Подход к оценке стойкости блочных шифров к линейному криптоанализу с использованием квантовых алгоритмов

Щербаченко А.А.

ООО «СФБ-Лаб»

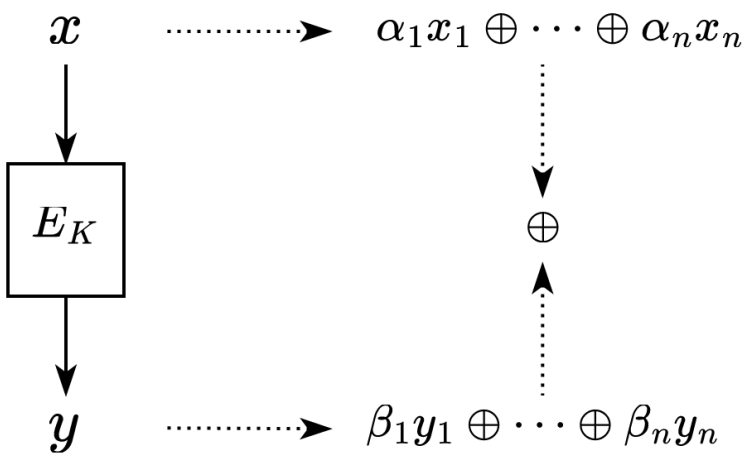
andrey.shcherbachenko@sfblaboratory.ru

РусКрипто'2023
23 марта 2023

конференция РусКрипто

Линейный криптоанализ

- Является одним из самых известных методов криптоанализа блочных шифров и примитивов, основанных на них
- Относится к классу статистических методов, основан на наблюдении статистических зависимостей между битами открытого текста и шифртекста
- Требует знания только пар открытый текст – шифртекст, не требует адаптивного выбора открытых текстов



Линейный криптоанализ

Основные этапы:

1. [Предварительный этап/Оффлайн] Нахождение эффективных линейных приближений для полнораундового или усеченного по числу раундов шифра
2. [Оперативный этап/Онлайн] Накопление материала с целью реализации одной из угроз:
   - Отличение выхода блочного шифра от случайной подстановки
   - Чтение открытого текста по шифртексту без знания ключа
   - Восстановление части ключа (или раундового ключа)

Линейный криптоанализ

Пусть $V = \{0, 1\}$, $F : V^n \to V^m$ – произвольное двоичное отображение

Выражение вида $L^F_{\alpha,\beta}(x) = \langle x, \alpha \rangle \oplus \langle F(x), \beta \rangle$ назовем *линейным приближением; α, β – маски*

$\langle x, \alpha \rangle = x_1\alpha_1 \oplus x_2\alpha_2 \oplus \cdots \oplus x_n\alpha_n$ **– скалярное произведение**

Определим *вероятность* выполнения линейного приближения:

$$\Pr\left[L^F_{\alpha,\beta}(x) = 0\right] = \frac{\sum_{x \in V^n} \mathrm{Ind}\left[L^F_{\alpha,\beta}(x) = 0\right]}{2^n},$$

где $\mathrm{Ind}[\,\cdot\,]$ – индикаторная функция

Характеристикой, определяющей эффективность линейного приближения, является *преобладание*:

$$\delta^F_{\alpha,\beta} = \left|2\Pr\left[L^F_{\alpha,\beta}(x) = 0\right] - 1\right|$$

В случае $m = 1$ обозначим $\delta^f_\alpha = \left|2\Pr\left[f(x) = \langle x, \alpha \rangle\right] - 1\right|$

Линейный криптоанализ

Пусть $\{E_K\}$, $K \in V^k$ – параметризованное семейство биективных двоичных отображений $V^n \to V^n$(блочный шифр)

Рассмотрим следующие характеристики, определяющие эффективность линейного приближения

Преобладание линейного приближения при фиксированном значении ключа (англ. *Linear Potential*):

$$LP_K(\alpha, \beta) = \delta_{\alpha,\beta}^{E_K}$$

Математическое ожидание преобладания при случайном равновероятном выборе ключа (англ. *Expected Linear Potential):*

$$ELP(\alpha, \beta) = \frac{1}{2^k} \sum_{K \in V^k} \delta_{\alpha,\beta}^{E_K} = \mathbb{M}_K \left[LP_K(\alpha, \beta) \right]$$

Линейный криптоанализ

Нас интересуют верхние оценки данных характеристик:

1. $MLP_K = \max\limits_{\alpha,\beta \in V^n \setminus \{0\}} LP_K(\alpha, \beta)$
2. $MELP = \max\limits_{\alpha,\beta \in V^n \setminus \{0\}} ELP(\alpha, \beta)$

Величина $\max\limits_{K \in V^k} \left(\max\limits_{\alpha,\beta \in V^n \setminus \{0\}} LP_K(\alpha, \beta) \right)$ – наиболее строгая оценка эффективности ЛК, не рассматривается

Для классического вычислителя перебор всех возможных $x, \alpha, \beta \in V^n$, $K \in V^k$ для получения **точных оценок** этих характеристик при больших n и k – невыполнимая задача

Смогут ли помочь квантовые вычисления?

Квантовый алгоритм Бернштейна-Вазирани

Bernstein, E., Vazirani, U.V. Quantum complexity theory, 1996: приведен алгоритм поиска неизвестных коэффициентов («скрытой строки») линейной булевой функции как пример алгоритма, разделяющий классы сложности BPP (классический полиномиальный вероятностный) и BQP (квантовый полиномиальный вероятностный)

Пусть $f : V^n \to V^1$ – булева функция, ее вычисление задается квантовым оператором («оракулом») U_f, который выполняет преобразование

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle,$$

где $|x\rangle = |x_1 x_2 \dots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$

Примечание. Пусть $|y\rangle$ находится в состоянии суперпозиции $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, тогда $U_f|x\rangle|-\rangle = \frac{1}{\sqrt{2}}|x\rangle(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) = (-1)^{f(x)}|x\rangle|-\rangle$, т.е. оракул инвертирует фазу («помечает») для таких $|x\rangle$, что $f(x) = 1$

Квантовый алгоритм Бернштейна-Вазирани

$|X\rangle := |0^{\otimes n}\rangle$ – n-кубитный регистр, $|1\rangle$ – дополнительный кубит

Алгоритм

1. К $|X\rangle \otimes |1\rangle$ применяется оператор Адамара $H^{\otimes n+1}$:

$$|X\rangle \otimes |1\rangle := \frac{1}{\sqrt{2^n}} \left(\sum_{x \in V^n} |x\rangle \right) \otimes \underbrace{\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)}_{|-\rangle}$$

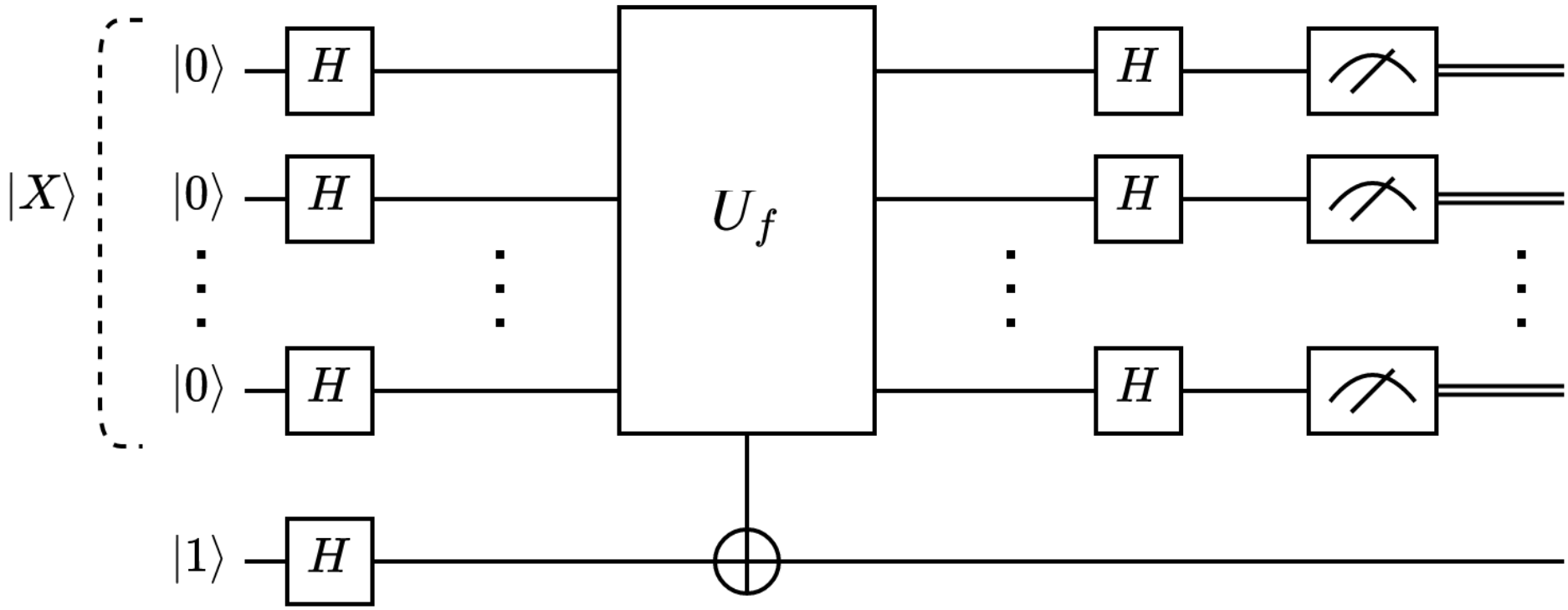
2. К $|X\rangle \otimes |-\rangle$ применяется оракул U_f:

$$|X\rangle \otimes |-\rangle := \frac{1}{\sqrt{2^n}} \left(\sum_{x \in V^n} (-1)^{f(x)} |x\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

3. К $|X\rangle$ применяется оператор Адамара $H^{\otimes n}$:

$$|X\rangle := \frac{1}{2^n} \sum_{x \in V^n} (-1)^{f(x)} \left(\sum_{\alpha \in V^n} (-1)^{\langle x, \alpha \rangle} |\alpha\rangle \right)$$

Квантовый алгоритм Бернштейна-Вазирани



Квантовая схема алгоритма Бернштейна-Вазирани

Квантовый алгоритм Бернштейна-Вазирани

На выходе алгоритма в регистре $|X\rangle$ имеем состояние

$$|X\rangle = \sum_{\alpha \in V^n} \hat{W}_f(\alpha)|\alpha\rangle,$$

где $\hat{W}_f(\alpha) = \frac{1}{2^n} \sum_{x \in V^n} (-1)^{f(x)+\langle x,\alpha\rangle}$ – нормализованный коэффициент Уолша-Адамара

Вероятность измерения исхода α на выходе алгоритма: $P(\alpha) = \left|\hat{W}_f(\alpha)\right|^2$

Согласно известным свойствам, $\left|\hat{W}_f(\alpha)\right| = |2\Pr[f(x) = \langle x, \alpha\rangle] - 1| = \delta_\alpha^f \Rightarrow$ вероятность измерения α тем выше, чем больше его преобладание

Сложность вычисления спектра Уолша-Адамара:

- В классическом случае: $O(n2^n)$
- В квантовом случае*: $O(n)$

  * получить доступ напрямую к результатам вычислений мы не можем, поскольку они «закодированы» в амплитудах квантовых состояний

Применение алгоритма Берштейна-Вазирани в криптоанализе

- Hong-Wei Li, Li Yang. A quantum algorithm to approximate the linear structures of Boolean functions, 2014
- Hong-Wei Li, Li Yang. Quantum Differential Cryptanalysis to the Block Ciphers, 2015
- Huiqin Xie, Li Yang. Using Bernstein-Vazirani Algorithm to Attack Block Ciphers Springer, 2019
- Hong-Wei Sun. Improved BV-based quantum attack on block ciphers, 2022

Работы посвящены поиску ε-*линейных структур*: таких $\alpha \in V^n$, что $\Pr[f(x) \oplus f(x \oplus \alpha) \equiv const] = \varepsilon$. Наличие линейных структур определяет *автокорреляционные свойства* булевой функции, что позволяет использовать их для нахождения эффективных дифференциалов шифра

Идея: Представляем шифр в виде совокупности координатных булевых функций $e_1, \ldots, e_n$ *(реализуются оракулом), для каждой выполняем алгоритм Б.-В. полиномиальное число раз* m*. Среди результатов измерений пытаемся найти общее* α*.*

Алгоритм Бернштейна-Вазирани для оценки линейной характеристики при фиксированном ключе

Построим квантовый оператор E, реализующий зашифрование входного блока в виде

$$E|x\rangle|K\rangle|0^{\otimes a}\rangle = |E_K(x)\rangle|K\rangle|A(x,K)\rangle,$$

где $a \geq 0$ – дополнительные кубиты («рабочее пространство оракула»), $A(x,K)$ – некоторое отображение, действующее на дополнительных кубитах

Без ограничения общности в дальнейшей записи дополнительные кубиты не учитываем

Определяется $E^\dagger$ – обратный к E оператор:

$$E^\dagger|E_K(x)\rangle|K\rangle|A(x,K)\rangle = |x\rangle|K\rangle|0^{\otimes a}\rangle$$

О реализации блочных шифров в виде квантовых схем см.:

- M.Grassl et al. Applying Grover's algorithm to AES: quantum resource estimates
- Д. В. Денисенко, Г. Б. Маршалко, М. В. Никитенкова, В. И. Рудской, В. А. Шишкин. Оценка сложности реализации алгоритма Гровера для перебора ключей алгоритмов блочного шифрования ГОСТ Р 34.12-2015

Алгоритм Бернштейна-Вазирани для оценки линейной характеристики при фиксированном ключе

$|X\rangle := |0^{\otimes n}\rangle$, $|B\rangle := |0^{\otimes n}\rangle$, K – фиксированный ключ

Алгоритм для фиксированного ключа

1. К $|X\rangle \otimes |B\rangle \otimes |1\rangle$ применяется оператор Адамара $H^{\otimes n} \otimes H^{\otimes n} \otimes H$:

$$|X\rangle \otimes |B\rangle \otimes |1\rangle := \frac{1}{\sqrt{2^n}} \left(\sum_{x \in V^n} |x\rangle \right) \otimes \frac{1}{\sqrt{2^n}} \left(\sum_{\beta \in V^n} |\beta\rangle \right) \otimes \underbrace{\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)}_{|-\rangle}$$

2. К $|X\rangle$ применяется оператор зашифрования E:

$$|X\rangle \otimes |B\rangle \otimes |-\rangle := \frac{1}{\sqrt{2^n}} \left(\sum_{x \in V^n} |E_K(x)\rangle \right) \otimes \frac{1}{\sqrt{2^n}} \left(\sum_{\beta \in V^n} |\beta\rangle \right) \otimes |-\rangle$$

Алгоритм Бернштейна-Вазирани для оценки линейной характеристики при фиксированном ключе

Алгоритм для фиксированного ключа (продолжение)

3. К парам кубитов $|X_i\rangle \otimes |B_i\rangle$ применяются вентили C^2NOT (Тоффоли) с выходом на регистре $|-\rangle$:

$$|X\rangle \otimes |B\rangle \otimes |-\rangle := \frac{1}{2^n} \sum_{\beta \in V^n} \sum_{x \in V^n} (-1)^{\langle E_K(x), \beta \rangle} |E_K(x)\rangle |\beta\rangle \otimes |-\rangle$$

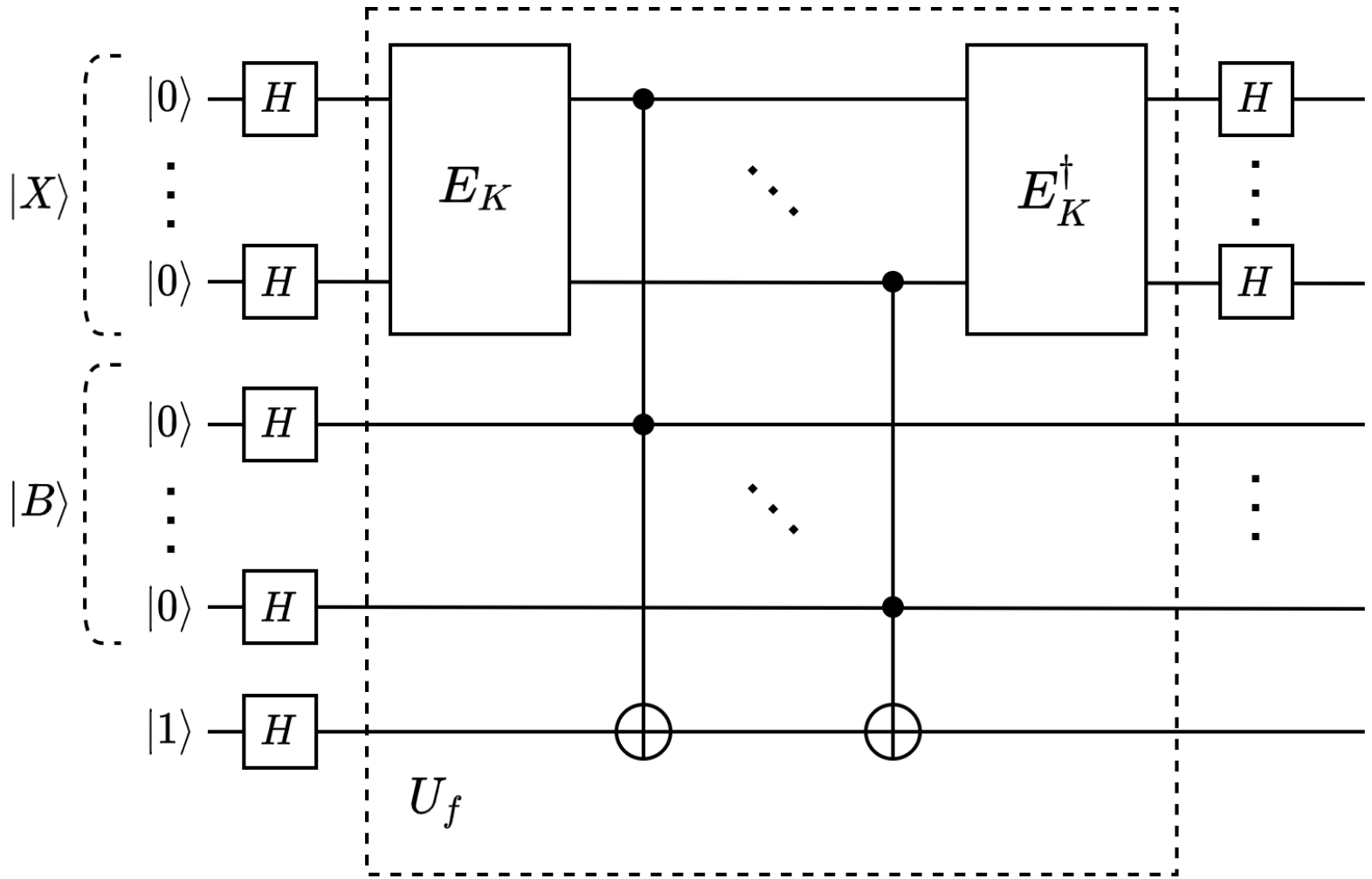
4. К $|X\rangle$ применяется оператор расшифрования $E^\dagger$:

$$|X\rangle \otimes |B\rangle \otimes |-\rangle := \frac{1}{\sqrt{2^n}} \sum_{\beta \in V^n} \sum_{x \in V^n} (-1)^{\langle E_K(x), \beta \rangle} |x\rangle |\beta\rangle \otimes |-\rangle$$

5. К $|X\rangle$ применяется оператор Адамара $H^{\otimes n}$:

$$|X\rangle \otimes |B\rangle \otimes |-\rangle := \frac{1}{\sqrt{2^n}} \sum_{\beta \in V^n} \sum_{\alpha \in V^n} \hat{W}_{\langle E_K, \beta \rangle}(\alpha) |\alpha\rangle |\beta\rangle \otimes |-\rangle$$

Алгоритм Бернштейна-Вазирани для оценки линейной характеристики при фиксированном ключе



Оценка максимальной амплитуды

В результирующем состоянии вида $\frac{1}{\sqrt{2^{\boldsymbol{n}}}} \sum_{\alpha,\beta \in \boldsymbol{V^n}} \hat{W}_{\langle \boldsymbol{E_K},\beta\rangle}(\alpha)|\alpha\rangle|\beta\rangle|-\rangle$ хотим оценить максимальную амплитуду:

$$MLP_K = \max_{\alpha,\beta \in \boldsymbol{V^n} \setminus \{0\}} |\hat{W}_{\langle \boldsymbol{E_K},\beta\rangle}(\alpha)|$$

«Наивный подход»: запускаем схему N раз и производим измерения, получаем выборку $\{(\alpha_i, \beta_i)\}_{i=1}^{N}$, подсчитываем частоты $\nu_{\alpha,\beta}$ и получаем оценку $\widetilde{MLP}_K = \max_{\alpha,\beta \in \boldsymbol{V^n} \setminus \{0\}} \sqrt{\nu_{\alpha,\beta}}$

Очевидный недостаток: для получения *приемлемой* оценки требуется экспоненциальное число перезапусков – $O(2^n)$

Корреляционная матрица

Корреляционная матрица (фактически – *таблица LAT*, англ. *Linear Approximation Table*) определяется как

$$\mathcal{W} = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & \hat{W}_{\alpha_1,\beta_1} & \dots & \hat{W}_{\alpha_1,\beta_{2^n-2}} & \hat{W}_{\alpha_1,\beta_{2^n-1}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \hat{W}_{\alpha_{2^n-2},\beta_1} & \dots & \hat{W}_{\alpha_{2^n-2},\beta_{2^n-2}} & \hat{W}_{\alpha_{2^n-2},\beta_{2^n-1}} \\ 0 & \hat{W}_{\alpha_{2^n-1},\beta_1} & \dots & \hat{W}_{\alpha_{2^n-1},\beta_{2^n-2}} & \hat{W}_{\alpha_{2^n-1},\beta_{2^n-1}} \end{bmatrix},$$

$\mathcal{W}$ – унитарная ($\mathcal{W}^{-1} = \mathcal{W}^T$)

Состояние после алгоритма Бернштейна-Вазирани можно представить в виде

$$\frac{1}{\sqrt{2^n}} \sum_{\beta \in V^n} |\mathcal{W}^{\downarrow}_{\beta}\rangle |\beta\rangle \text{ или } \frac{1}{\sqrt{2^n}} \sum_{\alpha \in V^n} |\mathcal{W}^{\rightarrow T}_{\alpha}\rangle |\alpha\rangle,$$

где $\mathcal{W}^{\downarrow}_{\beta}$ – β-ый столбец матрицы $\mathcal{W}$, $\mathcal{W}^{\rightarrow}_{\alpha}$ – α-я строка матрицы $\mathcal{W}$

Алгоритм Голдрейха-Левина

$$P\hat{W}_f^a(\alpha) = \sum_{x \in V^{n-len(a)}} (-1)^{f(a||x)+\langle a||x,\alpha\rangle}$$

– частичный коэффициент Уолша-Адамара

Алгоритм Голдрейха-Левина для оценки $\max_\alpha |\hat{W}_f(\alpha)|^2$:

1. Храним список префиксов $\mathcal{L} = \{a\}$, длину префикса s и текущую оценку δ^2_{max}
2. Для всех $a \in \mathcal{L}$ вычисляем $P\hat{W}_f^{0||a}(\alpha)$ и $P\hat{W}_f^{1||a}(\alpha)$
3. Если $\left(P\hat{W}_f^{i||a}(\alpha)\right)^2 \geq \delta^2_{max}$ $(i \in \{0,1\})$, то добавляем $i||a$ в список $\mathcal{L}$ и обновляем $\delta^2_{max} = P\hat{W}_f^{i||a}(\alpha)$, иначе отбрасываем
4. Удаляем a из $\mathcal{L}$
5. Если $s = n$, то конец алгоритма

Оценка максимальной амплитуды

Квантовый алгоритм для оценки $\max\limits_{\alpha,\beta \in V^n \setminus \{0\}} |\hat{W}_{\langle E_K,\beta\rangle}(\alpha)|$:

1. Выполняем алгоритм Бернштейна-Вазирани на регистрах $|X\rangle \otimes |B\rangle$
2. Будем выполнять алгоритм Голдрейха-Левина на префиксах регистра $|X\rangle$. Храним текущую оценку δ^2_{max} в отдельном регистре ($|\delta^2_{max}\rangle$). На i-ой итерации:
   - К префиксу $|x_1 \dots x_i\rangle$ «добавляем» кубит $|x_{i+1}\rangle$ (в состоянии $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
   - Выполняем оценку амплитуды состояния $c_0|x_1 \dots x_i\rangle|0\rangle + c_1|x_1 \dots x_i\rangle|1\rangle$, сохраняем значения в отдельных регистрах $|c_0^2\rangle$и $|c_1^2\rangle$
     Алгоритм QAE: Brassard, G., Hoyer, P., Mosca, M., & Tapp, A. Quantum Amplitude Amplification and Estimation.
   - Выполняем сравнение регистров $|c_0^2\rangle$ и $|c_1^2\rangle$ со значением $|\delta^2_{max}\rangle$:
     - если $c_0^2, c_1^2 \geq \delta^2_{max}$, то ничего не делаем
     - если $c_0^2 \geq \delta^2_{max}$, то применяем к $|x_{i+1}\rangle$ оператор H ($|x_{i+1}\rangle$ коллапсирует в $|0\rangle$)
     - если $c_1^2 \geq \delta^2_{max}$, то применяем к $|x_{i+1}\rangle$ оператор HX ($|x_{i+1}\rangle$ коллапсирует в $|1\rangle$
   - Обновляем $|\delta^2_{max}\rangle$
3. На выходе измеряем $|\delta^2_{max}\rangle$

Грубая оценка трудоемкости: $O(n2^{n/2})$, сильно зависит от сходимости алгоритма Г.-Л.

Алгоритм Бернштейна-Вазирани для оценки линейной характеристики в среднем по ключам

Сформируем суперпозицию всех возможных ключей $\frac{1}{\sqrt{2^k}} \sum_{K \in V^k} |K\rangle$.

Выполним описанный ранее алгоритм, имеем состояние

$$\frac{1}{\sqrt{2^{n+k}}} \sum_{K \in V^k} \sum_{\alpha,\beta \in V^n} \hat{W}_{\langle E_K, \beta \rangle}(\alpha) |\alpha\rangle |\beta\rangle |K\rangle |-\rangle$$

Амплитуда при каждом состоянии $|\alpha\rangle|\beta\rangle$:

$$\frac{1}{\sqrt{2^k}} \sum_{K \in V^k} \hat{W}_{\langle E_K, \beta \rangle}(\alpha),$$

причем

$$\left| \frac{1}{\sqrt{2^k}} \sum_{K \in V^k} \hat{W}_{\langle E_K, \beta \rangle}(\alpha) \right|^2 \leq \frac{1}{2^k} \sum_{K \in V^k} |\hat{W}_{\langle E_K, \beta \rangle}(\alpha)|^2 \approx MELP^2$$

(в силу формулы $D[\xi] = \mathbb{M}[\xi^2] - (\mathbb{M}[\xi])^2$ для с.в. ξ и предполагаемой малости дисперсии)

Применяя подход, который использовался для случая фиксированного ключа, получим *нижнюю оценку* на MELP

Другие подходы

Подходы к оценке нелинейности $N(f) = \frac{1}{2} - \frac{1}{2}\max_{\alpha}|\hat{W}_f(\alpha)|$ булевых функций предлагались в следующих работах:

- M. Hillery, E. Andersson. Quantum tests for the linearity and permutation invariance of Boolean functions, 2011

  Идея: Метод основан на вероятностном тесте на линейность BLR (Blum-Luby-Rubinfeld)

- C. A. Jothishwaran et al. A quantum algorithm to estimate the Gowers U_2 norm and linearity testing of Boolean functions, 2020

  Идея: Оценка нормы специального вида (U_2-норма Гауэра) с целью получения верхней оценки $N(f)$

- D. Bera, S. Tharrmashastha. Quantum and Randomised Algorithms for Non-linearity Estimation, 2021

  Идея: Комбинация алгоритма Бернштейна-Вазирани и Голдрейха-Левина, построение доверительного интервала для $N(f)$, зависящего от параметров λ, ε: $\Pr[N(f) \in (a, b)] \geq 1 - \varepsilon$, $b - a = \lambda$ *с трудоемкостью* $O\left(\frac{1}{\lambda}\log\frac{1}{\varepsilon}\right)$

Заключение

- В общем случае задача оценки нелинейности булевой функции (как следствие – стойкости примитивов к линейному криптоанализу) – сложная для классического компьютера,
  - к настоящему времени считается сложной и для квантового компьютера (не более чем квадратичное ускорение)
- В настоящем докладе предложены методы оценки стойкости блочного шифра к линейному криптоанализу:
  - нижняя оценка максимального преобладания при фиксированном значении ключа (MLP_K)
  - нижняя оценка максимального математического ожидания преобладания по всем значениям ключа ($MELP$)

Благодарю за внимание!