Math-Net.Ru

Общероссийский математический портал

А. А. Дмух, Об использовании подобия подстановок при определении ключа в сетях Фейстеля, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 3, 33–44

DOI: <https://doi.org/10.4213/mvk261>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.209.52.79

26 апреля 2023 г., 18:03:14

**Об использовании подобия подстановок
при определении ключа в сетях Фейстеля**

А. А. Дмух

Технический комитет по стандартизации (ТК 26), Москва

Получено 11.V.2017

Аннотация. Для сетей Фейстеля с ключевой разверткой, представляющей собой последовательность подвекторов ключевого вектора, рассматривается метод определения ключа с использованием подобия подстановок. Изучаются условия, при которых этот метод эффективнее тотального опробования. Приведены примеры применения метода к различным сетям Фейстеля указанного типа. Обсуждаются условия на ключевую развертку в сетях Фейстеля, обеспечивающие практическую невозможность применения как методов Исобе и Динура–Данкельмана–Шамира, так и метода с использованием подобия подстановок.

Ключевые слова: сеть Фейстеля, криптографический анализ, ключевая развертка, подобие подстановок

**On the use of conjugacy of substitutions in determining the key
in Feistel networks**

A. A. Dmukh

Technical committee for standardization (TC 26), Moscow

Abstract. For Feistel networks with the key schedule being a sequence of subvectors of the key vector we consider a method for determining the key based on the conjugacy of substitutions. Conditions under which this method is more effective than the brute force one are investigated. Examples of application of the method to some Feistel networks of the indicated type are given. We discuss conditions on the key schedule in Feistel networks ensuring the practical impossibility of using both Isobe and Dinur–Dunkelman–Shamir methods and a method using the conjugacy of substitutions.

Key words: Feistel network, cryptanalysis, key schedule, conjugacy of substitutions

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 3, pp. 33–44 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

1. Введение

Одна из особенностей сетей Фейстеля состоит в том, что преобразование расшифрования представляет собой преобразование зашифрования, но с итерационными (раундовыми) ключами, взятыми в обратном порядке. Это позволяет при выполнении ряда дополнительных условий эффективно применять при поиске раундовых ключей методы, основанные на так называемом свойстве отражения (reflection property) и существовании неподвижных точек подстановок, являющихся композицией нескольких итераций (раундов) зашифрования. Так, например, в методах Исобе [1] и Динура–Данкельмана–Шамира [2] используется тот факт, что преобразование зашифрования алгоритмом блочного шифрования ГОСТ 28147-89 [3] («Магма» [4]) при выполнении некоторых дополнительных условий может быть представлено в виде произведения преобразований

$$E = FFFF^{-1} = F^2,$$

где F обозначает 8 итераций алгоритма.

Вместе с тем преобразование зашифрования алгоритмом ГОСТ 28147-89 («Магма») всегда (т. е. без выполнения дополнительных условий) может быть представлено в виде

$$E = FFFTF^{-1} = FGF^{-1},$$

где T — перестановка двух 32-битных подвекторов 64-битного вектора. В силу подобия подстановок E и G наличие неподвижной точки у преобразования E означает одновременное наличие неподвижной точки у преобразования G . Если неподвижная точка x преобразования E известна, то задачу определения ключа можно свести к задаче определения ключа в системе

$$\begin{cases} F(x) = y \\ G(y) = y \end{cases} \quad (1)$$

при некотором неизвестном y .

Ниже будет рассмотрена возможность применения метода определения ключа с использованием подобия подстановок к сетям Фейстеля с ключевой разверткой, представляющей собой перестановку подвекторов ключевого вектора. Также будут получены условия на ключевую развертку в сетях Фейстеля рассматриваемого типа, гарантирующие невозможность применения как методов Исобе и Динура–Данкельмана–Шамира, так и метода с использованием подобия подстановок.

2. Условия, достаточные для эффективного применения метода определения ключа с использованием подобия подстановок

Далее рассматриваются сети Фейстеля, имеющие следующий общий вид. Длина блока равна $n = 2 \cdot l$ бит, длина ключа K равна $k = t \cdot l$ бит,

$$K \in V_k \equiv (GF(2)^k), \quad K = (K_1, \dots, K_t), \quad K_i \in V_l, \quad i \in \overline{1, t}.$$

Количество итераций (раундов) равно W . На итерации с номером $j \in \overline{1, W}$ раундовый ключ $M_j = K_{i_j}$ для некоторого $i_j \in \overline{1, t}$.

На итерации с номером $j \in \overline{1, W}$ входной блок $X = (X_2, X_1) \in V_n$, $X_1, X_2 \in V_l$, переходит в выходной блок $Y = (Y_2, Y_1) \in V_n$, $Y_1, Y_2 \in V_l$, по следующему правилу:

$$H_j(M_j, (X_2, X_1)) = (Y_2, Y_1) = (R(M_j, X_2) + X_1, X_2),$$

где «+» может обозначать либо побитовое сложение по модулю 2 векторов из V_l , либо сложение по модулю 2^l , $R: V_l \times V_l \rightarrow V_l$ — раундовая (итерационная) функция. После итерации с номером W применяется преобразование $T(X_2, X_1) = (X_1, X_2)$ — финальная перестановка полублоков.

Пусть ключевая развертка (порядок выбора раундовых ключей) такова, что преобразование зашифрования E представимо в виде $E = FGF^{-1}$. Отметим, что для выполнения этого условия достаточно, чтобы $M_1 = M_W$.

Замечание 1. Возможность представления преобразования E (при выполнении соответствующих равенств для раундовых ключей) в виде $E = FGF^{-1}$ следует из очевидных свойств $H_i^{-1} = TH_iT$, $T^2 = I$, где I — тождественное преобразование.

Отметим, что при заданной ключевой развертке одна и та же сеть Фейстеля может быть представлена более чем одним способом в виде $E = FGF^{-1}$. Так, например, алгоритм ГОСТ 28147-89 («Магма») может быть представлен в этом виде 8 различными способами.

Везде далее под трудоемкостью будем понимать среднее число Q операций (зашифрования), используемых в предложенном методе (при определении неизвестного ключа) при заданной вероятности успеха $p_{\text{усп}}$. Будем говорить, что метод определения ключа эффективно применим к сети Фейстеля рассматриваемого вида, если отношение его трудоемкости к $p_{\text{усп}}$ меньше трудоемкости метода тотального опробования ключа (т. е. $Q/p_{\text{усп}} < 2^k$).

Замечание 2. Везде в дальнейшем никаких ограничений на объем памяти накладываться не будет. Также будем предполагать, что в распоряжении криптоаналитика имеется весь доступный материал (соответствия между открытыми и шифрованными текстами) в количестве 2^n , полученный на неизвестном ключе (предположения полностью аналогичны предположениям работы [2]). Трудоемкость метода будем считать в операциях зашифрования E . Для простоты изложения «дроблением» алгоритма блочного шифрования при представлении $E = FGF^{-1}$ будем пренебрегать, так как соотношение между трудоемкостями вычисления F и G существенно зависит от конкретного вида ключевой развертки и точно учесть все нюансы в общем виде сложно, однако всегда трудоемкость вычисления F или G составляет не менее $1/W$ от трудоемкости вычисления E . Таким образом, далее трудоемкости вычисления E , F и G будем полагать равными. При необходимости (при применении метода к конкретным алгоритмам) будем проводить точный подсчет.

Через Q_* будем обозначать верхнюю оценку трудоемкости решения системы $\{F(x) = y, G(y) = y\}$ (определения неизвестного ключа $K \in V_k$) по всем возможным $x, y \in V_n$.

Изложим в общем виде метод с использованием подобия подстановок. Пусть преобразование зашифрования представимо в виде $E = FGF^{-1}$.

1 этап (предварительный)

В множестве N пар открытых и соответствующих шифрованных текстов ищем $x \in V_n: E(x) = x$. Если такой x найден, то переходим к этапу 2. В противном случае ключ найти не удалось.

2 этап (основной)

Перебираем все $y \in V_n$ и для каждого варианта y решаем систему $\{F(x) = y, G(y) = y\}$, при этом при необходимости (если $k > 4 \cdot l$) доопробуем найденный ключ на материале не более чем

$$\left\lceil \frac{t-4}{2} \right\rceil$$

пар открытого и шифрованного текстов.

Для сетей Фейстеля рассматриваемого вида получим достаточные условия эффективной применимости метода определения ключа с использованием подобия подстановок. Пусть $N = 2^n$.

Теорема. Если $Q_* < 2^{l \cdot (t-2)}$, то метод определения ключа с использованием подобия подстановок эффективно применим к сетям Фейстеля рассматриваемого вида.

Доказательство. Для доказательства теоремы рассчитаем трудоемкость метода определения ключа с использованием подобия подстановок для сетей Фейстеля.

Оценим вероятность появления события $E(x)=x$ в множестве N различных пар открытых и шифрованных текстов (т.е. вероятность успеха метода $p_{\text{усп}}$). При случайном выборе ключа K (неизвестного нам) преобразование E представляет собой случайную подстановку. Будем предполагать, что ее свойства аналогичны свойствам случайной равновероятной подстановки на V_n .

Пусть χ_{Nl} — число циклов длины l в случайной равновероятной подстановке степени N . Тогда согласно [8, с. 186]

$$\mathbf{P}\{\chi_{Nl}=s\} = \frac{1}{l^s s!} \sum_{j=0}^{[N/l]-s} \frac{(-1)^j}{l^j j!} \quad \text{при } s=0, 1, \dots, [N/l].$$

Нам интересен случай $l=1$ и $s=0$ (циклов длины 1 нет). В таком случае

$$\mathbf{P}\{\chi_{N1}=0\} = \sum_{j=0}^N \frac{(-1)^j}{j!}.$$

Учитывая, что согласно [8]

$$\lim_{N \rightarrow \infty} \mathbf{P}\{\chi_{N1}=s\} = \frac{e^{-1/l}}{l^s s!},$$

получаем, что $p_{\text{усп}} \approx 1 - e^{-1}$.

Таким образом, в множестве N пар открытого и шифрованного текстов с вероятностью $p_{\text{усп}} = 1 - e^{-1}$ будет найдена неподвижная точка. Следовательно, с вероятностью успеха $p_{\text{усп}} = 1 - e^{-1}$ первый (предварительный) этап метода имеет трудоемкость, не превосходящую N .

Далее, найдя на предварительном этапе неподвижную точку $X: E(X)=X$, получаем систему $\{F(X)=y, G(y)=y\}$ для некоторого неизвестного $y \in V_n$. Для решения данной системы в общем случае необходимо перебрать все возможные значения $y \in V_n$. Следовательно, трудоемкость поиска решения (возможно, не единственного) системы $\{F(X)=y, G(y)=y\}$ можно оценить величиной $2^n \cdot Q_*$.

Если $t > 4$, то при этом необходимо доопробование найденного ключа на материале не более чем $\lceil \frac{t-4}{2} \rceil$ пар открытого и шифрованного текстов.

Так как $n = 2 \cdot l$, то общая трудоемкость Q метода будет равна

$$N + 2^{2 \cdot l} \cdot Q_* + I\{t > 4\} \cdot 2^{l \cdot (t-4)},$$

где $I\{t > 4\}$ — индикатор события « $t > 4$ ».

Первое слагаемое отвечает за трудоемкость первого этапа. Учитывая, что $N \ll Q_*$, трудоемкостью первого этапа будем пренебрегать.

Третье слагаемое в выражении для трудоемкости соответствует доопробованию не отброшенных при решении системы (1) ключей. Отметим, что после решения системы (1) в среднем должно остаться $2^{l \cdot (t-4)}$ не отброшенных ключей (в случае если $t > 4$). При этом для минимизации трудоемкости Q на втором этапе для каждого полученного решения системы (1) сразу же будем проводить доопробование для не более чем $\lceil \frac{t-4}{2} \rceil$ пар открытого и шифрованного текстов. Это всегда возможно, поскольку, как указывалось выше, в произведении преобразований FG используется весь ключ $K \in V_k$. Значение Q практически не увеличится, так как хотя бы одно доопробование на дополнительном материале будет проводиться в среднем для не более чем $2^{-t \cdot (l-4)}$ доли ключей.

Тогда выражение для трудоемкости метода примет вид

$$Q = 2^{2 \cdot l} \cdot (Q_* + 1) \approx 2^{2 \cdot l} \cdot Q_*.$$

Следовательно, при $Q_* < 2^{l \cdot (t-2)}$ метод определения ключа с использованием подобия подстановок будет эффективно применим к сетям Фейстеля рассматриваемого вида. Теорема доказана. $\square$

Рассмотрим вопрос о вероятности успеха метода в случае, когда для $0 < \alpha \leq 1$ криптоаналитику доступны $N = \alpha \cdot 2^n$ пар открытого и шифрованного текста.

Вероятность того, что в случайной подстановке будет $s \geq 0$ неподвижных точек, как уже отмечалось, при больших n приблизительно равна $e^{-1}/s!$. Вероятность того, что из $s > 0$ неподвижных точек ни одна не окажется среди N имеющихся пар открытого и шифрованного текстов, при $N > 2^n - s$ равна 0, а при $N > 2^n - s$ равна

$$\begin{aligned} \frac{C_{2^n-s}^N}{C_{2^n}^N} &= \frac{(2^n-s)(2^n-s-1)\dots(2^n-s-N+1)}{2^n(2^n-1)\dots(2^n-N+1)} = \\ &= \frac{2^n-N}{2^n} \frac{2^n-N-1}{2^n-1} \dots \frac{2^n-s-N+1}{2^n-s+1}. \end{aligned}$$

Если $n \rightarrow \infty$, $N \sim \alpha 2^n$, $0 < \alpha < 1$, то $C_{2^n-s}^N/C_{2^n}^N \sim (1-\alpha)^s$. Тогда с учетом [8, с. 186] и формулы полной вероятности получаем, что при $\alpha \in (0, 1)$

$$p_{\text{усп}} = 1 - \sum_{s=0}^{2^n-N} \frac{C_{2^n-s}^N}{C_{2^n}^N} \frac{1}{s!} \sum_{j=0}^{2^n-s} \frac{(-1)^j}{j!} \approx 1 - \sum_{s=0}^{2^n-N} \frac{(1-\alpha)^s}{s!} e^{-1} \approx 1 - e^{-\alpha}.$$

Если $\alpha = 1$, то сумма в выражении для $p_{\text{усп}}$ содержит только одно слагаемое с $s = 0$ и поэтому $p_{\text{усп}} = 1 - e^{-1}$.

Таким образом, при любом фиксированном $\alpha \in (0, 1]$ при больших n справедлива оценка

$$p_{\text{усп}} = 1 - e^{-\alpha}.$$

Трудоемкость метода $Q = 2^{2 \cdot l} \cdot Q_*$.

3. Примеры применения метода с использованием подобия подстановок

Пример 1. Рассмотрим возможность применения метода к следующим представителям сетей Фейстеля: ГОСТ 28147-89 («Магма») и 2-ГОСТ [5] при различных разбиениях $E = FGF^{-1}$. С помощью теоремы можно показать, что при любых разбиениях метод не может быть эффективно применен к указанным алгоритмам блочного шифрования.

В качестве примера возьмем алгоритм ГОСТ 28147-89 («Магма») при разбиении $E = FGF^{-1}$, где F — первые 8 итераций алгоритма, $G = FFT$ — итерации с номерами 9–24 с последующей перестановкой полублоков. При этом $l = 32$, $n = 64$, $k = 256$, $t = 8$.

Известно [1], что трудоемкость решения уравнения $G(y) = y$ относительно неизвестного ключа K составляет 2^{192} операций зашифрования. Использование дополнительного уравнения $F(x) = y$ не дает возможности решать систему (1) с трудоемкостью, меньшей 2^{192} . Так как требуется решать $2^n = 2^{64}$ уравнений $G(y) = y$, то метод с использованием подобия подстановок не может быть эффективно применен к алгоритму ГОСТ 28147-89 («Магма»).

Пример 2. Рассмотрим алгоритм ГОСТ 28147-89 («Магма») с уменьшенным до 24 количеством итераций (с 9-й по 32-ю). В этом случае разбиение $E = FGF^{-1}$ имеет следующий вид: F — итерации с 9-й по 16-ю, $G = FT$ — итерации с 17-й по 24-ю с последующей перестановкой полублоков. При этом, как и в примере 1, $l = 32$, $n = 64$, $k = 256$, $t = 8$.

Система (1) может быть решена путем применения метода встречи посередине с трудоемкостью 2^{128} операций зашифрования. Следовательно, метод с использованием подобия подстановок может быть эффективно применен к алгоритму ГОСТ 28147-89 («Магма») с уменьшенным до 24 количеством итераций (с 9-й по 32-ю).

Пример 3. Пусть $n = 64$, $k = 256$, $W = 32$. Рассмотрим схему Фейстеля с ключевой разверткой, приведенной в таблице ниже. В ней на пересечении строки с номером $i \in \overline{0, 3}$ и столбца с номером $j \in \overline{1, 8}$ находится итерационный ключ $M_{8 \cdot i + j}$.

i/j	1	2	3	4	5	6	7	8
0	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
1	K_7	K_8	K_5	K_6	K_8	K_7	K_6	K_5
2	K_1	K_3	K_2	K_4	K_3	K_1	K_4	K_2
3	K_8	K_7	K_6	K_5	K_4	K_3	K_2	K_1

Отметим, что при такой ключевой развертке преобразование зашифрования E не представимо в виде $E = FFFTF^{-1}$ (без дополнительных условий равенства раундовых ключей), т. е. методы Исобе и Динура–Данкельмана–Шамира в данном случае неприменимы.

Рассмотрим разбиение $E = FGF^{-1}$, где F — итерации на первых 8 раундах, G — итерации на раундах с 9 по 24 с последующей перестановкой полублоков. Для $1 \leq i < j \leq 32$ через $H_{i,j}$ будем обозначать зашифрование на итерациях с i -й по j -ю, а через $H_{j,i}^{-1}$ — расшифрование на итерациях с j -й по i -ю.

При наличии неподвижной точки $x \in V_{64}$ преобразования E получаем систему уравнений $\{F(x) = y, G(y) = y\}$ для некоторого неизвестного $y \in V_{64}$. Тогда можно предложить следующий метод определения ключа (вариант метода встречи посередине).

Перебираем все $y \in V_{64}$, для каждого y выполняем следующие действия.

1. Перебираем все ключи $k = (K_1, K_2, K_3, K_4) \in V_{128}$, для каждого варианта k вычисляем

$$\begin{cases} H_{1,4}(k, x) = a \\ H_{24,17}^{-1}(k, y) = b \end{cases}$$

и по адресу (a, b) заносим в память ключ k .

2. Перебираем все ключи $k' = (K_5, K_6, K_7, K_8) \in V_{128}$, для каждого варианта k' вычисляем

$$\begin{cases} H_{9,16}(k', y) = a' \\ H_{8,5}^{-1}(k', y) = b' \end{cases}$$

и обращаемся в память по адресу (a', b') , откуда извлекаем ключ k . Доопробуем ключ $K = (k, k') \in V_{256}$ на не более чем двух парах открытого и зашифрованного текстов.

Рассчитаем параметры метода.

В предположении о случайном равновероятном распределении на выходе преобразований $H_{1,4}$ и $H_{24,17}^{-1}$ по каждому адресу в памяти будет находиться в среднем по одному ключу (K_1, K_2, K_3, K_4) .

Трудоемкость метода будем считать в операциях зашифрования. Трудоемкостью нахождения на предварительном этапе неподвижной точки x для преобразования E , не превосходящей 2^{64} , будем пренебрегать. Тогда

$$Q = 2^{64} \cdot (Q_1 + Q_2)$$

операций зашифрования. Здесь

$$Q_1 = 2^{128} \cdot \left(\frac{4}{32} + \frac{8}{32} \right) = 1,5 \cdot 2^{126}.$$

Отметим, что подавляющее большинство ложных ключей $K = (k, k')$ при доопробовании на втором этапе будет отсеяно уже на первой паре открытого и зашифрованного текстов, доопробовать на второй паре потребуется лишь 2^{64} ключей из 2^{128} , поэтому

$$Q_2 \approx 2^{128} \cdot \left(\frac{4}{32} + \frac{8}{32} + 1 \right) \approx 1,4 \cdot 2^{128}.$$

Следовательно,

$$Q = 2^{64} \cdot (Q_1 + Q_2) \approx 1,8 \cdot 2^{192}$$

операций зашифрования.

Как уже отмечалось, вероятность успеха метода на материале $N = 2^{64} \cdot \alpha$, $0 < \alpha \leq 1$, оценивается величиной $1 - e^{-\alpha}$; при $N = 2^{64}$ вероятность успеха приблизительно равна $e^{-1} \approx 0,63$.

Требуемая память равна $2^{128} \cdot 128 = 2^{135}$ бит. Объем памяти может быть существенно уменьшен с использованием так называемого подхода «угадай и определяй», изложенного в [2]. В данной работе не будем этого делать, так как ее основная цель — показать возможность применения метода с использованием подобия подстановок к сетям Фейстеля рассматриваемого типа, особенно когда методы Исобе и Динура–Данкельмана–Шамира неприменимы. Более того, даже объем памяти в 2^{199} бит считается допустимым (см., например, [6]).

4. Рекомендации по выбору ключевой развертки, исключающей применение метода с использованием подобия подстановок

Основной предпосылкой для возможности применения метода с использованием подобия подстановок к сетям Фейстеля рассматриваемого вида является тот факт, что преобразование зашифрования E может быть представлено в виде $E = FGF^{-1}$. При этом примеры 1 и 2 из раздела 3 показывают, что данное условие не является достаточным для эффективного применения метода.

В общем виде каким-то образом учесть и описать все ключевые развертки для сетей Фейстеля рассматриваемого типа, исключающие возможность эффективного применения метода, представляется достаточно сложной задачей. Более того, казалось бы, очевидное условие $M_1 \neq M_W$, не позволяющее представить преобразование E в виде $E = FGF^{-1}$, на самом деле не гарантирует невозможность применения предложенного метода. Объясним подробнее. Если, например, $M_1 \neq M_W$, но $M_2 = M_{W-1}$, то, перебрав итерационные ключи M_1, M_W , можно получить новое преобразование E' (зашифрование со 2-й по $(W-1)$ -ю итерации), которое уже представимо в виде $E' = F'G'F'^{-1}$. При этом может оказаться, что даже с учетом перебора итерационных ключей M_1, M_W метод с использованием подобия подстановок будет эффективно применим.

Условия

$$M_1 \neq M_W, \quad M_2 \neq M_{W-1}, \quad \dots, \quad M_{\lfloor \frac{W-1}{2} \rfloor} \neq M_{W - \lfloor \frac{W-1}{2} \rfloor + 1},$$

где $\lfloor p \rfloor$ — ближайшее целое число, не превосходящее $p \in \mathbb{R}$, представляются близкими к достаточным для неприменимости метода с использованием подобия подстановок.

Нетрудно видеть, что если ключевая развертка сети Фейстеля рассматриваемого типа удовлетворяет этим условиям, то методы Исобе и Динура–Данкельмана–Шамира также неприменимы к данной сети Фейстеля.

Примером, показывающим, что указанные условия не являются в полной мере достаточными, является случай

$$M_1 \neq M_W, \quad M_2 \neq M_{W-1} = M_1;$$

здесь, как и в приведенном в начале этого раздела примере, при переборе ключа M_W можно найти преобразование, представимое в виде $E' = F'G'F'^{-1}$.

5. Выводы

В работе для сетей Фейстеля рассматриваемого типа предложен метод определения ключа с использованием подобия подстановок. Получены достаточные условия, при которых он эффективнее тотального опробования.

Рассмотрен ряд примеров применения метода к различным алгоритмам блочного шифрования. В частности, показано, что метод не может быть эффективно применен к алгоритмам ГОСТ 28147-89 («Магма») и 2-ГОСТ. Также приведен пример сети Фейстеля, к которой методы Исобе и Динура–Данкельмана–Шамира неприменимы, а метод с использованием подобия подстановок оказывается применим и имеет трудоемкость, существенно меньшую трудоемкости тотального опробования. Это показывает, что он не является частным случаем методов Исобе и Динура–Данкельмана–Шамира.

Обсуждены условия на ключевую развертку сетей Фейстеля рассматриваемого типа, достаточные для невозможности применения как методов Исобе и Динура–Данкельмана–Шамира, так и метода с использованием подобия подстановок.

Видимо, основной предпосылкой для возможности применения к сетям Фейстеля рассмотренного метода с использованием подобия подстановок и методов Исобе и Динура–Данкельмана–Шамира является «простота» ключевой развертки. Она выражается, в частности, в том, что раундовые ключи представляют собой зависящие от номера итерации подвекторы ключевого вектора, над которыми не выполняется никаких дополнительных преобразований. Этот подход к построению ключевой развертки сетей Фейстеля до сих пор актуален, так как он позволяет синтезировать алгоритмы блочного шифрования, реализуемые на платформах с ограниченными ресурсами (см., например, [5, 7]) и удовлетворяющие требованиям даже к ультранизкоресурсным (т. е. требующим для своей аппаратной реализации менее 1000 GE) криптографическим алгоритмам.

Автор признателен А. М. Зубкову и Д. В. Шуваеву за интерес к работе и полезные замечания.

Список литературы

- [1] Isobe T., “A single-key attack on the full GOST block cipher”, Lect. Notes Comput. Sci., **6733**, 2011, 290–305
- [2] Dinur I., Dunkelman O., Shamir A., *Improved attacks on full GOST*, Cryptology ePrint Archive, Report 2011/558, <http://eprint.iacr.org/>.
- [3] *Стандарт криптографической защиты данных. ГОСТ 28147-89*: Гос. комитет СССР по стандартизации, 1989.

- [4] ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры», М.: Стандартинформ, 2015.
- [5] Dmukh A., Dygin D., Marshalko G., *A lightweight-friendly modification of GOST block cipher*, Cryptology ePrint Archive, Report 2015/065, <http://eprint.iacr.org/>.
- [6] Ashur T., Bar-On A., Dunkelman O., *Cryptanalysis of GOST2*, Cryptology ePrint Archive, Report 2016/532, <http://eprint.iacr.org>.
- [7] Poschmann A., Ling S., Wang H., “256 bit standardized Crypto for 650 GE — GOST Revisited”, *Lect. Notes Comput. Sci.*, **6225**, 2010, 219–233.
- [8] Сачков В. Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978 288 с.