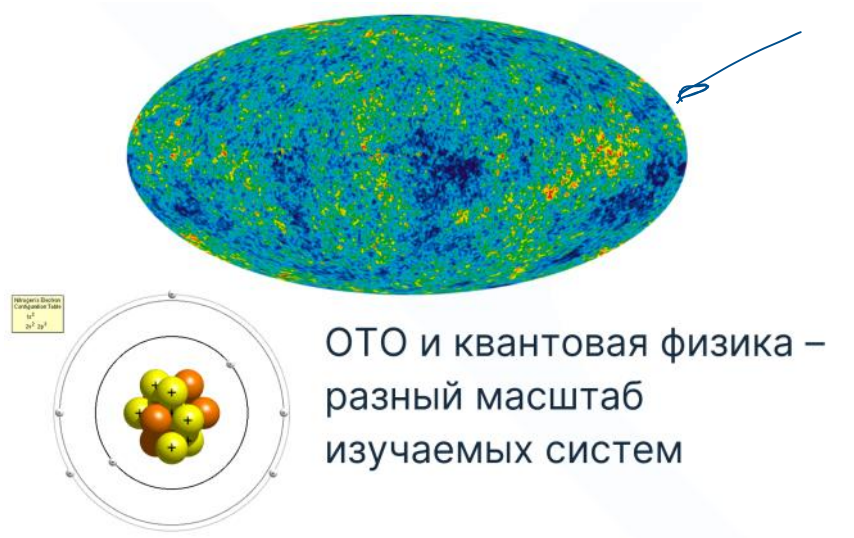
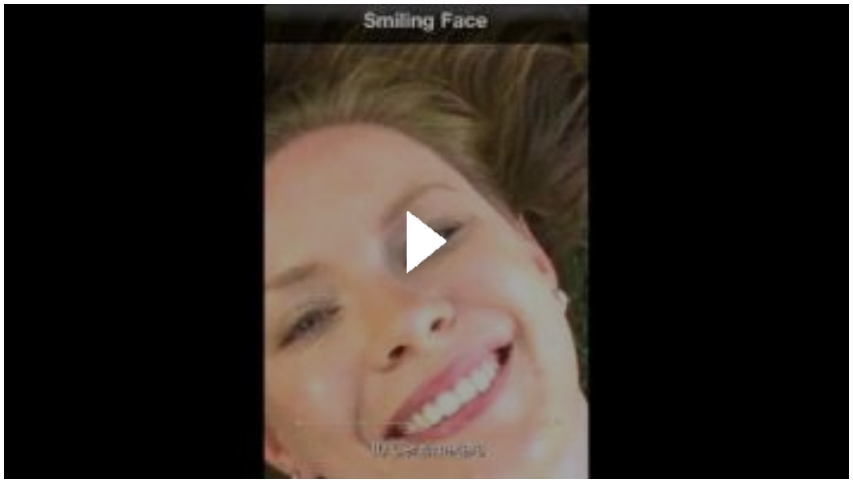
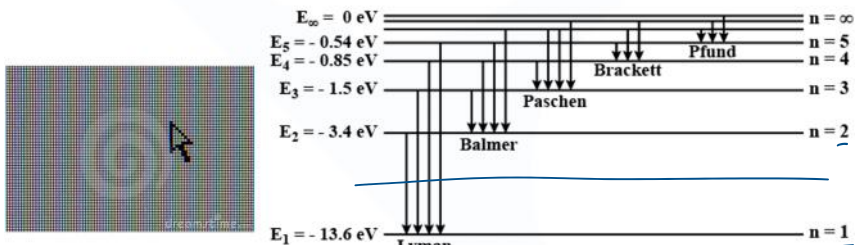
ДПП 11 презентация

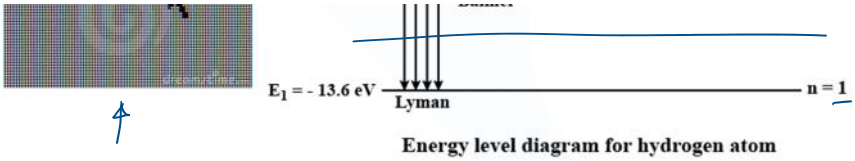
Monday, November 14, 2022 5:06 PM



[From atom to whole universe - Amazing scale video]



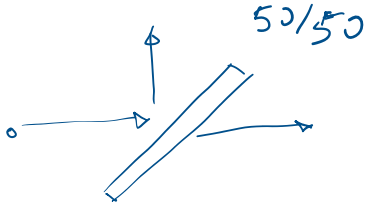


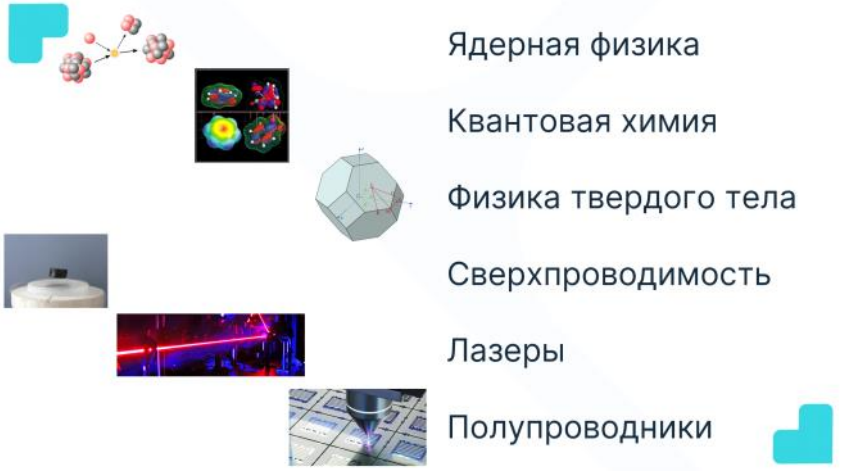


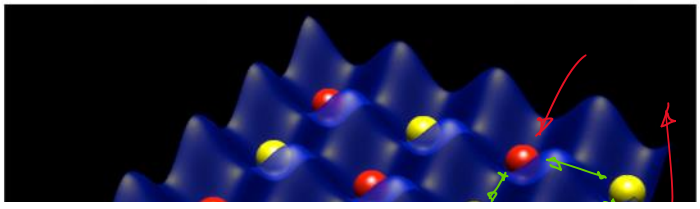
Energy level diagram for hydrogen atom

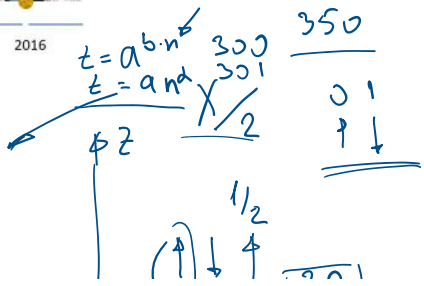
Дискретность микромира

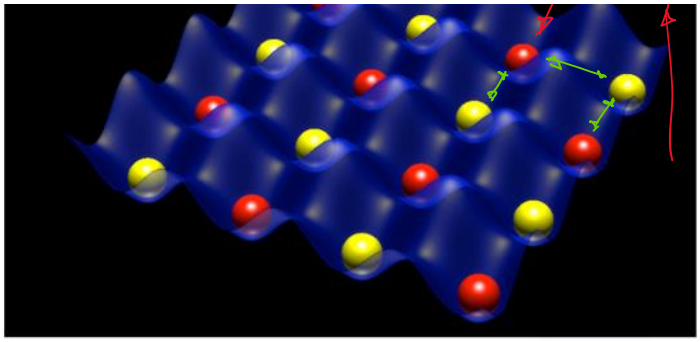
Истинная случайность



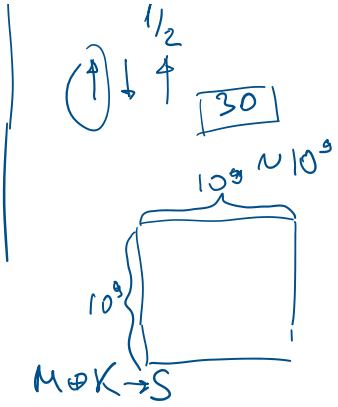


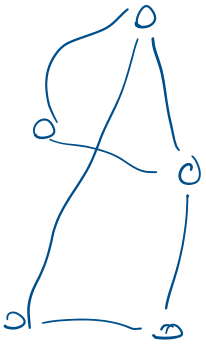




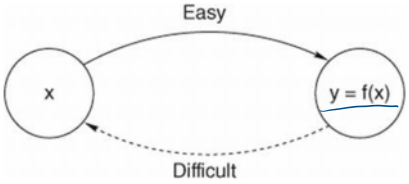


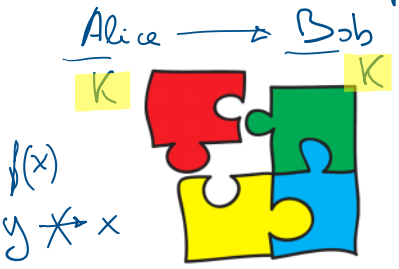
https://www.nist.gov/programs-projects/quantum-computation-and-simulation-neutral-atoms





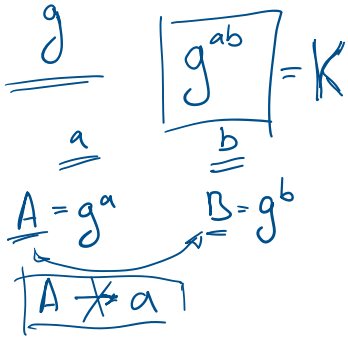
Асимметричное шифрование





В чём идея?

- Боб выбирает секретный закрытый ключ и использует его для вычисления открытого ключа
- Боб посылает открытый ключ Алисе. Его может видеть кто угодно, но вычислить закрытый ключ из открытого *трудно*
- Алиса шифрует сообщение с помощью открытого ключа
- Алиса посылает зашифрованное сообщение Бобу. Расшифровать сообщение без закрытого ключа *трудно*, а с закрытым ключом – легко.
- Боб расшифровывает сообщение Алисы с помощью закрытого ключа



- Для начала возьмем большое число g, оно известно Алисе и Бобу и вообще всем кому угодно.
- Алиса генерирует случайное число a и вычисляет $A = g^a$, отсылает это Бобу.
- Боб генерирует $B = g^b$, отсылает Алисе
- В результате оба имеют общее число g^{ab}, это и есть секретный ключ

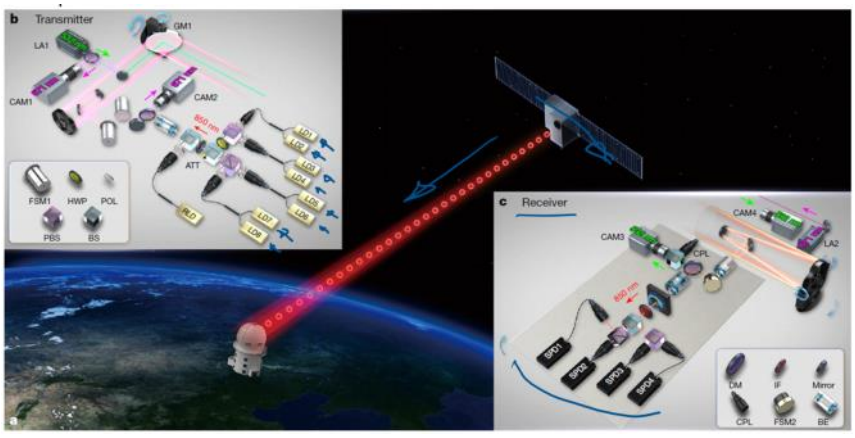
Квантовая криптография

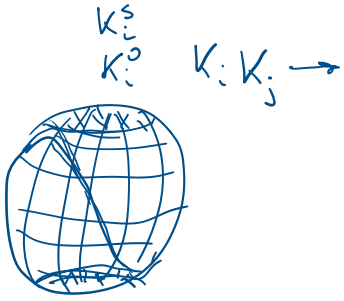
- Концепция
  - Информация кодируется в квантовом состоянии отдельных фотонов
  - Постулаты квантовой механики
    - → Фотон неделим
    - → Квантовое состояние одной частицы нельзя скопировать
    - → Измерение меняет или уничтожает состояние

⇒ Если канал подслушивается, это удаётся обнаружить

- Секретность гарантируется фундаментальными законами физики
- Безусловная устойчивость ко взлому доказана математически
- Естественный и элегантный способ защиты от квантового компьютера

Дата центр в Блаффдэйле, штат Юта. Данные, зашифрованные при помощи асимметричного шифрования могут быть сохранены и расшифрованы в будущем, когда технологии «дорастут»

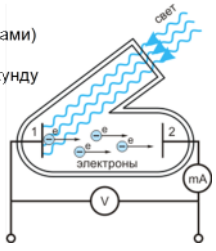




Арт Фридман, Леонард Сасскинд "Квантовая механика. Теоретический минимум"

Фотоны

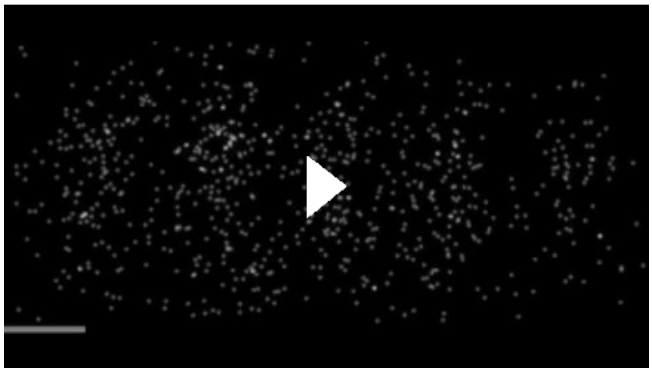
- Зарождение квантовой физики подстегнула проблема излучения абсолютно черного тела.
- В XIXв. в Германии развивалась промышленность. Вернер фон Сименс и Герман фон Гельмгольц изучали светимость тел. нужны были стандарты излучения для производства лампочек
- Фотоэффект объяснил Эйнштейн, 1905 г.
- Свет излучается не непрерывно, а порциями (квантами или фотонами)
- Энергия фотона пропорциональна частоте оптической волны
- В нормальных условиях в наши глаза попадает 10^{12} фотонов в секунду

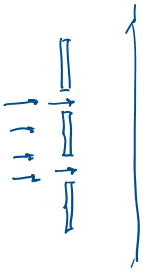


$$E = \hbar\omega$$

Постоянная Планка, 10^{-34} J · s Частота оптической волны, ~10^{15} s^{-1}

Корпускулярно-волновой дуализм, двухщелевой эксперимент
[The Double Slit Experiment Performed With Electrons]





Эксперимент Штерна-Герлаха
[spin : Stern and Gerlach experiment]

Эксперимент Штерна-Герлаха
spin : Stern and Gerlach experiment