

Введение

- Квантовая механика
- Квантовые вычисления
- Методы симметричного шифрования и алгоритм Гровера
- Методы несимметричного шифрования (RSA, Diffie-Hellman, Elliptic curve) и алгоритм Шора.

Двухуровневый атом

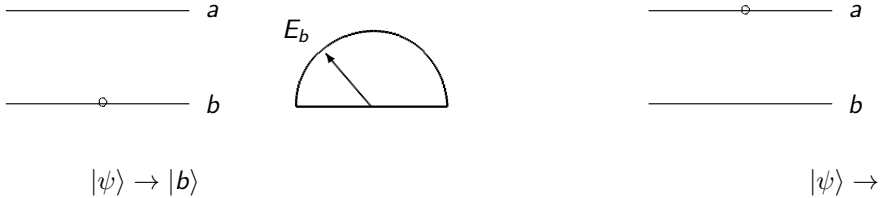


Рис.: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$.

Кот Шредингера

TBD

Отрицательные вероятности

TBD

Базовые блоки квантового компьютера

TBD

Задача о поиске иголки в стоге сена

TBD

Алгоритм Гровера

TBD

Влияние на рекомендации к использованию

$$AES_{128} \rightarrow AES_{256}$$

RSA и задача факторизации чисел

TBD

Diffie-Hellman, Elliptic curve и дискретный логарифм

TBD

Задача о нахождении периода функций и алгоритм Шора

TBD

Влияние на рекомендации к использованию

NSA не рекомендует использование алгоритмов на эллиптических кривых для внутреннего использования.

Что дальше?

TBD

Вопросы

TBD