Использование преобразований, задаваемых умножением на элемент кольца, в качестве линейных преобразований в XSL-схемах

Давыдов Степан

Лаборатория криптографии
«НПК «Криптонит»

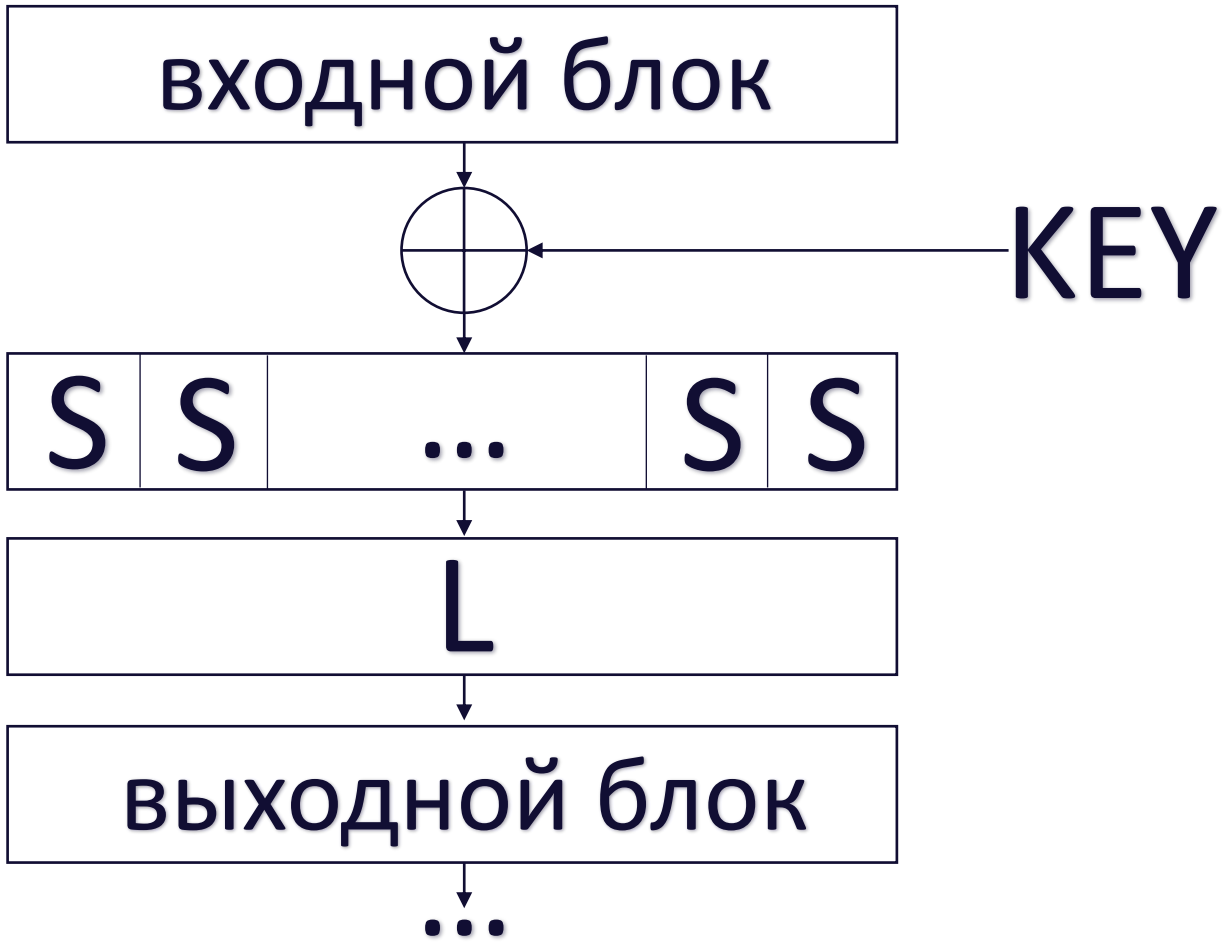
РусКрипто’2022

КРИПТОНИТ

КРИПТОНИТ

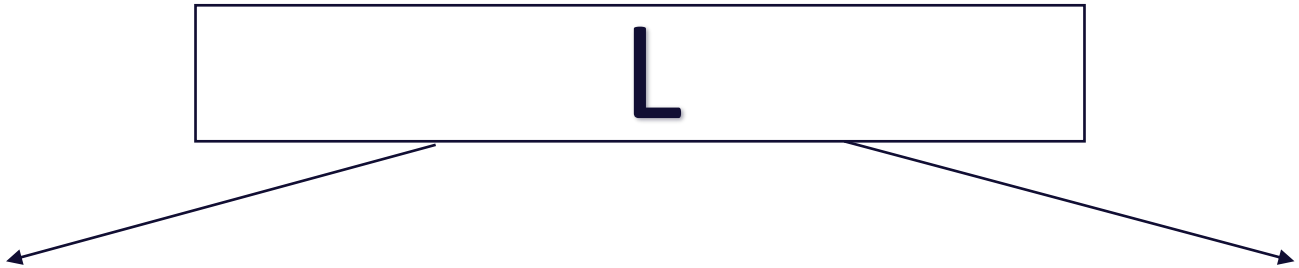
1 раунд XSL-схемы

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



КРИПТОНИТ

Линейный слой



Криптографические характеристики

- Показатели рассеивания матриц A, $A^T, A^{-1}, (A^T)^{-1}$

Если A – максимально рассеивающая матрица, то для ее реализации требуется либо существенный объем памяти, либо значительное число операций (инструкций процессора).

Эксплуатационные характеристики

- Количество инструкций процессора
- Объем требуемой памяти

КРИПТОНИТ

Преобразования, задаваемые умножением на элемент кольца

$x \rightarrow x\alpha$ в кольце $\mathbf{GF}(2)[\mathrm{x}]/(x^{mn}+1)$

n – длина векторов, которые преобразует S-блок, а m – количество таких блоков
то есть mn – длина блока, подаваемого на вход очередной итерации преобразования

Линейные преобразования, задаваемые умножением на элемент кольца

КРИПТОНИТ

Утверждение:

1. Матрица $A_{mn\times mn} = A(\alpha)$ линейного преобразования $x \to x\alpha$ в кольце $\mathrm{GF}(2)[\mathrm{x}]/(x^{mn}+1)$, элементы которого представлены векторами длины mn, является матрицей циркулянтом над полем $\mathrm{GF}(2)$ и может быть реализована на современных процессорах за две инструкции: $CLMUL$ и XOR. При этом в памяти необходимо хранить лишь только элементы α и α^{-1} (если требуется реализация обратного преобразования).

2. Для матриц $A = A(\alpha), A^T, A^{-1}, (A^T)^{-1}$ показатель рассеивания будет одинаковым.

Линейные преобразования, задаваемые умножением на элемент кольца

КРИПТОНИТ

Найденные путем оптимизированного перебора матрицы $A_{mn \times mn} = A(\alpha)$

Размер матрицы m×m	Размер n-блока	
	4 бита	8 бит
4×4	5 (MP)	5 (MP)
8×8	7	8
16×16	12	-

КРИПТОНИТ

Разложение произвольной матрицы через матрицы-циркулянты

Пусть $A \in GF(2)_{mn \times mn}$,

$$A = \sum_{i=1}^{2^{mn}-1} D_i C_i \,, \qquad (1)$$

где D_i – диагональные матрицы, $\sum_{i=1}^{2^{mn}-1} D_i = E_{mn \times mn}$ и общее число единиц во всех матрицах D_i равно mn, C_i – матрица-циркулянт, первая строка которой представляет двоичное представление числа i длины mn.

Линейные преобразования, задаваемые умножением на элемент кольца

КРИПТОНИТ

Теорема:

1. Для любой матрицы $A \in GF(2)_{mn \times mn}$ существует единственное разложение вида (1).

2. Число слагаемых в разложении (1) не превосходит *mn.*

3. Если число слагаемых в (1) равно *k*, то линейное преобразование $x \to xA$ может быть реализовано за *4k-1* инструкций процессора, а именно k инструкций $CLMUL$, *k* инструкций *AND* и *2k-1* инструкций XOR. В памяти при этом необходимо хранить *k* векторов из *mn* бит.

Линейные преобразования, задаваемые умножением на элемент кольца

КРИПТОНИТ

Пример:

Разложение матриц из п. 4.2 работы [1] содержит 8 слагаемых. Такие матрицы могут быть реализованы с использованием 31 инструкции процессора при хранении 8-ми 64-битных векторов.

Реализация линейного преобразования хэш-функции «Стрибог» через умножение вектора на матрицу требует в среднем 96 инструкций процессора и хранения 64-ех 64-битных векторов.

[1] Gupta, Kishan & Ghosh Ray, Indranil. (2014). On Constructions of Circulant MDS Matrices for Lightweight Cryptography. 8434. 564-576. 10.1007/978-3-319-06320-1_41.

Спасибо за внимание!

В работе над докладом принимали участие

Давыдов Степан

Специалист-исследователь,
Лаборатория криптографии «НПК «Криптонит»
s.davydov@kryptonite.ru

Василий Шишкин

Руководитель лаборатории,
Лаборатория криптографии «НПК «Криптонит»
v.shishkin@kryptonite.ru