Всероссийская научно-образовательная школа
"Квантовый скачок"

ПРОТОКОЛ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА BB84

Хомякова К.И.
Квантовый центр ТГУ
qtcenter.tsu.ru
Контакты:
+7 913 109 9359
Homiackowa.kristina@yandex.ru

- **Протокол передачи данных** — набор определённых правил или соглашений интерфейса логического уровня, который определяет обмен данными между различными программами. Эти правила задают единообразный способ передачи сообщений и обработки ошибок.

Основные виды протоколов квантового распределения ключей (QKD)

- **Протоколы с использованием одиночных квантовых систем (protocols using single quantum systems):** BB84,протокол с 6-ю состояниями, протокол “4+2”, протокол Гольденберга-Вайдмана, протокол Коаши-Имото и др.
- **Протоколы с использованием перепутанных состояний (protocols using entangled states):** протокол Экерта и протоколы с использованием перепутанных состояний многомерных квантовых систем.

Первый протокол квантовой криптографии BB84, 1984 г.

Американский физик-теоретик.
Чарльз Беннетт

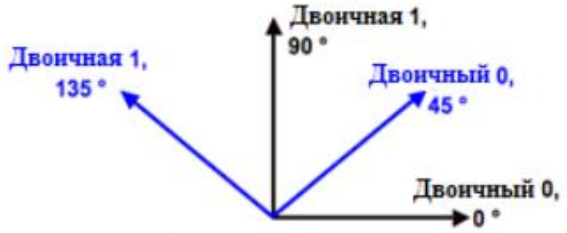
Канадский физик-теоретик.
Жиль Брассар

Основы протокола BB84

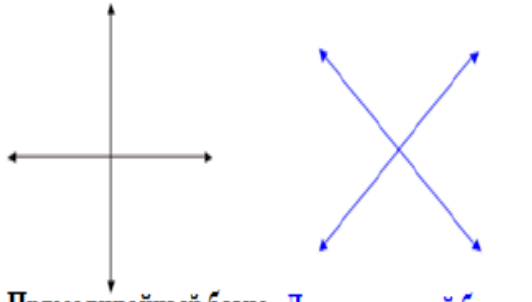
Протокол использует 4 квантовых состояния, образующих 2 базиса,
например поляризационные состояния света. Состояния внутри одного базиса ортогональны, но состояния из разных базисов — попарно неортогональны. Эта особенность протокола позволяет определить возможные попытки нелегитимного съёма информации.

Носителями информации в протоколе являются **фотоны**, поляризованные под углами 0°, 45°, 90°, 135°. С помощью измерения можно различить только 2 ортогональных состояния:

- фотон поляризован вертикально или горизонтально (0° или 90°);
- фотон поляризован диагонально (45° или 135°).



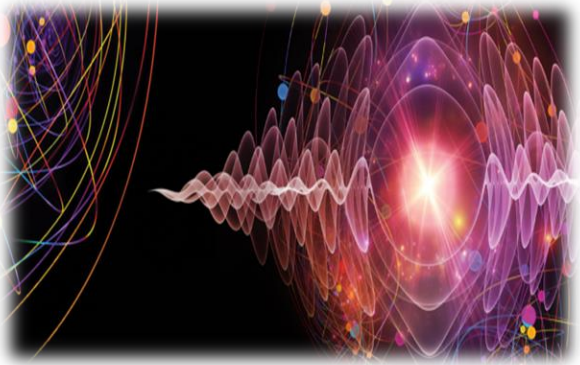
Поляризация фотонов


Прямолинейный базис Диагональный базис

Кодирование состояний

- В протоколе BB84 кодирование состояний осуществляется следующим образом:

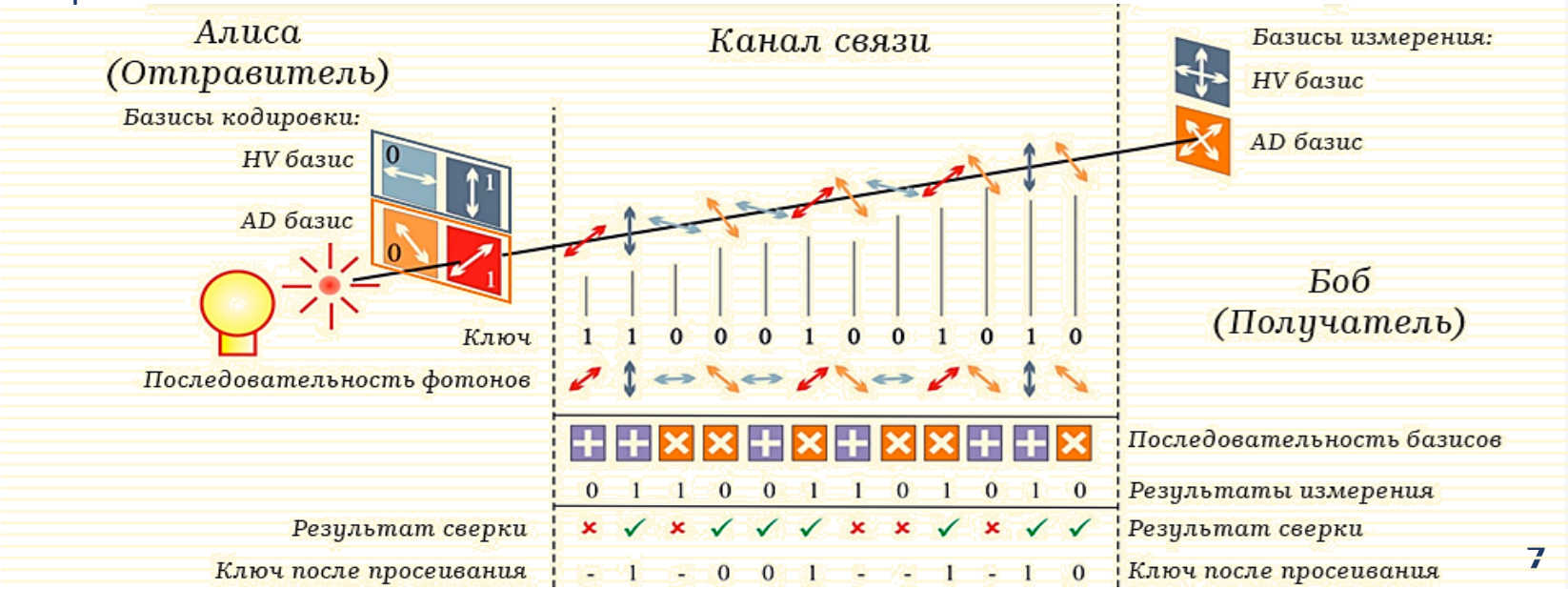
1. $|0\rangle$
   - $|\leftrightarrow\rangle$
   - $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle + |\leftrightarrow\rangle)$
2. $|1\rangle$
   - $|\updownarrow\rangle$
   - $|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle - |\leftrightarrow\rangle)$



Алгоритм распределения ключей

Этапы формирования ключей:

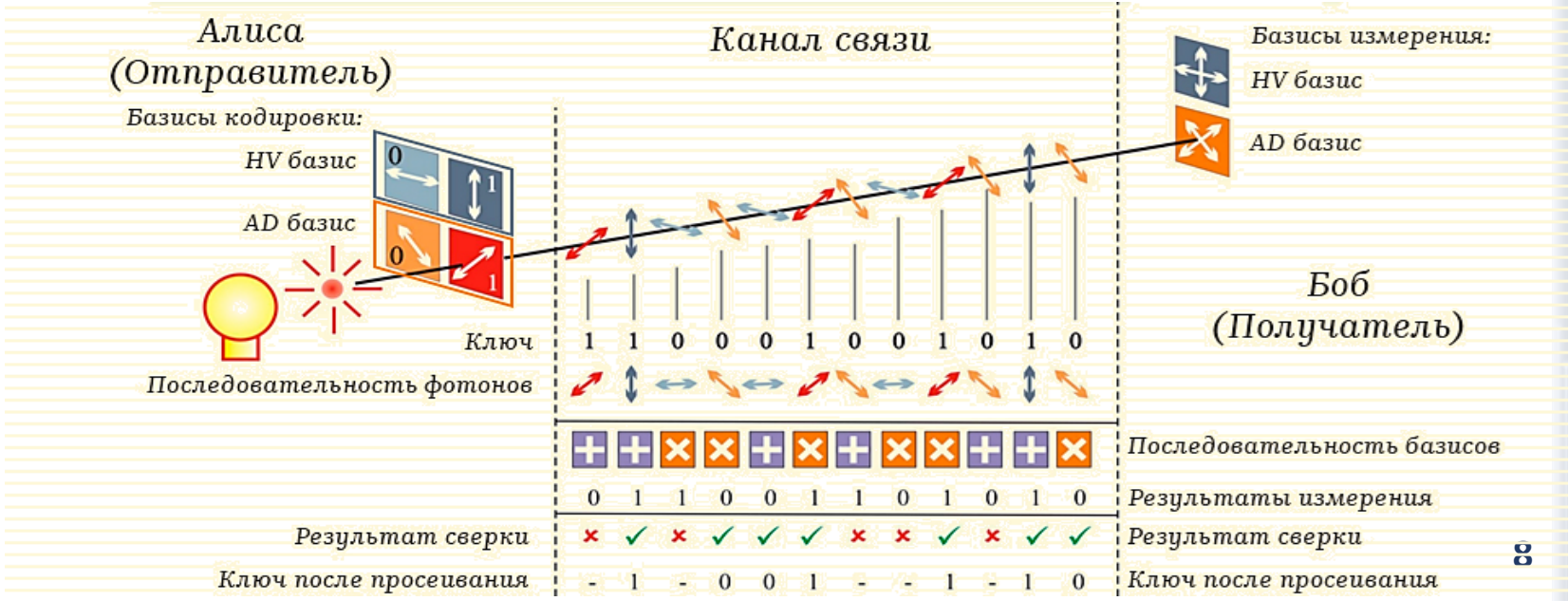
I. Алиса случайным образом выбирает один из базисов. Затем внутри базиса случайно выбирает одно из состояний, соответствующее 0 или 1, и посылает фотоны. Они могут посылаться все вместе или один за другим, но главное, чтобы Алиса и Боб смогли установить взаимно однозначное соответствие между посланным и принятым фотоном.



Алгоритм распределения ключей

II. Боб случайно и независимо от Алисы выбирает для каждого поступающего фотона: прямолинейный или диагональный базис, и измеряет в нём значение фотона.

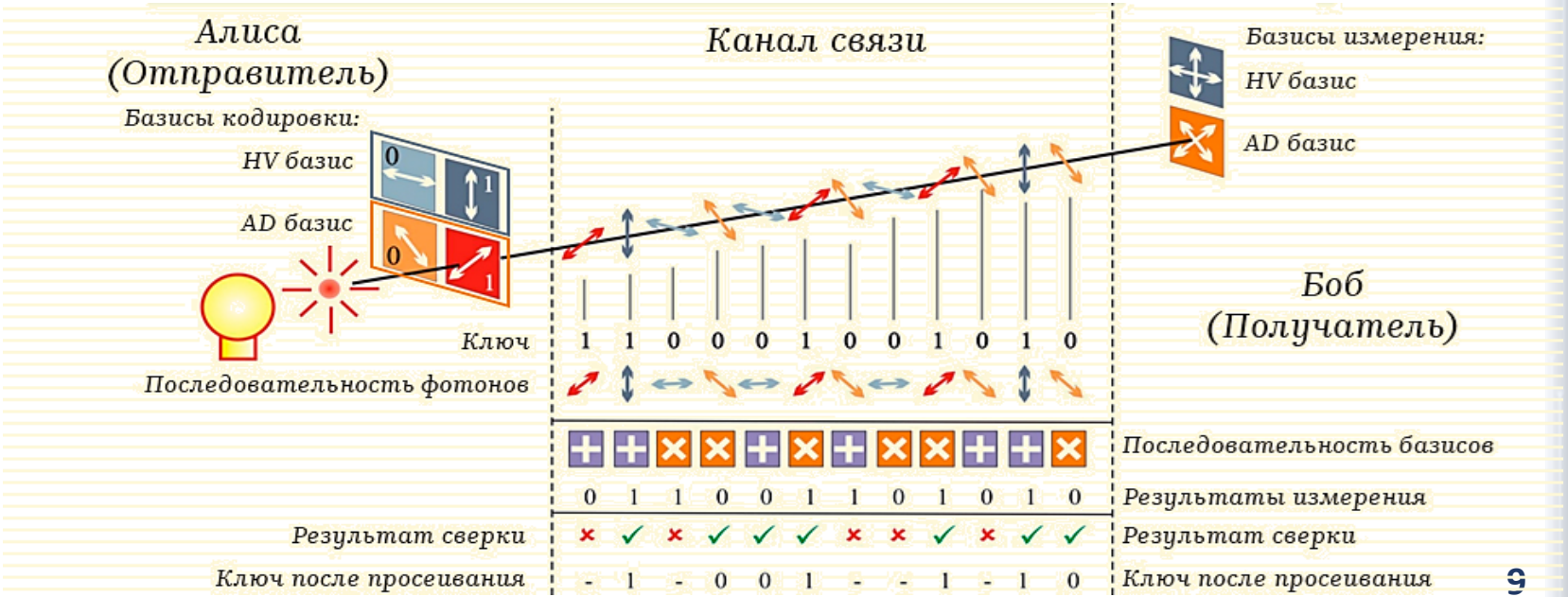
III. Для каждого переданного состояния Боб открыто сообщает, в каком базисе проводилось измерение кубита, но результаты измерений остаются в секрете.



Алгоритм распределения ключей

IV. Алиса сообщает Бобу по открытому общедоступному каналу связи, какие измерения были выбраны в соответствии с исходным базисом Алисы.

V. Пользователи оставляют только те случаи, в которых выбранные базисы совпали. Эти случаи переводят в биты (0 и 1), и составляют ключ.



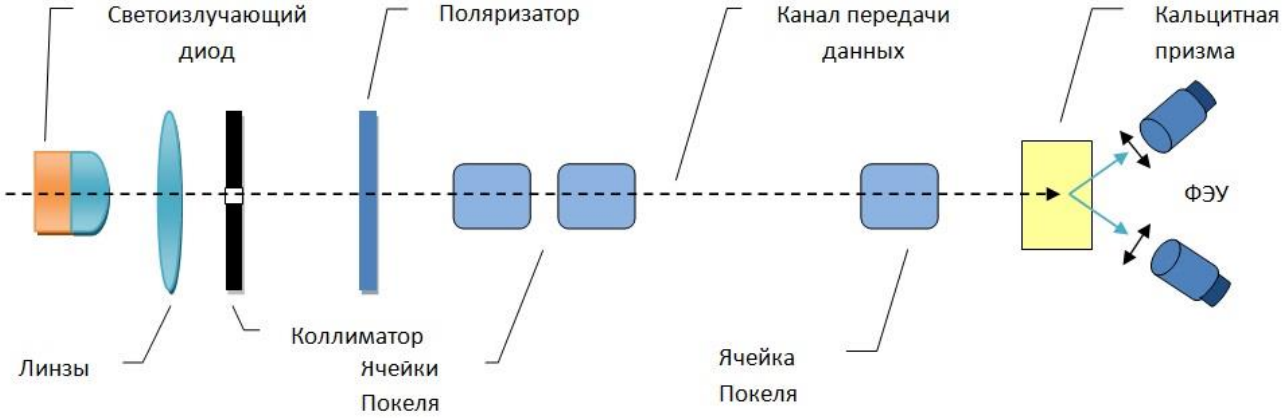
Атака разделения числа фотонов на протокол BB84

Вероятностное распределение Пуассона:

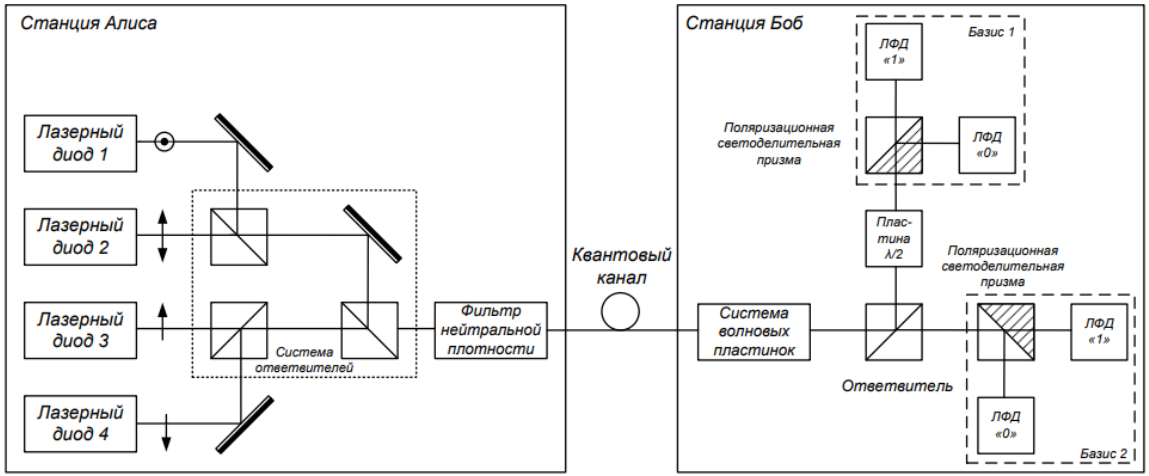
$$P_{n,\text{loss}} = e^{-\eta\mu}\frac{(\eta\mu)^n}{n!},$$

где μ — среднее число фотонов в импульсе, η — коэффициент передачи канала.

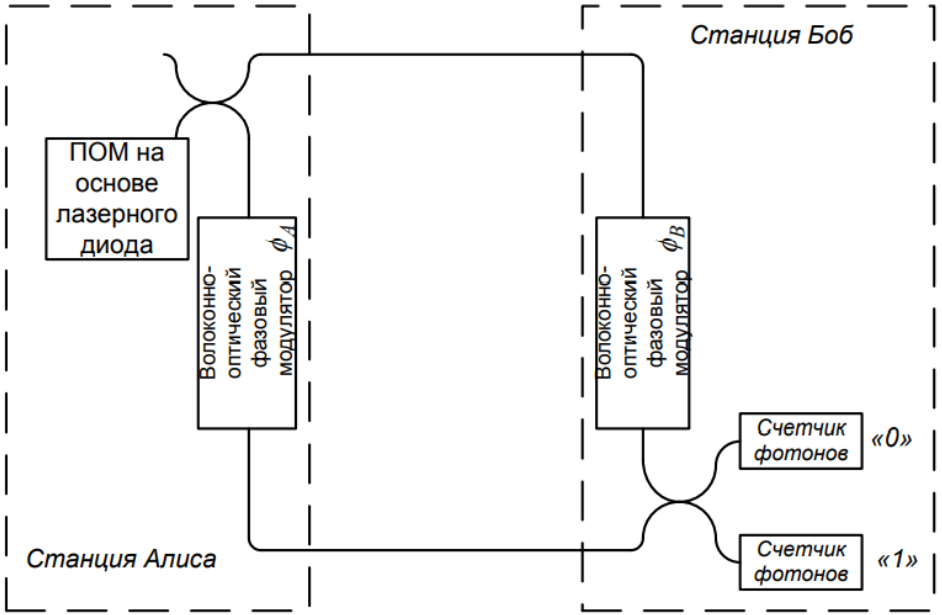
Первая практическая реализация



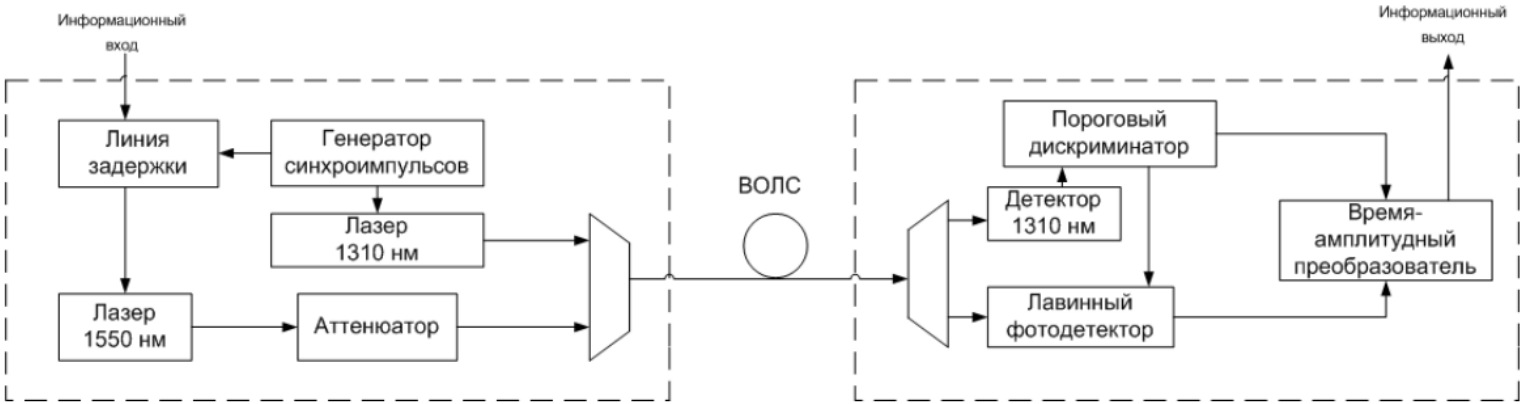
Практическая реализация системы с поляризационным кодированием



Практическая реализация системы с фазовым кодированием



Практическая реализация системы с временным кодированием



СПАСИБО ЗА ВНИМАНИЕ!

Квантовый центр ТГУ
qtcenter.tsu.ru