зультатам моделирования осуществляется визуализация распространения возбуждения на поверхности сердца пациента.

Литература

1. Сердечно − сосудистые заболевания. Информационный бюллетень N°317. // Сайт Всемирной организации здравоохранения [Электронный ресурс]. – 2013. – Режим доступа: http://www.who.int/mediacentre/factsheets/fs317/ru/index.html. – Загл. с экрана.
2. Alexander Muirhead // Wikipedia.com: [Электронный ресурс]. – режим доступа: http://en.wikipedia.org/wiki/Alexander_Muirhead(дата обращения: 11.02.2014).
3. Сердце человека // Wikipedia.ru: [Электронный ресурс]. – режим доступа: http://ru.wikipedia.org/wiki/Сердце_человека (дата обращения: 18.02.2014)
4. Простейшие модели возбудимых сред // Mathematical Cell: [Электронный ресурс]. – режим доступа: http://www.mathcell.ru/ru/obzors/obzor_Elkin2 (дата обращения: 10.03.2014)

АНАЛИЗ СТОЙКОСТИ КВАНТОВЫХ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

В.А. Эттель, доц, к.т.н., А.Н. Кайралапова, магистрант
Карагандинский государственный технический университет
100000,г. Караганда, Бульвар мира, 56, тел.:+7(7212)567592
E-mail:aknur_kan91@mail.ru

Квантовая криптография как наука зародилась в 1984 году, когда был разработан первый квантовый протокол распределения ключей, названный BB84 [1]. В настоящее время квантовая криптография включает несколько разделов: квантовые протоколы распределения ключей (КПРК), квантовые протоколы защищенной прямой связи, аутентификацию квантовых сообщения и квантовую цифровую подпись.

Квантовое распределение ключей – метод, с помощью которого между двумя абонентами (Алиса и Боб) может быть распределен секретный ключ, если они имеют доступ к квантовому каналу связи, т.е. каналу для передачи отдельных квантовых частиц, например, фотонов, и открытому обычному каналу с возможностью аутентификации отправителя сообщения. Основным преимуществом квантового распределения ключей перед обычными классическими схемами является принципиальная возможность обнаружить подслушивающего агента, который, в силу законов квантовой физики, при подслушивании вынужден возмущать состояния передаваемых квантовых частиц [2]. Таким образом, подслушивающий агент, по традиции называемый Евой, вносит в передаваемую последовательность бит определенный процент ошибок. Если уровень ошибок при передаче значительно превышает естественный уровень помех в канале, то это служит сигналом к прерыванию процедуры передачи ключа.

Целью настоящей работы является анализ стойкости двух протоколов с передачей кубитов к различным стратегиям атак подслушивающего агента.

Следует отметить, что доказательство стойкости всего протокола квантового распределения ключа является трудной теоретической задачей квантовой криптографии, которая в настоящее время не решена полностью ни для одного протокола. Однако некоторые аспекты безопасности различных КПРК уже анализировались в литературе. В частности для некоторых протоколов и для некоторых конкретных стратегий атак уже получены зависимости $I_{AE}(D)$.

Стратегии атак подслушивающего агента

Простейшим видом съема информации в обычных оптических телекоммуникационных системах является разделение пучка фотонов. Однако в протоколах квантовой криптографии передача должна происходить посредством одиночных фотонов, и в таком случае Ева не может ответвить часть сигнала. Поэтому данный вид атак не применим в квантово-криптографических системах в идеальных условиях однофотонных сигналов. На практике в настоящее время используют слабые когерентные импульсы, излучаемые лазерными светодиодами [3]. В настоящее время и в квантовой криптографии возможны атаки с разделением пучка фотонов.

Основные стратегии атак, которые может использовать Ева в случае, когда все сигналы содержат строго один фотон, подразделяют на два класса [2]. К первому классу относят *некогерентные* или индивидуальные атаки. При таких атаках Ева обрабатывает каждый фотон Алисы отдельно. Простейшим вариантом является атака перехвата – повторной отправки фотона. Ева перехватывает

посылаемые Алисой фотоны, измеряет их состояния и отправляет затем новые фотоны Бобу в измеренных ею состояниях.

Второй класс атак – так называемые *когерентные* атаки, при которых Ева может любым (унитарным) способом перепутать пробу любой размерности с целой группой передаваемых одиночных фотонов. Предельный вариант такой атаки, когда Ева перепутывает свою пробу со всей последовательностью переданных Алисой фотонов, иногда называют *объединенной* (*joint*) атакой [3].

Атака разделения числа фотонов на протокол BB84

Как отмечено выше на практике используют слабые когерентные импульсы, излучаемые лазерными светодиодами [3]. Вероятность того, что импульс содержит *n* фотонов определяется распределением Пуассона:

$$\rho_n = e^{-\mu}\frac{\mu^n}{n!}, \quad (1)$$

где μ – среднее число фотонов в импульсе.

В случае квантового канала с потерями, вероятность того, что Боб зарегистрирует в полученном импульсе *n* фотонов определяется формулой:

$$\rho_{n,loss} = e^{-n\mu}\frac{(n\mu)^n}{n!}, \quad (2)$$

где η – коэффициент передачи канала.

Вероятность зарегистрировать в импульсе более одного фотона дается формулой

$$\rho_{n>1,loss} = 1 - e^{-n\mu}(1+\eta\mu) \quad (3)$$

Таким образом, становится возможной атака разделения числа фотонов. Для каждого импульса Ева должна выполнить квантовое неразрушающее измерение числа фотонов в импульсе, не влияя при этом на их поляризацию. Отметим, что такое измерение очень сложно выполнить, однако в настоящее время это технически возможно [4].

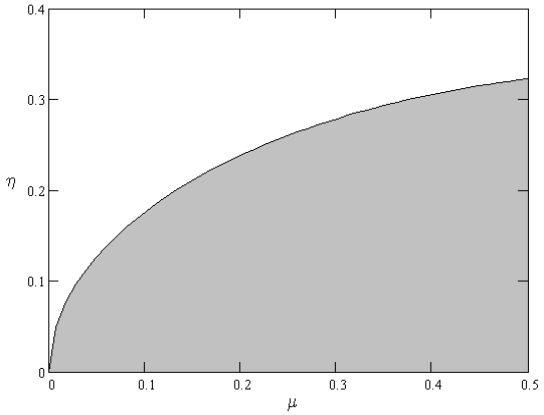

Рис. 1. Область параметров η и μ, где атака разделения числа фотонов будет успешна при замене исходного канала с потерями на идеальный

Для Евы также есть возможность заменить квантовый канал с потерями, который используют Алиса и Боб, на канал без потерь. В этом случае Ева получает возможность блокировать некоторую часть однофотонных импульсов так, чтобы Боб в результате получил приблизительно ожидаемое им число пустых импульсов. Для исходного канала с очень большими потерями такая стратегия позволяет Еве получить почти полное знание ключа, не внося никаких ошибок. Кроме того, существует некоторая область параметров η и μ, где атака разделения числа фотонов позволяет Еве сохранить не только ожидаемую Бобом долю пустых сигналов, но также и всю статистику числа фотонов в импульсе [5]. На рис. 1 эта область выделена серым цветом. Отметим, что на практике для передачи ключа по протоколу BB84 с помощью слабых когерентных импульсов используют источники с μ порядка 0,1. Этому на рисунке 1соответствует серая область $\eta < 0{,}176$, т.е. Ева может остаться необнаруженной и получить при этом полную информацию о ключе, только, если потери в исходном канале очень велики. Отсюда в частности следует, что Алиса и Боб на практике должны использовать

квантовый канал ограниченной длины так, чтобы его коэффициент передачи оставался достаточно высоким [6].

Вероятность для Евы правильно измерить состояние пробы, перепутанной с фотоном Алисы, дается выражением [4]:

$$P_{correct} = \frac{1 - e^{-\mu}(1+\mu) + (1+k)\mu e^{-\mu}(\frac{1}{2} + \sqrt{D(1-D)})}{1 - e^{-\mu}(1+\mu k)} \quad (4)$$

Так как вероятность для Евы неверно измерить состояние пробы равна (1- $P_{correct}$), то $I_{AE}(D)$ для описанной атаки просто равна

$$I_{AE}(D) = \frac{1}{2}\phi[1 - 2(1 - P_{correct})] \quad (5)$$

Для практической реализации протокола рекомендуется использовать слабые когерентные импульсы cμ ≤ 0,1. Обратной стороной этого является низкая скорость передачи, так как даже при полном отсутствии потерь в канале и при μ = 0,1, в среднем только один из десяти импульсов содержит хотя бы один фотон.

Атаки на протокол с 6-ю состояниями для случая однофотонных сигналов

Этот протокол является расширением BB84 и использует максимально возможное число базисов для двухуровневых систем – три сопряженных базиса, в отличие от двух для BB84. Эффективность протокола с 6-ю состояниями меньше эффективности BB84,так как для генерации ключа здесь используется в среднем только 1/3переданныхкубитов.

Взаимная информация между Алисой и Евой для оптимальной некогерентной атаки на протокол с 6-ю состояниями дается выражением:

$$I_{AE}(D) = 1 + (1-D)[f(D) + (1 - f(D))\log_2(1 - f(D))], \quad (6)$$

где $f(D) = \frac{1}{2(1 + \frac{\sqrt{D(2-3D)}}{1-D})}$.

Взаимная информация между Алисой и Евой для когерентной атаки на протокол с 6-юсостояниями вычисляется по той же схеме, что и для протокола BB84. При этом вместо условий , b=c=d, $d = \frac{1}{2}ND$. Тогда выражение можно окончательно привести к следующему виду:

$$I_{AE}(D) = -\frac{1}{2[(1 - \frac{3}{2}D)\log_2(1 - \frac{3}{2}D) + \frac{3}{2}D\log_2(\frac{1}{2}D)]}. \quad (7)$$

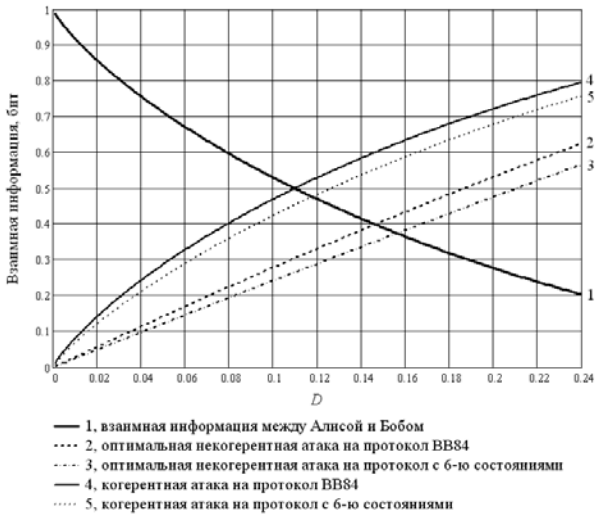

Рис. 2. Взаимная информация $I_{AE}(D)$ (кривая 1) и $I_{AF}(D)$ для различных стратегий атак на протокол с 6-ю состояниями (кривые 2–5)

На рис. 2 показаны зависимости $I_{AE}(D)$ для оптимальной некогерентной атаки на протоколы BB84 и с 6-ю состояниями, а также для когерентной атаки на эти протоколы. Видно, что при всех *D* кривые для протокола с 6-юсостояниями лежат ниже соответствующих кривых для BB84. Это означает несколько большую стойкость протокола с 6-ю состояниями к указанным атакам.

Если Ева применяет лишь простую атаку перехвата – повторной отправки кубитов, протокол BB84 будет безопасным вплоть до *D*≈17%. Для оптимальной некогерентной атаки Евы соответствующие границы *D*≈14,6% для BB84 и *D*≈15,6% для протокола с 6-юсостояниями. Для когерентной атаки *D*≈11% и *D*≈11,8% соответственно. Таким образом, протокол с 6-ю состояниями может быть успешно реализован при несколько более высоком уровне ошибок, чем протокол BB84, независимо от типа применяемой атаки.

Что касается атаки разделения числа фотонов на протокол BB84, то приведем соответствующую границу для $\mu = 0{,}1$ и $\eta = 0{,}9$, что приблизительно соответствует параметрам используемого на практике оборудования. Эта граница *D*≈13,8% и лежит между соответствующих границ для некогерентной и когерентной атак на однофотонные сигналы, ближе к границе для оптимальной некогерентной атаки. Такой результат вполне естественен, так как Ева блокирует долю *k* однофотонных импульсов (*k*= 0,101 для указанных μи η), а к остальным применяет оптимальную некогерентную атаку. Так как в данном случае *k* мало, то стойкость протокола BB84 к атаке разделения числа фотонов не намного меньше, чем к оптимальной некогерентной атаке.

Заключение

В работе проанализированы различные виды атак на два КПРК с целью сравнения стойкости этих протоколов к различным атакам. Протокол считается более стойким, если он допускает более высокий уровень ошибок, при котором Алиса и Боб могут установить секретный ключ с использованием процедур исправления ошибок и усиления секретности.

Исходя из вышеназванного критерия, следует сделать вывод, что протокол с 6-юсостояниями является более стойким, чем протокол BB84. Однако преимущество протокола с 6-ю состояниями невелико – при заданном*D* Ева получает меньше информации максимум на 5,8 % при оптимальной некогерентной атаке и максимум на 4,7 % при когерентной. С другой стороны, верхняя граница уровня ошибок, при которой протокол может быть реализован с использованием процедуры усиления секретности, для протокола с 6-ю состояниями также не намного выше, чем для BB84: 11,8% против 11%. Учитывая, что средняя эффективность протокола с 6-ю состояниями равна 1/3, в то время как для BB84 она равна 1/2, что приводит к значительно меньшей скорости передачи, включая в протоколе с 6-юсостояниями, можно сделать вывод, что этот протокол практически не имеет никаких преимуществ по сравнению с протоколом BB84.

Атака разделения числа фотонов на протокол BB84 является достаточно мощной. Однако при использовании в качестве источника сигналов слабых когерентных импульсов со средним числом фотонов в импульсе порядка 0,1, а также при использовании квантовых каналов с малыми потерями ($\eta = 0{,}9 \div 1$), при такой атаке Алиса и Боб смогут установить секретный ключ, если уровень ошибок при передаче не превышает ~14%. Платой за секретность в данном случае является очень низкая эффективность протокола и, соответственно, низкая скорость передачи ключа.

Литература.

1. Bennet C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc.of IEEE Int. Conf. on Comput. Sys. And Sign. Proces., Bangalore, India, - 1984.
2. БаумейстерД.,ЭкертА., ЦайлингерА. Физика квантовой информации.- Москва:«Постмаркет», 2002.
3. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Reviews of ModernPhysics.- 2002.- V. 74, №1.- P. 145-195.
4. Williamson M., Vedral V. Eavesdropping on practical quantum cryptography // Journal ofModern Optics.- 2003.- V. 50, № 13.- P. 1989-2011.
5. Lutkenhaus N., Jahma M. Quantum key distribution with realistic states: photon-numberstatistics in the photon-number splitting attack // New Journal of Physics.- 2002.- V. 4.- P.44.1-44.9.
6. Niederberger A., Scarani V., Gisin N. Photon-number-splitting versus cloning attacks inpractical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography// Physical Review A.- 2005.- V. 71.- Art. 042316.