О программной реализации алгоритмов шифрования с аутентификацией

Алексей Нестеренко
anesterenko@hse.ru, https://www.hse.ru/org/persons/47634770

24 марта 2021 г.

Постановка задачи

Шифрование данных при защищенном хранении и передаче по каналам связи

$$\begin{aligned} Enc(eKey, Message, eIvec) &\rightarrow CipherText, \\ Imito(iKey, Header||Message, iIvec) &\rightarrow Im, \end{aligned}$$

[AEAD – частный случай с одним ключом и одной синхропосылкой]
[имеем Р 1323565.1.026-2019]

Реализация:

- аппаратная (FPGA или ASIC)
  - итерационные алгоритмы (малая площадь $\rightarrow$ дешивизна),
  - конвейерные алгоритмы (скорость, до 100 Gb),
- программная реализация (`https://github.com/axelkenzo/libakrypt-0.x`)

Программная реализация

Шифр «Магма»

Режим	Скорость, MBs	%
ecb-magma	49,411111	100
ctr-magma	48,110868	97
ofb-magma	48,040074	97
cfb-magma	47,849739	96
cbc-magma	49,273965	99
xts-magma	47,586117	95
acpkm-magma	46,089132	93
cmac-magma	48,340254	97
mgm-magma	23,424500	47
ctr-cmac-magma	24,101876	48
ctr-hmac-magma-streebog256	35,713519	72
ctr-hmac-magma-streebog512	35,713049	72

Программная реализация

Шифр «Кузнечик»

Режим	Скорость, MBs	%
ecb-kuznechik	148,898152	100
ctr-kuznechik	131,583606	88
ofb-kuznechik	128,942234	86
cfb-kuznechik	129,088006	86
cbc-kuznechik	129,898637	87
xts-kuznechik	124,315330	83
acpkm-kuznechik	65,034391	43
cmac-kuznechik	127,687063	85
mgm-kuznechik	62,764779	42
ctr-cmac-kuznechik	64,808306	43
ctr-hmac-kuznechik-streebog256	67,545720	45
ctr-hmac-kuznechik-streebog512	67,537448	45

Программная реализация

Выводы (по существующим алгоритмам)

- Ожидаемая скорость - не более 50 % от скорости ecb,
- Накладные расходы - изменение внутреннего состояния (шифрование + имитозащита) - зависимость от длины блока,
- Целесообразность использования MGM (только в снижении ключевого множества)

- Ключи – *iKey*, *eKey*
- $\{x_i\}$ – блоки открытого текста, $\{c_i\}$ – блоки шифрованного текста
- $\theta_n = \theta_0 \alpha^n$, где $\alpha, \theta \in \mathbb{F}_{2^{128}}, < \alpha >= \mathbb{F}^*_{2^{128}}, \theta_0 = cbc(iKey, iv), n = 1, 2, \ldots$
- шифрование $c_{2n-\epsilon} = \xi_{2n-\epsilon} \oplus d_{2n-\epsilon}$, где

$$d_{2n-\epsilon} = ecb(eKey, x_{2n-\epsilon} \oplus \xi_{2n-\epsilon}), \quad \epsilon = 1, 0$$

и

$$\theta_n = \xi_{2n-1} || \xi_{2n}.$$

Возможен вариант xts (xor-enryption-xor) с 256 битным вектором θ_n

[1] Об одном семействе универсальных функций хеширования // МВК — 2015.

[2] A new authenticated encryption mode for arbitrary block cipher based on universal hash function // Математические вопросы криптографии (МВК)– 2017.

$$(xor)\sum_{i=1}^{t}\pi(\theta_n,\{\gamma_i\}_{i=1}^{r},\{x_{2n-1},x_{2n}\}) \quad (\text{сумма в} \quad \mathbb{V}_m).$$

Свойства и атаки:

1. коммутативность => **атака**: перестановка слагаемых => непредсказуемость θ_i => зависимость θ_i от ключа;
2. аддитивность => **атака**: добавление слагаемых (в сумме дающих ноль) => контроль (подсуммирование) длины;
3. линейность => **атака**: решение линейных систем и определение θ_i по выходу => шифрование значения суммы;
4. преобразование π – хорошие разностые характеристики в $\mathbb{V}_m$ и непредсказуемость ($\gamma_1,\ldots,\gamma_r$ – секретные параметры отображения π).

- Производные ключи $(\underbrace{\theta_0}_{128} || \underbrace{\gamma_1}_{64} || \ldots || \gamma_r) = cbc(iKey, iv||0),$
- Преобразование π (r - раундовая сеть Фейстеля), где i-й раунд определяется

$$(l_i, s_i) \to (s, s \oplus L(\pi(l_i \oplus \gamma_i))),$$

для L, π, определенных в ГОСТ Р 34.11-2012.

- На вход сети Фейстеля подаются (промежуточные) значения d_{2n-1}, d_{2n}.

Алгоритм xtsmac

Результаты программной реализации

Режим	Скорость, MBs	%
mgm-magma	23,424500	47
xtsmac-magma (r=4)	45,877878	92
xtsmac-magma (r=4, xts-256)	45,691290	92
xtsmac-magma (r=6)	44,866156	90
xtsmac-magma (r=8)	43,812546	88
mgm-kuznechik	62,764779	42
xtsmac-kuznechik (r=4)	106,946651	71
xtsmac-kuznechik (r=4, xts-256)	105,967335	71
xtsmac-kuznechik (r=6)	98,079706	69
xtsmac-kuznechik (r=8)	89,690888	61