ФЕСТИВАЛЬ НАУКИ 2012

КВАНТОВАЯ КРИПТОГРАФИЯ

Алексей Федоров

МГТУ им. Н.Э. Баумана

Institute for
Quantum Information Science
at the University of Calgary

Outline

- **Информационное общество**
- **Классическая криптография**
- **Квантовая физика: гипотеза Планка**
- **Мысленный эксперимент: кот Шредингера.**
- **Парадокс Эйнштейна-Подольского-Розена**
- **Протокол BB84**
- **Квантовые компьютеры**

ЧТО ТАКОЕ КВАНТОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ?

Institute for
Quantum Information Science
at the University of Calgary

ИНФОРМАЦИОННОЕ ОБЩЕСТВО

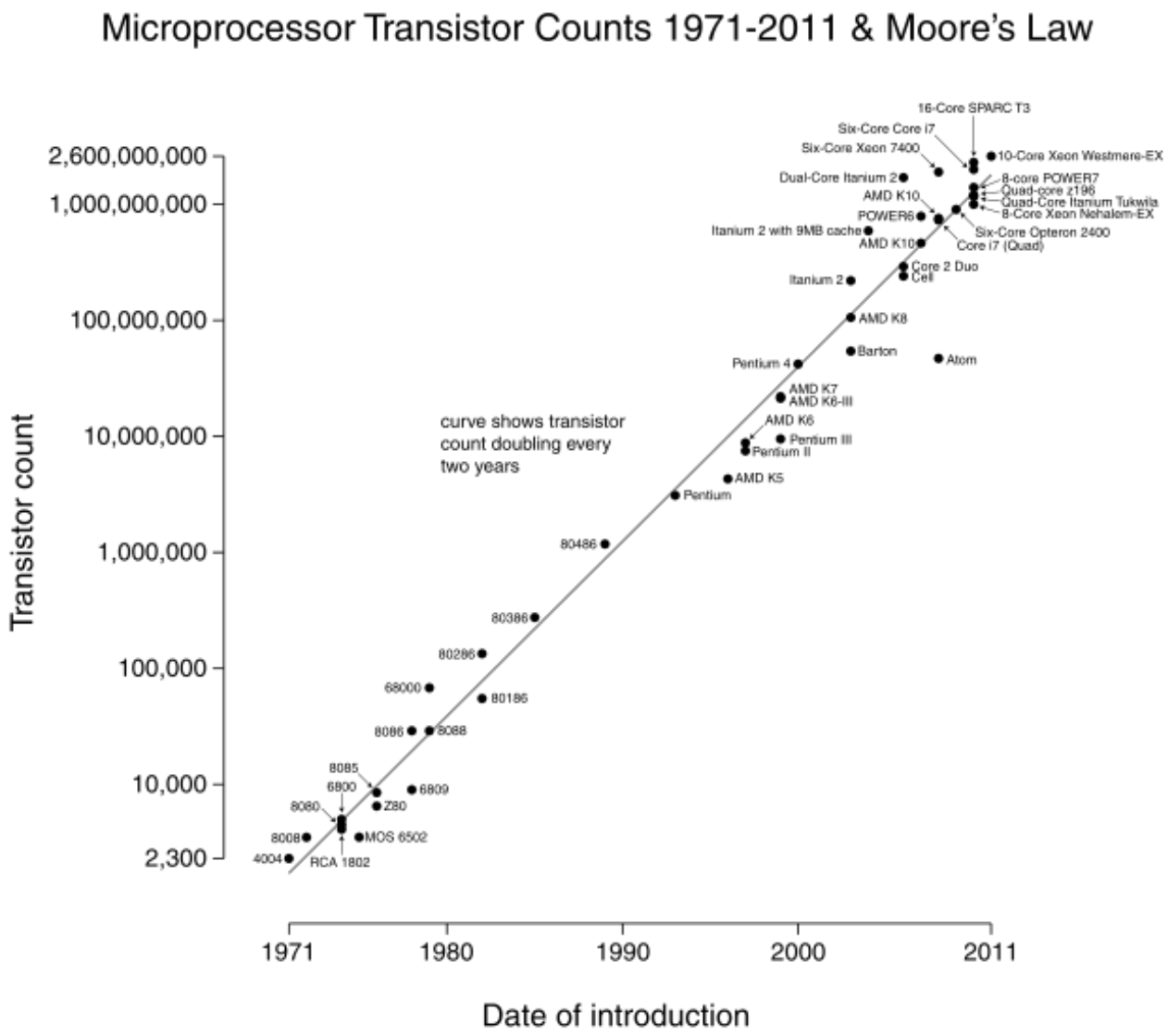
- **Защита информации: криптография?**

Классическая криптография

- **Симметричные шифр: проблема распределения ключа.**
- **Асимметричные шифры: классификация классов сложности задач.**
- **Дискретное логарифмирование: алгоритм Диффи-Хелммана.**
- **Факторизация больших чисел : алгоритм RSA.**

$$N=NP?$$

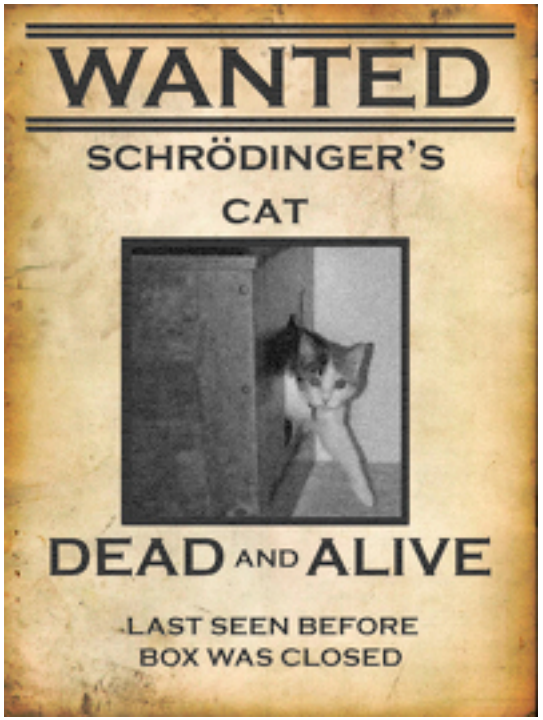
Как развиваются классические ЭВМ?



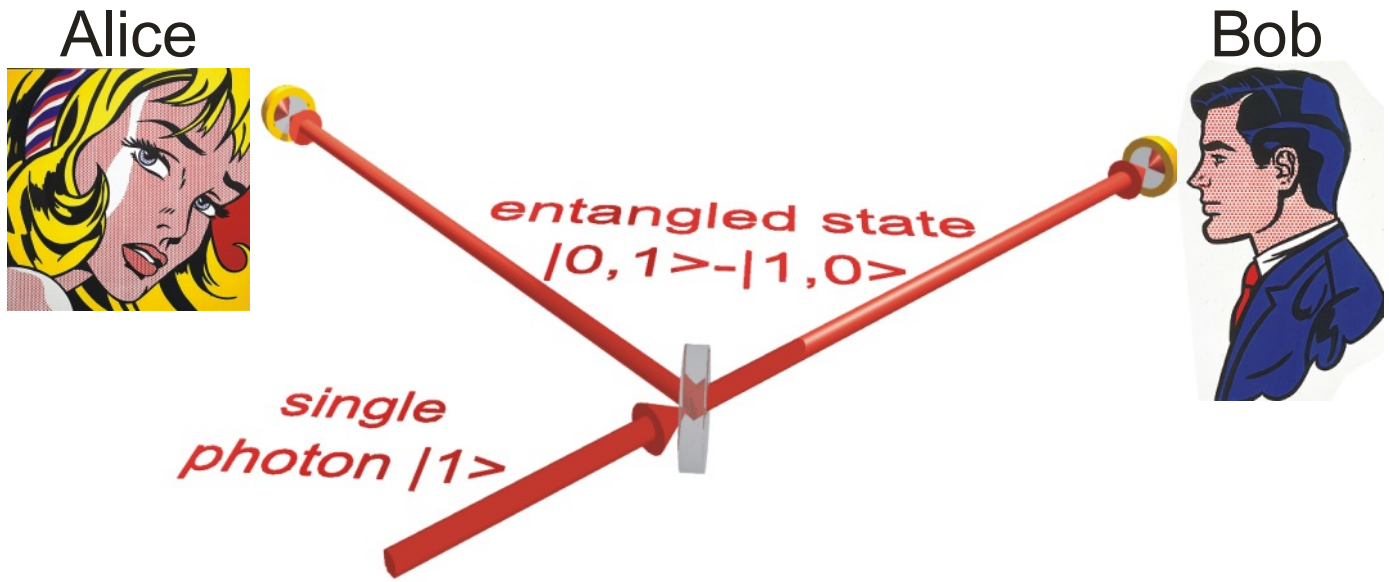
Квантовая физика: гипотеза Планка

Мысленный эксперимент: кот Шредингера

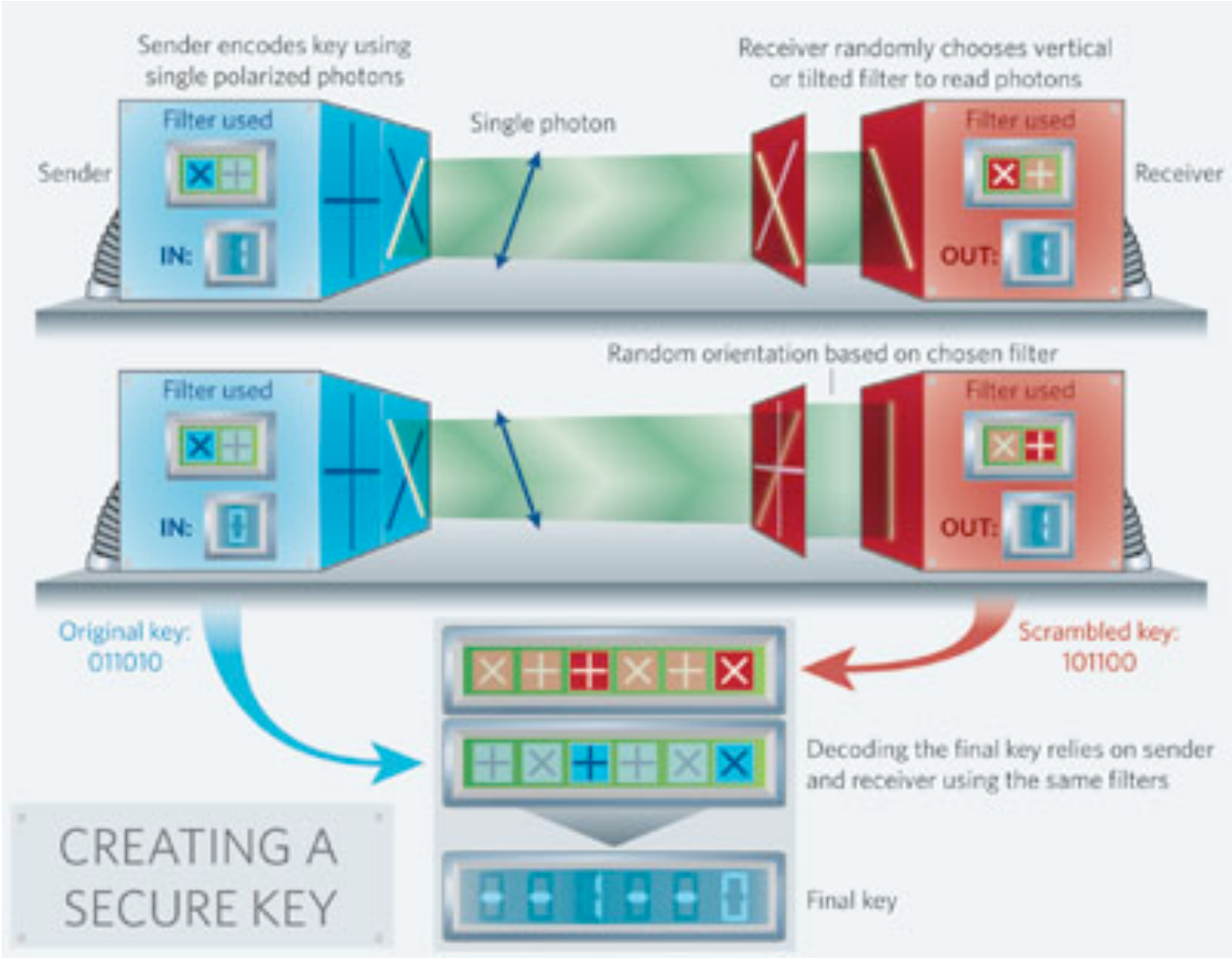
1927 (Э. Шредингер)



Парадокс Эйнштейна-Подольского-Розена

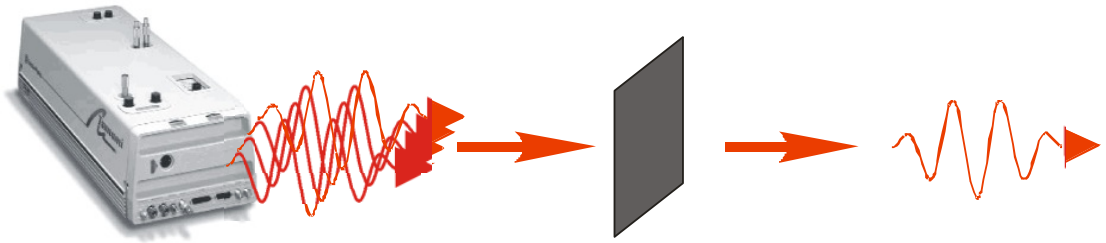


Квантовое распределение ключа BB84

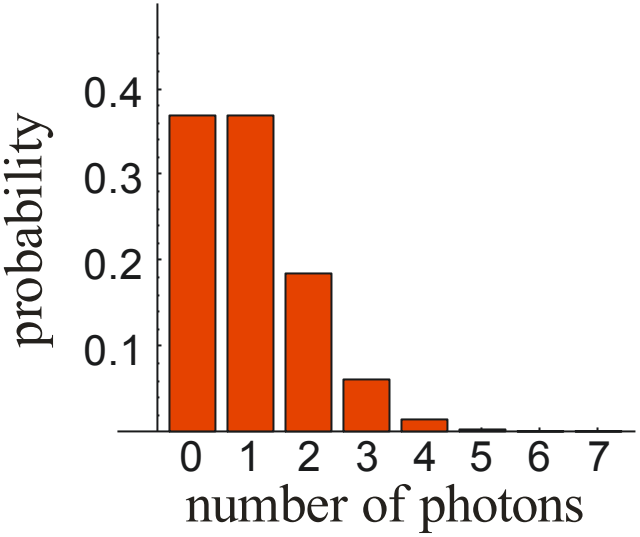


Как можно генерировать единичные фотоны?

- **Слабый лазерный луч?**

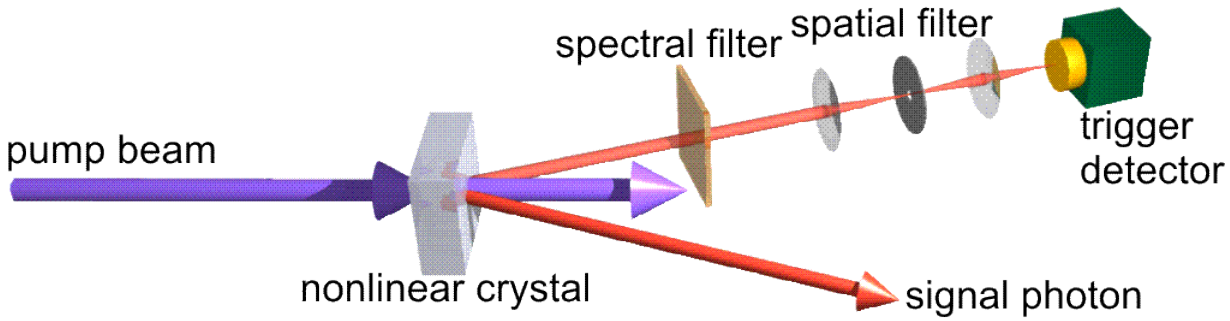


Статистика Пуассона: иногда нуль фотонов, иногда два



Как можно генерировать единичные фотоны?

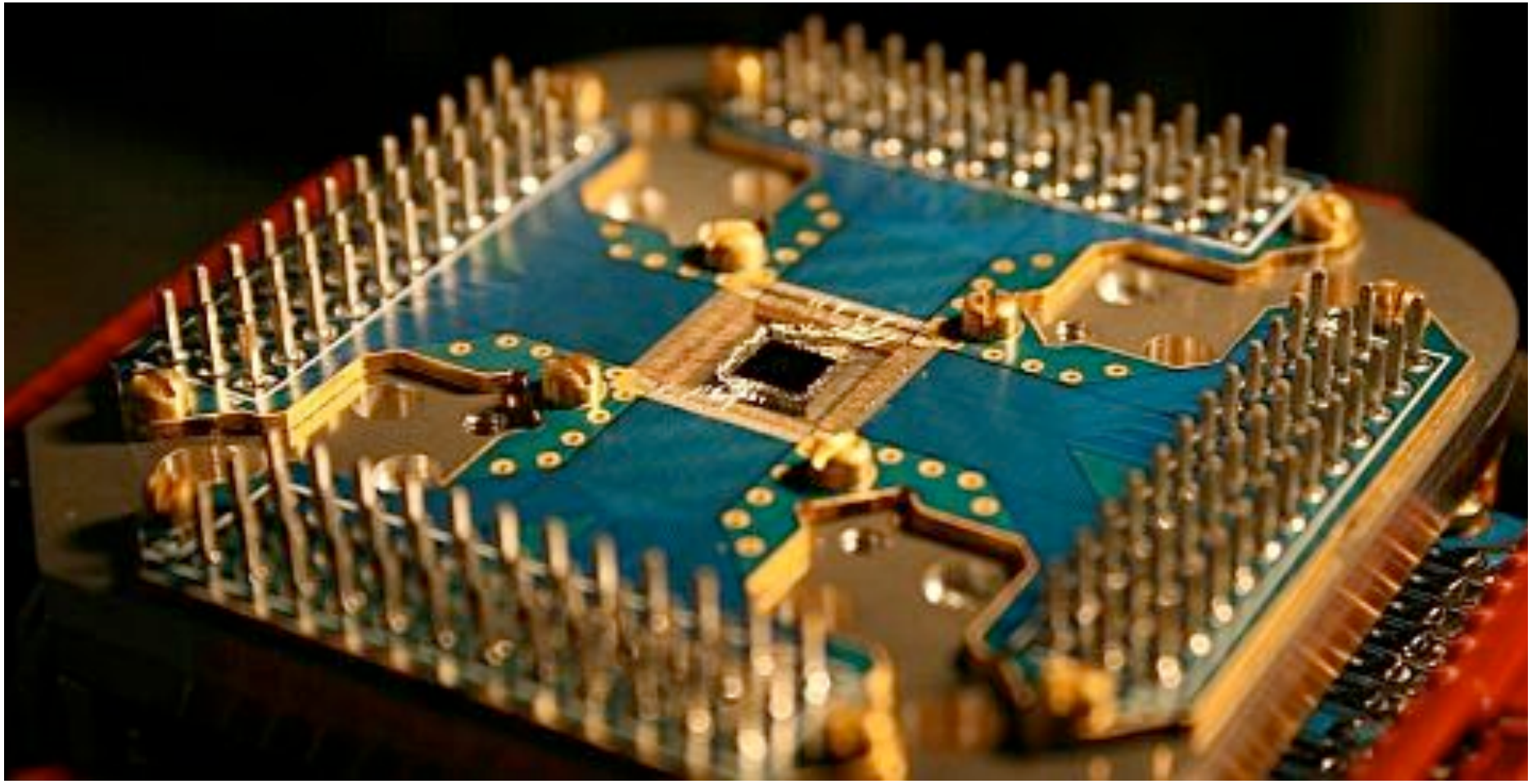
- **Параметрическое рассеяние**



Единичный фотон «не по требованию»

Высокая эффективность

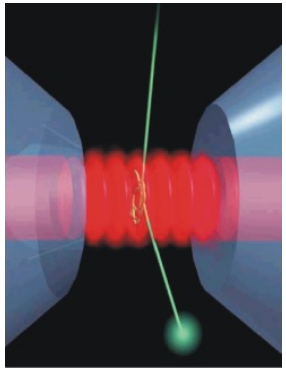
Квантовые компьютеры: квантовые биты



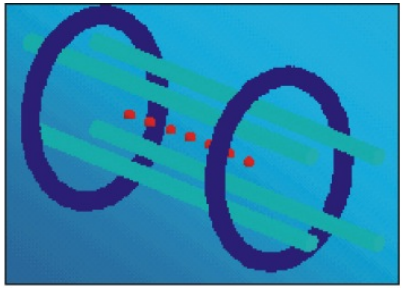
Фотоны как квантовые биты

- Множество систем для выполнения квантовых вычислений

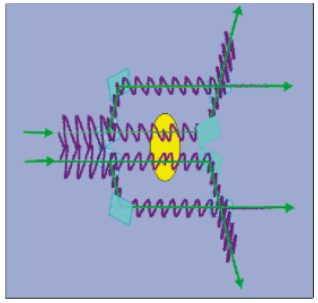
- cavity QED



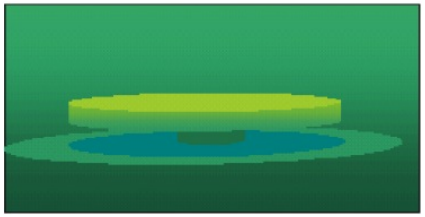
- trapped ions



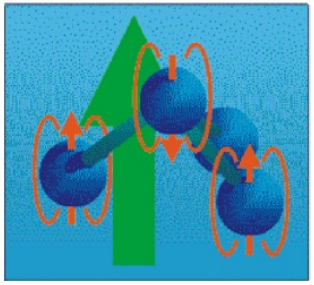
- nonlinear optics



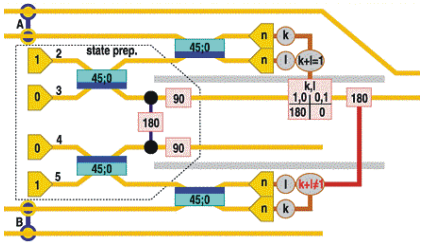
- quantum dots



- NMR



- linear optics



почему фотоны?

Фотоны как квантовые биты

- **Преимущество:**
  - Легко использовать для передачи информации
- **Направление исследований:**
  - Синтез
  - Управление
  - Характеристика
  - Хранение
  - Контроль взаимодействия

Открытые вопросы

- **Как генерировать единичные фотоны?**
- **Как хранить квантовые состояния?**
- **Software для квантового компьютера?**

Спасибо за внимание!

Institute for
Quantum Information Science
at the University of Calgary

Summary

"If you think the photon is something simple, think again…"