УДК 004.056.55

Зар Ни Аунг, Чан Мья. Хейн

Московский физико-технический институт (государственный университет)

Существуют ли риски протокола BB84?

Используется стратегия атаки для протокола распределения ключей BB84 в квантовой криптографии, мы называем эту стратегию, использующую свойство квантовой нелокальности *косвенной копирующей атакой*. Возможно, в соответствии с этой стратегией, квантовые криптографические протоколы BB84 подвержены риску и может ли подслушивающее устройство точно получить информацию между законными пользователями без обнаружения? В ответе на этот вопрос используются атаки расщепления фотонного числа (PNS), которые обнаруживаются с определенной степенью уверенности, максимизируя квантовую пропускную способность системы без каких-либо дополнительных затрат.

Ключевые слова: распределение квантовых ключей, расщепление фотонного числа.

Zar Ni Aung, Chan Myae Hein

Moscow Institute of Physics and Technology (State University)

Are there risks of BB84 protocol?

The attack strategy for the key distribution protocol BB84 in quantum cryptography is used. We call this strategy using the quantum nonlocality property the *indirect replicating attack*. Possibly according to this strategy, BB84 quantum cryptographic protocols are at risk and can the eavesdropper accurately obtain information between legitimate users without detection? The answer to this question uses photon number splitting (PNS) attacks, which are detected with a certain degree of confidence maximizing the quantum bandwidth of the system at no additional cost.

Key words: quantum key distribution, photon number splitting.

1. Введение

В последние годы возникло чёткое и строгое понимание того, каким условиям должен удовлетворять абсолютно стойкий шифр при использовании в квантовой криптографии. Неформально шифр является абсолютно стойким, если: ключ секретен – известен только легитимным пользователям; длина ключа в битах не меньше длины сообщения; ключ случаен; ключ используется только один раз. В этом случае зашифрованное сообщение статически независимо от исходного сообщения.

Впервые идея использовать квантовую механику для защиты информации была высказана С. Визнером в 1973 г. (идея «квантовых» денег), но была опубликована лишь спустя десятилетие [1]. Интересно отметить, что идеи использования квантовой механики для защиты информации появились раньше, чем классическая криптография с открытым ключом.

Возникновение квантовой криптографии связано с опубликованием в 1984 г. замечательной работы Беннета и Брассара, в которой был предложен первый криптографический протокол BB84, ставший впоследствии классическим [2].

В 1976 году был предложен принцип несимметричных криптосистем или систем с открытым ключом. Этим системам соответствуют пара ключей. Один из них (открытый ключ) используется для шифрации. В то время как другой (секретный ключ) – для дешифрации сообщений. Но только в 1978 году Р. Райвесту, А. Шамиру и Л. Эдльману удалось найти такую функцию, которая была применена в алгоритме, известном как RSA (Rivest, Shamir, Adleman). Алгоритм RSA считается достаточно защищенным для многих применений современной криптографии. В 1984 году они предположили возможность создания фундаментально защищённого канала с помощью квантовых состояний. После этого ими была предложена схема (BB84), в которой легальные пользователи (Алиса и Боб) обмениваются сообщениями, представленными в виде поляризованных фотонов, по квантовому каналу. Он исследовал последовательность бит, которая является черновым вариантом ключа, подлежащим уточнению. Для кодирования информации протокол использует четыре квантовых состояния микросистемы, формируя два сопряжённых базиса. В этой работе реализован протокол распространения ключа – секретной последовательности нулей и единиц с помощью одиночных, поляризованных в двух неортогональных базисах фотонов. В это время Артур Экерт работал над протоколом квантовой криптографии, основанном на спутанных состояниях. Опубликование результатов его работ состоялось в 1991 году. В основу положены принципы парадокса Эйнштейна–Подольского–Розенберга, в частности принцип нелокальности спутанных квантовых объектов. Протокол B92 был предложен Беннеттом в 1992 году, который показал, что для кодирования «0» и «1» могут быть использованы не четыре, как в протоколе BB84, а любые два неортогональных поляризованных состояния, произведение которых лежит в интервале (0, 1). Он сделал измерение и формирование квантового канала по протоколу B92.

В первой экспериментальной демонстрации установки квантового распределения ключей, проведенной в 1989 году, в лабораторных условиях, передача осуществлялась через открытое пространство на расстояние тридцати сантиметров. Далее эти эксперименты были проведены с использованием оптического волокна в качестве среды распространения. После первых экспериментов Мюллера и др. в Женеве, в 1995 году, с использованием оптоволокна длиной 1,1 км, расстояние передачи было увеличено до 23 км через оптическое волокно, проложенное под водой. Приблизительно в то же время Таунсендом из British Telecom была продемонстрирована передача на 30 км. Рекорд по дальности передачи информации принадлежит объединению ученых Лос-Аламоса и Национального института стандартов и технологий и составляет 184 км. В нем использовались однофотонные приемники, охлаждаемые до температур, близких к нулевым по Кельвину.

2. Распределение квантовых ключей

Впервые Визнер [1] предложил идею кодирования информации на поляризованных фотонах с использованием двух конъюгатных баз. В 1984 году Беннетт и Брассард распространили эту идею, представив первый протокол QKD, известный как «BB84», для генерации совместного секретного ключевого материала между двумя сторонами [2]. Сегодня QKD привлекает внимание как важное развитие в пространстве решений для кибербезопасности из-за его способности генерировать неограниченное количество симметричных материалов для использования с One-Time-Pad (OTP) – единственный известный алгоритм шифрования для достижения идеальной секретности. Таким образом, QKD обеспечивает нерушимую связь и вдохновляет исследовательские усилия в Азии, Европе и Северной Америке. BB84 в первую очередь рассматривается в этой работе, поскольку он остается популярным выбором реализации и относительно легко понятным.

3. Каковы риски протокола BB84?

Рассматриваемая схема основана на «косвенном копировании» с использованием свойства квантовой нелокальности. Согласно этой схеме, подслушиватель может получить ин-

формацию, передаваемую между легальными пользователями без своего обнаружения с достаточно высокой вероятностью, определяемой с помощью соотношения неопределенности [3]. В протоколе BB84 ОКС представляют собой четыре некоммутирующих состояния $|0\rangle, \left|\frac{\pi}{2}\right\rangle, \left|\frac{\pi}{4}\right\rangle, \left|\frac{3\pi}{4}\right\rangle$, линейно поляризованные состояния $|0\rangle, \left|\frac{\pi}{2}\right\rangle$ и круговые поляризованные состояния $\left|\frac{\pi}{4}\right\rangle, \left|\frac{3\pi}{4}\right\rangle$ являются ортогональными соответственно. Квантовые состояния $|\pi\rangle$ и $\left|\frac{\pi}{2}\right\rangle$ измеряются так называемым *прямолинейным типом измерения.* Представляя этот прямолинейный измерительный тип как L, имеем

$$Ł\,|0\rangle = \lambda_1\,|0\rangle\,, \tag{1}$$

$$Ł\left|\frac{\pi}{2}\right\rangle = \lambda_2\left|\frac{\pi}{2}\right\rangle, \tag{2}$$

где $\lambda_i, i = 1, 2$ – собственные значения. Поскольку состояния образуют базу гильбертова пространства, произвольное квантовое состояние может быть расширено этим основанием, т.е.

$$|\Psi\rangle = C_1\,|0\rangle + C_2\left|\frac{\pi}{2}\right\rangle, \tag{3}$$

$$\left|\frac{\pi}{4}\right\rangle = \frac{\sqrt{2}}{2}\,|0\rangle + \frac{\sqrt{2}}{2}\left|\frac{\pi}{2}\right\rangle, \tag{4}$$

$$\left|\frac{3\pi}{4}\right\rangle = \frac{\sqrt{2}}{2}\,|0\rangle - \frac{\sqrt{2}}{2}\left|\frac{\pi}{2}\right\rangle. \tag{5}$$

Собственное вспомогательное квантовое состояние имеет вид

$$|\alpha\rangle = \frac{\sqrt{3}}{2}\,|0\rangle + \frac{1}{2}\left|\frac{\pi}{2}\right\rangle. \tag{6}$$

Произведение вспомогательного квантового состояния $|\alpha\rangle$ и кванта ОКС дает

$$|\alpha \mid 0\rangle = \frac{\sqrt{3}}{2} \to m_1 = \frac{3}{4} = 0.75, \tag{7}$$

$$\left|\alpha \mid \frac{\pi}{2}\right\rangle = \frac{1}{2} \to m_2 = \frac{1}{4} = 0.25, \tag{8}$$

$$\left|\alpha \mid \frac{\pi}{4}\right\rangle = \frac{\sqrt{6}+\sqrt{2}}{4} \to m_3 = \frac{(\sqrt{3}+\sqrt{1})^2}{8} \approx 0.9, \tag{9}$$

$$\left|\alpha \mid \frac{3\pi}{4}\right\rangle = \frac{\sqrt{6}-\sqrt{2}}{4} \to m_4 = \frac{(\sqrt{3}-1}{8} \approx 0.07, \tag{10}$$

здесь m_j, $J = 1, 2, 3, 4$ соответствуют только основному квантовому состоянию, $k = 1, 2, 3, 4$.

Из этого следует, что протокол BB84 достаточно надежен и риски дешифровки его Евой' достаточно низкие.

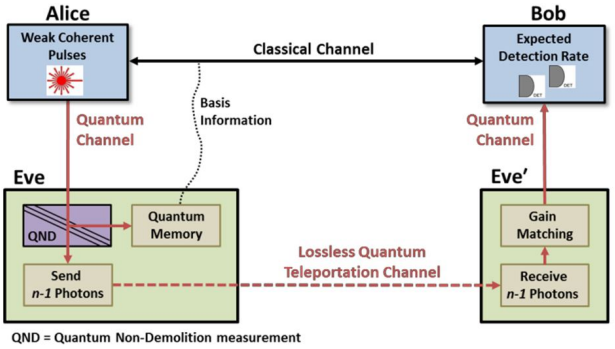

Рис. 1. Подслушивающее устройство (Ева и Ева') показано проводящей атаку расщепления числа фотонов (PNS) против системы распределения квантовых ключей

4. Возможная схема атаки расщепления числа фотонов (PNS-атака)

Атака PNS – мощная атака, предназначенная для использования многофотонной уязвимости с получением полной копии разделяемых секретных ключей Алисы и Боба без введения ошибок и, таким образом, увеличения QBER [4]. Здесь приводится краткое введение в атаку PNS с подробным, но легко понятным инженерно-ориентированным объяснением. На рис. 1 показано упрощенное изображение перехватчика «Ева», проводящего атаку PNS против системы QKD (т. е. Алисы и Боба). В соответствии с доказательствами безопасности QKD Ева является всесильным противником, ограниченным только законами квантовой механики. Ей разрешен полный контроль над квантовым каналом, чтобы ввести потери или ошибки. Она может подслушивать, но не производить сообщения, обмениваемые по классическому каналу. Чтобы провести атаку PNS, Ева заменяет квантовый канал квантовым каналом телепортации, который позволяет без потерь передавать фотоны от Алисы Бобу с использованием свойств запутанных квантовых систем. Нахождение Евы' также требуется в непосредственной близости от Боба, чтобы регулировать передачу фотонов без потерь и чтобы не превышать ожидаемую скорость обнаружения Боба, таким образом избегая очевидного обнаружения.

Для каждого импульса, генерируемого Алисой, Ева выполняет специальное квантовое измерение без разрушения (QND) для определения количества фотонов в каждом импульсе $n = 0, 1, 2, 3, ..., N$. Если $n \leqslant 1$, Ева блокирует импульс и ничего не посылает Бобу. Если $n \geq 2$, а затем Ева расщепляет один фотон из импульса и сохраняет его в своей квантовой памяти. Затем она проквантовывает оставшиеся $n - 1$ фотоны Боба. Эта схема атаки позволяет Еве хранить идентичную закодированную копию каждого фотона, отправленного Бобу, без введения дополнительных ошибок (которые обычно используются для обнаружения подслушивающих устройств). После того как Алиса и Боб закончили свой квантовый обмен, они должны объявить основную информацию об измерениях по классическому каналу. Ева может затем правильно измерить каждый сохраненный фотон и, таким образом, получить полную копию генерируемых QKD «безопасных» битов ключа.

5. Заключение

В этом исследовании анализируется и демонстрируется способность состояния приманки, позволяющей QKD-системам обнаруживать атаки PNS. Атаки PNS обнаруживаются с высокой степенью уверенности. О возможности определения Евой состояния одного фотона можно заметить следующее. Квантовая криптография является областью, в которой законы квантовой физики непосредственно используются, чтобы дать существенное преимущество в обработке информации [5, 6]. Но эти же законы квантовой физики может использовать и подслушиватель. В схеме запутанности подслушиватель использует несу-

щую частицу во взаимодействии с ее собственной квантовой системой, называемой зондом, так что частицы и зонд остаются в запутанном состоянии, а последующее измерение зонда дает нужную информацию.

Литература

1. *Wiesner S.* SIGACT news // 1983. V. 15, N 1. P. 78.
2. *Bennett C.H., Brassard G.* Quantum cryptography: public-key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India10-12 December, New York: IEEE Press, 1984. V. 560. P. 175–179.
3. *Griffiths R.B., Niu C.S.* Optimal eavesdropping in quantum cryptography. II. A quantum circuit // Phys. Rev. L. 1997. A. 56. P. 1173.
4. *Mailloux L., Hodson D., Grimaila M., Engle R., Mclaughlin C., Baumgartner G.* Using Modeling and simulation to study photon number splitting attacks // IEEE Access. 2016. V. 4. P. 2188–2197.
5. *Rybakov Yu P., Kamalov T. F.* Bell's Theorem and Entangled Solitons // International Journal of Theoretical Physics. 2015. V. 55, N 9. P. 4075-4080.
6. *Kamalov T.F.* Hidden Variables and the Nature of Quantum Statistics // J. of the Russian Laser Researh. 2001. V. 22, N 5. P. 475–479.

References

1. *Wiesner S.* SIGACT news. 1983. V. 15, N 1. P. 78.
2. *Bennett C. H., Brassard G.* Quantum cryptography: public-key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India10-12 December, New York: IEEE Press, 1984. V. 560. P. 175–179.
3. *Griffiths R. B., Niu C. S.* Optimal eavesdropping in quantum cryptography. II. A quantum circuit. Phys. Rev. L. 1997. A. 56. P. 1173.
4. *Mailloux L., Hodson D., Grimaila M., Engle R., Mclaughlin C., Baumgartner G.* Using Modeling and simulation to study photon number splitting attacks. IEEE Access. 2016. V. 4. P. 2188–2197.
5. *Rybakov Yu P., Kamalov T. F.* Bell's Theorem and Entangled Solitons. International Journal of Theoretical Physics. 2015. V. 55, N 9. P. 4075-4080.
6. *Kamalov T.F.* Hidden Variables and the Nature of Quantum Statistics. J. of the Russian Laser Researh. 2001. V. 22, N 5. P. 475-479.

Поступила в редакцию 06.12.2018