2014 Математические методы криптографии №1(23)

DOI 10.17223/20710410/23/5

УДК 519.7

ПОИСК ОПТИМАЛЬНОГО ЛИНЕЙНОГО ПРИБЛИЖЕНИЯ СЕТЕЙ ФЕЙСТЕЛЯ

Г. И. Шушуев

Новосибирский государственный университет, г. Новосибирск, Россия

E-mail: g.shushuev@gmail.com

Предлагается подход к нахождению линейных приближений сети Фейстеля, математическая постановка задачи о линейном приближении и алгоритм, позволяющий находить оптимальное линейное приближение обобщённой сети Фейстеля.

Ключевые слова: *линейный криптоанализ, сеть Фейстеля.*

Введение

Для применения линейного криптоанализа к итеративному блочному шифру требуется найти линейное приближение на определённое число раундов. Если известно лучшее приближение, то можно определить минимальную трудоёмкость линейного криптоанализа шифра, т. е. оценить криптографическую стойкость шифра. 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.

В работе предлагается подход к нахождению линейных приближений сети Фейстеля, математическая постановка задачи о линейном приближении и алгоритм, позволяющий находить оптимальное линейное приближение обобщённой сети Фейстеля.

В п. 1 приведено описание обобщённой сети Фейстеля, вводятся линейные приближения, замечаются некоторые их свойства, вводится понятие раундового преобладания, используемое для сравнения приближений раундов. В п. 2 даётся математическая постановка задачи о линейном приближении, вводится понятие дерева шаблонов, рассматриваются его свойства и предлагается алгоритм поиска оптимального пути в дереве шаблонов, что является оптимальным линейным приближением для некоторой сети Фейстеля.

1. Линейные приближения обобщённой сети Фейстеля

Линейный криптоанализ использует линейное приближение шифра, в которое входят биты открытого текста, шифртекста и ключа. Линейное приближение шифра характеризуется вероятностью, с которой оно выполняется, и чем она выше, тем линейное приближение лучше, так как криптоанализ на его основе будет менее трудоёмок.

Рассмотрим процедуру построения линейного приближения шифра.

1.1. Обобщённая сеть Фейстеля

Обобщённая сеть Фейстеля — один из методов построения блочных шифров. Алгоритм шифрования реализуется несколькими итерациями преобразования сети с использованием ключа MK. Ценность метода заключается в том, что преобразование сети Фейстеля обратимо.

Обобщённая сеть Фейстеля характерна тем, что входное слово разбивается на два или более подслов, часть из которых на каждом раунде преобразуется по определённому закону. Если длины подслов совпадают, то такую сеть называют *сбалансированной*.

Приведём схему сбалансированной обобщённой сети Фейстеля с r раундами (рис. 1). Открытый текст P, шифртекст C имеют длину N бит, ключ MK — M бит. Открытый текст представляется как n m-битных подслов $P = X^0 = (X_1^0, X_2^0, X_3^0, \ldots, X_n^0)$, X^i — промежуточный шифртекст после i-го раунда, где $i = 1, 2, \ldots, r$; $F : (\mathbb{Z}_2^m)^n \to \mathbb{Z}_2^m$ — нелинейная раундовая функция. Раундовые подключи K^i длины k бит *однозначно* задаются ключом MK.

Процесс шифрования осуществляется следующим образом.

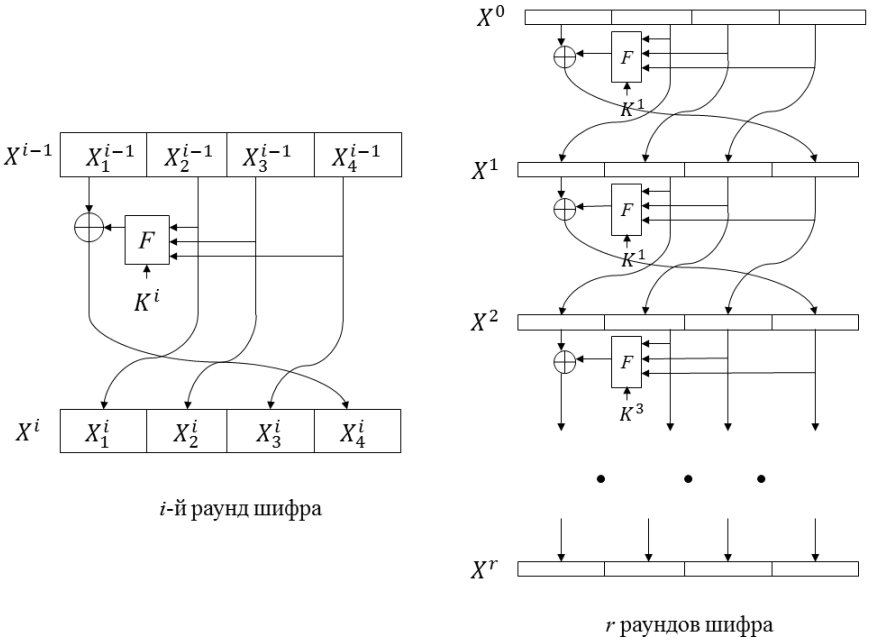
1. Входной открытый текст $P = X^0 = (X_1^0, X_2^0, X_3^0, \ldots, X_n^0)$.

2. Для i от 1 до r

$X_n^i = X_1^{i-1} \oplus F(K^i, X_2^{i-1}, X_3^{i-1}, \ldots, X_n^{i-1})$,

$X^i = (X_1^i, X_2^i, \ldots, X_n^i) = (X_2^{i-1}, X_3^{i-1}, \ldots, X_n^{i-1}, X_1^{i-1} \oplus F(K^i, X_2^{i-1}, X_3^{i-1}, \ldots, X_n^{i-1}))$.

3. Выходной шифртекст $C = X^r = (X_1^r, X_2^r, X_3^r, \ldots, X_n^r)$.



i-й раунд шифра

r раундов шифра

Рис. 1. Обобщённая сеть Фейстеля на примере SMS4 [1]

1.2. Описание и история линейного криптоанализа

Линейный криптоанализ — статистический метод, предложенный в 1992–1993 гг. японским криптографом Мицуру Мацуи. Сначала он вместе с А. Ямагиши исследовал этот метод для блочного шифра FEAL [2], а позднее применил его к шифру DES [3] и провёл экспериментальный криптоанализ полных его 16-ти раундов [4]. Линейный криптоанализ заключается в исследовании линейного приближения шифра на парах

«открытый текст — шифртекст» для получения информации о ключе. М. Мацуи предложил два алгоритма линейного криптоанализа, первый для нахождения линейного соотношения, выполняющегося на битах ключа, второй для нахождения части ключа.

Для проведения криптоанализа необходимо знание структуры шифра, а также достаточный объём выборки, состоящей из пар открытого текста и шифртекста, полученных на одном и том же *неизвестном* криптоаналитику ключе.

Большое число работ посвящено обобщениям и применениям линейного криптоанализа. Детальное исследование этого метода провела К. Ньюберг [5]. Для повышения эффективности метода в [6] предложено для одной комбинации битов ключа рассматривать одновременно несколько линейных приближений. Авторы [7] привели способ улучшения метода, предложив учитывать при приближении вероятностное поведение битов вместо их фиксированных значений. Общий метод уменьшения временной сложности линейного криптоанализа блочных шифров (в том числе SP-сетей и сетей Фейстеля) за счёт использования быстрых преобразований Фурье описывается в [8]. В [9] предложены идеи по использованию в линейном криптоанализе квадратичных соотношений специального вида.

1.3. Приближение раундовой функции

Линейные приближения раундовой функции находятся путём анализа конструкции конкретного шифра. Рассмотрим некоторые свойства линейных приближений и введём ряд определений для работы с ними.

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 обобщённой сети Фейстеля удовлетворяет некоторым ограничениям, например является простой (применяется в SMS4 [1]) или псевдопростой (DES [10], TEA [11]).

Определение 2. Раундовая 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 $G : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$.

Определение 3. Раундовая 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 $L_i : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ не тождественно нулевые.

Определение 4. *Скалярное произведение* векторов $X, Y \in \mathbb{Z}_2^m$, где $X = (x_1, x_2, \ldots, x_m)$, $Y = (y_1, y_2, \ldots, y_m)$, $x_j, y_j \in \mathbb{Z}_2$, вычисляется следующим образом:

$$X \cdot Y = x_1 y_1 \oplus x_2 y_2 \oplus \ldots \oplus x_m y_m.$$

Определение 5. *Линейной комбинацией* битов вектора $X \in \mathbb{Z}_2^m$ называется скалярное произведение X и некоторого вектора $b \in \mathbb{Z}_2^m$. Вектор b назовём *маской* для вектора X.

Линейной комбинацией битов X_i является

$$b_i \cdot X_i = b_{i1} x_{i1} \oplus b_{i2} x_{i2} \oplus \ldots \oplus b_{im} x_{im},$$

где $b_i = (b_{i1}, b_{i2}, \ldots, b_{im})$; $X_i = (x_{i1}, x_{i2}, \ldots, x_{im})$; $b_{ij}, x_{ij} \in \mathbb{Z}_2$, $j = 1, \ldots, m$, $i = 1, \ldots, n$.

Определение 6. *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 $1/2 + \varepsilon$ при случайном равновероятном выборе X_i, где $|\varepsilon| \leqslant 1/2$; $a, b_i \in \mathbb{Z}_2^m$, $i = 1, 2, \ldots, n$. Величину ε назовём *линейным преобладанием соотношения*, или просто *преобладанием*.

Пример линейного приближения раундовой функции изображён на рис. 2.

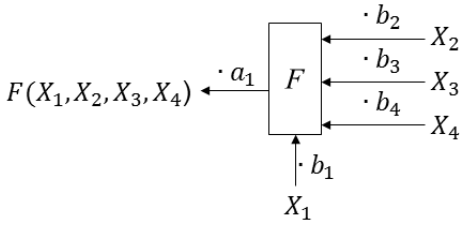


Рис. 2. Линейное приближение раундовой функции F, случай $n = 4$

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). Несложно доказать следующую вспомогательную лемму.

Лемма 1. Пусть $X \in \mathbb{Z}_2^l$, $y \in \mathbb{Z}_2$ — независимые случайные величины. Тогда равенство $f(X) \oplus y = 0$, где $f : \mathbb{Z}_2^l \to \mathbb{Z}_2$, выполняется с вероятностью $1/2$ для любого натурального $l > 0$.

Доказательство. Пусть $f(X) = 0$ в $(2^{l-1} + p)$ случаях и $f(X) = 1$ в $(2^{l-1} - p)$ случаях, $p \in \{0, 1, \ldots, 2^{l-1}\}$. Покажем, что при любом значении p равенства $f(X) \oplus y = 0$ и $f(X) \oplus y = 1$ выполняются одинаково часто (в 2^l случаях).

Так как X не зависит от y, то пусть X пробегает все значения при фиксированном $y = 0$, тогда $f(X) \oplus y$ принимает значения 0 и 1 в $(2^{l-1} + p)$ и $(2^{l-1} - p)$ случаях соответственно. При $y = 1$ ситуация обратная, т. е. $f(X) \oplus y$ принимает значения 0 и 1 в $(2^{l-1} - p)$ и $(2^{l-1} + p)$ случаях соответственно. Значит, $f(X) \oplus y = 0$ в 2^l случаях и $f(X) \oplus y = 1$ в 2^l случаях, т. е. $f(X) \oplus y = 0$ с вероятностью $1/2$. ■

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

Доказательство. Пусть $b_1 = b$, $b_2 = b \oplus b_2'$, $\ldots$, $b_n = b \oplus b_n'$. Тогда соотношение (1) можно представить в виде $b \cdot X_1 \oplus b \cdot X_2 \oplus b_2' \cdot X_2 \oplus \ldots \oplus b \cdot X_n \oplus b_n' \cdot X_n = a \cdot G(X_1 \oplus \ldots \oplus X_n)$. После группировки слагаемых получим

$$b \cdot (X_1 \oplus \ldots \oplus X_n) \oplus (b_2' \cdot X_2 \oplus \ldots \oplus b_n' \cdot X_n) = a \cdot G(X_1 \oplus \ldots \oplus X_n). \tag{2}$$

Положим $X_1 \oplus \ldots \oplus X_n = X$ и заметим, что векторы X и $X_2 \oplus \ldots \oplus X_n$ независимы. Действительно, так как X_1 не зависит от $X_2 \oplus \ldots \oplus X_n$, то и X принимает всевозможные значения независимо от $X_2 \oplus \ldots \oplus X_n$.

Предположим, что $b'_i \neq 0$ для некоторого $i \in \{2, \ldots, n\}$. Тогда линейная функция $l(X_2, \ldots, X_n) = b'_2 \cdot X_2 \oplus \ldots \oplus b'_n \cdot X_n$ не является тождественно нулевой и, следовательно, принимает значения 0 и 1 одинаковое число раз. Перепишем соотношение (2) в введённых обозначениях, перенеся всё в левую часть:

$$b \cdot X \oplus l(X_2, \ldots, X_n) \oplus a \cdot G(X) = 0. \tag{3}$$

По лемме 1 получаем, что вероятность выполнения равенства (3) равна 1/2, следовательно, $R_F(b_1, \ldots, b_n, a) = 1/2$, что противоречит условию. ■

Следствие 1. Пусть F является псевдопростой, $F(X_1, X_2, \ldots, X_n) = G(L_1(X_1) \oplus \oplus L_2(X_2) \oplus \ldots \oplus L_n(X_n))$ и $R_F(b_1, \ldots, b_n, a) = 1/2 + \varepsilon$, где $|\varepsilon| > 0$ для некоторых фиксированных $b_1, \ldots, b_n, a$. Пусть функции $l_1, \ldots, l_n$ выбраны так, что $b_i \cdot X_i = l_i(b_i) \cdot L_i(X_i)$ для любого $X_i \in \mathbb{Z}_2^m$. Тогда выполняется $l_1(b_1) = l_2(b_2) = \ldots = l_n(b_n)$, причём если одна из масок b_i нулевая, то $b_1 = \ldots = b_n = 0$.

Доказательство. Линейное приближение (1) можно переписать в виде

$$l_1(b_1) \cdot L_1(X_1) \oplus \ldots \oplus l_n(b_n) \cdot L_n(X_n) = a \cdot G(L_1(X_1) \oplus \ldots \oplus L_n(X_n)).$$

По утверждению 1 получим, что $l_1(b_1) = l_2(b_2) = \ldots = l_n(b_n)$, так как $R_F(b_1, \ldots, b_n, a) = = R_G(l_1(b_1), \ldots, l_n(b_n), a) = 1/2 + \varepsilon$, где $|\varepsilon| > 0$.

Если $b_i = 0$, то $b_i \cdot X_i = l_i(b_i) \cdot L_i(X_i) = 0$, значит, $l_i(b_i) = 0$. Обратное тоже верно: если $l_i(b_i) = 0$, то $b_i = 0$. Получаем, что $l_1(b_1) = l_2(b_2) = \ldots = l_n(b_n) = b_1 = \ldots = b_n = 0$, если $b_i = 0$. ■

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

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

Доказательство. Если $b_1 = b_2 = \ldots = b_n = a = 0$, то $R_F(b_1, \ldots, b_n, a) = 1$, так как в этом случае линейное приближение (1) функции F выглядит так: $0 = 0$. Если нулевой является одна из масок $b_1, \ldots, b_n$, то, по следствию 1, выполняется либо $b_1 = \ldots = b_n = 0$, либо $R_F(b_1, \ldots, b_n, a) = 1/2$. Осталось рассмотреть два случая:

— маска a является нулевой, маски $b_1, \ldots, b_n$ не все одновременно нулевые;
— маски $b_1, \ldots, b_n$ все одновременно нулевые, маска a ненулевая.

Оба случая соответствуют ситуации, когда линейное приближение (1) есть некоторая линейная комбинация битов равная нулю. Так как линейная комбинация является сбалансированной булевой функцией, то на всевозможных наборах она принимает значение 0 и 1 одинаковое количество раз, а значит, $R_F(b_1, \ldots, b_n, a) = 1/2$. ■

1.4. Раундовое приближение

Рассмотрим, как с помощью линейного приближения псевдопростой раундовой функции построить линейное приближение для одного раунда шифра. Промежуточный шифртекст до r-го раунда обозначим через $X^{r-1} = (X_1^{r-1}, X_2^{r-1}, \ldots, X_n^{r-1})$, после r-го раунда — $X^r = (X_1^r, X_2^r, \ldots, X_n^r)$, где $X^{r-1}, X^r \in (\mathbb{Z}_2^m)^n$; $X_j^r \in \mathbb{Z}_2^m$. На r-м раунде используется ключ $K^r \in \mathbb{Z}_2^m$.

Определение 7. *Линейным приближением раунда* r называется соотношение

$$a^{r-1} \cdot X^{r-1} \oplus a^r \cdot X^r \oplus \alpha^r = d^r \cdot K^r, \tag{4}$$

выполняющееся с вероятностью $1/2 + \varepsilon_r$, где $\varepsilon_r > 0$; $\alpha^r \in \mathbb{Z}_2$; $a^{r-1}, a^r \in (\mathbb{Z}_2^m)^n$; $d^r \in \mathbb{Z}_2^m$; a^{r-1}, a^r — маски входа и выхода раунда соответственно.

Пример линейного приближения раунда изображён на рис. 3.

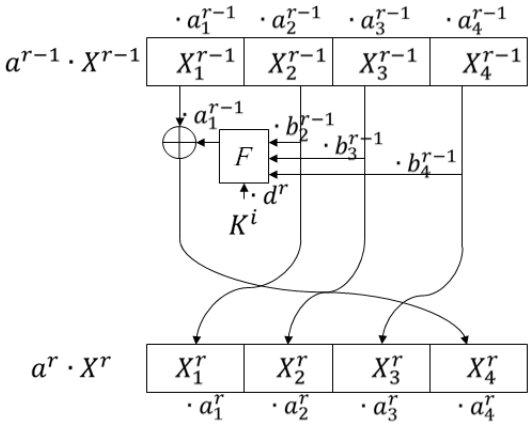


Рис. 3. Линейное приближение r-го раунда, случай $n = 4$

Поскольку шифртексты X^r и X^{r-1} находятся в зависимости

$$X^r = (X_1^r, X_2^r, \ldots, X_n^r) = (X_2^{r-1}, X_3^{r-1}, \ldots, X_n^{r-1}, F(K^r, X_2^{r-1}, X_3^{r-1}, \ldots, X_n^{r-1})),$$

которую можно представить как

$$\begin{cases} X_i^r = X_{i+1}^{r-1}, \ i = 1, \ldots, n-1, \\ X_n^r = F(K^r, X_2^{r-1}, \ldots, X_n^{r-1}), \end{cases}$$

приближение (1) раундовой функции в данном случае выглядит так:

$$d^r \cdot K^r \oplus b_2^{r-1} \cdot X_2^{r-1} \oplus \ldots \oplus b_n^{r-1} \cdot X_n^{r-1} = a_1^{r-1} \cdot F(K^r, X_2^{r-1}, \ldots, X_n^{r-1}).$$

Получаем, что маски $a^r = (a_1^r, \ldots, a_n^r)$ и $a^{r-1} = (a_1^{r-1}, \ldots, a_n^{r-1})$ связаны следующим образом:

$$\begin{cases} a_i^r = a_{i+1}^{r-1} \oplus b_{i+1}^{r-1}, \ i = 1, \ldots, n-1, \\ a_n^r = a_1^{r-1}, \end{cases}$$

где ввиду $R_F(d^r, b_2^{r-1}, \ldots, b_n^{r-1}, a_1^{r-1}) \neq 1/2$ по следствию 1 маски $b_2^{r-1}, \ldots, b_n^{r-1}$ однозначно определяются по d^r. Значение ε_r совпадает с модулем ε, вычисленным по приближению раундовой функции $R_F(d^r, b_2^{r-1}, \ldots, b_n^{r-1}, a_1^{r-1}) = 1/2 + \varepsilon$, а α^r подбирается так, чтобы $\varepsilon_r > 0$ (если $\varepsilon > 0$, то $\alpha^r = 0$; если $\varepsilon < 0$, то $\alpha^r = 1$).

Если хотя бы одна из масок $d^r, b_2^{r-1}, \ldots, b_n^{r-1}, a_1^{r-1}$ является нулевой, то по следствию 2, для того чтобы выполнялось $R_F(d^r, b_2^{r-1}, \ldots, b_n^{r-1}, a_1^{r-1}) \neq 1/2$, все они должны быть нулевыми; значит, соотношение (4) упрощается:

$$a^{r-1} \cdot X^{r-1} \oplus a^r \cdot X^r = 0$$

и выполняется с вероятностью 1, а маски $a^r = (a_1^r, \ldots, a_n^r)$ и $a^{r-1} = (a_1^{r-1}, \ldots, a_n^{r-1})$ связаны следующим образом:

$$\begin{cases} a_i^r = a_{i+1}^{r-1}, \ i = 1, \ldots, n-1, \\ a_n^r = a_1^{r-1} = 0. \end{cases} \tag{5}$$

Пример 1. Рассмотрим приближение одного раунда некоторого шифра с $n = 2$ и $m = 6$. Пусть имеется приближение раундовой функции $b_1 \cdot X_1 \oplus b_2 \cdot X_2 = a \cdot F(X_1, X_2)$, выполняющееся с вероятностью $1/2 + \varepsilon$, в котором $\varepsilon = -1/8$, $b_1 = (1, 0, 1, 0, 1, 0)$, $b_2 = (0, 1, 0, 1, 0, 1)$, $a = (0, 0, 1, 1, 0, 0)$. Функция R_F в данном случае примет вид $R_F(b_1, b_2, a) = 1/2 - 1/8$.

Составим линейное приближение первого раунда, построенное из имеющегося приближения раундовой функции. Шифртекст $X^1 = (X_1^1, X_2^1)$ вычисляется по $X^0 = (X_1^0, X_2^0)$ как $X^1 = (X_1^1, X_2^1) = (X_2^0, F(K^1, X_2^0))$; тогда имеющееся приближение раундовой функции F представимо в виде $d^1 \cdot K^1 \oplus b_2^0 \cdot X_2^0 = a_1^0 \cdot F(K^1, X_2^0)$. Получаем $R_F(d^1, b_2^0, a_1^0) = 1/2 - 1/8$. Осталось определить $a^0 = (a_1^0, a_2^0)$ и $a^1 = (a_1^1, a_2^1)$. Часть a^0, а именно $a_1^0 = (0, 0, 1, 1, 0, 0)$, уже зафиксирована приближением раундовой функции; a_2^0 может быть любым вектором длины 6, допустим $(0, 1, 0, 0, 0, 0)$. Из следующей системы находится a^1:

$$\begin{cases} a_1^1 = a_2^0 + b_2^0, \\ a_2^1 = a_1^0. \end{cases}$$

Подставим известные значения a_2^0, b_2^0, a_1^0 и получим

$$a_1^1 = (0, 1, 0, 0, 0, 0) \oplus (0, 1, 0, 1, 0, 1) = (0, 0, 0, 1, 0, 1), \quad a_2^1 = (0, 0, 1, 1, 0, 0).$$

В итоге линейным приближением первого раунда является соотношение

$$a^0 \cdot X^0 \oplus a^1 \cdot X^1 \oplus \alpha^1 = d^1 \cdot K^1,$$

выполняющееся с вероятностью $1/2 + 1/8$. Его можно представить в виде

$$x_{1,3}^0 \oplus x_{1,4}^0 \oplus x_{2,2}^0 \oplus x_{1,4}^1 \oplus x_{1,6}^1 \oplus x_{2,3}^1 \oplus x_{2,4}^1 \oplus 1 = k_1^1 \oplus k_3^1 \oplus k_5^1.$$

Заметим, что таким образом мы получаем некую информацию о битах ключа, а именно о битах k_1^1, k_3^1 и k_5^1.

1.5. Схема согласования раундовых приближений

Определение 8. *Схемой согласования раундовых приближений порядка p* называется система, состоящая из уравнений вида (4)

$$\begin{cases} a^0 \cdot X^0 \oplus a^1 \cdot X^1 \oplus \alpha^1 = d^1 \cdot K^1, \\ a^1 \cdot X^1 \oplus a^2 \cdot X^2 \oplus \alpha^2 = d^2 \cdot K^2, \\ \ldots \\ a^{r-1} \cdot X^{r-1} \oplus a^r \cdot X^r \oplus \alpha^r = d^r \cdot K^r, \\ \ldots \\ a^{p-1} \cdot X^{p-1} \oplus a^p \cdot X^p \oplus \alpha^p = d^p \cdot K^p, \end{cases} \tag{6}$$

в которой определены маски a^0, a^r, d^r, биты α^r и преобладания ε_r, $r = 1, \ldots, p$. Маски a^0 и a^p назовём *начальной* и *конечной* масками соответственно.

На рис. 4 изображён пример схемы согласования раундов.

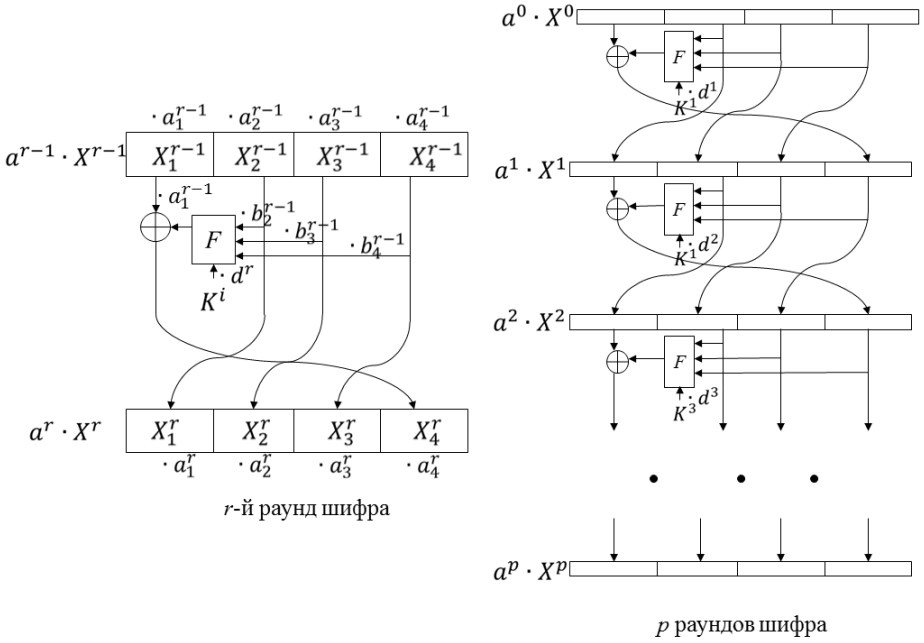


Рис. 4. Схема согласования раундовых приближений, случай $n = 4$

Схема согласования раундовых приближений порядка p порождает *линейное приближение p раундов шифра*. Заметим, что если сложить по модулю два все уравнения, то останутся только биты X^0, X^p и раундовых ключей.

Определение 9. *Линейным приближением p раундов шифра* называется соотношение

$$a^0 \cdot X^0 \oplus a^p \cdot X^p \oplus \alpha = d^1 \cdot K^1 \oplus \ldots \oplus d^p \cdot K^p, \tag{7}$$

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

Бит α находится как $\alpha = \alpha^1 \oplus \alpha^2 \oplus \ldots \oplus \alpha^p$. Вероятность выполнения линейного приближения, полученного из схемы (6), вычисляется с помощью известной леммы Мацуи [3].

Лемма 2 (Мацуи). Пусть ξ_i $(1 \leqslant i \leqslant n)$ — независимые случайные величины, каждая из которых принимает значение 0 с вероятностью $1/2 + \varepsilon_i$ и значение 1 — с вероятностью $1/2 - \varepsilon_i$ $(-1/2 \leqslant \varepsilon_i \leqslant 1/2)$. Тогда случайная величина $\xi_1 \oplus \xi_2 \oplus \ldots \oplus \xi_n$ принимает значение 0 с вероятностью $1/2 + \varepsilon$ и значение 1 — с вероятностью $1/2 - \varepsilon$, где $\varepsilon = 2^{n-1} \prod\limits_{i=1}^{n} \varepsilon_i$.

Таким образом получаем преобладание, с которым выполняется соотношение (7), равное $\varepsilon = 2^{p-1} \prod\limits_{r=1}^{p} \varepsilon_r$, где ε_r взяты из схемы согласования.

Если начальная и конечная маски совпадают, то схема согласования раундовых приближений (6) называется *замкнутой*. Линейное приближение (7), порождённое замкнутой схемой согласования, называется *замкнутым* и имеет вид

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

Замкнутые приближения хороши тем, что их можно применять последовательно, получая тем самым линейное приближение на произвольное количество раундов.

Пусть $(a^i)_1, (b^i)_1, (\alpha^i)_1$ и $(a^i)_2, (b^i)_2, (\alpha^i)_2$ — параметры двух схем согласования. Введём отношение эквивалентности среди замкнутых схем согласования раундов.

Определение 10. Две замкнутые схемы согласования p раундов являются *эквивалентными*, если для каждого $i = 0, 1, \ldots, p$ выполнено $(a^i)_1 = (a^j)_2$, $(d^i)_1 = (d^j)_2$, $(\alpha^i)_1 = (\alpha^j)_2$, где $j = (i + t) \pmod p$ для некоторого $t \in \{0, \ldots, p-1\}$.

Замкнутые линейные приближения, порождённые эквивалентными схемами согласования раундов, называются *эквивалентными*. Нетрудно заметить, что преобладания эквивалентных замкнутых линейных приближений совпадают. Маски α и β называются *эквивалентными*, если существуют эквивалентные замкнутые схемы согласования, у которых эти маски являются начальными. Будем писать $\alpha \sim \beta$.

Утверждение 2. Маски α и β являются эквивалентными, если и только если существует замкнутая схема согласования p раундов с начальной маской $\alpha = a^0$ и для некоторого t, $0 \leqslant t \leqslant p-1$, выполнено $\beta = a^t$.

Доказательство. Необходимость. Пусть $\alpha \sim \beta$. Рассмотрим эквивалентные замкнутые схемы согласования с начальными масками $\alpha = (a^0)_1$ и $\beta = (a^0)_2$. По определению эквивалентных замкнутых схем согласования, для некоторого $t \in \{0, \ldots, p-1\}$ выполнено $\beta = (a^0)_2 = (a^t)_1 = a^t$. Необходимость доказана.

Достаточность. Замкнутая схема согласования с начальной маской $\alpha = a^0 = (a^0)_1$ эквивалентна замкнутой схеме согласования с начальной маской $\beta = a^t = (a^t)_1 = (a^0)_2$, в которой $(\alpha^j)_1 = (\alpha^i)_2$, где $j = (i + t) \pmod p$. ■

Утверждение 3 (о спуске). Если в одном из уравнений системы (6) маска входа $a^r = (a^r_1, a^r_2, \ldots, a^r_m)$ раунда $r+1$ такая, что $a^r_i = 0$, где $i = 1, \ldots, q$, $q < m$, то можно произвести спуск на q раундов, т. е. получить линейное соотношение $a^r \cdot X^r \oplus a^{r+q} \cdot X^{r+q} = 0$, выполняющееся с вероятностью 1. Маска a^{r+q} при этом будет иметь следующий вид: $a^{r+q} = (a^r_{q+1}, a^r_{q+2}, \ldots, a^r_m, a^r_1, a^r_2, \ldots, a^r_q) = (a^r_{q+1}, a^r_{q+2}, \ldots, a^r_m, 0, 0, \ldots, 0)$.

Доказательство. Так как $a^r_1 = 0$, то по следствию 2 маска $a^{r+1} = (a^{r+1}_1, a^{r+1}_2, \ldots, a^{r+1}_m)$ находится из системы (5), а именно $a^{r+1}_1 = a^r_2$, $a^{r+1}_2 = a^r_3$, $\ldots$, $a^{r+1}_{m-1} = a^r_m$, $a^{r+1}_m = a^r_1 = 0$, и соотношение $a^r \cdot X^r \oplus a^{r+1} \cdot X^{r+1} = 0$ выполняется с вероятностью 1. Теперь, если a^r_2 нулевая маска, то a^{r+1}_1 тоже нулевая и a^{r+2} находится аналогичным способом. Таким образом находим маски $a^{r+1}, a^{r+2}, \ldots, a^{r+q}$. В итоге получаем $a^{r+q} = (a^r_{q+1}, a^r_{q+2}, \ldots, a^r_m, a^r_1, a^r_2, \ldots, a^r_q) = (a^r_{q+1}, a^r_{q+2}, \ldots, a^r_m, 0, 0, \ldots, 0)$ и систему, описывающую q раундов:

$$\begin{cases} a^r \cdot X^r \oplus a^{r+1} \cdot X^{r+1} = 0, \\ a^{r+1} \cdot X^{r+1} \oplus a^{r+2} \cdot X^{r+2} = 0, \\ \ldots \\ a^{r+q-1} \cdot X^{r+q-1} \oplus a^{r+q} \cdot X^{r+q} = 0, \end{cases}$$

т. е. подсистему системы (6), в которой $d^r = d^{r+1} = \ldots = d^{r+q} = 0$ и $\alpha^1 = \alpha^2 = \ldots = \alpha^{r+p} = 0$. Так как все уравнения в системе выполняются с вероятностью 1, то, если сложим их, по лемме 2 получим, что приближение $a^r \cdot X^r \oplus a^{r+p} \cdot X^{r+p} = 0$ выполняется с вероятностью 1. ■

1.6. Раундовое преобладание

Для применения линейного криптоанализа требуется найти линейное приближение на конкретное число раундов. Очевидно, что лучшим считается то, преобладание которого максимально. Как правило, число раундов довольно большое, а линейное

приближение получается последовательным применением некоторого замкнутого линейного приближения и, если требуется, анализом ещё нескольких раундов. Таким образом, для нахождения лучшего линейного приближения на шифр нужно найти лучшее замкнутое линейное приближение, а для этого нужно научиться их сравнивать. Критерием сравнения линейных приближений является раундовое преобладание.

Определение 11. *Раундовым преобладанием* линейного приближения p раундов назовём величину

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

где ε является преобладанием линейного приближения p раундов.

С помощью раундового преобладания можно сравнивать замкнутые линейные приближения на различное количество раундов и определять оптимальное.

Будем говорить, что замкнутое раундовое приближение L_1 *лучше* замкнутого раундового приближения L_2, если раундовое преобладание приближения L_1 больше раундового преобладания приближения L_2. *Оптимальным линейным приближением раундов* называется замкнутое линейное приближение, раундовое преобладание которого максимально.

Преобладание линейного приближения, построенного путём последовательного применения замкнутого линейного приближения, вычисляется по лемме 2. Поэтому из оптимального линейного приближения получается линейное приближение, требуемое для линейного криптоанализа шифра, с максимальным преобладанием. Имея такое линейное приближение, можно говорить о стойкости шифра к линейному криптоанализу, о минимальном количестве пар статистики, требуемом для определения ключа.

2. Математическая постановка задачи о линейном приближении

2.1. Дерево шаблонов

Для нахождения оптимального линейного приближения строится бинарное дерево, корень которого фиксирован и каждая вершина имеет двух сыновей, левого и правого. Назовём такое дерево *деревом шаблонов*. Вершины дерева шаблонов будем обозначать v, каждой вершине в таком дереве соответствует некоторый набор означиваний.

Пусть $a_1, a_2, \ldots, a_m$ здесь и далее принимают произвольные значения из $\mathbb{Z}_2^n$. Определим функции

$$left : \{(a_1, a_2, a_3, \ldots, a_m) : a_1 = 0\} \to (\mathbb{Z}_2^n)^m,$$
$$right : \{(a_1, a_2, a_3, \ldots, a_m) : a_1 \neq 0\} \to \mathcal{P}((\mathbb{Z}_2^n)^m)$$

следующим образом:

$$left((0, a_2, a_3, \ldots, a_m)) = (a_2, a_3, \ldots, a_m, 0),$$
$$right((a_0, \ldots, a_m)) =$$
$$= \{(a_2 \oplus b_2, \ldots, a_m \oplus b_m, a_1) : R_F(b_1, b_2, \ldots, b_m, a_1) \neq 1/2; b_1, b_2, \ldots, b_m \in \mathbb{Z}_2^n\}.$$

Пусть V — это множество вершин, v — вершина. *Означенной вершиной* $\overline{v}$ назовём вектор из $(\mathbb{Z}_2^n)^m$. *Функция означивания* f — это многозначная функция, действующая из V в $(\mathbb{Z}_2^n)^m$, т. е. $\overline{v} = (a_1, a_2, a_3, \ldots, a_m) \in f(v)$, где $a_1, \ldots, a_m \in \mathbb{Z}_2^n$.

Определим функцию означивания следующим образом. Если v — корень, то $f(v) = (\mathbb{Z}_2^n)^m$. Пусть v_l и v_r — соответственно левый и правый сыновья вершины v_p,

тогда

$$f(v_l) = \{left(\overline{v}) : \overline{v} \in \mathrm{dom}(left) \cap f(v_p)\},$$
$$f(v_r) = \bigcup_{\overline{v} \in \mathrm{dom}(right) \cap f(v)} right(\overline{v}).$$

Шаблон пути l — это упорядоченный набор вершин $(v_0, v_1, v_2, \ldots, v_r)$, где каждая пара (v_i, v_{i+1}) является ребром в дереве шаблонов. Если v_0 — корень дерева, то шаблон пути от корня до вершины v_r обозначим $l(v_r)$, заметим, что $l(v_r)$ единственный. Если v_0 не является корнем, то шаблон пути от v_0 до v_r будем обозначать $l(v_0, v_r)$.

Означенным ребром назовём упорядоченную пару означенных вершин $(\overline{v}, \overline{w})$, для которых выполнено либо $\overline{w} = left(\overline{v})$, либо $\overline{w} \in right(\overline{v})$. *Путь* L — это упорядоченный набор означенных вершин $(\overline{v_0}, \overline{v_1}, \overline{v_2}, \ldots, \overline{v_r})$, где каждая пара $(\overline{v_i}, \overline{v_{i+1}})$ является означенным ребром. Путь L от $\overline{v_0}$ до $\overline{v_r}$ будем обозначать $L(\overline{v_0}, \overline{v_r})$.

Длиной пути L назовём количество рёбер, входящих в путь L. Длину пути L будем обозначать $|L|$. Аналогично, длину шаблона пути l будем обозначать $|l|$. Заметим, что означенное ребро является путём длины один.

2.2. Поиск итерируемого пути в дереве

Каждому означенному ребру $(\overline{v_i}, \overline{v_j})$ ставится в соответствие значение функции ε. Функция действует из множества путей на отрезок $[0, 1/2]$. Путь $L(\overline{v_0}, \overline{v_r}) = (\overline{v_0}, \overline{v_1}, \overline{v_2}, \ldots, \overline{v_r})$ можно задать также и рёбрами $((\overline{v_0}, \overline{v_1}), (\overline{v_1}, \overline{v_2}), \ldots, (\overline{v_{r-1}}, \overline{v_r}))$. Пусть действие функции ε определено на означенных рёбрах. Определим действие функции ε на пути следующим образом:

$$\varepsilon(L(\overline{v_0}, \overline{v_r})) = \frac{1}{2^r} \prod_{i=1}^{r} \varepsilon(\overline{v_{i-1}}, \overline{v_i}) = \frac{1}{2^r} \prod_{i=1}^{r} \varepsilon_i, \tag{8}$$

где $\varepsilon(\overline{v_{i-1}}, \overline{v_i}) = \varepsilon_i$.

Определим функцию $\tilde{\varepsilon}$. Функция действует из множества путей на отрезок $[0, 1/2]$. Пусть L — некоторый путь, $\varepsilon = \varepsilon(L)$, $r = |L|$, тогда

$$\tilde{\varepsilon}(L) = (\varepsilon \cdot 2^{1-r})^{1/r}. \tag{9}$$

Будем говорить, что L_1 *лучше, чем* L_2, и писать $L_1 > L_2$, если $\tilde{\varepsilon}(L_1) > \tilde{\varepsilon}(L_2)$; будем писать $L_1 \geqslant L_2$, если $\tilde{\varepsilon}(L_1) \geqslant \tilde{\varepsilon}(L_2)$.

Итерируемым путём назовём путь $L(\overline{v_0}, \overline{v_r})$, такой, что $\overline{v_0} = \overline{v_r}$. Введём отношение эквивалентности на итерируемых путях. Два итерируемых пути $L(\overline{v_0}, \overline{v_r})$ и $L(\overline{w_0}, \overline{w_r})$ назовём *эквивалентными с параметром* t и будем писать $L(\overline{v_0}, \overline{v_r}) \sim L(\overline{w_0}, \overline{w_r})$, если для каждого i верно $\overline{v_i} = \overline{w_j}$, где $j = (i + t) \mod r$ для некоторого t. Означенная вершина $\overline{w_r}$ определяется однозначно, так как $\overline{w_r} = \overline{w_0}$.

Проверим, что введённое отношение действительно является отношением эквивалентности. Рефлексивность выполняется при $t = 0$. Симметричность: если $L_1 \sim L_2$ с параметром t_1, то $L_2 \sim L_1$ с параметром $t_2 = -t_1$. Транзитивность: если $L_1 \sim L_2$ с параметром t_1, $L_2 \sim L_3$ с параметром t_2, то $L_1 \sim L_2$ с параметром $t_3 = t_1 + t_2$.

Оптимальным путём назовём итерируемый путь L_1, такой, что для любого итерируемого пути L_2 выполнено $L_1 \geqslant L_2$.

Утверждение 4. Пусть L_1 — некоторый путь. Тогда если существует итерируемый путь L_2, такой, что $L_2 > L_1$ и $|L_2| > |L_1|$, то L_2 либо его эквивалент содержит подпуть L_3, такой, что $|L_3| = |L_1|$ и $L_3 > L_1$.

Доказательство. Пусть $\tilde{\varepsilon}_1 = \tilde{\varepsilon}_1(L_1)$, $\tilde{\varepsilon}_2 = \tilde{\varepsilon}_2(L_2)$. Поскольку $L_2 > L_1$, то $\tilde{\varepsilon}_2 > \tilde{\varepsilon}_1$. Пусть $|L_1| = r_1$, $|L_2| = r_2$, тогда по формуле (8) выполняется $(\varepsilon_2 \cdot 2^{1-r_2})^{1/r_2} > (\varepsilon_1 \cdot 2^{1-r_1})^{1/r_1}$; преобразуем далее по формуле (9) и получим

$$\left(\left(2^{r_2-1}\prod_{i=1}^{r_2}\varepsilon_{2_i}\right)2^{1-r_2}\right)^{1/r_2} > \left(\left(2^{r_1-1}\prod_{i=1}^{r_1}\varepsilon_{1_i}\right)2^{1-r_1}\right)^{1/r_1},$$

что то же самое, что и $\left(\prod_{i=1}^{r_2}\varepsilon_{2_i}\right)^{1/r_2} > \left(\prod_{i=1}^{r_1}\varepsilon_{1_i}\right)^{1/r_1}$. Для того чтобы нашёлся требуемый подпуть L_3, такой, что $|L_3| = |L_1| = r_1$ и $L_3 > L_1$, нужно, чтобы нашёлся такой номер j, $1 \leqslant j \leqslant r_2$, что $\left(\prod_{i=j+1}^{j+r_1}\varepsilon_{2_i}\right)^{1/r_1} > \left(\prod_{i=1}^{r_1}\varepsilon_{1_i}\right)^{1/r_1}$, где суммы $j+1$ и $j+r_1$ берутся по модулю r_1.

Заметим, что $\tilde{\varepsilon}_2 = \left(\prod_{i=1}^{r_2}\varepsilon_{2_i}\right)^{1/r_2} = (\varepsilon_{2_1}\varepsilon_{2_2}\cdot\ldots\cdot\varepsilon_{2_{r_2}})^{1/r_2} = ((\varepsilon_{2_1}\varepsilon_{2_2}\cdot\ldots\cdot\varepsilon_{1_{r_1}})(\varepsilon_{2_2}\varepsilon_{2_3}\times$ $\times\ldots\cdot\varepsilon_{1_{r_1+1}})\cdot\ldots\cdot(\varepsilon_{1_{r_2}}\varepsilon_{2_1}\cdot\ldots\cdot\varepsilon_{1_{r_1-1}}))^{1/(r_1r_2)} = ((\varepsilon_{2_1}\varepsilon_{2_2}\cdot\ldots\cdot\varepsilon_{2_{r_1}})^{1/r_1}(\varepsilon_{2_2}\varepsilon_{2_3}\cdot\ldots\cdot\varepsilon_{2_{r_1+1}})^{1/r_1}\cdot\ldots\times$ $\times(\varepsilon_{2_{r_2}}\varepsilon_{2_1}\cdot\ldots\cdot\varepsilon_{2_{r_1-1}})^{1/r_1})^{1/r_2}$, т. е. $\tilde{\varepsilon}_2$ представимо в виде среднего геометрического слагаемых вида $(\varepsilon_{2_{j+1}}\varepsilon_{2_{j+2}}\cdot\ldots\cdot\varepsilon_{2_{j+r_1}})^{1/r_1}$, где суммы $j+1, j+2, \ldots, j+r_1$ рассматриваются по модулю r_2, $j = 0, \ldots, r_2 - 1$. Очевидно, что среднее геометрическое неотрицательных чисел не может превосходить все эти числа, значит, найдётся хотя бы один такой номер j, что $(\varepsilon_{2_{j+1}}\varepsilon_{2_{j+2}}\cdot\ldots\cdot\varepsilon_{2_{j+r_2}})^{1/r_1} \geqslant \tilde{\varepsilon}_2$. Таким образом, так как $0 \leqslant \varepsilon_{2_i} \leqslant 1/2$, $r_1 \geqslant 1$, получаем $\left(\prod_{i=j+1}^{j+r_1}\varepsilon_{2_i}\right)^{1/r_1} = (\varepsilon_{2_{j+1}}\varepsilon_{2_{j+1}}\cdot\ldots\cdot\varepsilon_{2_{j+r_1}})^{1/r_1} \geqslant \tilde{\varepsilon}_2 > \tilde{\varepsilon}_1 = \left(\prod_{i=1}^{r_1}\varepsilon_{1_i}\right)^{1/r_1}$ ■

Теорема 1. Если существует итерируемый путь L_1, такой, что среди вершин на глубине, не большей $|L_1|$, нет таких, что означивание пути от корня до них даёт путь лучше, чем L_1, то путь L_1 является оптимальным.

Доказательство. Допустим, что существует итерируемый путь L_2, такой, что $L_2 > L_1$. Тогда по условию $|L_2| > |L_1|$. По утверждению 4 итерируемый путь L_2 либо его эквивалент содержит подпуть L_3, такой, что $|L_3| = |L_1|$ и $L_3 > L_1$. Найдём путь в дереве от корня, эквивалентный L_1. Поскольку $|L_3| = |L_1|$ и $L_3 > L_1$, то это значит, что на глубине $|L_1|$ нашлась вершина, которая порождает путь, лучше чем L_1, противоречие. ■

Замечание 1. В доказательстве используется отсутствие итерируемых путей L_2, таких, что $L_2 > L_1$, поэтому посылку теоремы можно ослабить и требовать отсутствие *итерируемых* путей, лучших чем L_1, на глубине меньшей $|L_1|$. На глубине $|L_1|$ отсутствие путей, лучших чем L_1, категорично.

Следствие 3. Пусть вершина $\overline{v_1}$ такова, что $L(\overline{v_1})$ итерируем и

1) не существует вершины $\overline{v_2}$, такой, что $L(\overline{v_2})$ итерируем и $|L(\overline{v_2})| < |L(\overline{v_1})|$;
2) для любой вершины $\overline{v_3}$, такой, что $|L(\overline{v_3})| = |L(\overline{v_1})|$, выполнено $L(\overline{v_1}) \geqslant L(\overline{v_3})$.

Тогда путь $L(\overline{v_1})$ является оптимальным.

Другими словами, самая первая вершина (если искать её в дереве по ярусам, увеличивая глубину), дающая итерируемый путь, который является лучшим среди всех путей на этой глубине, даёт оптимальный путь.

Следствие 4. Пусть вершина $\overline{v_1}$ такова, что $L(\overline{v_1})$ итерируем и

1) не существует вершины $\overline{v_2}$, такой, что $L(\overline{v_2})$ итерируем и $|L(\overline{v_2})| < |L(\overline{v_1})|$;
2) $\overline{w_1}, \ldots, \overline{w_m}$ — все вершины, такие, что $|L(\overline{w_i})| = |L(\overline{v_1})|$ и $L(\overline{w_i}) \geqslant L(\overline{v_1})$.

Тогда любой итерируемый путь $L(\overline{w})$, лучший, чем $L(\overline{v_1})$, содержит одну из вершин $\overline{w_1}, \ldots, \overline{w_m}$.

2.3. Алгоритм

Сложность поиска оптимального пути в том, что дерево может быть бесконечно. Не ясно, когда завершить поиск, как понять, что дальнейший поиск бесперспективен. Опишем алгоритм поиска оптимального пути, который имеет конкретное условие остановки и рассматривает меньше означиваний, чем исчерпывающий поиск; он основан на следующем утверждении.

Утверждение 5. Пусть $L(\overline{v_1})$ — некоторый путь. Тогда для любой вершины $\overline{v_2}$, такой, что $L(\overline{v_1}) \geqslant L(\overline{v_2})$ и $|L(\overline{v_1})| \leqslant |L(\overline{v_2})|$, верно, что если она принадлежит некоторому итерируемому пути $L(\overline{w_2})$, лучшему, чем $L(\overline{v_1})$, то у $L(\overline{w_2})$ найдётся эквивалент с подпутём $L(\overline{v'})$, таким, что $|L(\overline{v_2})| = |L(\overline{v'})|$ и $L(\overline{v'}) > L(\overline{v_1})$.

Доказательство. Допустим, что у вершины $\overline{v_2}$ нашёлся потомок $\overline{w_2}$, такой, что $L(\overline{w_2})$ итерируем и $L(\overline{w_2}) > L(\overline{v_1})$. Тогда, раз $L(\overline{w_2}) > L(\overline{v_1}) \geqslant L(\overline{v_2})$, то $L(\overline{w_2}) > L(\overline{v_2})$ и по утверждению 4 эквивалент пути $L(\overline{w_2})$ — некоторый путь $L(\overline{w_3})$ — содержит подпуть $L(\overline{v_3})$, такой, что $|L(\overline{v_3})| = |L(\overline{v_2})|$ и $L(\overline{v_3}) > L(\overline{v_2})$. Если $L(\overline{v_3}) > L(\overline{v_1})$, то $L(\overline{v_3})$ — искомый подпуть. Если же $L(\overline{v_3}) \leqslant L(\overline{v_1})$, то $L(\overline{w_3}) = L(\overline{w_2}) > L(\overline{v_1}) \geqslant L(\overline{v_3})$, т. е. $L(\overline{w_3}) > L(\overline{v_3})$ и по утверждению 4 эквивалент пути $L(\overline{w_3})$ содержит подпуть, лучший, чем $L(\overline{v_3})$ и той же длины. Если он лучше $L(\overline{v_1})$, то он искомый, иначе применяем утверждение 4 дальше, пока не найдём $L(\overline{v'})$, который будет лучше $L(\overline{v_1})$.

Пусть $L(\overline{v_i})$ — произвольный подпуть длины $|L(\overline{v_2})|$ пути, эквивалентного $L(\overline{w_2})$. Покажем, что $L(\overline{v'})$ обязательно найдётся. Действительно, если он не найдётся, т. е. для всех $L(\overline{v_i})$ выполнено $L(\overline{v_i}) \leqslant L(\overline{v_1})$, то пусть среди них $L(\overline{v_m})$ — самый лучший, т. е. такой, что $L(\overline{v_m}) \geqslant L(\overline{v_i})$ для всех $L(\overline{v_i})$. Путь $L(\overline{v_m})$ является подпутём $L(\overline{w_m})$, который эквивалентен $L(w_2)$, значит, $L(\overline{w_m}) = L(\overline{w_2}) > L(\overline{v_1}) \geqslant L(\overline{v_m})$, т. е. $L(\overline{w_m}) > L(\overline{v_m})$ и по утверждению 4 эквивалент пути $L(\overline{w_m})$ содержит подпуть длины $|L(\overline{v_2})|$, лучший, чем $L(\overline{v_m})$, противоречие. ■

Замечание 2 (о корректности алгоритма). Если алгоритм останавливается, то он даёт оптимальный путь L_c. При работе алгоритма учитываются все кандидаты на оптимальный путь, не отбрасывается ничего нужного. Из утверждения 5 следует, что каждое новое заполнение множества кандидатов C содержит все пути, которые могут дать пути, лучшие, чем уже найденные. Если таких нет, то найденный путь является лучшим.

Алгоритм является алгоритмом поиска оптимального линейного приближения обобщённой сети Фейстеля, т. е. найденный оптимальный путь является оптимальным линейным приближением.

Каждое новое заполнение множества C даёт линейное приближение, лучшее, чем предыдущее, и соответствует рассмотрению ещё одного раунда; обобщённая сеть Фейстеля состоит из конечного числа раундов (пусть r). Отсюда следует, что если алгоритм не остановился за r перезаполнений, то лучшим приближением для r раундов будет лучшее приближение из последнего заполнения множества кандидатов C.

Алгоритм 1. Поиск оптимального пути

Вход: функции $left$, $right$; корень v_0
Выход: оптимальный путь L_c

$C := \{L(\overline{v}, \overline{v}), \overline{v} \in f(v_0)\}$, $NC := \varnothing$.
Пока C не пусто
  Для $L(\overline{v_0}, \overline{v}) \in C$
    Для $\overline{w} \in right(\overline{v}) \cup \{left(\overline{v})\}$
      Если $\overline{w} = \overline{v}_0$, **то**
        Если L_c не определён, **то**
          $L_c := L(\overline{v_0}, \overline{w})$;
        иначе
          Если $L(\overline{v_0}, \overline{w}) > L_c$, **то**
            $L_c := L(\overline{v_0}, \overline{w})$.
    Для $\overline{w} \in right(\overline{v}) \cup \{left(\overline{v})\}$
      Если L_c определён, **то**
        Если $L(\overline{v_0}, \overline{w}) > L_c$, **то**
          добавляем $L(\overline{v_0}, \overline{w})$ в NC;
      иначе
        добавляем $L(\overline{v_0}, \overline{w})$ в NC.
  $C := NC$, $NC := \varnothing$.

Заключение

В работе получены следующие результаты:

— предложен общий подход к нахождению линейных приближений обобщённой сети Фейстеля;
— дана математическая постановка задачи о линейном приближении;
— разработан алгоритм поиска оптимального линейного приближения обобщённой сети Фейстеля.

Результаты работы могут быть применены при проведении линейного криптоанализа блочных шифров, построенных на основе сети Фейстеля, а также при получении оценок стойкости таких шифров к линейному криптоанализу.

ЛИТЕРАТУРА

1. *Diffie W.* SMS4 encryption algorithm for wireless networks // Cryptology ePrint Archive. Report 2008/329, 2008. `http://eprint.iacr.org/2008/329`
2. *Matsui M. and Yamagishi A.* A new method for known plaintext attack of FEAL cipher // EUROCRYPT'92. LNCS. 1993. V. 658. P. 81–91.
3. *Matsui M.* Linear cryptanalysis method for DES cipher // EUROCRYPT'93. LNCS. 1993. V. 765. P. 386–397.
4. *Matsui M.* The first experimental cryptanalysis of the Data Encryption Standard // CRYPTO'94. LNCS. 1994. V. 839. P. 1–11.
5. *Nyberg K.* Linear approximation of block ciphers // EUROCRYPT'94. LNCS. 1995. V. 950. P. 439–444.
6. *Kaliski B. and Robshaw M.* Linear cryptoanalysis using multiple approximations // CRYPTO'94. LNCS. 1994. V. 839. P. 26–39.

7. *Sakurai K. and Furuya S.* Improving linear cryptanalysis of LOKI91 by probabilistic counting method // FSE'97. LNCS. 1997. V 1267. P. 114–133.
8. *Collard B., Standaert F.-X., and Quisquater J.-J.* Improving the time complexity of Matsui's linear cryptanalysis // ICISC'2007. LNCS. 2007. V. 4817. P. 77–88.
9. *Токарева Н. Н.* О квадратичных аппроксимациях в блочных шифрах // Проблемы передачи информации. 2008. Т. 44. № 3. С.105–127.
10. *Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2005.
11. *Wheeler D. J. and Needham R. M.* TEA, a tiny encryption algoritm // LNCS. 1994. V. 1008. P. 363–366.