Об оценке трудоемкости перебора ключей алгоритмом Гровера с неравновзвешенным состоянием на входе

Андрей Щербаченко

ООО «СФБ Лаб»,
НИУ ВШЭ

РусКрипто’2024
21 марта 2024

andrey.shcherbachenko@sfblaboratory.ru

Квантовая криптография

Цель квантовой криптографии – распределить ключ между двумя легитимными участниками (Алисой и Бобом) посредством передачи квантовых состояний так, чтобы он был недоступен противнику (Еве).

Квантовая криптография

Цель квантовой криптографии – распределить ключ между двумя легитимными участниками (Алисой и Бобом) посредством передачи квантовых состояний так, чтобы он был недоступен противнику (Еве).

Недоступность в квантовой криптографии характеризуется ограничением на следовое расстояние (ε-секретность ключа), которое можно связать со сложностью алгоритмов восстановления ключа, имеющих некоторую (отличную от единицы) вероятность успеха.

ε-секретность

Критерий ε-секретности, в простой форме ($p_\perp = 0$)[1]

$$\frac{1}{2}\left\|\rho_{KE} - \hat{\rho}_K \otimes \rho_E\right\|_1 < \varepsilon,$$

где

- $\rho_{KE} = \sum_{k\in K} P_K(k)|k\rangle\langle k| \otimes \rho_E^k$ – матрица плотности системы, соответствующая вторжению Евы в канал
- $\hat{\rho}_K \otimes \rho_E = \left(\frac{1}{|K|}\sum_{k\in K}|k\rangle\langle k|\right) \otimes \rho_E$ – матрица плотности системы, соответствующая отсутствию вторжения Евы в канал

Оценка ε может быть получена для конкретного протокола в зависимости от алгоритмических и физических параметров системы КРК.

[1] C. Portmann, R. Renner. 'Security in Quantum Cryptography'. Reviews of Modern Physics 94, no. 2 (June 2022). https://doi.org/10.1103/revmodphys.94.025008.

Усеченные алгоритмы опробования

Алгоритм восстановления ключа – опробование начального отрезка из t ключей в упорядоченном ряду апостериорных вероятностей. Минимальная средняя трудоемкость (по числу опробований) при ограничении на вероятность успеха p:

$$Q_{min}^{classic}(p) = \min_{t\,:\,p(t)\geq p} \frac{T(t)}{p(t)},$$

где $T(t)$ – среднее число шагов (трудоемкость) алгоритма в каждом эксперименте, $p(t)$ – вероятность успеха.

Арбеков И.М.

Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой

№ 23 URSS. 2022. 168 с.

Связь ε-секретности с трудоемкостью опробования

Средняя трудоемкость на восстановление одного ключа

Установлена связь с ε-секретностью ($N = |K|$):

$$Q_{min}^{classic}(p) \geq \left(1 - \frac{\varepsilon}{p}\right) \frac{N(1-4\varepsilon)+1}{2}, \quad \varepsilon < p$$

$Q_{max} = \frac{N+1}{2}$ – средняя трудоемкость при равновероятном распределении ключей (достигается при тотальном опробовании: $t = N$, $p(N) = 1$).

Арбеков И.М.

Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой

№ 23 URSS. 2022. 168 с.

Алгоритм Гровера (1)

Алгоритм Гровера

$f : \{0,1\}^n \to \{0,1\}$ – булева функция от n переменных, доступ к которой задается оракулом

$$O^{f(\cdot)} : |x\rangle_n |y\rangle \to |x\rangle_n |y \oplus f(x)\rangle$$

Задача: найти $x \in \{0,1\}^n$, такой, что $f(x) = 1$.

Сложность: $O(\sqrt{2^n})$ вызовов оракула.

L. Grover

A fast quantum mechanical algorithm for database search

Symposium on the Theory of Computing (1996).

Алгоритм Гровера (2)

Псевдокод алгоритма Гровера

Вход: оператор $O^{f(\cdot)}$.

1. Инициализировать систему в состоянии $|0^{\otimes n}\rangle|1\rangle$;
2. Применить оператор $H^{\otimes n+1}$; // $\left(|\hat{\psi}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\right) \otimes |-\rangle$
3. Для $i := 1$ до t:
   - 3.1 Вызвать $O^{f(\cdot)}$;
   - 3.2 Применить $H^{\otimes n} \otimes I$;
   - 3.3 Применить $(2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I^{\otimes n}) \otimes I$;
   - 3.4 Применить $H^{\otimes n} \otimes I$;
4. Провести измерение.

Построение оракула в алгоритме Гровера

Функция f выбирается целесообразно решаемой задаче.

1. Перебор ключей алгоритмов блочного шифрования: $f(k) = \bigwedge_{i=1}^{q} I\{E(k, P_i) = C_i\}$, где $(P_1, C_1), \ldots, (P_q, C_q)$ – известные пары ОТ/ШТ
2. Нахождение прообраза хэш-функции: $f(x) = I\{H(x) = h\}$, где h – хэш-код, для которого ищется прообраз
3. Нахождение коллизии хэш-функции: $f(x) = I\{H(x) \in L \bigwedge L\,[H(x)] \neq x\}$, где L – предвычисленная хэш-таблица, не содержащая коллизий
4. и т.д.

Оракул $O^{f(\cdot)}$ реализует вычисление соответствующего криптопримитива в виде унитарного оператора.

Квантовое опробование обобщенным алгоритмом Гровера

Будем рассматривать алгоритм Гровера в общем виде

$$G(t) := U_t O_t^{f(\cdot)} \dots U_2 O_2^{f(\cdot)} U_1 O_1^{f(\cdot)},$$

где операторы U_i и входное состояние $|\psi\rangle$ – произвольные, оракулы $O_i^{f(\cdot)}$ одинаково действуют на базисные состояния, но допускают разную реализацию.

Вероятность успеха в нахождении ключа k ($f(k) = 1$):

$$p(G(t), |\psi\rangle) = |\langle k|G(t)|\psi\rangle|^2$$

Единица квантового опробования

Единица квантового опробования – одно обращение к оракулу. Почему?

1. Вызовы оракула – наиболее затратная часть алгоритма
2. Как правило, оракул реализует унитарное вычисление реального криптопримитива (единицы, в которых удобно мерить классическую трудоемкость – «одно зашифрование», «одно вычисление хэш-функции» и т.д.)
3. Вызовы оракула могут происходить в режиме «онлайн» (модель Q2 в доказуемой стойкости) и учитываются отдельно от вычислительных ресурсов

При необходимости можно получить оценку вычислительных операций в конкретной алгебре операторов (Клиффорд + T, Тоффоли и т.д.).

Атака Евы

Вариант действий Евы:

1. Ева **не** измеряет свою систему ρ_E после унитарной атаки на протокол

Атака Евы

Вариант действий Евы:

1. Ева **не** измеряет свою систему ρ_E после унитарной атаки на протокол
2. Выполняет над состоянием унитарные преобразования, соответствующие шагам протокола (усиление секретности путем хэширования)

Атака Евы

Вариант действий Евы:

1. Ева **не** измеряет свою систему ρ_E после унитарной атаки на протокол
2. Выполняет над состоянием унитарные преобразования, соответствующие шагам протокола (усиление секретности путем хэширования)
3. Перехватывает обработанные сообщения в классическом канале, формирует оракул $O^{f(\cdot)}$ (или множество оракулов), который помечает истинный ключ

Атака Евы

Вариант действий Евы:

1. Ева **не** измеряет свою систему ρ_E после унитарной атаки на протокол
2. Выполняет над состоянием унитарные преобразования, соответствующие шагам протокола (усиление секретности путем хэширования)
3. Перехватывает обработанные сообщения в классическом канале, формирует оракул $O^{f(\cdot)}$ (или множество оракулов), который помечает истинный ключ
4. Использует преобразованное состояние ρ_E (или его часть) как вход алгоритма Гровера с оракулом $O^{f(\cdot)}$, выполняя **квантовое опробование**

Возможные ситуации (1)

Пусть выполнено $\frac{1}{2}\left\|\rho_{KE} - \hat{\rho}_K \otimes \rho_E\right\|_1 < \varepsilon$, рассмотрим следующую ситуацию:

- $\rho_{KE} = \sum_{k \in K} P_K(k)|k\rangle\langle k| \otimes \underbrace{|\psi\rangle\langle\psi|}_{\rho_E}$ – состояние Евы не коррелировано с ключами, но распределение на ключах P_K неравновероятное

Полагаем, что состояние Евы является **чистым**: $\rho_E = |\psi\rangle\langle\psi|$, $|\psi\rangle = \sum_{z \in K} \alpha_z |z\rangle$, оно поступает на вход алгоритма Гровера и известно Еве (с точностью до амплитуд α_z)

Возможные ситуации (2)

Пусть выполнено $\frac{1}{2}\left\|\rho_{KE} - \hat{\rho}_K \otimes \rho_E\right\|_1 < \varepsilon$, рассмотрим следующую ситуацию:

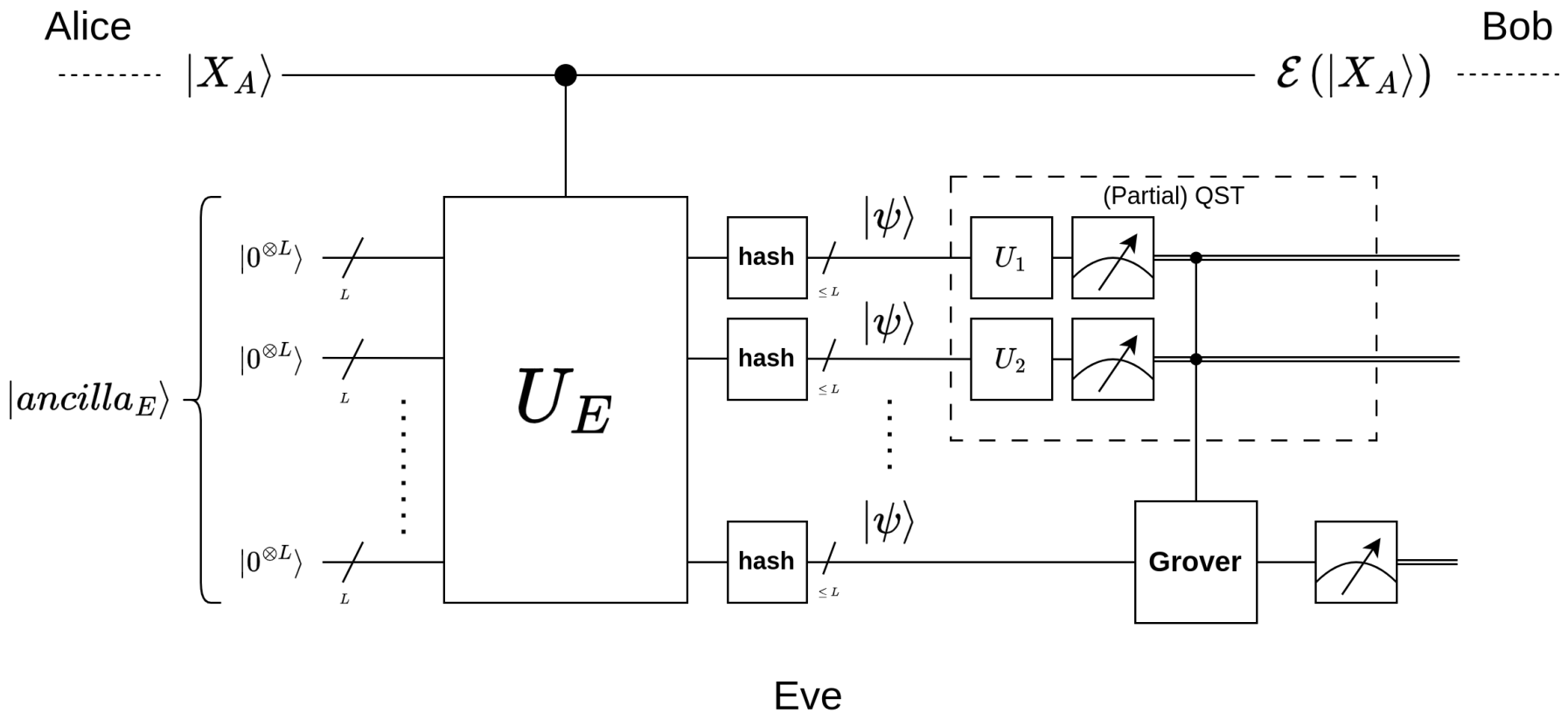
- $\rho_{KE} = \sum_{k \in K} P_K(k)|k\rangle\langle k| \otimes \underbrace{|\psi_k\rangle\langle\psi_k|}_{\rho_E^k}$– состояние Евы

  коррелировано с ключами, распределение на ключах P_K неравновероятное

Полагаем, что состояние Евы является **смешанным**:
$\rho_E = \sum P_K(k)|\psi_k\rangle\langle\psi_k|$, $|\psi_k\rangle = \sum_{z \in K} \alpha_{z|k}|z\rangle$, на вход алгоритма Гровера поступает состояние $|\psi_k\rangle$ из ансамбля с вероятностью $P_K(k)$

Как Ева может узнать состояние, с которым работает?

В пользу Евы полагаем, что она может проводить томографию состояния, которое подается на вход алгоритма Гровера, и адаптировать его для достижения наилучшей трудоемкости



Трудоемкость квантового опробования

Определим минимум средней трудоемкости алгоритма квантового опробования по аналогии с «классическим» случаем:

$$Q_{min}^{quant}(p) = \min_{t, G(t), |\psi\rangle : \overline{p} \geq p} \frac{T(G(t), |\psi\rangle)}{\overline{p}(G(t), |\psi\rangle)},$$

где

- $T(G(t), |\psi\rangle)$ – среднее (по распределению на множестве ключей $P_K(k)$) число итераций алгоритма при начальном состоянии $|\psi\rangle = \sum_z \alpha_z |z\rangle$ и эволюции $G(t)$
- $\overline{p}(G(t), |\psi\rangle) = \sum_k P_K(k) \left|\langle k| G(t) |\psi\rangle\right|^2$ – средняя вероятность успеха алгоритма

Минимум трудоемкости берется одновременно по всем возможным эволюциям $G(t)$ и входным состояниям, и с учетом ограничения на следовое расстояние.

Нижняя оценка

Метод: оценивается сверху и снизу математическое ожидание (распределение P_K) квадрата отклонения по следовой норме действия оператора $G(t)$ с произвольной эволюцией между вызовами оракула на произвольное состояние $|\psi\rangle$ и возможными решениями $|k\rangle$.

Оценка минимума средней трудоемкости квантового опробования

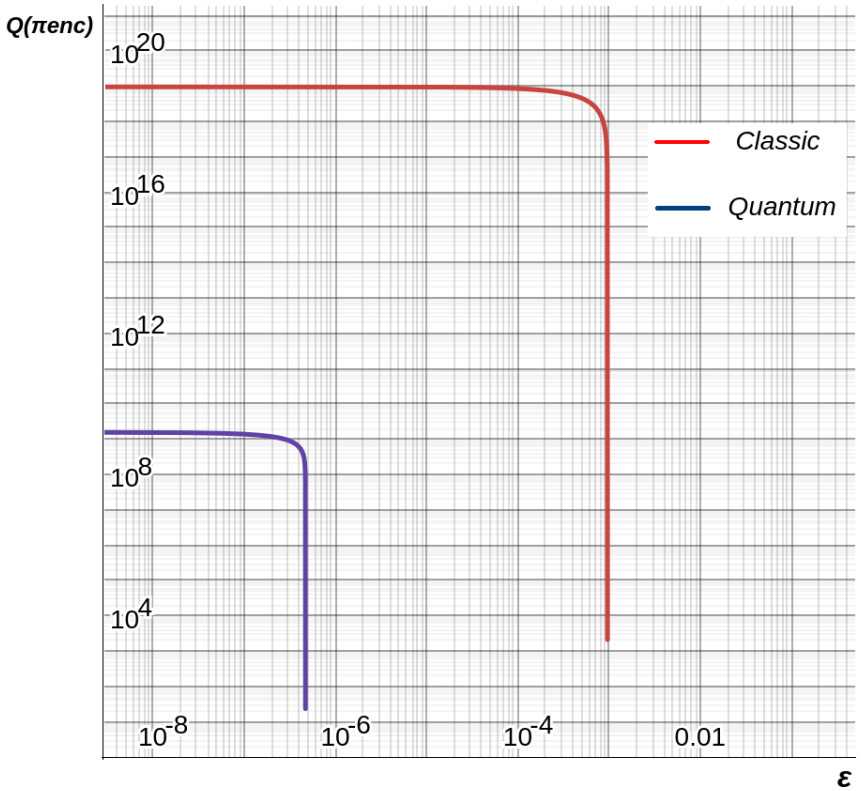
Получена следующая оценка:

$$Q(p) \geq \sqrt{\frac{N\left(1 - 2\frac{\varepsilon}{p^2}\right)}{8}}$$

Графики для классической и квантовой трудоемкости

π_{enc} – максимально допустимое значение вероятности эффективного применения методов криптографического анализа (Р 1323565.1.005–2017)

Пример при $\pi_{enc} = 2^{-10}, N = 2^{64}$



Заключение

1. Получена нижняя оценка трудоемкости опробования неравновероятных ключей на квантовом вычислителе (конкретным классом Гровер-подобных алгоритмов)

Заключение

1. Получена нижняя оценка трудоемкости опробования неравновероятных ключей на квантовом вычислителе (конкретным классом Гровер-подобных алгоритмов)
2. При соблюдении требований безопасности к системе КРК (малости величины ε) распределяемые ключи стойкие к рассмотренному классу переборных атак квантового противника

Заключение

1. Получена нижняя оценка трудоемкости опробования неравновероятных ключей на квантовом вычислителе (конкретным классом Гровер-подобных алгоритмов)
2. При соблюдении требований безопасности к системе КРК (малости величины ε) распределяемые ключи стойкие к рассмотренному классу переборных атак квантового противника
3. Вопрос о точности полученной оценки остается открытым: возможно ли в явном виде построить алгоритм, трудоемкость которого близка к данной оценке?

Благодарю за внимание!

Андрей Щербаченко

ООО «СФБ Лаб»,
НИУ ВШЭ
РусКрипто’2024
21 марта 2024

andrey.shcherbachenko@sfblaboratory.ru

Обозначения

- $|\psi\rangle = (\alpha_0, \dots, \alpha_{2^n-1}) \in \mathbb{C}^{2^n}$ – кет-вектор, $\sum_i |\alpha_i|^2 = 1$
- $\langle\psi| = (\alpha_0^*, \dots, \alpha_{2^n-1}^*)^T \in \mathbb{C}^{2^n}$ – бра-вектор
- $\langle\psi|\varphi\rangle$ – скалярное произведение
- $|\psi\rangle\langle\psi|$ – матрица плотности чистого состояния
- $\rho = \sum_\psi p_\psi |\psi\rangle\langle\psi|$ – матрица плотности смешанного состояния
- Измерение:
  $|\psi\rangle \overset{\{\Pi_x\}}{\to} \left(P(|0\rangle) = |\alpha_0|^2, P(|1\rangle) = |\alpha_1|^2, \dots, P(|2^n-1\rangle) = |\alpha_{2^n-1}|^2\right)$
- $d(\rho_1, \rho_2) = \frac{1}{2}\left\|\rho_1 - \rho_2\right\|_1 = \frac{1}{2} Tr\left(\sqrt{(\rho_1 - \rho_2)^*(\rho_1 - \rho_2)}\right)$ – следовое расстояние
- $I\{A(x)\}$ – индикаторная функция от предиката $A(x)$, $I\{A(x)\} = 1$ если $A(x)$ истинно, иначе $I\{A(x)\} = 0$