Стойкость алгоритма Кузнечик к обобщенной инвариантной атаке

Фомин Денис Бониславович
dfomin@hse.ru

Национальный исследовательский университет «Высшая школа экономики»

25 марта 2021 г.

Рассмотрим XSL-шифр с длиной блока n, $n = m \cdot k$. Не теряя общности предполагаем, что обрабатываются блоки открытого текста вида $v = (v_1, \ldots, v_k)$, $v_i \in V_m$, $i \in \overline{1,k}$.

Преобразование i-го раунда задается по формуле:

$$F[X_i] \colon V_n \to V_n,\ F[X_i] = \mathrm{LS}(v) \oplus X_i,$$

где

- $\mathrm{S} \colon V_m^k \to V_m^k$, $\mathrm{S}(v) = (\pi(v_1), \ldots, \pi(v_k))$, $\pi \in S(V_m)$,
- $\mathrm{L} \colon V_m^k \to V_m^k$, $\mathrm{L}(v) = v \cdot L$, $L = (L_{i,j})_{m,m}$, $L_{i,j} \in \mathrm{GL}(m, 2)$.

Частным случаем является стандартизированный алгоритм «Кузнечик».

Найти множество U такое, что для «достаточно большого» количества ключей X_i выполняется равенство:

$$F[X_i](U) = U.$$

При этом, нас, как правило, интересуют множества U «большой мощности».

Как правило такое множество ищут следующим образом:

- Ищут инвариатное множество для нелинейного (или наоборот линейного) слоя;
- Проверяют является ли это множество инвариантом для линейного (соответсвенно нелинейного) слоя.

Множество U, как правило, ищут среди множеств специального вида.

Приведем некоторые результаты работы Д.И. Трифонова, Д.Б. Фомина «Об инвариантных подпространствах в XSL-шифрах».

Пусть имеется пара семейств множеств $(\mathcal{A}, \mathcal{B})$, где

$$\mathcal{A} = \{A_1, A_2, \ldots, A_{e_a}\},\ A_i \subseteq V_m,$$

$$\mathcal{B} = \{B_1, B_2, \ldots, B_{e_b}\},\ B_i \subseteq V_m$$

и для любого $i \in \{1, \ldots, e_a\}$ существует $j \in \{1, \ldots, e_b\}$ такой, что $A_i^\pi \subseteq B_j$.

Рассмотрим семейства $\mathcal{A}^k$ и $\mathcal{B}^k$ — декартовы степени множеств $\mathcal{A}$ и $\mathcal{B}$ соответственно. Тогда для любого элемента $A_{i_1} \times \ldots \times A_{i_k} \in \mathcal{A}^k$ существует элемент $B_{j_1} \times \ldots \times B_{j_k} \in \mathcal{B}^k$ такой, что

$$(A_{i_1} \times \ldots \times A_{i_k})^{\mathrm{S}} = \left(A_{i_1}^\pi \times \ldots \times A_{i_k}^\pi\right) \subseteq B_{j_1} \times \ldots \times B_{j_k}.$$

Множество U будем искать среди подмножеств множества $\mathcal{A}^m$.
То есть верна следующая диаграмма:

$$A_{i_1} \times \ldots \times A_{i_k} \xrightarrow{\mathrm{S}} \underbrace{B_{j_1} \times \ldots \times B_{j_k}}_{\in \mathcal{B}^k} \xrightarrow{\mathrm{L}} \underbrace{C_{l_1} \times \ldots \times C_{l_k}}_{\in \mathcal{C}} \xrightarrow{\mathrm{X}[K]} \underbrace{A_{i_1} \times \ldots \times A_{i_k}}_{\in \mathcal{A}^k}.$$

То есть:

- Множество $\mathcal{C}$ тоже имеет вид $C_{l_1} \times \ldots \times C_{l_k}$.

Можем рассмотреть следующее обобщение:

$$A_{i_1} \times \ldots \times A_{i_m} \xrightarrow{\mathrm{S}} B_{j_1} \times \ldots \times B_{j_m} \xrightarrow{\mathrm{L}} C_{l_1} \times \ldots \times C_{l_k} \xrightarrow{\mathrm{X}[K_i]} \xrightarrow{\mathrm{X}[K_i]} A_{o_1} \times \ldots \times A_{o_k} \xrightarrow{\mathrm{X}[K_{i+r}]} \ldots \xrightarrow{\mathrm{X}[K_{i+r}]} A_{i_1} \times \ldots \times A_{i_m}.$$

Или иными словами:

$$F[X_{i+r}] \ldots F[X_i](U) = U.$$

Очевидно в этом случае:

- Мощности всех множеств A_{*_*}, B_{*_*}, C_{*_*} равны.

Можно рассмотреть ориентированный граф, вершинами которого являются элементы семейства $\mathcal{A}^k$, дуга между двумя вершинами существует, если есть ключ X, такой, что раундовое преобразование $F[X]$ переводит одно множество в другое. Нас интересует поиск циклов в таком графе.

Из мощностных соображений можно показать, что:

- Достаточно рассмотреть только такие $A \in \mathcal{A}$, что A и $\pi(A)$ являются смежными классами по некоторому подпространству пространства V_m.
- Тогда после линейного преобразования элементы C_{*_*} являются смежными классами по некоторому подпространству пространства V_k, при этом существует такой $x \in V_m$, что $\pi(C_{*_*} \oplus x)$ тоже являются смежными классами по некоторому подпространству пространства V_m.

1. Найдем все подпространства A' и B' пространства V_m такие, что существуют $a, b \in V_m$, что для подстановки алгоритма «Кузнечик» π_K верно равенство:

$$\pi_K(A' \oplus a) = B' \oplus b.$$

2. Для всех найденных пар A' и B' и всех $j \in 1, \ldots, k$ построим множества U_j вида $U_j = \underbrace{\{0\} \times \ldots \times \{0\} \times B'}_{j} \times \{0\} \times \ldots \times \{0\}$ и вычислим соответствующее множество $W_j = U_j^{\mathrm{L}}$.
3. Для каждого вычисленного W_j проверим является ли $W_j(l)$ смежным классом по некоторому подпространству пространства V_m.

Как известно, для подстановки π_K найдены различные представления, которые в том числе позволяют эффективно ее реализовать на различных платформах.

Данные разложения позволяют достаточно просто осуществить 1 пункт рассмотренного выше алгоритма и доказать

При выполнении предположений (слайд 6) для алгоритма «Кузнечик» не существует множества U вида

$$U = A_{i_1} \times \ldots \times A_{i_k},\ i_1, i_2, \ldots, i_k \in 1, \ldots, 2^n,$$

такого, что будет выполняться равенство

$$F[X_{i+r}] \ldots F[X_i](U) = U.$$

В работе Yosuke Todo and Gregor Leander and Yu Sasaki «Nonlinear Invariant Attack – Practical Attack on Full SCREAM, iSCREAM, and Midori64» предложен метод нелинейных инвариантов, суть которого заключается в поиске инвариантов для функции зашифрования на некотором множестве ключей шифрования.

Функция $f\colon V_n \to \{0,1\}$ называется нелинейным инвариантом преобразования $g\colon V_n \to V_n$, если для любого $x \in V_n$ и некоторой константы $c \in \{0,1\}$ выполняется равенство

$$f(x) + f(g(x)) = c.$$

В известных работах, посвященных методу нелинейных инвариантов, нелинейные инварианты для XSL-алгоритмов представлялись в виде

$$f(x_1, \ldots, x_n) = \varphi\left(g_1(x_1, \ldots, x_k), \ldots, g_k(x_{m(b-1)-1}, \ldots, x_{mk})\right)$$

и, как правило, в качестве функции φ выступала функция

$$\varphi(y_1, \ldots, y_m) = y_1 + \ldots + y_k.$$

В работе Бурова Д.А. «Об условия применимости одного известного подхода к построению нелинейных инвариантов XSL-алгоритмов» (представлена для опубликования в журнале «Дискретная математика»), в частности показано, что преобразование SL алгоритма «Кузнечик» не имеет нелинейных инвариантов с нетривиальными пространствами линейных трансляторов (то есть те, которые имеют более одного «слабого ключа») в следующих случаях:

1. $\varphi(y_1, \ldots, y_k) = y_1 + \ldots + y_k$,
2. функция φ имеет тривиальное пространство линейных трансляторов,
3. функции $g_1, \ldots, g_k$ являются инвариантами для подстановки алгоритма «Кузнечик».

Спасибо за внимание!

Вопросы?