



Quantum Cryptography

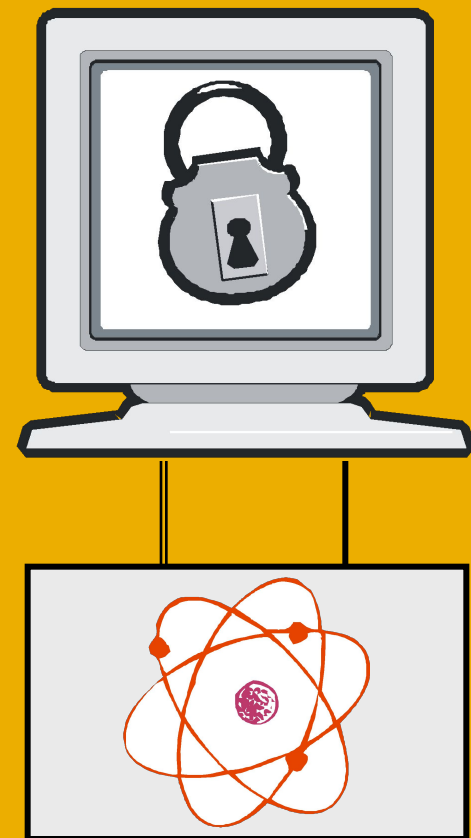
Головдинова Алина

План доклада

- Введение
 - Основные понятия
 - 3 базовых задачи
- Элементы квантовой механики
 - Кубиты
 - Опыт Юнга
- Начала **Quantum cryptography**
 - Протокол BB84

Введение

- **Quantum cryptography** является лучшим применением квантовых вычислений на сегодняшний день
- **Впервые в истории** появилась надежда реализовать с помощью **Quantum cryptography** совершенную секретность
- **Quantum cryptography** работает!

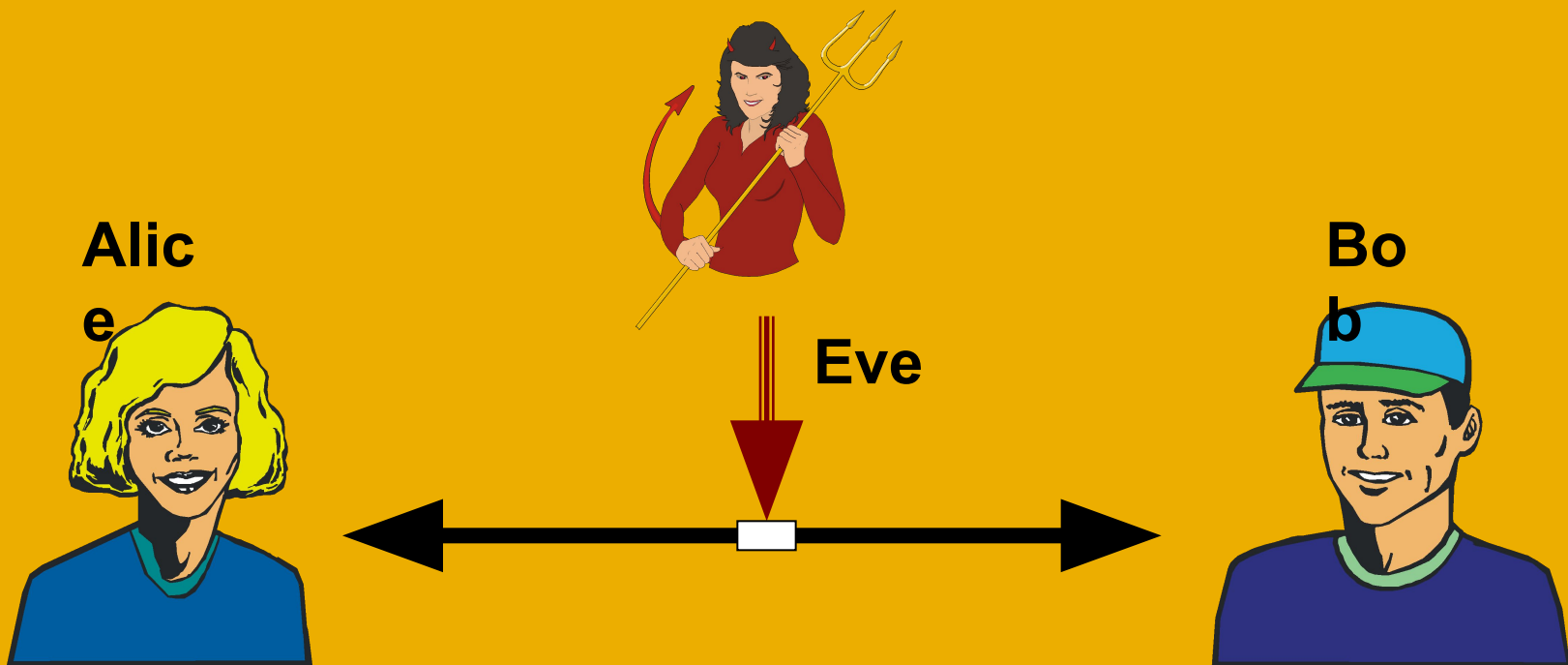


Состояние на сегодня

- Classical Cryptosystems, например RSA, базируется на проблеме разложения на множители.
- Quantum Computers могут взломать такие шифры.
- Нам нужна новая система шифрования!

Основные понятия

- Исходный текст P , ключ K
 $e(P, K) = C$ - шифрованный текст
 $d[e(M, K), K] = P$ - расшифрованный



Проблемы

- Первоначальной секретности
- Аутентификации
- Обнаружение подслушивателя



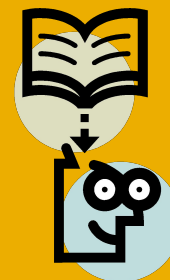
$$\text{Prob}(P|C) = \text{Prob}(C)$$

One-Time Pad (OTP)

$P = P_1, P_2, P_3$ $K = K_1, K_2, K_3$ $C = C_1, C_2, C_3$

$C_i = P_i + K_i \pmod{2}$ for $i=1, 2, 3, \dots$

$P = 11\ 01$ $K = 01\ 00$ $C = P + K = 10\ 01$



Вычислительная безопасность

Определение:

f называется односторонней функцией, если:

- 1) f легко вычислить
- 2) обратную к ней трудно



$E_a \square \square E_b$



Alice : $D_a(Alice)$ $C_s = E_b(P + D_a(Alice)) \square$ Bob

Bob: $D_b(C_s) = P + D_a(Alice)$ $E_a(D_a(Alice)) = Alice$

$$[QC = QKD + OTP]$$

- **QKD: Quantum Key Distribution**
- Используя квантовые методы мы можем передавать ключи в абсолютной секретности
- В результате **совершенная криптосистема:**

$$QC = QKD + OTP$$



Элементы квантовой

механики

■ Измерение

- Наблюдение или **измерение** QS “портит” ее. Опыт Юнга.
- Например **кубит**:

$$|\psi\rangle = a \cdot |0\rangle + b \cdot |1\rangle$$

- При измерении его кубит становится простым битом, т.е. “0” с вероятностью a и “1” с вероятностью b

ФОТОНЫ

■ Физические кубиты

- Подойдет любая субатомная частица, например электрон
- **Фотон** более подходящий
- У фотонов наблюдаются **волновые свойства**



Поляризация

- У фотона есть свойство поляризации, направление, в котором он колеблется.
- Разные поляризации фотона реализуют разные состояния кубита:

$$\theta = 0^\circ \Rightarrow \text{state } |0\rangle$$

$$\theta' = 90^\circ \Rightarrow \text{state } |1\rangle$$

Поляризация и базисы

- Существует устройство, позволяющее узнать поляризацию фотона.
- Введем 2 базиса измерения кубитов:

Прямой:

$$\theta = 0^\circ \Rightarrow \text{state } |0\rangle$$

$$\theta' = 90^\circ \Rightarrow \text{state } |1\rangle$$

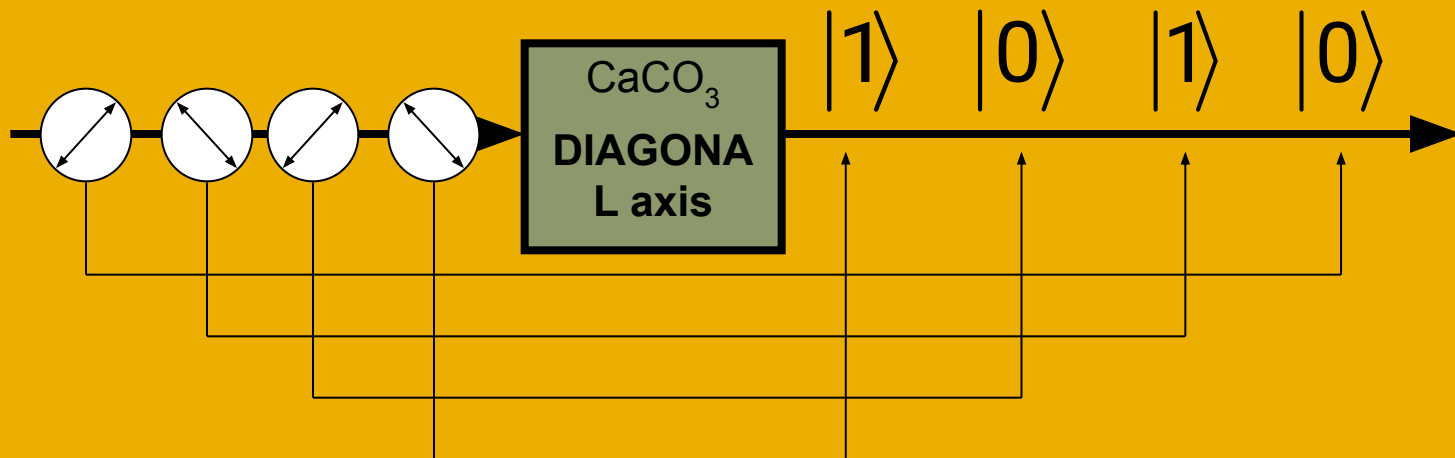
Косой:

$$\theta = 45^\circ \Rightarrow \text{state } |0\rangle$$

$$\theta' = 135^\circ \Rightarrow \text{state } |1\rangle$$

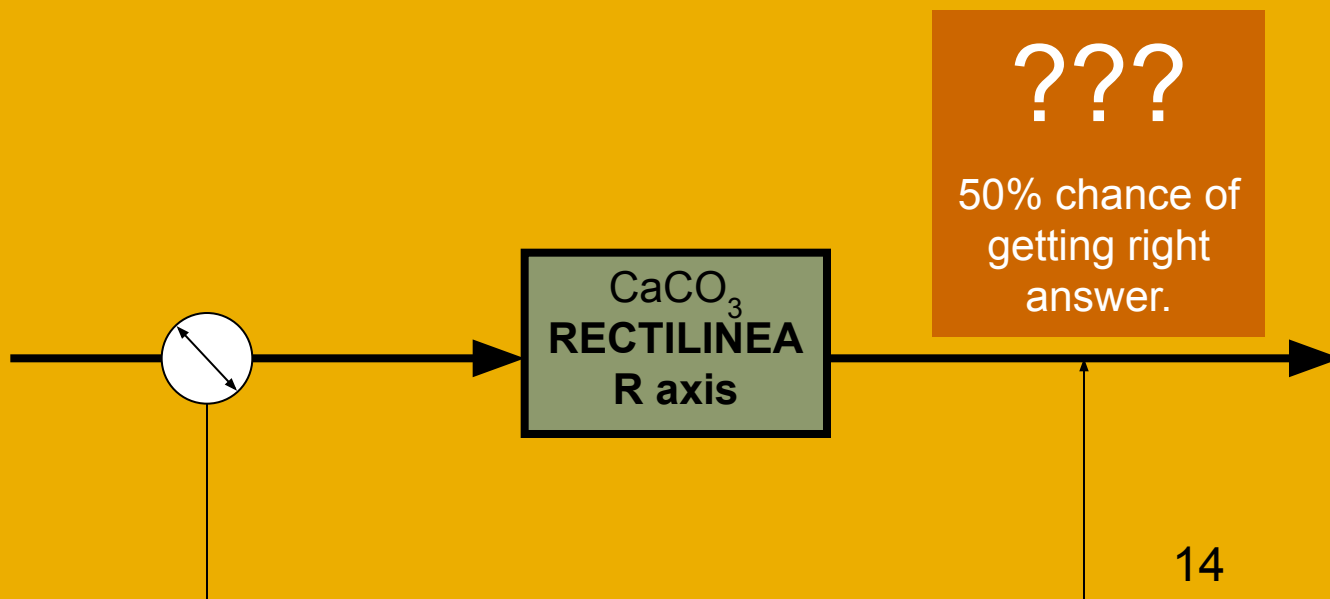
Измерение фотонов

- Например кристаллы, которые проецируют фотоны на базис.



Принцип неопределенности

- Как будет измерен “косополяризованный” фотон, если его спроецировать на прямой базис?



Начала квантовой криптографии

- **Quantum Key Distribution** позволяет избежать подслушивания.
- Если Eve попытается перехватить информацию, то Алиса и Боб узнают об этом.
- **BB84, B92, Entanglement-Based QKD.**






BB84 ...

- **BB84**-это первый безопасный протокол для передачи ключа.
- Он основан на идеях **поляризации фотонов**.
- **Ключ** состоит из битов ,которые передаются как фотоны.

BB84 без подслушивания






- Алиса случайно создает ключ.
- Биты ключа кодируются случайным из 2х базисов.
- Полученные фотоны посылает Бобу.



Bit	0	1	0	1	1
Basis	+	×	×	+	×
Photon					

BB84 без подслушивания (2)

- Боб получает фотоны и считывает их по своим случайным базисам.

Photon					
Basis?	+	+	×	+	×
Bit?	0	0	0	1	1

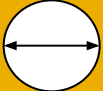


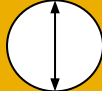
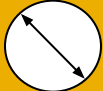
- **Некоторые** базисы он угадал.



ВВ84 без подслушивания (3)

- Алиса и Боб понимают через открытый канал, какие базисы у них совпали.
- Те биты, у которых совпали базисы, формируют (“raw key”) ключ.

Сравнение

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon					
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1



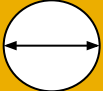


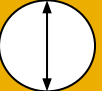

Тестируемые биты позволяют Алисе и Бобу понять, безопасный канал или нет.

Test bits

Проверка

- Если совпали тестовые биты, то никто не подслушивал.
- Тестовые биты удаляются из ключа, и получается (the final key) конечный ключ!

Получение конечного ключа

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon					
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

Test bits
discarde

d

Final Key = 01₂₂

Проверка с подслушивающим

- Если канал подслушивали, то с вероятностью 25% в тестовых битах это будет обнаружено.
- Считывание фотонов Ивом с вер. 0.25 будет раскрыта.
- Фотоны нельзя клонировать.

Работающие экземпляры

- Уже проведены опыты по передаче квантовых битов через оптоволокно на расстояние **23км.**



Первый прототип применения quantum cryptography.

(IBM, 1989)

Выводы

- Quantum cryptography – это основное выдающееся достижение в области безопасности.
- Когда QC получит широкое применение, это позволит в безопасности производить:
 - Банковские транзакции
 - Правительственные переговоры
 - Торговые секреты

Литература

- “A talk on Quantum Cryptography or how Alice outwits Eve” Samuel J. Lomonaco, Jr.
- “Quantum Cryptography” Rajagopal Nagarajan, Nick Papanikolaou.