конференция
РусКрипто

Ежегодная международная научно-практическая конференция
«РусКрипто'2022»

Задача скрытой подгруппы в квантовом криптоанализе

Поляков Михаил
Ассистент кафедры «Информационная безопасность»,
МГТУ им. Н.Э.Баумана

Введение

- 1994г. П. Шор опубликовал два полиномиальных алгоритма для решения задачи дискретного логарифмирования и факторизации
- 1995г. работа Д.Бонэ по криптоанализу систем со «скрытым сдвигом» на квантовом компьютере
- 1997г. А.Китаев показал, что существует полиномиальный алгоритм для поиска стабилизатора в произвольной конечной абелевой группе

Алгоритм Саймона. Задача скрытой подгруппы

- Атаки на сети Фейстеля на основе подобранных открытых текстов
- Построение различителей для обобщенных сетей Фейстеля
- Атаки на схемы аутентификационного шифрования и FX-конструкции
- Проблема изоморфизма двух графов
- Задача о кратчайшем векторе решетки

Поиск линейных структур с помощью алгоритма Саймона

- Рассмотрим булев оператор $\boldsymbol{F}:\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ (векторную булеву функцию)
- $\boldsymbol{F}$ обладает линейной структурой, если

$$\forall \boldsymbol{x} \in \mathbb{Z}_2^n \;\; \boldsymbol{F}(\boldsymbol{x}) \oplus \boldsymbol{F}(\boldsymbol{x} \oplus \boldsymbol{a}) = \delta,$$

где $(\boldsymbol{a}, \delta) \in \mathbb{Z}_2^n \backslash \{0\} \times \mathbb{Z}_2^n \backslash \{0\}$

Поиск линейных структур с помощью алгоритма Саймона

- Начальное состояние

$$|\varphi_1\rangle = |\mathbf{0}, \delta\rangle$$

- Суперпозиция состояний

$$|\varphi_2\rangle = |H^{\otimes n}(\mathbf{0})\rangle|\delta\rangle = \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} |\boldsymbol{x}\rangle|\delta\rangle$$

- Обращение к оракулу $U_{\boldsymbol{F}}$

$$|\varphi_3\rangle = U_{\boldsymbol{F}}(|\varphi_2\rangle) = \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} |\boldsymbol{x}\rangle|\boldsymbol{F}(\boldsymbol{x}) \oplus \delta\rangle$$

Поиск линейных структур с помощью алгоритма Саймона

- Измерение второго регистра

$$|\varphi_4\rangle = M(|\varphi_3\rangle) = \frac{1}{\sqrt{2}}(|\boldsymbol{x}\rangle \oplus |\boldsymbol{x} \oplus \boldsymbol{a} \oplus \delta\rangle)$$

- Гейт Адамара к первому регистру

$$|\varphi_5\rangle = H(|\varphi_4\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{\boldsymbol{y} \in \mathbb{Z}_2^n} \left((-1)^{\langle \boldsymbol{x},\boldsymbol{y}\rangle} + (-1)^{\langle \boldsymbol{y},\boldsymbol{x}\oplus\boldsymbol{a}\oplus\delta\rangle}\right)|\boldsymbol{y}\rangle$$

Обобщение задачи поиска линейных структур

- Рассмотрим $g \in S_n(\mathbb{Z}_2^n)$, которая обладает линейной структурой, если

$$\forall \boldsymbol{x} \in \mathbb{Z}_2^n \;\; \boldsymbol{x}^g \oplus (\boldsymbol{x} \oplus \boldsymbol{a})^g = \delta$$

- Пусть G – некоторая группа, S – произвольное конечное множество. $\boldsymbol{F}: G \to S$ скрывает подгруппу $H \leq G$, если

$$\forall x, y \in G \;\; \boldsymbol{F}(x) = \boldsymbol{F}(y) \Leftrightarrow x^{-1}y \in H.$$

Обобщение задачи поиска линейных структур

- Подготовка начального состояния – суперпозиции элементов исследуемой группы
- Схема дискретного преобразования Фурье для $g \in S_n$
- Получение информации из финального состояния

Обобщение задачи поиска линейных структур

- G – некоторая конечная группа
- $\mathrm{GL}_n(\mathbb{C})$ – полная линейная группа
- Гомоморфизм $\rho\colon \mathrm{G} \to \mathrm{GL}_n(\mathbb{C})$ называется *представлением группы* G
- n – размерность представления (также справедливо обозначение d_ρ)
- ρ – *неприводимое*, если его нельзя разложить в прямую сумму двух других представлений

Квантовое преобразование Фурье

- Для неабелевой группы G квантовое преобразование Фурье

$$|x\rangle \mapsto \frac{d_\rho}{\sqrt{|\mathrm{G}|}} \sum_{\rho \in \widehat{\mathrm{G}}} |\rho, \rho(x)\rangle ,$$

где $x \in \mathrm{G}$, $\widehat{\mathrm{G}}$ - множество всех неприводимых представлений G, $|\rho(x)\rangle$ - состояние, амплитуда которого задается матрицей размерности d_ρ^2:

$$|\rho(x)\rangle = \left(\rho(x) \otimes I_{d_\rho}\right) \sum_{j=1}^{d_\rho} \frac{|j, j\rangle}{\sqrt{d_\rho}} = \sum_{j,k=1}^{d_\rho} \frac{\rho(x)_{j,k} |j, k\rangle}{\sqrt{d_\rho}}$$

Алгоритм для группы S_n

- Начальное состояние

$$|\varphi_1\rangle = |\mathbf{0}, \delta\rangle$$

- Суперпозиция состояний

$$|\varphi_2\rangle = \frac{1}{\sqrt{|S_n|}} \sum_{g \in \mathrm{G}} |g\rangle |\delta\rangle$$

- Обращение к оракулу $U_{\boldsymbol{F}}$:

$$|\varphi_3\rangle = \frac{1}{\sqrt{|S_n|}} \sum_{g \in \mathrm{G}} |g\rangle |\delta \oplus \boldsymbol{F}(g)\rangle$$

Алгоритм для группы S_n

- Измерение второго регистра, в первом получаем состояние

$$|\varphi_4\rangle = \frac{1}{\sqrt{|\mathrm{H}|}} \sum_{h \in \mathrm{H}} |gh\rangle\,|s \oplus \delta\rangle$$

- Квантовое преобразование Фурье к первому регистру

$$|\varphi_5\rangle = \frac{d_\rho}{\sqrt{|\mathrm{H}|}} \sum_{\rho \in \widehat{\mathrm{G}}} |\rho, \rho(gh)\rangle$$

Алгоритм для группы S_n

- Если переписать состояние $|\varphi_5\rangle$

$$\sqrt{\frac{d_\rho}{|\mathrm{G}|}} \sum_{\rho \in \widehat{\mathrm{G}}} \sum_{j,k=1}^{d_\rho} \left[\sum_{h \in \mathrm{H}} \rho(gh)_{j,k} \right] |\rho, j, k\rangle$$

- «Слабое» сэмплирование Фурье – собираем информацию на основе амплитуды состояния $|\rho\rangle$
- «Сильное» сэмплирование Фурье – интересует амплитуда состояния $|\rho, j, k\rangle$

Вопросы

???

Контактная информация

Электронная почта:

m.polyakov@bmstu.ru

Телефон:

+7 926 469-96-83