КРИПТОНИТ

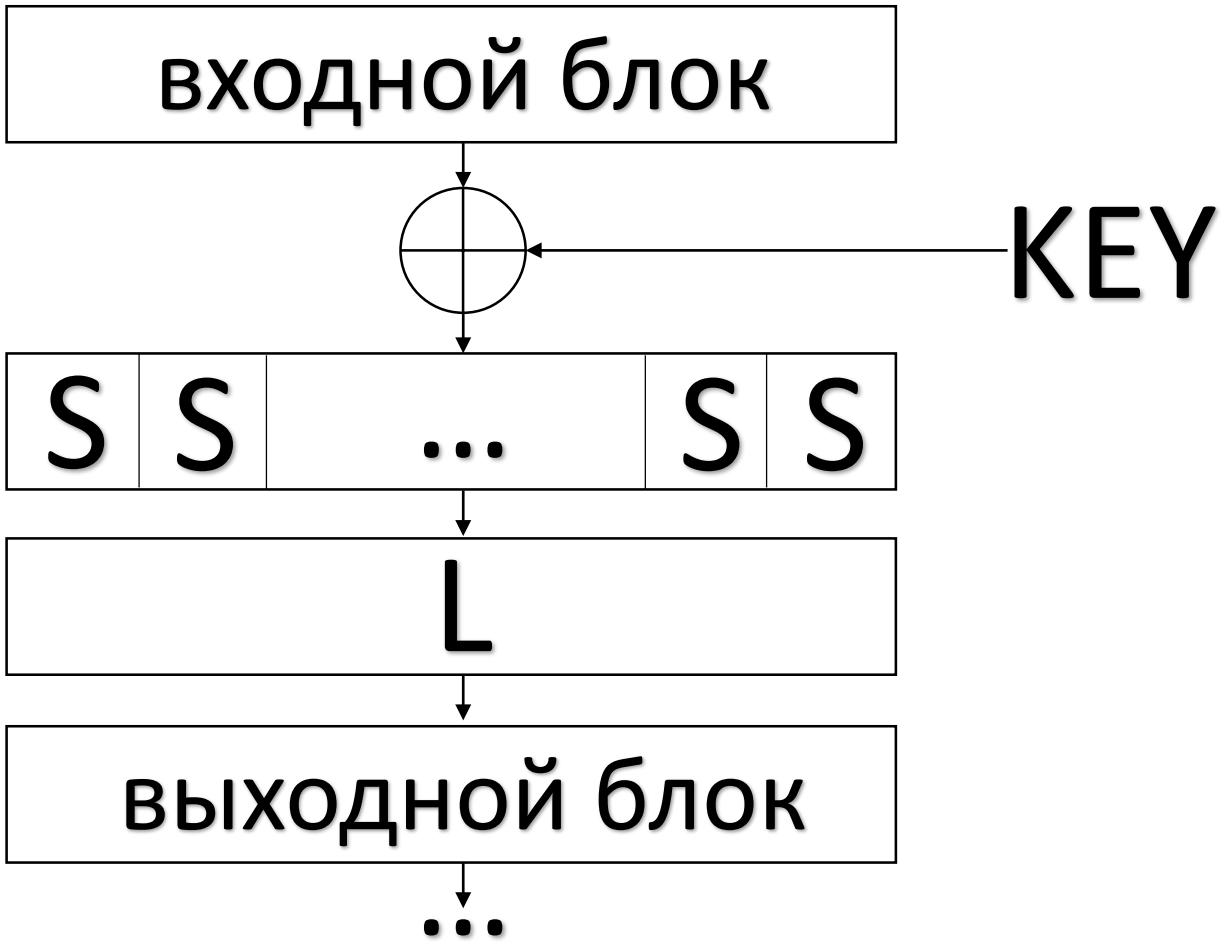
Разложение рекурсивных матриц и его применение к реализации XSL-схем

С.А. Давыдов, В.А. Шишкин

Москва 2021г.

1 раунд XSL-схемы

1. Кузнечик
2. AES
3. Стрибог
4. PHOTON



Пусть $\boldsymbol{P} = \boldsymbol{GF}(\boldsymbol{q^n})$ – конечное поле из q^n элементов

$\boldsymbol{f}(\boldsymbol{x}) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in P[x]$ – многочлен над полем $\boldsymbol{P}$

Сопровождающей матрицей многочлена $\boldsymbol{f}(\boldsymbol{x})$ будем называть матрицу следующего вида:

$$\boldsymbol{S_{m\times m}} = \boldsymbol{S}\big(\boldsymbol{f}(\boldsymbol{x})\big) = \begin{pmatrix} f_{m-1} & 1 & 0 & \ldots & 0 \\ f_{m-2} & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ f_1 & 0 & 0 & \ldots & 1 \\ f_0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Рекурсивной матрицей будем называть матрицу $\boldsymbol{S^k}$, где $S = S\big(f(x)\big)$ для некоторого $f(x)$ и $k > 1$

Пусть $\boldsymbol{R = P[x] \,/\, f(x)}$ - факторкольцо многочленов, $\boldsymbol{\varphi: P^m \rightarrow R}$ – отображение, переводящее координатную строку вектора в соответствующий многочлен:

$$\varphi(a_{m-1},\ldots, a_1, a_0) = a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$$

Будем говорить, что матрица $\boldsymbol{A_{m\times m} \in P_{m,m}}$ *реализует умножение на элемент* $\boldsymbol{\alpha(x)}$ кольца $\boldsymbol{R}$, если матрица $\boldsymbol{A}$ реализует следующие линейное преобразование

$$\vec{a} \rightarrow \varphi^{-1}\,(\,\alpha(x)\cdot\varphi(\vec{a})\,)$$

Обозначаем указанное свойство $\boldsymbol{A = A_\alpha}$

Утверждение: Матрица $\boldsymbol{A_{m\times m} \in P_{m,m}}$ равна матрице $\boldsymbol{A_\alpha}$ для некоторого элемента $\boldsymbol{\alpha(x)}$ кольца $\boldsymbol{R}$ тогда и только тогда, когда для всех $i \in \{1,..,m-1\}$ $\varphi\left(\overrightarrow{A_i}\right) = x^i \cdot \varphi\left(\overrightarrow{A_0}\right)$ в кольце $\boldsymbol{R}$. В условиях утверждения $\boldsymbol{\alpha(x) = \varphi\left(\overrightarrow{A_0}\right)}$

Пример 1: *Матрица циркулянт*

Умножене на $\boldsymbol{\alpha(x) = a_{m-1}x^{m-1} + \ldots + a_1x + a_0}$ в кольце $\boldsymbol{R = P[x]/(x^m - 1)}$

$$\begin{pmatrix} a_0 & a_{m-1} & \ldots & a_2 & a_1 \\ a_1 & a_0 & \ldots & a_3 & a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m-2} & a_{m-3} & \ldots & a_0 & a_{m-1} \\ a_{m-1} & a_{m-2} & \ldots & a_1 & a_0 \end{pmatrix}$$

Пример 2: *Транспонирование сопровождающей матрицы*

Умножение на $\boldsymbol{\alpha(x) = x}$ в кольце $\boldsymbol{R = P[x]/f(x)}$

$$S^T = \begin{pmatrix} f_{m-1} & f_{m-2} & \ldots & f_1 & f_0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

Подобие сопровождающей матрицы

Теорема 1: Пусть $\boldsymbol{P} = GF(q^n)$ – конечное поле из q^n элементов, $(\boldsymbol{c_i})$ – ЛРП над $\boldsymbol{P}$ с характеристическим многочленом $\boldsymbol{f(x)} = x^m - f_{m-1}x^{m-1} - \ldots - f_0$, $\boldsymbol{S} = \boldsymbol{S}(\boldsymbol{f(x)})$

Тогда справедливо следующее разложение $\boldsymbol{S} = \boldsymbol{C^{-1}S^TC}$, где

$$\boldsymbol{C} = \begin{pmatrix} c_{2m-2} & c_{2m-3} & \ldots & c_m & 1 \\ c_{2m-3} & c_{2m-4} & \ldots & 1 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ c_m & 1 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix}, \boldsymbol{C^{-1}} = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & 1 & -f_{m-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 1 & \ldots & -f_3 & -f_2 \\ 1 & -f_{m-1} & \ldots & -f_2 & -f_1 \end{pmatrix}$$

Разложения рекурсивной матрицы

Теорема 2: В условиях Теоремы 1 для рекурсивной матрицы $\boldsymbol{S(f(x))^m}$ справедливы следующие разложения:

- $$\boldsymbol{S^m} = \begin{pmatrix} f_{m-1} & f_{m-2} & \dots & f_1 & f_0 \\ f_{m-2} & f_{m-3} & \dots & f_0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ f_1 & f_0 & \dots & 0 & 0 \\ f_0 & 0 & \dots & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c_{m-1} & c_{m-2} & \dots & c_1 & 1 \\ c_{m-2} & c_{m-3} & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ c_1 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix};$$
- $\boldsymbol{S^m = C^{-1}(S^T)^m C}$,

где матрица $\boldsymbol{(S^T)^m}$ реализует умножение на элемент $\boldsymbol{x^m}$ в кольце $\boldsymbol{P[x]/f(x)}$

Intel Core i5 8265U

3.9 ГГц
256Кб
1 Мб
6Мб

Реализация линейного преобразования	XOR/SHFT/MEM	Объем памяти	Скорость шифрования
1. Вычисление ЛРП без таблицы умножения	242/32/17 + 208 MUL	256 байт	1,7 Мб/с
2. Вычисление ЛРП с таблицей умножения	242/32/225	2 Кб	9,7 Мб/с
3. Использование предвычисленных LUT-таблиц	34/0/17	64 Кб	113,8 Мб/с
4. Разложение рекурсивной матрицы	50/42/33	8 Кб	87,1 Мб/с
5. Умножение на элемент кольца	66/76/49	6 Кб	27,9 Мб/с

Спасибо за внимание!

Давыдов Степан Андреевич, специалист-исследователь лаборатории криптографии АО НПК «Криптонит», s.davydov@kryptonite.ru

Шишкин Василий Алексеевич, руководитель лаборатории криптографии АО НПК «Криптонит», v.shishkin@kryptonite.ru