УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Том 148, кн. 1 Физико-математические науки *2006*

УДК 535.2+535.37

ПЕРЕНОС ИНФОРМАЦИИ С ПОМОЩЬЮ БИФОТОНОВ В ПРОТОКОЛАХ КВАНТОВОЙ КРИПТОГРАФИИ

Д.А. Калашников, А.А. Калинкин, А.В. Шкаликов, В.В. Самарцев

Аннотация

Теоретически показано, что использование бифотонов позволяет создать стойкий криптографический ключ для защиты информации при ее передаче в сетях повышенной секретности. Рассмотрен ряд схем генерации ключа на основе квантовых свойств коррелированных пар фотонов. Результаты работы представляют интерес для квантовой криптографии.

Введение

Бурное развитие квантовых технологий и волоконно-оптических линий связи (ВОЛС) привело к появлению квантово-криптографических систем. Они являются предельным случаем защищенных ВОЛС. Использование квантовой механики для защиты информации позволяет получать результаты, не достижимые как техническими методами защиты ВОЛС, так и традиционными методами математической криптографии. Применение в качестве носителя информации одиночных фотонов, источником которых обычно является ослабленный луч лазера, дает высокую вероятность того, что в импульсе содержится более одного фотона, в таком случае для злоумышленника (Евы) не составляет труда перехватить передаваемый ключ, не производя шума в канале. Использование коррелированных пар фотонов (бифотонов), генерируемых в процессе спонтанного параметрического рассеяния света (СПР), позволяет избавиться от этого недостатка, так как рождение в один момент времени более одной пары фотонов крайне маловероятно, причём случайность этого процесса гарантирует случайность генерации ключа.

1. Протокол Экерта

Протокол напрямую реализует свойства перепутанных систем. Он был реализован в 1991 г. [1]. Алиса и Боб получают по фотону спутанной пары (рис. 1), затем измеряют их с помощью поляризаторов, случайным образом выбирая одну из трёх возможных поляризаций. Для проверки конфиденциальности процесса передачи, Алиса и Боб проводят проверку на нарушение неравенств Бэлла. Только в случае если до измерений, проводимых Алисой и Бобом, система не была возмущена, то есть Ева не перехватывала кубиты, неравенства Бэлла будут нарушаться. В то же время Алиса и Боб могут создавать ключ, проводя измерения с помощью параллельных поляризаторов, так как за счёт антикорелляции состояний они должны получать противоположные результаты. Таким образом, ключ создается непосредственно во время измерений, а процесс его создания абсолютно случаен.

В данном случае нарушение неравенств Бэлла является достаточным критерием для ограничения обобщённой информации Евы о ключе [2], то есть канал

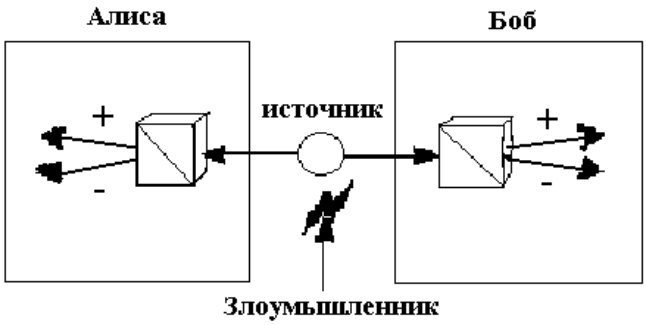

Рис. 1. Схема протокола Экерта

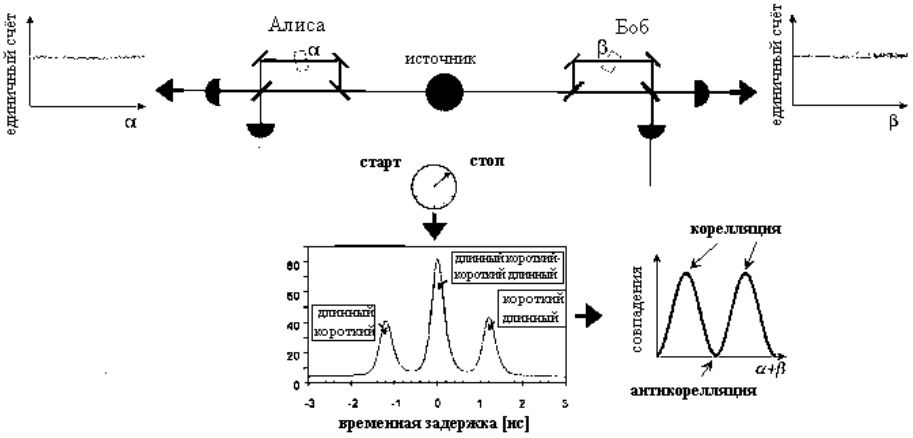

Рис. 2. Схема кодирования по фазе на основе перепутанных по энергии-времени фотонов

является достаточно защищённым, когда параметр Бэлла $S \geqslant 2$. При уровне ошибок ε имеем

$$S = 2\sqrt{2}(1 - 2\varepsilon)$$

и получаем классический предел $S = 2$ при $\varepsilon \approx 0.14644$.

2. Кодирование по фазе

Схема основывается на проверке неравенств Бэлла (рис. 2) [3]. В ней используются «перепутанные по энергии-времени» состояния бифотонов. Источник создаёт скореллированные по энергии пары фотонов, рождённые в одно и то же, но неизвестное время. Пара фотонов далее разделяется, а затем каждый из фотонов посылается по квантовому каналу одной из сторон. Каждая из сторон обладает несбалансированным интерферометром Маха–Цендера. Так, если Алиса или Боб по отдельности изменяют фазу своего интерферометра, то никакого изменения в количестве фотоотсчётов не происходит, поскольку несбалансированность интерферометров исключает возможность интерференции одного фотона.

В зависимости от времени регистрации фотонов Бобом и Алисой существует три возможности. Первая – каждый из фотонов может пройти коротким путём. Вторая – первый фотон проходит через длинное плечо интерферометра Алисы, а

Рис. 3. Схема, реализующая кодирование по фазе и времени со вторым набором интерферометров

второй – через короткое плечо интерферометра Боба, или наоборот. Наконец, в-третьих, оба фотона могут пройти длинным путём. Когда пути интерферометров выровнены с точностью до длины когерентности фотонов, короткий-короткий и длинный-длинный пути неразличимы, так как разность путей меньше длины когерентности фотона накачки. При регистрации центрального пика мы наблюдаем двухфотонную интерференцию, которая зависит от суммы относительных фаз в интерферометрах Алисы и Боба. Фазы интерферометров Алисы и Боба могут, к примеру, быть подобраны таким образом, чтобы оба фотона всегда появлялись на одинаковых выходах (регистрировались одинаковыми детекторами). Тогда возможно организовать передачу кубитов, связав их значения с двумя возможными выходами.

Для того чтобы избежать возможного прослушивания, необходимо ввести второй измерительный базис. Это можно сделать, добавив второй набор интерферометров (рис. 3).

В таком случае фотоны случайным образом входят в один или другой интерферометр. Относительные фазы во втором наборе интерферометров могут быть выбраны таким образом, чтобы возникала конструктивная интерференция между выходами. Конечно, фазы должны быть подобраны так, чтобы в случае, когда фотоны попадают в несвязанные друг с другом интерферометры, их результаты были некореллированы.

3. Кодирование по фазе и времени

Данная схема была предложена в 1999 г. (рис. 4) [4]. Если Алиса регистрирует время прибытие фотонов относительно времени импульса накачки t_0, то возможно зарегистрировать фотоны в одном из трёх временных интервалов. Например, регистрация фотона в первом интервале соответствует случаю, когда и фотон накачки и фотон, полученный в результате СПР, проходят через короткое плечо. Для простоты обозначим подобную альтернативу через $|S\rangle_P$, $|S\rangle_A$.

Для того чтобы теперь создать секретный ключ, Алиса с Бобом договариваются о событиях, когда они оба регистрируют фотоны в одном из боковых пиков, но без объявления в каком именно, либо когда оба регистрируют фотон в центральном пике, но без объявления каким детектором. Это – процедура просеяния ключа.

Например, в случае, приведённом выше, если Боб говорит Алисе, что он зарегистрировал фотон в боковом пике, то она знает, что это левый пик. Это объясняется тем, что поскольку фотон накачки проходит коротким путём, следовательно, Боб мог зарегистрировать фотон либо в центральном, либо в левом пике. То же самое

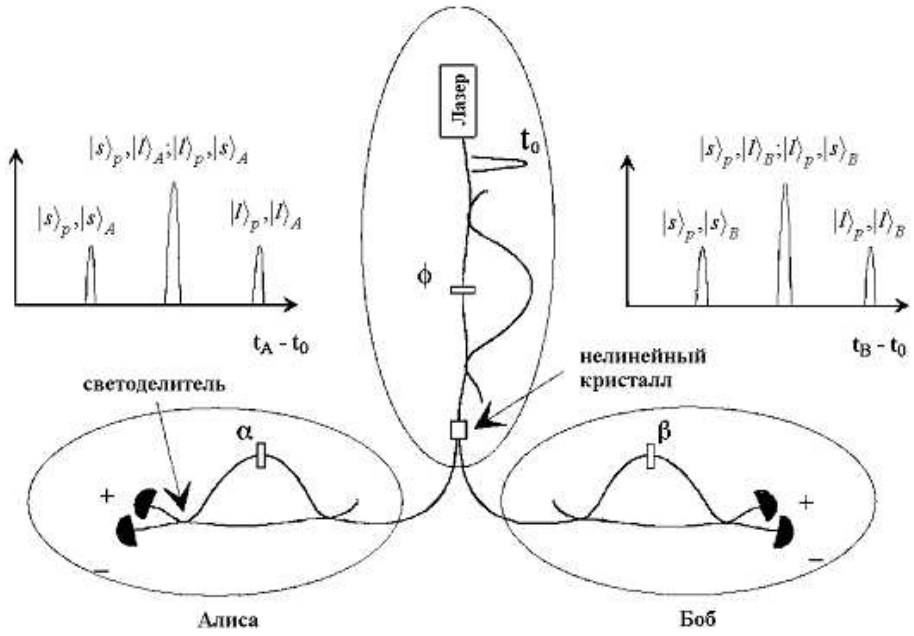

Рис. 4. Схема, реализующая кодирование по фазе и времени

применимо и к Бобу, который теперь знает, что фотон Алисы прошёл коротким путём. Поэтому в случае совместного детектирования фотонов в боковых пиках у Алисы и Боба должны быть скореллированы времена регистрации. Приписывая значение бита к боковому пику, Алиса и Боб могут организовать обмен последовательности битов. Второй базис, когда фотоны регистрируются в центральном временном интервале. Они относятся к случаям $|S\rangle_P$;$|l\rangle_A$, $|l\rangle_B$ и $|l\rangle_P$;$|S\rangle_A$, $|S\rangle_B$. Если они неразличимы, то возникает двухфотонная интерференция. Подобрав фазы, возможно получить корелляцию между выходами интерферометров Алисы и Боба, создав второй базис для обмена битами.

Заключение

Дальнейшее развитие квантовых сетей видится в увеличении дальности передачи ключа. Системы на основе единичных фотонов достаточно ограничены в этом плане, порядка 100 километров, в то время как с помощью обмена перепутывания возможно покрыть большее расстояние, соединяя множество небольших отрезков. Ещё более многообещающей является возможность сохранять кубиты в течение долгого времени, тогда возможно переносить квантовую память с перепутанными состояниями в любое место и в любое время и использовать для передачи ключа. Также возможно построение квантовых сетей, где каждый кубит памяти хранится у посредника, и которые с помощью обмена перепутывания могут быть преобразованы в перепутывание между частицами для конфиденциального обмена информации.

Работа выполнена при финансовой поддержке РФФИ (проекты № 04-02-81009-Бел2004а, 04-02-16932-а, 05-02-16003-а, 05-02-16169-а, 04-02-17082-а); программы Президиума РАН «Квантовая макрофизика», ОФН РАН «Оптическая спектроскопия и стандарты частоты», «Фонда содействия отечественной науке».

Summary

D.A. Kalashnikov, A.A. Kalinkin, A.V. Shkalikov, V.V. Samartsev. Transfer information by using biphotons in quantum cryptography.

This work describes some schemes using entangled photons for quantum key distribution which is fundamental of the new field called quantum communication. Depending on the circumstances, various protocols are used for the exchange of information.

Литература

1. *Ekert A.K.* Quantum cryptography based on Bell's theorem // Phys. Rev. Lett. – 1991. – V. 67. – P. 661–663.
2. *Fuchs C.A., Gisin N., Grifiths R.B., Chi-Sheng Niu, Peres A.* Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy // Phys. Rev. A. – 1997. – V. 56. – P. 1163–1172.
3. *Franson J. D.* Bell inequality for position and time // Phys. Rev. Lett. – 1989. – V. 62. – P. 2205–2208.
4. *Brendel J., Gisin N., Tittel W., Zbinden H.* Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication // Phys. Rev. Lett. – 1999. – V. 82. – P. 2594–2597.

Поступила в редакцию
28.02.06

Калашников Дмитрий Андреевич – студент Казанского государственного университета

E-mail: *dimonk@hitv.ru*

Калинкин Александр Александрович – кандидат физико-математических наук, научный сотрудник Казанского физико-технического института им. Е.К. Завойского КНЦ РАН.

E-mail: *kalinkin@kfti.knc.ru*

Шкаликов Андрей Викторович – младший научный сотрудник Казанского физико-технического института им. Е.К. Завойского КНЦ РАН.

E-mail: *shkalikov@mail.knc.ru*

Самарцев Виталий Владимирович – доктор физико-математических наук, академик РАЕН, профессор, заведующий лабораторией нелинейной оптики Казанского физико-технического института им. Е.К. Завойского КНЦ РАН.

E-mail: *samartsev@kfti.knc.ru*