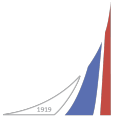
О свойствах безопасности одного режима работы блочных шифров при наличии у нарушителя доступа к квантовому оракулу

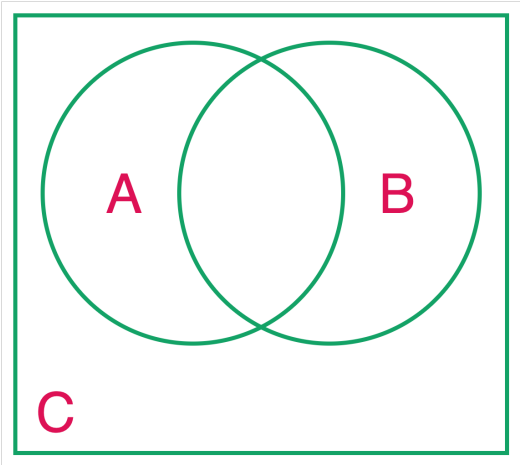
Коренева А.М.[1,2], Фирсов Г.В.[1,3]

[1]ООО «Код Безопасности»
[2]Финансовый университет при Правительстве РФ
[3]НИЯУ МИФИ

21 марта 2024



Днём ранее...



A — Алгоритмы, на которые построена “классическая” атака.

B — Алгоритмы, для которых показано, что

$$\exists \mathcal{A} : \mathbf{Adv}(\mathcal{A}) \neq negl(\lambda).$$

C — Нестойкие алгоритмы.

Маршалко Г. Б., Фомин Д. Б. Показуемая стойкость в задаче обфускации криптографических исследований. РусКрипто’2024.

Структура доклада

1. Необходимые определения
2. Режим DEC
3. Модель qROP-qfdeCPA
4. Предварительные сведения
5. Построение атаки

Научный фундамент

1. Schrottenloher A. Quantum Algorithms for Cryptanalysis and Quantum-safe Symmetric Cryptography. Sorbonne Université, 2021.
2. Nakahara M., Ohmi T. Quantum computing : from linear algebra to physical realizations, 2008.
3. Firsov G. and Koreneva A. On one block cipher mode of operation used to protect data on block-oriented storage devices // Modern Inform. Technologies and IT-Education, 2022.
4. Рекомендации по стандартизации Р 1323565.1.042–2022 «Информационная технология. Криптографическая защита информации. Режим работы блочных шифров, предназначенный для защиты носителей информации с блочно-ориентированной структурой». М.: Стандартинформ, 2022.
5. Nemoz T., Amblard Z., Dupin A. Characterizing the qIND-qCPA (in)security of the CBC, CFB, OFB and CTR modes of operation. Cryptology ePrint Archive, Paper 2022/236, 2022.
6. Maria Naya-Plasencia. New Results on Symmetric Quantum Cryptanalysis and Perspectives. Indocrypt 2021, 2021.

Принятые сокращения

ПДШ (FDE)	—	Полнодисковое шифрование
CPA	—	Chosen plaintext attack (атака по подобранному открытому тексту)
DEC	—	Режим Disk Encryption with Counter

Кубит и квантовый регистр

Кубит — единица информации в квантовом компьютере. Кубит описывается *вектором состояния* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.
Вектор $|\psi\rangle$ принадлежит гильбертову пространству $\mathcal{H}$.

Квантовый регистр длины n описывается состоянием $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$, которое для краткости будем записывать как $|\psi_1, \ldots, \psi_n\rangle$ или как $|\psi\rangle$, если длина регистра ясна из контекста.

Знак тензорного произведения ($\otimes$) иногда будем опускать для краткости записи.

Изменение квантового состояния

Состояние изменяется под воздействием на него *унитарного оператора* U, что записывается следующим образом: $|\phi\rangle = U|\psi\rangle$.

Пусть $n \geq 1$, $U : \mathcal{H} \to \mathcal{H}$, $|\psi\rangle \in \mathcal{H}^{\otimes n}$. Воздействие оператора $U^{\otimes n}$ на состояние $|\psi\rangle$ будем записывать короче: $U|\psi\rangle$.

Некоторые операторы

- I — тождественный оператор, задается матрицей $\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}$.
- H — оператор Адамара, задается матрицей $\frac{1}{\sqrt{2}} \begin{Vmatrix} 1 & 1 \\ 1 & -1 \end{Vmatrix}$.
- CX — оператор контролируемого «НЕ», задается матрицей $\begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{Vmatrix}$.

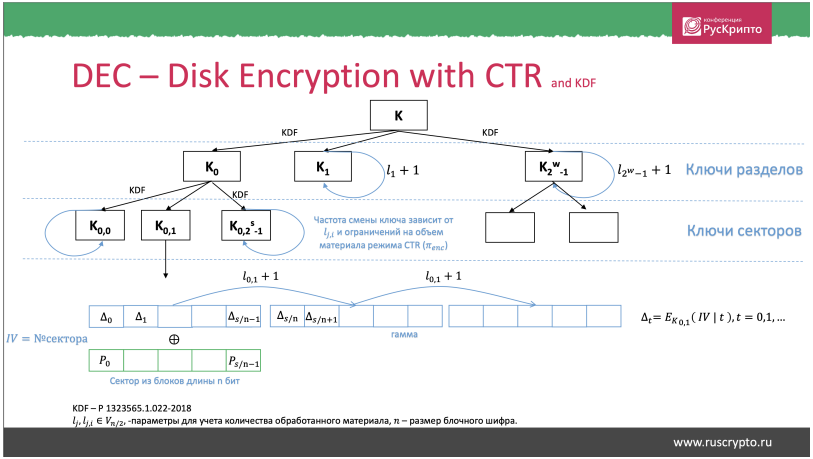
Запутанные состояния

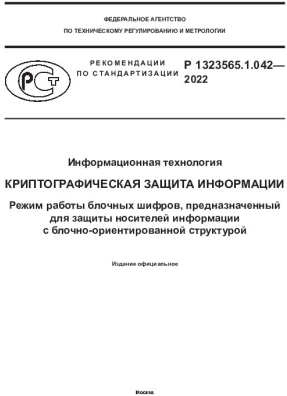
Состояние $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ называется *запутанным*, если для любых $|\psi_1\rangle \in \mathcal{H}_1$ и $|\psi_2\rangle \in \mathcal{H}_2$ верно: $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$.

Обозначения

V_m	—	множество двоичных строк длины $m \in \mathbb{N}$
V^*	—	множество двоичных строк конечной длины
$l \in \mathbb{N}$	—	длина блока блочного шифра
$n \in \mathbb{N}$	—	количество блоков в секторе
$\mathrm{Perm}\,[X]$	—	множество подстановок некоторого множества X
$\mathcal{H}_x$, $\mathcal{H}_y$	—	пространства, такие, что для состояния $\|x\rangle\|y\rangle \in \mathcal{H}$: $\mathcal{H} = \mathcal{H}_x \otimes \mathcal{H}_y$, $\|x\rangle \in \mathcal{H}_x$, $\|y\rangle \in \mathcal{H}_y$.

Режим DEC





ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.042—2022

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режим работы блочных шифров, предназначенный для защиты носителей информации с блочно-ориентированной структурой

Издание официальное

Москва
Российский институт стандартизации
2022

Схема работы режима DEC
Богданов Д., Ноздрунов В. Шифрование носителей информации. Режим DEC. РусКрипто'2021

Модель qROP-qfdeCPA

Модель qROP-qfdeCPA (Real Or Permutation Indistinguishability under Chosen Plaintext Attack with quantum queries and FDE restrictions) определяется следующим образом:

- $\tilde{\mathcal{E}}$ — настраиваемый шифр;
- $\mathcal{K}$ — ключевое множество;
- $\mathcal{M} = V^*$ — множество открытых текстов;
- $\mathcal{T}$ — множество настроек;
- $\tilde{E}$ — функция зашифрования шифра $\tilde{\mathcal{E}}$.

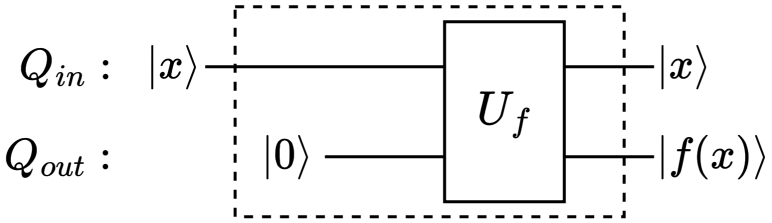
Случайно и равновероятно выбирается значение $b \in \{0, 1\}$, неизвестное нарушителю $\mathcal{A}$. Экспериментатор $\mathbf{Exp}$ случайно и равновероятно выбирает ключ $k \in \mathcal{K}$.

Модель qROP-qfdeCPA

Нарушитель $\mathcal{A}$ совершает запросы вида $|\mathcal{L}_i\rangle|m_i\rangle$, в ответ на которые получает:

$$|\mathcal{L}_i\rangle|m_i\rangle \left|\tilde{E}\left(k, S(\mathcal{L}_i, s_i), \phi_i^b(m_i)\right)\right\rangle,$$

где $i \geq 1$, $\mathcal{L}_i \in \mathcal{T}$, $m_i \in \mathcal{M}$, $\phi_i \in \text{Perm}\left[V_{|m_i|}\right]$ выбрана случайно и равновероятно, $s_i \in \mathcal{S}$ — внутреннее состояние экспериментатора, $\mathcal{S}$ — множество внутренних состояний экспериментатора, $S : \mathcal{T} \times \mathcal{S} \to \mathcal{T}$.



Модель qROP-qfdeCPA

Далее нарушитель $\mathcal{A}$ возвращает $b' \in \{0, 1\}$ (будем записывать $\mathcal{A} \Rightarrow b'$).

Преобладанием нарушителя $\mathcal{A}$ назовем величину:

$$\mathbf{Adv}_{\bar{\mathcal{E}}}^{\text{qROP-qfdeCPA}}(\mathcal{A}) = \Pr\left[\mathcal{A} \Rightarrow 1 | b = 1\right] - \Pr\left[\mathcal{A} \Rightarrow 1 | b = 0\right].$$

Модель qROP-qfdeCPA

Модель qROP-qfdeCPA относится к классу моделей Q_2 [6]: нарушитель может совершать квантовые запросы к квантовому оракулу.

Предварительные сведения

Лемма 1

Пусть $f : V_m \to V_n$ для некоторых $m, n \in \mathbb{N}$. Рассмотрим состояние $\frac{1}{2^{m/2}} \sum\limits_{x \in V_m} |x\rangle|f(x)\rangle$.

Подействуем на него оператором $\mathrm{H} \otimes \mathrm{I}$. Тогда при измерении первого регистра вероятность получить $|0\rangle$ равна:

$$\Pr\left[|0\rangle\right] = \frac{1}{2^{2m}} \sum_{y \in V_n} \left|f^{-1}(y)\right|^2,$$

где $f^{-1} : V_n \to \mathcal{P}(V_m)$ — функция, возвращающая для $y \in V_n$ множество его прообразов относительно функции f.

Построение атаки

Теорема 1

Пусть $\pi \in \mathrm{Perm}\,[V_l]$ — случайная подстановка множества V_l. Тогда существует такой нарушитель $\mathcal{A}$, что:

$$\mathbf{Adv}^{\text{qROP-qfdeCPA}}_{\overline{\text{DEC}^{\pi}}}(\mathcal{A}) = 1 - 2^{1-nl}.$$

При этом $\mathcal{A}$ совершает один запрос к экспериментатору $\mathbf{Exp}$.

Построение атаки

Доказательство теоремы 1

Нарушитель $\mathcal{A}$ подготавливает состояние $|\psi\rangle = |\mathcal{L}\rangle|+\rangle$, где $|+\rangle$ — сокращенное обозначение состояния $|+\rangle^{\otimes nl} = \sum\limits_{x \in V_{nl}} |x\rangle$, $\mathcal{L} \in \mathcal{T}$ выбрано произвольно так, что $|\mathcal{L}\rangle$ — один из векторов вычислительного базиса пространства $\mathcal{H}_{\mathcal{L}}$. Положим $\mathcal{L} = 0$.

Далее нарушитель посылает $|\psi\rangle$ оракулу зашифрования.

Построение атаки

Доказательство теоремы 1

В ответ нарушитель получает состояние:

$$|r\rangle = \begin{cases} |\mathcal{L}\rangle \sum\limits_{x \in V_{nl}} |x\rangle|\phi(x) \oplus \gamma\rangle, & b = 0, \\ |\mathcal{L}\rangle \sum\limits_{x \in V_{nl}} |x\rangle|x \oplus \gamma\rangle, & b = 1, \end{cases}$$

где ϕ — подстановка, случайно и равновероятно выбранная из $\mathrm{Perm}\,[V_{nl}]$, $\gamma = \gamma(\pi, \mathcal{L})$ — двоичная строка, выработанная по описанному в [4] алгоритму с помощью подстановки π и пары $\mathcal{L}$ (номеров раздела и сектора).

Построение атаки

Доказательство теоремы 1

Возьмем частичный след по пространству $\mathcal{H}_{\mathcal{L}}$ от матрицы плотности $|r\rangle\langle r|$.
В действительности, так как первый регистр не запутан с двумя другими, взятие частичного следа эквивалентно просто «отбрасыванию» первого регистра. Обозначим такое состояние через $|r_1\rangle$:

$$|r_1\rangle = \begin{cases} \sum\limits_{x \in V_{nl}} |x\rangle|\phi(x) \oplus \gamma\rangle, & b = 0, \\ \sum\limits_{x \in V_{nl}} |x\rangle|x \oplus \gamma\rangle, & b = 1. \end{cases}$$

Построение атаки

Доказательство теоремы 1

Подействуем на $|r_1\rangle$ оператором $U_1 = \mathrm{CX}$:

$$|r_2\rangle = U_1|r_1\rangle = \begin{cases} \sum\limits_{x \in V_{nl}} |x\rangle|x \oplus \phi(x) \oplus \gamma\rangle, & b = 0, \\ \sum\limits_{x \in V_{nl}} |x\rangle|\gamma\rangle, & b = 1. \end{cases}$$

Заметим, что при $b = 1$ регистры более не являются запутанными:

$$\sum_{x \in V_{nl}} |x\rangle|\gamma\rangle = \left(\sum_{x \in V_{nl}} |x\rangle \right) |\gamma\rangle.$$

Построение атаки

Доказательство теоремы 1

Пусть $U_2 = \mathrm{H} \otimes \mathrm{I}$.

Нарушитель $\mathcal{A}$ проводит измерение первого регистра состояния $U_2|r_1\rangle$ и возвращает 1, если был получен $|0\rangle$, и 0 – в противном случае.

Построение атаки

Доказательство теоремы 1

При $b = 1$ измерение первого регистра состояния $U_1|r_2\rangle$ дает $|0\rangle$ с вероятностью 1, так как:

$$U_2|r_2\rangle = U_2\left(|+\rangle|\gamma\rangle\right) = |0\rangle|\gamma\rangle.$$

Таким образом:

$$\Pr\left[\mathcal{A} \Rightarrow 1 | b = 1\right] = 1. \tag{1}$$

Построение атаки

Доказательство теоремы 1

Рассмотрим теперь случай $b = 0$. Пусть $f = x \mapsto x \oplus \phi(x) \oplus \gamma$. По лемме 1 вероятность получения $|0\rangle$ при измерении первого регистра состояния $U_2|r_2\rangle$ равна:

$$\frac{1}{2^{2nl}} \sum_{y \in V_{nl}} \left|f^{-1}(y)\right|^2 = \frac{1}{2^{nl}} \left(\frac{1}{2^{nl}} \sum_{y \in V_{nl}} \left|f^{-1}(y)\right|^2 \right) = \frac{1}{2^{nl}} \mathrm{M}\left[\left|f^{-1}(y)\right|^2\right], \tag{2}$$

где $\mathrm{M}[X]$ — математическое ожидание с.в. X, а $f^{-1} : V_{nl} \to \mathcal{P}(V_{nl})$ — функция, ставящая в соответствие элементу $y \in V_{nl}$ множество его прообразов относительно функции f.

Заметим, что сумма в (2) пробегает все возможные значения y, следовательно эквивалентно рассматривать функцию $f = x \mapsto x \oplus f(x)$.

Построение атаки

Доказательство теоремы 1

Заметим, что для каждого $y \in V_{nl}$:

$$\left|f^{-1}(y)\right|^2 = \left|\{(x_1, x_2) | \phi(x_1) = x_1 \oplus y \wedge \phi(x_2) = x_2 \oplus y\}\right|.$$

Отсюда:

$$\mathrm{M}\left[\left|f^{-1}(y)\right|^2\right] = \sum_{\substack{x_1 \in V_{nl} \\ x_2 \in V_{nl}}} \Pr\left[\phi(x_1) = x_1 \oplus y \wedge \phi(x_2) = x_2 \oplus y\right] =$$

$$= \sum_{x_1 \in V_{nl}} \Pr\left[\phi(x_1) = x_1 \oplus y\right] + \sum_{\substack{x_1 \in V_{nl} \\ x_2 \in V_{nl} \\ x_2 \neq x_1}} \Pr\left[\phi(x_1) = x_1 \oplus y \wedge \phi(x_2) = x_2 \oplus y\right]$$

Построение атаки

Доказательство теоремы 1

$$\sum_{x_1 \in V_{nl}} \Pr\left[\phi(x_1) = x_1 \oplus y\right] = 1,$$

так как сумма содержит 2^{nl} слагаемых, каждое из которых равно $\frac{1}{2^{nl}}$.

$$\sum_{\substack{x_1 \in V_{nl} \\ x_2 \in V_{nl} \\ x_2 \neq x_1}} \Pr\left[\phi(x_1) = x_1 \oplus y \wedge \phi(x_2) = x_2 \oplus y\right] = 1,$$

так как сумма содержит $2^{nl}(2^{nl} - 1)$ слагаемых, каждое из которых равно $\frac{1}{2^{nl}(2^{nl}-1)}$.

Построение атаки

Доказательство теоремы 1

Таким образом:

$$\mathrm{M}\left[\left|f^{-1}(y)\right|^2\right] = 2.$$

С учетом (2) вероятность получить $|0\rangle$ при измерении первого регистра состояния $U_2|r_2\rangle = U_2 \sum\limits_{x \in V_{nl}} |x\rangle|x \oplus \phi(x) \oplus \gamma\rangle$ равна 2^{1-nl}. Таким образом:

$$\Pr\left[\mathcal{A} \Rightarrow 1 | b = 0\right] = 2^{1-nl}. \tag{3}$$

Построение атаки

Доказательство теоремы 1

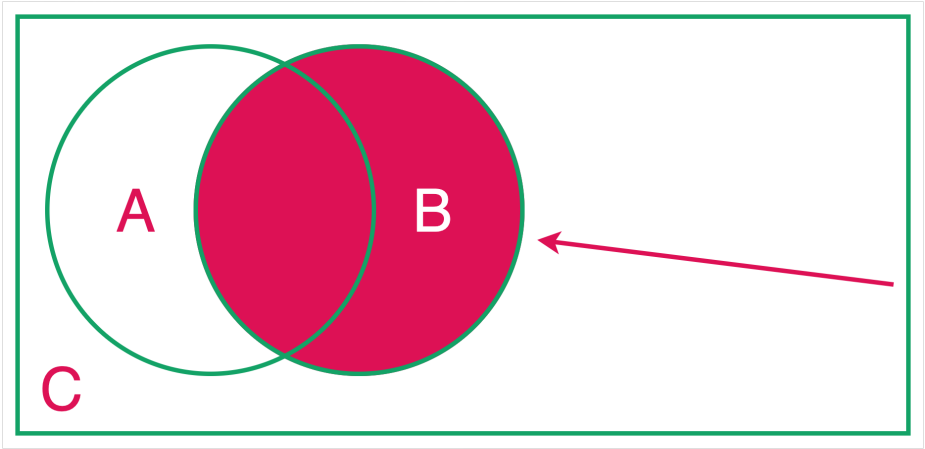
Из (1) и (3) следует:

$$\mathbf{Adv}^{\mathsf{qROP\text{-}qfdeCPA}}_{\overline{\mathsf{DEC}^{\pi}}}(\mathcal{A}) = 1 - 2^{1-nl}.$$

Теорема доказана.

Результаты

- Предложена модель qROP-qfdeCPA, формализующая обеспечение конфиденциальности информации на носителе с блочно-ориентированной структурой при наличии у нарушителя доступа к квантовому оракулу.
- Предложена адаптация известной атаки к режиму DEC и модели qROP-qfdeCPA.



Спасибо за внимание!

Контактная информация

- Коренева Алиса Михайловна: A.Koreneva@securitycode.ru
- Фирсов Георгий Валентинович: G.Firsov@securitycode.ru