полупрозрачная атака (и при использовании $d + 1$, и при использовании двух базисов) несколько слабее *IR*-атаки при использовании двух базисов. Отметим, что такой переход происходит приблизительно при $d = 16$ и такая картина остается справедливой и для бóльших d.

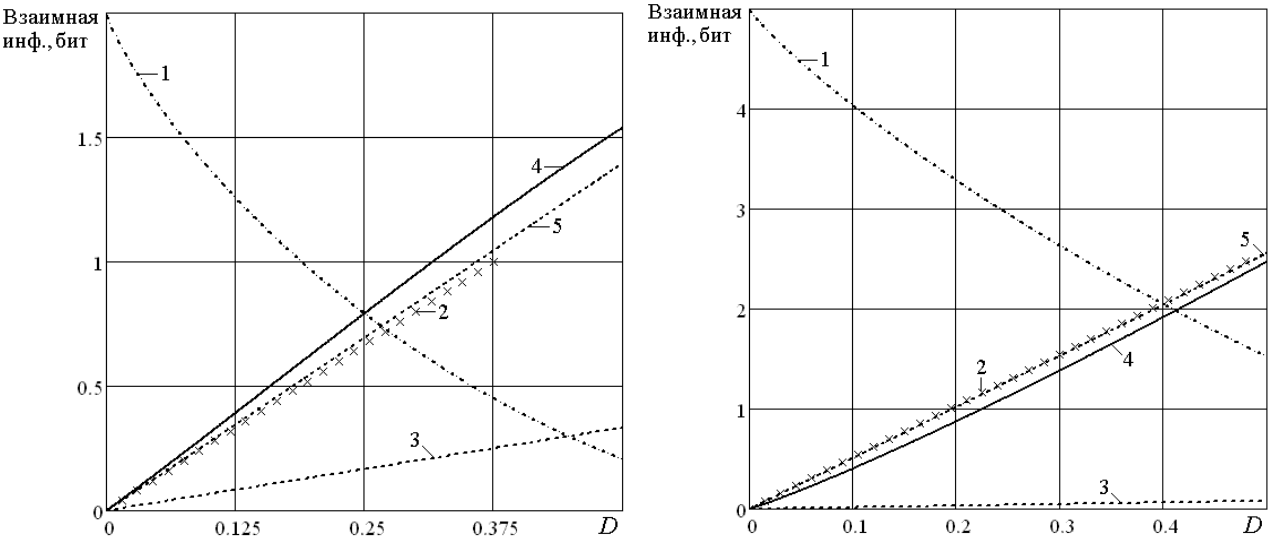


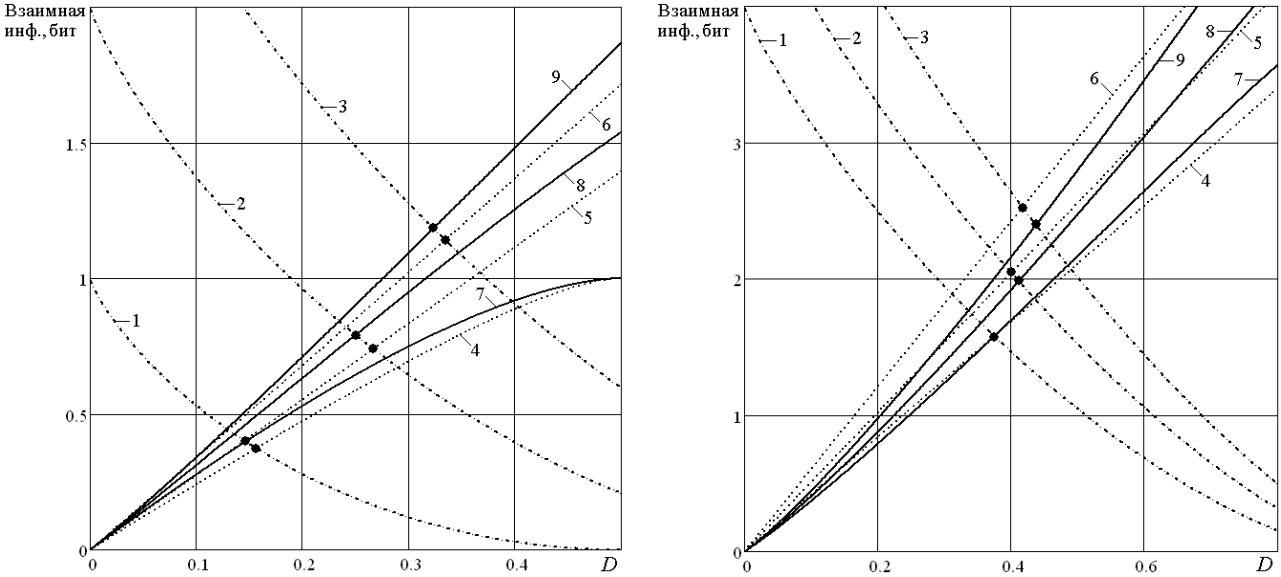
Рисунок 1 – Взаимная информация для *IR*-атаки и некогерентной полупрозрачной атаки:
а) $d = 4$; б) $d = 32$. 1 – $I_{\mathrm{AB}}(D)$ (1); 2 – $I_{\mathrm{AE}\text{-}IR}^{(2)}(D)$ (2); 3 – $I_{\mathrm{AE}\text{-}IR}^{(d+1)}(D)$ (3); 4 – $I_{\mathrm{AE}}^{(2)}(D)$ (6); 5 – $I_{\mathrm{AE}}^{(d+1)}(D)$ (4)

Сравним теперь мощность полупрозрачной атаки для различных d при использовании легитимными пользователями двух или $d + 1$ базисов. На рис. 2,а представлены зависимости $I_{\mathrm{AB}}(D)$ (1), $I_{\mathrm{AE}}^{(d+1)}(D)$ (4) и $I_{\mathrm{AE}}^{(2)}(D)$ (6) для небольших d. Видно, что при небольшой размерности кудитов и при всех значениях D кривые для протоколов с $d + 1$ базисами (кривые 4, 5, 6) лежат ниже соответствующих кривых для протоколов с двумя базисами (кривые 7, 8, 9 соответственно). Это означает, что использование в протоколе всех возможных $d + 1$ взаимно несмещенных базисов обеспечивает несколько большую стойкость протокола к полупрозрачной атаке, чем использование только двух базисов. Однако, как и для протоколов с кубитами [10], разница в информации, которую может получить Ева при использовании двух или $d + 1$ базисов, невелика и составляет максимум несколько процентов (при фиксированном D).

На рис. 2,б показаны те же зависимости для $d = 16$, 32 и 64. Видно, что при $d = 16$ (кривые 4 и 7) полупрозрачная атака дает Еве практически одинаковую информацию независимо от того, два или $d + 1$ базисов используют Алиса и Боб, вплоть до $D \sim 0{,}5$ и только при бóльших D кривые взаимной информации слегка расходятся. При $d = 32$ Ева получит уже несколько больше информации в широком диапазоне уровня ошибок D, если Алиса и Боб используют $d + 1$ базисов (кривые 5 и 8), а

при d = 64 Ева получает больше информации при использовании d + 1 базисов уже при всех D (кривые 6 и 9).

Следовательно, при малой размерности кудитов – до $d \sim 16$ – стойкость протоколов типа "приготовление – измерение" к полупрозрачной некогерентной атаке выше при использовании d + 1 базисов, а при бóльших d наоборот – стойкость протокола выше при использовании двух базисов. При этом разница в информации, которую получит Ева, если в протоколе использовать d + 1 или два базиса, невелика в "рабочей" области протокола, т.е. в области небольшого уровня ошибок D у Алисы и Боба. Отсюда можно сделать вывод, что, в отличие от *IR*-атаки, количество используемых базисов мало влияет на стойкость протокола к полупрозрачной атаке, по крайней мере, при размерности кудитов до d = 64.



а б

Рисунок 2 – Взаимная информация для полупрозрачной некогерентной атаки:
1, 2, 3 – $I_{\mathrm{AB}}(D)$ (1) для d = 2, 4, 8 (а) и d = 16, 32, 64 (б) соответственно;
4, 5, 6 – $I_{\mathrm{AE}}^{(d+1)}(D)$ (4) для d = 2, 4, 8 (а) и d = 16, 32, 64 (б) соответственно;
7, 8, 9 – $I_{\mathrm{AE}}^{(2)}(D)$ (6) для d = 2, 4, 8 (а) и d = 16, 32, 64 (б) соответственно

Таким образом, наш анализ показывает, что стойкость протоколов типа "приготовление – измерение" с многомерными квантовыми системами к *IR*-атаке и к полупрозрачной некогерентной атаке зависит, как от размерности используемых легитимными пользователями квантовых систем (кудитов), так и от количества используемых ими взаимно несмещенных базисов. При небольшой размерности кудитов (до $d \sim 16$) полупрозрачная атака мощнее *IR*-атаки, причем наибольшая разница в мощности этих атак наблюдается для кубитов. С ростом d разница в мощности этих двух атак постепенно уменьшается (только при использовании легитимными пользователями двух базисов) и практически исчезает при d = 16. При большей размерности кудитов и использовании легитимными пользователями двух базисов IR-атака становится мощнее полупрозрачной атаки, причем с ростом d разница в мощности этих атак медленно увеличивается. Интересно отметить, что кривые взаимной информации Алисы и Евы при IR-атаке и использовании двух базисов $I_{\mathrm{AE}\text{-}IR}^{(2)}(D)$ и при полупрозрачной атаке и использовании d + 1 базисов $I_{\mathrm{AE}}^{(d+1)}(D)$ практически полностью совпадают при d > 16 (для d = 32 см, кривые 2 и 5 на рис. 1,б). Мы полагаем, что такое совпадение является случайным. Наконец отметим, что самой слабой является *IR*-атака при использовании Алисой и Бобом d + 1 базисов, причем мощность этой атаки быстро убывает с ростом размерности используемых квантовых систем. Однако при использовании d + 1 базисов так же быстро убывает и эффективность квантового протокола распределения ключа.

3. Анализ стойкости протоколов с многомерными квантовыми системами по критерию Цизара-Кернера. Стек КПРК с кудитами состоит из следующих стадий: передача кудитов по

квантовому каналу связи; исправление ошибок в строках, полученных в результате передачи; оценка утечки информации к Еве; усиление секретности и формирования окончательного ключа. Утечка информации происходит при выполнении первых двух стадий стека.

Сравним стойкость протоколов с многомерными квантовыми системами по критерию, вытекающему из теоремы Цизара и Кернера [11]. Согласно этой теореме, Алиса и Боб могут установить секретный ключ посредством процедуры усиления секретности, если взаимная информация между ними больше взаимной информации между Алисой и Евой, т.е. ключ может быть установлен посредством этой процедуры только в том интервале ошибок D, где $I_{\mathrm{AB}}(D) > I_{\mathrm{AE}}(D)$. Поэтому верхней границей допустимого уровня ошибок считается значение $D_{\max}$, получаемое из равенства $I_{\mathrm{AB}}(D_{\max}) = I_{\mathrm{AE}}(D_{\max})$. При этом пренебрегают возможным небольшим изменением величины $D_{\max}$ при учете утечки информации к Еве на второй стадии протокола – исправлении ошибок.

Таким образом, величину $D_{\max}$, получаемую из равенства $I_{\mathrm{AB}}(D_{\max}) = I_{AE}(D_{\max})$, в квантовой криптографии принято считать критерием стойкости данного протокола к определенной атаке. Отметим, что установка секретного ключа, информация Евы о котором будет пренебрежимо мала, возможна и при $D > D_{\max}$ путем использования процедуры преимущественной дистилляции [2], однако при этом нужно пожертвовать большей частью переданной по квантовому каналу информации (возможно 90% и более), что сильно снижает эффективность всего протокола. Поэтому в КПРК процедуру преимущественной дистилляции обычно не применяют.

На рис. 2 значения $D_{\max}$ для протоколов с разными d и полупрозрачной атаки соответствует точкам пересечения соответствующих кривых и отмечены жирными точками. Видно, что увеличение размерности квантовой системы d значительно увеличивает верхнюю границу уровня ошибок $D_{\max}$, при которой ключ может быть установлен посредством усиления секретности. Учитывая также тот факт, что чем больше d, тем больше информации несет один кудит, можно сделать вывод, что увеличение размерности используемой в протоколе квантовой системы увеличивает, как стойкость, так и эффективность протокола. Что касается вопроса об использовании двух или $d + 1$ базисов, то в первом случае эффективность протокола равна $\frac{\log_2 d}{2}$ бит/кудит и логарифмически растет с ростом d, а во втором случае – равна $\frac{\log_2 d}{d+1}$ бит/кудит и быстро убывает с ростом d, начиная с $d = 5$. Поскольку, как показывает наш анализ, стойкость протокола к полупрозрачной некогерентной атаке при использовании $d + 1$ базисов практически такая же, как и при использовании двух базисов, и при этом практически такая же, как и стойкость к IR-атаке при использовании двух базисов, то окончательный вывод следующий: самым оптимальным из протоколов с кудитами типа "приготовление – измерение" является протокол с квантовыми системами наибольшей доступной (с практической точки зрения) размерности d и использованием двух взаимно несмещенных базисов.

В табл. 2 приведены значения $D_{\max}$ для *IR* и полупрозрачной атак на протоколы типа "приготовление – измерение", полученные с использованием формул (1)…(7), а также для некогерентной атаки клонирования на протоколы с перепутанными кудитами [7]. Видно, что значения в столбцах 3, 4 и 5 становятся практически одинаковыми при $d \sim 16$, что подтверждает сделанные выше заключения. Что касается протоколов с перепутанными кудитами, то атака несимметричного клонирования [7] на эти протоколы имеет практически такую же мощность (по критерию Цизара-Кернера), что и полупрозрачная атака на протоколы типа "приготовление – измерение" (ср. значения в столбцах 4, 5, 6), а атака с симметричным клонированием является несколько более слабой, так как значения $D_{\max}$ при такой атаке выше. Отсюда можно сделать вывод, что протоколы с перепутанными кудитами обладают практически такой же стойкостью к некогерентным атакам, как и протоколы типа "приготовление – измерение".

4. Сравнительный анализ эффективности КПРК с многомерными квантовыми системами. Будем рассматривать эффективность протокола в идеальных условиях, т.е. пренебрегать влиянием на нее потерь в квантовом канале, ошибок, создаваемых подслушиванием, а также уменьшением длины полученного ключа после усиления секретности, поскольку все эти факторы зависят от конкретных условий реализации протокола, а не от его схемы.

Таблица 2 – Значения $D_{\max}$ для некогерентных атак на протоколы с кудитами

Протоколы типа "приготовление – измерение"					Протоколы с перепутанными кудитами	
1	**2**	**3**	**4**	**5**	**6**	**7**
d	$D_{\max}$					
	d+1 базис, *IR*-атака	2 базиса, *IR*-атака	d+1 базис, полупрозрач, атака	2 базиса, полупрозрач, атака	атака несимметрич, клонирования	атака симметрич, клонирования
2	0,22709	0,17054	0,15637	0,14645	0,14645	0,14645
3	0,35885	0,23591	0,22671	0,21132	0,22472	0,23974
4	0,44764	0,27187	0,26656	0,25	0,26582	0,29428
5	0,51245	0,2951	0,2923	0,27639	0,29196	0,32984
7	0,60191	0,324	0,32388	0,31102	0,32377	0,37343
8	0,63436	0,33376	0,33436	0,32322	0,33429	0,38776
9	0,66147	0,34168	0,34278	0,33333	0,34273	0,39916
10	0,68452	0,34826	0,34971	0,34189	0,34968	0,40845
11	0,70437	0,35385	0,35554	0,34924	0,35539	0,41617
13	0,73692	0,36285	0,36484	0,36132	0,36451	0,42825
16	0,77346	0,37281	0,37498	0,375	0,37486	0,44099

Эффективность протоколов типа "приготовление – измерение" при использовании двух и d + 1 базисов равна $\frac{\log_2 d}{2}$ и $\frac{\log_2 d}{d+1}$ бит/кудит соответственно, а эффективность протоколов с перепутанными кудитами [7] равна $\frac{\log_2 d}{8}$ бит/кудит. В табл. 3 приведены значения эффективности протоколов типа "приготовление – измерение" и протоколов с перепутанными кудитами для $d = 2\ldots16$.

Таблица 3 – Эффективность протоколов, бит/кудит

d	2	3	4	5	7	8	9	11	13	16
Протоколы "приготовление–измерение", 2 базиса	0,5	0,792	1,0	1,161	1,404	1,5	1,585	1,73	1,85	2,0
Протоколы "приготовление–измерение", d+1 базис	0,333	0,396	0,4	0,387	0,351	0,333	0,317	0,288	0,264	0,235
Протоколы с перепутанными кудитами	0,125	0,198	0,25	0,29	0,351	0,375	0,396	0,432	0,463	0,5

Как видно из таблицы, при $d < 7$ эффективность протоколов "приготовление – измерение" выше эффективности протоколов с перепутанными кудитами, а при бóльших d эффективность первых при использовании d + 1 базисов становится меньше эффективности вторых, но при использовании в первых двух базисов остается больше. Следовательно, при небольших d протоколы типа "приготовление – измерение", независимо от количества используемых базисов, эффективнее протоколов с перепутанными кудитами. При больших d наиболее эффективны протоколы "приготовление – измерение" с двумя базисами, затем протоколы с перепутанными кудитами и наконец, наименьшую эффективность имеют протоколы "приготовление – измерение" с d + 1 базисами. Поскольку, как следует из вышеприведенного анализа, стойкость всех этих протоколов к полупрозрачной некогерентной атаке приблизительно одинакова, то мы можем обобщить сделанный ранее вывод о преимуществе протоколов типа "приготовление – измерение" с двумя базисами и по отношению к протоколам с перепутанными кудитами. А именно – при одновременном учете эффективности и стойкости к некогерентным атакам оптимальными из всех типов протоколов с кудитами являются протоколы типа "приготовление – измерение" с использованием двух взаимно несмещенных базисов.

В заключение отметим следующее. Проведено сравнительное исследование протоколов с

передачей кудитов типа "приготовление – измерение" с использованием $d + 1$ и двух взаимно несмещенных базисов, а также протоколов с перепутанными кудитами одновременно по критериям эффективности протокола и его стойкости к некогерентным атакам с целью определения оптимальных протоколов. Показано, что при небольшой размерности кудитов (до $d \sim 16$) полупрозрачная атака на протоколы "приготовление – измерение" мощнее *IR*-атаки, причем наибольшая разница в мощности этих атак наблюдается для кубитов. С ростом d разница в мощности этих двух атак постепенно уменьшается (при использовании легитимными пользователями двух базисов) и практически исчезает при $d = 16$. При большей размерности кудитов и использовании двух базисов IR-атака становится мощнее полупрозрачной атаки, причем с ростом d разница в мощности этих атак медленно увеличивается. Самой слабой является IR-атака при использовании легитимными пользователями $d + 1$ базисов, причем мощность этой атаки быстро убывает с ростом размерности d используемых квантовых систем.

Показано также, что стойкость к полупрозрачной некогерентной атаке протоколов типа "приготовление – измерение" и протоколов с перепутанными кудитами приблизительно одинакова (при заданном d), следовательно, *оптимальными* по критериям стойкости и эффективности будут протоколы *с наибольшей эффективностью*. Таковыми являются протоколы типа "приготовление – измерение" с использованием двух взаимно несмещенных базисов.

Литература

1. *Бернет С.* Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. – М.: ООО "Бином-Пресс", 2007. – 384 с.
2. *Quantum* cryptography / Gisin N., Ribordy G., Tittel W., Zbinden H. // Reviews of Modern Physics. – 2002. – V. 74. – №1. – P. 145 – 195.
3. *Lutkenhaus N.* Estimates for practical quantum cryptography / Lutkenhaus N. // Physical Review A. – 1999. – V. 59. – №5. – P. 3301 – 3319.
4. *Bruß D*. Optimal eavesdropping in cryptography with three-dimensional quantum states / D. Bruß, C. Macchiavello // Physical Review Letters. – 2002. – V. 88. – №12. – Art. 127901.
5. *Security* of quantum key distribution using d-level systems / [Cerf N.J., Bourennane M., Karlsson A., Gisin N.] // Physical Review Letters. – 2002. – V. 88. – №12. – Art. 127902.
6. *Bourennane M*. Quantum key distribution using multilevel encoding / Bourennane M., Karlsson A., Bjork G.// Quantum Communication, Computing, and Measurement 3. – N.Y.: Springer US, 2002. – P. 295 – 298.
7. Security of quantum key distributions with entangled qudits / [Durt T., Kaszlikowski D., Chen J.-L., Kwek L.C.] // Physical Review A. – 2004. – V. 69, №3. – Art. 032313.
8. *Niederberger A.* Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography / Niederberger A., Scarani V., Gisin N. // Physical Review A. – 2005. – V. 71. – №4. – Art. 042316.
9. *Hwang W.* Eavesdropper's optimal information in variations of Bennett–Brassard 1984 quantum key distribution in the coherent attacks / Hwang W., Ahn D., Hwang S. // Physics Letters A. – 2001. – V. 279, № 3 – 4. – P. 133 – 138.
10. *Василиу Е.В.* Стойкость квантовых протоколов распределения ключей типа "приготовление – измерение" [Электронный ресурс] / Е.В. Василиу // Georgian Electronic Scientific Journal: Computer Science and Telecommunications. – 2007. – № 2(13). – С. 50 – 62. – Режим доступа к журн.: http://gesj.internet-academy.org.ge/gesj_articles/1306.pdf
11. *Csiszar I*. Broadcast channels with confidential messages / I. Csiszar, J. Korner // IEEE Trans. on Inform. Theory. –1978. – V. IT-24. – № 3. – P. 339 – 348.