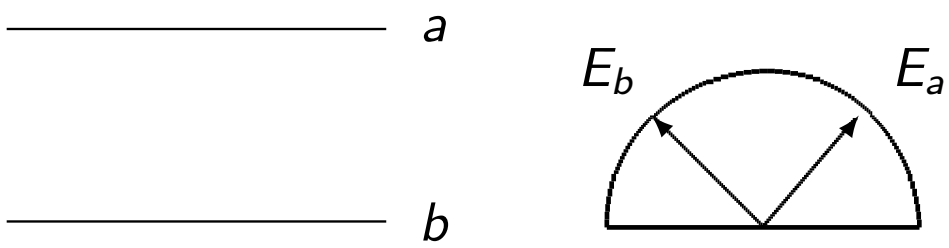
Введение

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

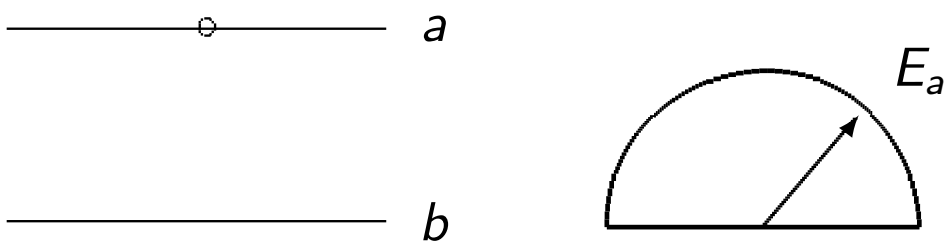
Двухуровневый атом



$$|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$$

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

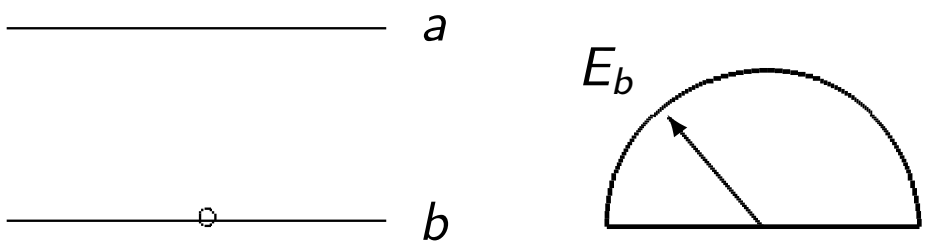
Двухуровневый атом. Измерение E_a



$$|\psi\rangle \to |a\rangle$$

Рис.: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Прибором регистрируется значение энергии E_a. При измерении происходит следующая редукция $|\psi\rangle \to |a\rangle$

Двухуровневый атом. Измерение E_b



$$|\psi\rangle \to |b\rangle$$

Рис.: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Прибором регистрируется значение энергии E_b. При измерении происходит следующая редукция $|\psi\rangle \to |b\rangle$

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 элиптических кривых для внутреннего использования.

Что дальше?

TBD

Вопросы

TBD