ЛИТЕРАТУРА

1. *Rivest R., Shamir A., and Tauman Y.* How to Leak a Secret // Proc. 7th Internat. Conf. on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, 2001. P. 552–565.
2. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. `http://bitcoin.org/bitcoin.pdf`. 2009.
3. *Rivest R., Micali S., and Goldwasser S.* A Digital Signature Scheme Secure against Adaptive Chosen-Message Attacks // SIAM J. Computing. 1988. V. 17. No. 2. P. 281–308.
4. *Cramer R., Damgard I., and Schoenmakers B.* Proofs of partial knowledge and simplified design of witness hiding protocols // LNCS. 1994. V. 839. P. 174–187.

УДК 519.7

# ОПТИМАЛЬНЫЕ ЛИНЕЙНЫЕ ПРИБЛИЖЕНИЯ СЕТЕЙ ФЕЙСТЕЛЯ. ОЦЕНКА СТОЙКОСТИ ШИФРА SMS4 К ЛИНЕЙНОМУ КРИПТОАНАЛИЗУ

Г. И. Шушуев

Для применения линейного криптоанализа к итеративному блочному шифру требуется найти линейное приближение для конкретного числа раундов. Если известно лучшее приближение, то можно определить минимальную трудоёмкость линейного криптоанализа шифра, то есть оценить его криптографическую стойкость. Таким образом, задача оценки криптографической стойкости сводится к поиску линейных приближений и нахождению среди них лучшего. В связи с этим возникает ряд проблем, так как, помимо того, что нужно исследовать раундовую функцию, необходимо правильно согласовывать приближения раундов. Как правило, при проведении линейного криптоанализа выбирается некоторое найденное линейное приближение без доказательства того, что оно является лучшим.

Для поиска лучшего приближения можно перебирать всевозможные линейные соотношения, но на это может потребоваться больше времени, чем на составление словаря, поэтому необходимо придумывать другие способы. Предлагается подход к нахождению линейных приближений сети Фейстеля и поиску оптимального.

**Определение 1.** *Раундовая функция* — функция вида $F : (\mathbb{Z}_2^m)^n \to \mathbb{Z}_2^m$. Пусть $F(X_1, X_2, \ldots, X_n) = Y$, где $Y, X_i \in \mathbb{Z}_2^m, i = 1, 2, \ldots, n$.

Как правило, раундовая функция сети Фейстеля удовлетворяет некоторым ограничениям, например, является простой (применяется в SMS4) или псевдо-простой (DES, TEA). Функция $F$ называется *простой*, если $F(X_1, X_2, \ldots, X_n) = G(X_1 \oplus X_2 \oplus \ldots \oplus X_n)$ для некоторой функции $G : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$. Функция $F$ называется *псевдопростой*, если $F(X_1, X_2, \ldots, X_n) = G(L_1(X_1) \oplus L_2(X_2) \oplus \ldots \oplus L_n(X_n))$ для некоторых функции $G : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ и набора функций $L_1, \ldots, L_n$, где $L_i : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$.

**Определение 2.** *Линейным приближением* функции $F$ называется соотношение

$$b_1 \cdot X_1 \oplus b_2 \cdot X_2 \oplus \ldots \oplus b_n \cdot X_n = a \cdot F(X_1, \ldots, X_n), \tag{1}$$

выполняющееся с вероятностью $1/2 + \varepsilon$, где $|\varepsilon| \leqslant 1/2$, $a, b_i \in \mathbb{Z}_2^m$, $i = 1, 2, \ldots, n$.

Величину $\varepsilon$ назовём *линейным преобладанием соотношения* или просто *преобладанием*. Вектор $b_i$ назовём *маской* для вектора $X_i$. Определим функцию

$R_F : (\mathbb{Z}_2^m)^{n+1} \to \mathbb{R}$, действующую на масках $b_1, \ldots, b_n, a$ следующим образом:

$$R_F(b_1, \ldots, b_n, a) = \frac{1}{2} + \varepsilon.$$

Функция $R_F$ на масках $b_1, \ldots, b_n, a$ принимает значение вероятности, с которой выполняется соответствующее линейное приближение (1).

**Утверждение 1.** Если $F$ является простой и $R_F(b_1, \ldots, b_n, a) = 1/2 + \varepsilon$, где $|\varepsilon| > 0$, то выполняется $b_1 = b_2 = \ldots = b_n$.

**Следствие 1.** Пусть $F$ является псевдопростой и $R_F(b_1, \ldots, b_n, a) = 1/2 + \varepsilon$, где $|\varepsilon| > 0$. Тогда для некоторого набора функций $l_1, \ldots, l_n$ выполняется $l_1(b_1) = l_2(b_2) = \ldots = l_n(b_n)$. При этом если одна из масок $b_i$ является нулевой, то $b_1 = \ldots = b_n = 0$.

**Следствие 2.** Если $F$ является псевдопростой и хотя бы одна из масок $b_1$, $b_2$, …, $b_n$, $a$ является нулевой, то

$$R_F(b_1, \ldots, b_n, a) = \begin{cases} 1, & \text{если } b_1 = b_2 = \ldots = b_n = a = 0, \\ 1/2 & \text{иначе.} \end{cases}$$

Открытый текст обозначим через $X^0$, промежуточный шифртекст после $i$-го раунда — через $X^i$, где $X^i \in (\mathbb{Z}_2^m)^n$, $i = 0, 1, \ldots$ На $i$-м раунде используется ключ $K^i \in \mathbb{Z}_2^m$.

**Определение 3.** *Линейным приближением раунда $r$* называется соотношение

$$a^{r-1} \cdot X^{r-1} \oplus a^r \cdot X^r \oplus \alpha^r = d^r \cdot K^r$$

выполняющееся с вероятностью $1/2 + \varepsilon_r$, где $\varepsilon_r > 0$, $\alpha^r \in \mathbb{Z}_2$, $a^{r-1}, a^r \in (\mathbb{Z}_2^m)^n$, $d^r \in \mathbb{Z}_2^m$.

Линейное приближение раунда строится на основе линейного приближения раундовой функции $F$. Путём последовательного приближения раундов получаем приближение нескольких раундов шифра.

**Определение 4.** *Линейным приближением $p$ раундов шифра* называется соотношение

$$a^0 \cdot X^0 \oplus a^p \cdot X^p \oplus \alpha = d^1 \cdot K^1 \oplus \ldots \oplus d^p \cdot K^p, \tag{2}$$

выполняющееся с вероятностью $1/2 + \varepsilon$, $\varepsilon > 0$.

Если $a^0$ совпадает с $a^p$, то линейное приближение (2) называется *замкнутым* и имеет следующий вид:

$$a^0 \cdot X^0 \oplus a^0 \cdot X^p \oplus \alpha = d^1 \cdot K^1 \oplus \ldots \oplus d^p \cdot K^p.$$

Лучшим линейным приближением шифра считается то, преобладание которого максимально. Как правило, число раундов сети Фейстеля довольно большое, а линейное приближение получается последовательным применением некоторого замкнутого линейного приближения и, если требуется, анализом ещё нескольких раундов. В данной работе для нахождения лучшего линейного приближения шифра предлагается найти лучшее замкнутое линейное приближение, а для этого нужно научиться их сравнивать. Для сравнения замкнутых линейных приближений с использованием piling-up леммы [1] вводится *раундовое преобладание*.

**Определение 5.** *Раундовым преобладанием* линейного приближения $p$ раундов назовём величину

$$\tilde{\varepsilon} = (\varepsilon \cdot 2^{1-p})^{\frac{1}{p}},$$

где $\varepsilon$ является преобладанием линейного приближения $p$ раундов.

С помощью раундового преобладания можно сравнивать замкнутые линейные приближения различного количества раундов и определять оптимальное. *Оптимальным линейным приближением раундов* назовём замкнутое линейное приближение, такое, что его раундовое преобладание максимально. Оптимальное линейное приближение находится среди линейных приближений различного числа раундов.

Проведена оценка стойкости шифра SMS4 (стандарт блочного шифр KHP для защиты беспроводных сетей WLAN [2]) к линейному криптоанализу.

**Теорема 1.** Замкнутое линейное приближение пяти раундов SMS4

$$a \cdot X^0 \oplus a \cdot X^5 = \gamma \cdot K^4 \oplus \gamma \cdot K^5,$$

где $a, X^0, X^5 \in (\mathbb{Z}_2^{32})^4$, $\gamma, K^4, K^5 \in \mathbb{Z}_2^{32}$ и маска $a$ имеет вид $(0, 0, 0, \gamma)$, $\gamma =$ `0x0011ffba`, является оптимальным.

**Теорема 2.** Минимальная трудоёмкость линейного криптоанализа девяти раундов блочного шифра SMS4 достигается при объёме статистики $2^{84}$ и составляет $2^{115}$ зашифрований.

## ЛИТЕРАТУРА

1. *Matsui M.* Linear Cryptoanalysis Method for DES Cipher // LNCS. 1994. V. 765. P. 386–397.
2. *Diffie W. and Ledin G.* SMS4 encyption algorithm for wireless networks — Cryptology ePrint Archive, Report 2008/329 // `http://eprint.iacr.org/2008/329`, 2008.