Math-Net.Ru

Общероссийский математический портал

М. А. Пудовкина, Г. И. Хоруженко, О классах слабых ключей обобщенной шифрсистемы PRINT, *Матем. вопр. криптогр.*, 2013, том 4, выпуск 2, 113–125

DOI: <https://doi.org/10.4213/mvk87>

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: 54.162.85.209

26 апреля 2023 г., 15:10:35

О классах слабых ключей обобщенной шифрсистемы PRINT

М. А. Пудовкина, Г. И. Хоруженко

Национальный исследовательский ядерный университет (МИФИ), Москва

Получено 18.IX.2012

Шифрсистема PRINT предложена на конференции CHES-2010. В настоящей работе вводится обобщенная шифрсистема PRINT (GPRINT). Для нее описывается класс ключей шифрования, для которых раундовые функции сохраняют некоторое нетривиальное подмножество блоков текстов. Также построен класс ключей, слабых относительно линейного метода.

Ключевые слова: линейный метод, инвариантное подпространство, слабые ключи, блочная шифрсистема

On classes of weak keys of generalized cryptosystem PRINT

M. A. Pudovkina, G. I. Khoruzenko

National Nuclear Research University, Moscow

Abstract. The block cipher PRINTcipher was presented at CHES in 2010. In this paper, a generalized PRINT cipher, called GPRINT, is introduced. Weak key classes of GPRINT in relation to invariant coset attacks and linear cryptanalysis are described.

Key words: linear method, invariant subspace, weak keys, block cipher

Citation: *Mathematical Aspects of Cryptography*, 2013, vol. 4, no. 2, pp. 113–125 (Russian).

1. Введение

Шифрсистема PRINT предложена на конференции CHES-2010 [1] в двух вариантах — PRINT-48 и PRINT-96 — в зависимости от размера блока открытого текста и длины ключа шифрования. Она относится к классу блочных шифрсистем, предназначенных для использования в средах с ограниченными ресурсами. Ее конструкция во многом схожа с шифрсистемой PRESENT [2]. Основной структурной особенностью шифрсистемы PRINT является различное использование двух подблоков ключа шифрования. Первый подблок ключа задает линейное преобразование алгоритма шифрования, а второй подблок используется для сложения с промежуточным текстом.

К шифрсистеме PRINT применены различные методы криптоанализа. Простой алгоритм развертывания ключа приводит к наличию у шифрсистемы PRINT классов слабых ключей, относительно которых она уязвима к некоторым атакам. В работах [3, 4] проводится анализ на основе инвариантных подпространств. Основная идея атаки заключается в поиске подмножеств открытых текстов и ключей шифрования, сохраняемых раундовой функцией алгоритма шифрования. Также предложены атаки на основе нескольких методов: разностного [5], линейного [6], их комбинации [7]. В работе [8] рассматривается стойкость шифрсистемы относительно алгебраического метода.

В настоящей работе вводится обобщенная шифрсистема PRINT, обозначаемая далее как GPRINT. Для нее описывается класс ключей шифрования, для которых раундовые функции сохраняют некоторое нетривиальное подмножество блоков текстов. Данный результат обобщает инвариантные подпространства шифрсистемы PRINT, приведенные в работе [3]. Описываются классы слабых ключей шифрования шифрсистемы GPRINT для алгоритмов развертывания ключа, схожих с алгоритмом развертывания ключа шифрсистемы ГОСТ 28147-89. Показано, что раундовые функции таких алгоритмов развертывания ключа также сохраняют некоторое подмножество блоков текстов. Приведен слабый класс ключей шифрсистемы GPRINT относительно линейного метода криптоанализа.

2. Описание шифрсистемы GPRINT и основные обозначения

Пусть $\mathbb{N}$ — множество натуральных чисел; V_t — векторное пространство размерности t над полем $GF(2)$, $t \in \mathbb{N}$; $S(X)$ — симметрическая группа, заданная на множестве X ; $\|\alpha\|$ — вес Хемминга вектора α ; $\oplus$ — операция

покоординатного по модулю два сложения векторов из V_i ; $GL_n(2)$ — полная линейная группа преобразований пространства V_n ; $m, d, p \in \mathbb{N}$, $n = md$; $\hat{s} = (\underbrace{s, \dots, s}_d)$, $s \in S(V_m)$; $\alpha^g = \alpha g$ — образ элемента $\alpha \in X$ при действии

на него подстановкой $g \in S(X)$; $\alpha^G = \{\alpha^g | g \in G\}$, $G \subseteq S(X)$; линейное преобразование $h \in GL_n(2)$ в стандартном базисе задается подстановочной матрицей $\mathbf{h}$, где

$$(\alpha_{n-1}, \dots, \alpha_0)\mathbf{h} = (\alpha_{(n-1)\sigma}, \dots, \alpha_{0\sigma}), \quad \sigma \in S(\{0, \dots, n-1\}).$$

Далее, действие s -блока $\hat{s}$ на вектор $\alpha = (\alpha_{d-1}, \dots, \alpha_0) \in V_m^d$ определяется формулой $\alpha^{\hat{s}} = (\alpha_{d-1}^s, \dots, \alpha_0^s)$, поэтому мы рассматриваем $\hat{s}$ как подстановку на V_n .

Поскольку каждый вектор $\alpha = (\alpha_{n-1}, \dots, \alpha_1, \alpha_0) \in V_n$ можно рассматривать как двоичную запись числа $\tilde{\alpha} = 2^{n-1}\alpha_{n-1} + \dots + 2\alpha_1 + \alpha_0$, мы в работе будем отождествлять вектор α с числом $\tilde{\alpha}$.

Приведем описание алгоритма развертывания ключа шифрсистемы GPRINT. Рассмотрим два подблока $k^{(0)} \in V_n$, $k^{(1)} = (k_{d-1}^{(1)}, \dots, k_0^{(1)}) \in V_p^d$ ключа шифрования $k = (k^{(0)}, k^{(1)}) \in V_n \times V_p^d$. Раундовым ключом в каждом раунде является ключ шифрования k .

Подблок $k^{(1)}$ задает линейное преобразование $\hat{\rho}_{k^{(1)}}: V_n \rightarrow V_n$ следующим образом:

$$(\beta_{d-1}, \dots, \beta_0)^{\hat{\rho}_{k^{(1)}}} = \left(\rho_{k_{d-1}^{(1)}}(\beta_{d-1}), \dots, \rho_{k_0^{(1)}}(\beta_0) \right),$$

где $(\beta_{d-1}, \dots, \beta_0) \in V_m^d$. Преобразование $\rho_\kappa \in GL_m(2)$, осуществляющее перестановку координат векторов из V_m , для каждого $\kappa \in V_p$ задано как

$$(\gamma_{m-1}, \dots, \gamma_0)^{\rho_\kappa} = (\gamma_{(m-1)\bar{\rho}_\kappa}, \dots, \gamma_{0\bar{\rho}_\kappa}), \quad \bar{\rho}_\kappa \in S(\{0, \dots, m-1\}).$$

Таким образом, в зависимости от подблока $k^{(1)}$ ключа шифрования k преобразование $\hat{\rho}_{k^{(1)}}$ осуществляет перестановку координат векторов из V_n . Обозначим данную перестановку как $\varrho_{k^{(1)}}$.

Раундовая функция алгоритма шифрования GPRINT на j -м раунде $g_k^{(j)}: V_n \rightarrow V_n$ имеет вид

$$\alpha^{g_k^{(j)}} = \left(\left(\alpha \oplus k^{(0)} \right)^h \oplus c^{(j)} \right)^{\hat{\rho}_{k^{(1)}}^{\hat{s}}},$$

где $c^{(j)} = (c_{n-1}^{(j)}, \dots, c_0^{(j)})$ — константа из V_n , зависящая от номера раунда j , и l -раундовая функция зашифрования $f_k^{(l)}$ есть $f_k^{(l)} = g_k^{(l)} \dots g_k^{(1)}$.

Шифрсистемы PRINT-48 и PRINT-96 являются частными случаями шифрсистемы GPRINT. Например, для PRINT-48 имеем $n = 48$, $m = 3$, $d = 16$, $p = 2$, $l = n$ — число раундов, подстановка σ есть

$$i^\sigma = \begin{cases} 3i - 2 \pmod{n-1}, & \text{если } i \in \{1, \dots, n-2\}, \\ n-1, & \text{если } i = n-1, \end{cases}$$

преобразование ρ_κ для $\kappa \in V_2$ задается равенством

$$(\beta_2, \beta_1, \beta_0)^{\rho_\kappa} = \begin{cases} (\beta_2, \beta_1, \beta_0), & \text{если } \kappa = (0, 0), \\ (\beta_1, \beta_2, \beta_0), & \text{если } \kappa = (0, 1), \\ (\beta_2, \beta_0, \beta_1), & \text{если } \kappa = (1, 0), \\ (\beta_0, \beta_1, \beta_2), & \text{если } \kappa = (1, 1), \end{cases}$$

$$s = (0)(1)(2, 3, 6, 5, 4, 7),$$

$$c^{(j)} = (c_{47}^{(j)}, \dots, c_0^{(j)}) = (\underbrace{0, \dots, 0}_{42}, \gamma_5^{(j)}, \dots, \gamma_0^{(j)}),$$

где $(\gamma_5^{(j)}, \dots, \gamma_0^{(j)}) \in V_6$, $j = 1, \dots, n$. Заметим, что преобразование ρ_κ для любого $\kappa \in V_2$ осуществляет перестановку координат векторов из V_3 .

Таким образом, в отличие от шифрсистем PRINT-48 и PRINT-96, шифрсистема GPRINT использует произвольные s -блок, подстановки σ , $\bar{\rho}_\kappa$ и длину n блока открытого текста.

Пусть $a(u) = (a_{\delta\varepsilon}(u))$ — разностная матрица подстановки $u \in S(V_m)$, т.е.

$$a_{\delta\varepsilon}(u) = 2^{-m} |\{\beta \in V_m | (\beta \oplus \delta)^u \oplus \beta^u = \varepsilon\}|,$$

где $\delta, \varepsilon \in V_m$.

3. Классы ключей шифрования, для которых функция зашифрования сохраняет подмножество из V_n

Пусть l — число раундов алгоритма шифрования, $l \in \mathbb{N}$. В работе [3] описаны классы ключей шифрсистемы PRINT, для которых раундовая функция $g_k^{(j)}$ сохраняет некоторое подмножество блоков открытого текста, $j = 1, \dots, l$. В частности, в работе [3] показано наличие таких собственного подпространства $U < V_n$, векторов $\lambda, \lambda' \in V_n$ и множества ключей шифрования $K = K' \times K''$, $K \subset V_n \times V_{pd}$, $K' = U \oplus \lambda' \oplus \lambda$, $K'' \subseteq V_{pd}$, что для всех

$k = (k^{(0)}, k^{(1)}) \in K, j \in \{1, \dots, l\}$ справедливо равенство

$$(U \oplus \lambda)^{g_k^{(j)}} = (U \oplus \lambda \oplus k^{(0)})^{g_{k'}^{(j)}} = (U \oplus \lambda')^{g_{k'}^{(j)}} = U \oplus \lambda,$$

где $k' = (\vec{0}, k^{(1)})$. Таким образом, множество $U \oplus \lambda$ стабилизируется в целом раундовыми функциями $g_k^{(j)}$.

Опишем классы ключей шифрования шифрсистемы GPRINT, при зашифровании на которых раундовые функции стабилизируют в целом некоторое нетривиальное подмножество из V_n . В данном разделе ключи из такого класса будем считать слабыми.

Нам понадобятся следующие обозначения:

$$C^{(j)} = \{i \in \{0, \dots, d-1\} | c_i^{(j)} = 0\}, \quad j = 1, \dots, l, \quad C = \bigcap_{j=1}^l C^{(j)},$$

$$X_i = \{i \cdot m, i \cdot m + 1, \dots, (i+1) \cdot m - 1\}, \quad i = 0, \dots, d-1,$$

$$Y_{(m)} = \{y \pmod{m} | y \in Y\}, \quad Y \subseteq \{0, \dots, n-1\}.$$

Для

$$J = \{i_1, \dots, i_{|J|}\} \subset \{0, \dots, b-1\}, \delta = (\delta_{b-|J|-1}, \dots, \delta_0) \in V_{b-|J|}$$

положим

$$V_{b,J}(\delta) = \{(\delta_{b-|J|-1}, \dots, \delta_{i_{|J|}+1}, \gamma_{|J|}, \delta_{i_{|J|}-1}, \dots, \delta_{i_1}, \gamma_1, \delta_{i_1-1}, \dots, \delta_0) | \gamma_1, \dots, \gamma_{|J|} \in \{0, 1\}\},$$

т.е. множество $V_{b,J}(\delta)$ состоит из всех таких векторов, у которых значения координат с номерами из множества J не фиксированы, а значения координат с номерами, не принадлежащими множеству J , фиксированы.

В общем виде наличие класса слабых ключей у шифрсистемы GPRINT обусловлено комбинацией свойств подстановки σ и s -блока. Приведем условия на преобразования σ и s , при которых существуют классы слабых ключей.

Утверждение 1. Пусть для чисел $r \in \{1, \dots, m-1\}$ и $q \in \mathbb{N}$ существуют:

1. множество $X \subseteq \{0, \dots, n-1\} \setminus C$, для которого $|X \cap X_i| \in \{0, m-r\}$ и $|X^\sigma \cap X_i| \in \{0, m-r\}$ при $i = 0, \dots, d-1$;
2. множества $J^{(i)}, J'^{(i)} \subseteq \{0, \dots, m-1\}$ мощности $r \geq 1$ каждое, множества $\Theta_{J^{(i)}}, \Theta'_{J'^{(i)}} \subseteq V_{m-r}$ и биективное отображение $\phi: \Theta_{J^{(i)}} \rightarrow \Theta'_{J'^{(i)}}$, для которых справедливо равенство $(V_{m,J^{(i)}}(\theta))^s = V_{m,J'^{(i)}}(\phi(\theta))$ для каждого $\theta \in \Theta_{J^{(i)}}$, $i = 1, \dots, q$;

3. множество $K'' \subseteq V_{pd}$, для которого $X^{\sigma_{k^{(1)}}} = X'$ при каждом $k^{(1)} \in K''$, где X' — такое множество, что если $i \in \{0, \dots, d-1\}$ и $X' \cap X_i \neq \emptyset$, то $\{0, \dots, m-1\} \setminus J^{(t_i)} = (X' \cap X_i)_{(m)}$ и $\{0, \dots, m-1\} \setminus J'^{(t_i)} = (X \cap X_i)_{(m)}$ для некоторого $t_i \in \{1, \dots, q\}$.

Тогда существуют такие подпространство $U < V_n$ и векторы $\lambda, \lambda' \in V_n$, что для любых $k = (k^{(0)}, k^{(1)}) \in (U \oplus \lambda') \times K''$ и $j \in \mathbb{N}$ выполняется равенство $(U \oplus \lambda)^{g_k^{(j)}} = U \oplus \lambda$.

ЗАМЕЧАНИЕ. а) В утверждении 1 фигурируют пространство U и векторы λ, λ' . Если подстановка σ и s -брокс таковы, что для каждого $i \in \{0, \dots, d-1\}$, удовлетворяющего соотношению $X' \cap X_i \neq \emptyset$, существует такое $t_i \in \{1, \dots, q\}$, что $J^{(t_i)} = J'^{(t_i)}$, то $X^{\sigma_{k^{(1)}}} = X$ для каждого $k^{(1)} \in K''$.

б) Число q определяется свойством s -брокса, а именно оно равно числу всех четверок подмножеств $\Theta_{J^{(i)}}, \Theta'_{J'^{(i)}} \subseteq V_{m-r}$, $J^{(i)}, J'^{(i)} \subset \{0, \dots, m-1\}$, удовлетворяющих равенству $(V_{m,J^{(i)}}(\theta))^s = V_{m,J'^{(i)}}(\phi(\theta))$.

в) Условию 2 утверждения 1 при $r = 1$ удовлетворяют, например, подстановки $s \in S(V_m)$, у которых $a_{ij}(s) > 0$ хотя бы для одной пары $i, j \in \{0, \dots, 2^m - 1\}$ с $\|i\| = \|j\| = 1$, т. е. хотя бы одна разность веса один под действием подстановки s переходит в разность также веса один. В работе [9] показано, что при $m = 4$ таким свойством обладают все инволюции на V_4 .

г) Класс слабых ключей есть $(U \oplus \lambda') \times K''$. Его мощность оценивается снизу величиной $2^{n-|X|}$, а число всех ключей есть 2^{n+pd} .

Доказательство. Для $i = 0, \dots, d-1$ положим $U = U^{(d-1)} \times \dots \times U^{(0)}$, где

$$U^{(i)} = \begin{cases} V_m, & \text{если } X \cap X_i = \emptyset, \\ V_{m,J'^{(t_i)}}(\vec{0}), & \text{если } X \cap X_i \neq \emptyset. \end{cases}$$

Пусть $I = \{i \in \{0, \dots, d-1\} | X \cap X_i \neq \emptyset\}$. Зафиксируем произвольный элемент $\theta_{t_j} \in \Theta_{J'^{(t_j)}}$ для каждого $j \in I$; для $i = 0, \dots, d-1$ положим

$$\Lambda^{(i)} = \begin{cases} V_m, & \text{если } i \notin I, \\ \left\{ \beta \in V_m | \beta \oplus V_{m,J'^{(t_i)}}(\vec{0}) = V_{m,J'^{(t_i)}}(\phi(\theta_{t_i})) \right\}, & \text{если } i \in I. \end{cases}$$

Зафиксируем произвольный вектор $\lambda \in \Lambda^{(d-1)} \times \dots \times \Lambda^{(0)}$. Тогда $U \oplus \lambda$ можно представить в виде

$$U \oplus \lambda = U^{(d-1)}(\lambda) \times \dots \times U^{(0)}(\lambda),$$

где

$$U^{(i)}(\lambda) = \begin{cases} V_m, & \text{если } i \notin I, \\ V_{m, J'(t_i)}(\phi(\theta_{t_i})), & \text{если } i \in I. \end{cases}$$

Согласно определению U, λ

$$(U \oplus \lambda)^{\widehat{s}^{-1}} = U'^{(d-1)}(\lambda) \times \dots \times U'^{(0)}(\lambda),$$

где

$$U'^{(i)}(\lambda) = \begin{cases} V_m, & \text{если } X \cap X_i = \emptyset, \\ V_{m, J'(t_i)}(\vec{0}), & \text{если } X \cap X_i \neq \emptyset. \end{cases}$$

Для произвольного $k^{(1)} \in K''$ обозначим

$$U''(\lambda, k^{(1)}) = (U \oplus \lambda)^{\widehat{s}^{-1} \widehat{\rho}_{k^{(1)}}^{-1}} \oplus c^{(j)}.$$

Тогда $U''(\lambda, k^{(1)})$ является декартовым произведением некоторых множеств $U''^{(d-1)}(\lambda, k^{(1)}), \dots, U''^{(0)}(\lambda, k^{(1)})$, т. е.

$$U''(\lambda, k^{(1)}) = U''^{(d-1)}(\lambda, k^{(1)}) \times \dots \times U''^{(0)}(\lambda, k^{(1)}).$$

Зафиксируем произвольный элемент $k^{(1)} \in K''$. Из условий 1 и 3 данного утверждения и того, что $\widehat{\rho}_{k^{(1)}}$ осуществляет перестановку координат векторов из V_n при любом $k^{(1)} \in K''$, имеем $U^{(i)}(\lambda) = U''^{(i)}(\lambda, k^{(1)}) = U''^{(i)}(\lambda, k^{(1)})$, $i = 0, \dots, d-1$. Таким образом, множество $U''(\lambda, k^{(1)})$ одно и то же для всех $k^{(1)} \in K''$. Поэтому положим $U''(\lambda) = U''(\lambda, k^{(1)})$ для некоторого $k^{(1)} \in K''$.

Пусть

$$\Lambda'(\lambda) = \{\beta \in V_n \mid U \oplus \lambda = U''(\lambda) \oplus \beta\}.$$

Зафиксируем произвольный вектор $\lambda' \in \Lambda'(\lambda)$. Тогда для любого $k = (k^{(0)}, k^{(1)}) \in (U \oplus \lambda') \times K''$ выполняется равенство

$$(U \oplus \lambda)^{g_k^{(j)}} = (U \oplus \lambda \oplus k^{(0)})^{g_{k'}^{(j)}} = (U \oplus \lambda')^{g_{k'}^{(j)}} = U \oplus \lambda,$$

где $k' = (\vec{0}, k^{(1)})$. $\square$

Для шифрсистемы PRINT-48 имеем $r = 1$, $p = 2$, $J^{(1)} = J'^{(1)} = \{0\}$, $J^{(2)} = J'^{(2)} = \{1\}$, $J^{(3)} = J'^{(3)} = \{2\}$, $\Theta_{J^{(1)}} = \Theta'_{J'^{(1)}} = \{(0, 0)\}$, $\Theta_{J^{(2)}} = \{(1, 0)\}$, $\Theta'_{J'^{(2)}} = \{(1, 1)\}$, $\Theta_{J^{(3)}} = \{(1, 1)\}$, $\Theta'_{J'^{(3)}} = \{(1, 0)\}$. В этом случае отображение ϕ задается однозначно, где $\phi(\Theta_{J^{(i)}}) = \Theta'_{J'^{(i)}}$, $i = 1, 2, 3$. Таким образом,

$$\begin{aligned} (V_{3,J^{(1)}}(0, 0))^s &= V_{3,J'^{(1)}}(\phi(0, 0)), (V_{3,J^{(2)}}(1, 0))^s = V_{3,J'^{(2)}}(\phi(1, 1)), \\ (V_{3,J^{(3)}}(1, 1))^s &= V_{3,J'^{(3)}}(\phi(1, 0)). \end{aligned}$$

Отметим, что разностная матрица $a(s) = (a_{ij})$, $i, j = 0, \dots, 7$, для s -блока шифрсистемы PRINT есть

$$a(s) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/4 & 0 & 1/4 & 0 & 1/4 & 0 & 1/4 \\ 0 & 0 & 1/4 & 1/4 & 0 & 0 & 1/4 & 1/4 \\ 0 & 1/4 & 1/4 & 0 & 0 & 1/4 & 1/4 & 0 \\ 0 & 0 & 0 & 0 & 1/4 & 1/4 & 1/4 & 1/4 \\ 0 & 1/4 & 0 & 1/4 & 1/4 & 0 & 1/4 & 0 \\ 0 & 0 & 1/4 & 1/4 & 1/4 & 1/4 & 0 & 0 \\ 0 & 1/4 & 1/4 & 0 & 1/4 & 0 & 0 & 1/4 \end{pmatrix},$$

и наличие множества $V_{3,J^{(i)}}(\beta_1^{(i)}, \beta_0^{(i)})$ обусловлено тем, что три разности веса один переходят в разности веса один.

Рассмотрим такую шифрсистему, у которой алгоритм шифрования совпадает с алгоритмом шифрования шифрсистемы GPRINT, а алгоритм развертывания ключа состоит в том, что на i -м раунде используется раундовый ключ $k_i = (k^{(0,i)}, k^{(1)}) \in (U \oplus \lambda') \times K''$ (K'' удовлетворяет условию 3 утверждения 1). Тогда равенство $(U \oplus \lambda)^{g_{k_i}^{(i)}} = U \oplus \lambda$ выполняется для некоторых $U < V_n$, $\lambda, \lambda' \in V_n$, $i \in \mathbb{N}$.

Приведем еще один класс шифрсистем, у которых имеется класс слабых ключей шифрования, а функция зашифрования сохраняет некоторое инвариантное пространство.

Пусть $m, d, p \in \mathbb{N}$, $n = md$, $\hat{s} = (\underbrace{s, \dots, s}_d)$, $s \in S(V_m)$, $h \in GL_n(2)$ в стандартном базисе задается подстановочной матрицей $\mathbf{h}$, где $(\alpha_{n-1}, \dots, \alpha_0)\mathbf{h} = (\alpha_{(n-1)^\sigma}, \dots, \alpha_{0^\sigma})$, $\sigma \in S(\{0, \dots, n-1\})$.

Рассмотрим алгоритм развертывания ключа, похожий на алгоритм развертывания ключа шифрсистемы ГОСТ 28147-89. Пусть $k = (k_1, \dots, k_c)$ — ключ шифрования из V_n^c , l — число раундов, $\delta: \{1, \dots, l\} \rightarrow \{1, \dots, c\}$. Тогда раундовый ключ $k^{(i)}$ i -го раунда есть $k^{(i)} = k_{\delta(i)}$, $i = 1, \dots, l$.

Пусть раундовая функция $g_{k(i)}: V_n \rightarrow V_n$ рассматриваемой шифрсистемы задается равенством $\alpha^{g_{k(i)}} = (\alpha \oplus k^{(i)})^{\hat{s}^h}$, $\alpha \in V_n$, $i = 1, \dots, l$.

Приведем условия на преобразования σ и s , при которых имеются классы слабых ключей.

Утверждение 2. Пусть $r \in \{1, \dots, m-1\}$, $q \in \mathbb{N}$ — такие числа, что:

1. существуют множества $J^{(i)}, J'^{(i)} \subseteq \{0, \dots, m-1\}$ мощности $r \geq 1$ каждое, множества $\Theta_{J^{(i)}}, \Theta'_{J'^{(i)}} \subseteq V_{m-r}$ и биективное отображение $\phi: \Theta_{J^{(i)}} \rightarrow \Theta'_{J'^{(i)}}$, для которых справедливо равенство $(V_{m, J^{(i)}}(\theta))^s = V_{m, J'^{(i)}}(\phi(\theta))$ при любых $\theta \in \Theta_{J^{(i)}}$, $i = 1, \dots, q$,
2. существует такое множество $X \subseteq \{0, \dots, n-1\}$, что $|X \cap X_i| \in \{0, m-r\}$ и если $i \in \{0, \dots, d-1\}$ и $X \cap X_i \neq \emptyset$, то $\{0, \dots, m-1\} \setminus J^{(t_i)} = (X \cap X_i)_{(m)}$ для некоторого $t_i \in \{1, \dots, q\}$,
3. $X'^s = X$, где $X' \subseteq \{0, \dots, n-1\}$ — такое множество, что для каждого $i \in \{0, \dots, d-1\}$ существует $t_i \in \{1, \dots, q\}$, для которого $\{0, \dots, m-1\} \setminus J'^{(t_i)} = (X' \cap X_i)_{(m)}$, если $X \cap X_i \neq \emptyset$.

Тогда существуют такие подпространство $U < V_n$ и векторы $\lambda, \lambda' \in V_n$, что для любого ключа шифрования $k \in (U \oplus \lambda')^c$ выполняется равенство $(U \oplus \lambda)^{g_{k(i)}} = U \oplus \lambda$ для $i = 1, \dots, l$.

Доказательство аналогично доказательству утверждения 1. $\square$

Отметим, что если функция усложнения $g_{k(i)}$ алгоритма шифрования Фейстеля удовлетворяет утверждению 2 и $U^{g_{k(i)}} = U$ для некоторого собственного подпространства $U < V_n$, то раундовая функция

$$\hat{f}_{k(i)}: (\alpha^{(1)}, \alpha^{(0)}) \rightarrow (\alpha^{(0)}, \alpha^{(1)} \oplus \alpha^{(0)g_{k(i)}})$$

сохраняет подпространство $U \times U$.

4. Слабые ключи шифрсистемы GPRINT относительно линейного метода криптоанализа

Приведем класс ключей шифрования шифрсистемы GPRINT, являющийся слабым относительно метода линейного криптоанализа. Отметим, что в статье используются терминология и подход, принятые в методе линейного криптоанализа (см., например, [10]).

В настоящей работе рассматриваются *однобитовые* линейные характеристики, которые зависят от одного бита открытого текста, одного бита

шифртекста и от некоторой линейной комбинации бит ключа шифрования вида $\bigoplus_{l=1}^j k_{i_l}^{(0)}$, $i_l \in \{0, \dots, n-1\}$, где $j \in \{1, \dots, n\}$ — число раундов, на которое распространяется характеристика. Ее можно представлять также тройкой

$$(t_0, t_1, (i_1, \dots, i_j)),$$

где t_0 — номер бита открытого текста, t_1 — номер бита шифртекста, i_q — номер бита ключа шифрования, входящего в характеристику на j -м раунде, $t_0, t_1, i_q \in \{1, \dots, n\}$, $q \in \{1, \dots, j\}$.

Структура шифрсистемы GPRINT такова, что при построении линейных характеристик необходимо учитывать не только свойства s -блока, но и свойства преобразования $\hat{\rho}_{k^{(1)}}$. В данном разделе исследуется возможность построения линейных характеристик, зависящих только от некоторых фиксированных бит подблока $k^{(1)}$, но не от всего $k^{(1)}$, и с наименьшим числом активных подстановок в s -блоке. Поэтому рассматриваются подстановки $s \in S(V_m)$, у которых существует хотя бы одна координатная функция, линейная только по одной переменной.

Под *слабыми* ключами относительно линейного метода криптоанализа будем понимать ключи шифрования, для которых можно построить линейную характеристику, зависящую не от всех бит подблока ключа $k^{(1)}$.

Обозначим через $O^{(s)}$ множество всех таких пар $(i, j) \in \{0, \dots, m-1\}^2$, что i -я координатная функция s_i подстановки s линейна по j -й переменной. Отметим, что множество $O^{(s)}$ непусто согласно накладываемому на подстановку $s \in S(V_m)$ условию.

Зададим функцию $u^{(s)}: \{0, \dots, m-1\} \rightarrow \{0, 1\}$ и преобразование $\pi^{(s)}: \{0, \dots, m-1\} \rightarrow \{0, \dots, m-1\}$ условиями

$$u^{(s)}(i) = \begin{cases} 1, & \text{если } \exists j \in \{0, \dots, m-1\} : (j, i) \in O^{(s)}, \\ 0 & \text{в противном случае,} \end{cases}$$

$$\pi^{(s)}(i) = \begin{cases} j, & \text{если } \exists j \in \{0, \dots, m-1\} : (j, i) \in O^{(s)}, \\ 0 & \text{в противном случае,} \end{cases}$$

где $i \in \{0, \dots, m-1\}$.

В следующем утверждении описываются классы ключей шифрсистемы GPRINT, слабых относительно метода линейного криптоанализа. Для получения таких классов слабых ключей рассматриваются характеристики, повторяющиеся через t раундов, $t < d$.

Для $i, q \in \{0, \dots, n-1\}$ положим

$$v_q(i) = i - mq \pmod{n}, \quad v_q^{-1}(i) = i + qm \pmod{n},$$

тогда $i^{v_q v_q^{-1}} = i$.

Утверждение 3. Пусть $i \in \{0, \dots, n-1\}$, $r \in \{1, \dots, d\}$, $l(0), \dots, l(r-1) \in \{0, \dots, d-1\}$ и существуют такие числа $n_r \in \mathbb{N}$, $t(0), \dots, t(n_r-1) \in \{0, \dots, r-1\}$, что справедливы следующие соотношения:

$$1. \quad i^{(s)} \left(i^{\sigma v_{l(t(0))} \pi^{(s)} \varrho_{k_{l(t(0))}^{(1)}} v_{l(t(0))}^{-1} \dots \sigma v_{l(t(j-1))} \pi^{(s)} \varrho_{k_{l(t(j-1))}^{(1)}}} \right) = 1, \quad j = 1, \dots, n_r.$$

$$2. \quad 0 \leq i^{\sigma v_{l(t(0))} \pi^{(s)} \varrho_{k_{l(t(0))}^{(1)}} v_{l(t(0))}^{-1} \dots \sigma v_{l(t(j-1))} \pi^{(s)} \varrho_{k_{l(t(j-1))}^{(1)}}} \leq m-1, \quad j = 1, \dots, n_r.$$

$$3. \quad i^{\sigma v_{l(t(0))} \pi^{(s)} \varrho_{k_{l(t(0))}^{(1)}} v_{l(t(0))}^{-1} \dots \sigma v_{l(t(n_r-1))} \pi^{(s)} \varrho_{k_{l(t(n_r-1))}^{(1)}} v_{l(t(n_r-1))}^{-1}} = i.$$

Тогда существует класс ключей, слабых относительно метода линейного криптоанализа, имеющий мощность $2^{n+p(d-r)}$.

Доказательство. Рассмотрим произвольный открытый текст $\alpha^{(0)} = (\alpha_{n-1}^{(0)}, \dots, \alpha_0^{(0)}) \in V_n$, ключ шифрования $k = (k^{(0)}, k^{(1)}) \in V_n \times V_{pd}$ и соответствующие им промежуточные тексты $\alpha^{(j)} = g_k^{(j)}(\alpha^{(j-1)}), j \in \mathbb{N}$.

Рассмотрим действие раундовой функции на $\alpha_i^{(0)}, i \in \{0, \dots, n-1\}$. После применения подстановки σ на блок текста действует преобразование $v_{l(t(0))}$, которое не участвует в алгоритме шифрования GPRINT, а в настоящем утверждении используется для обеспечения корректности переходов между преобразованиями с различными областями значений. Далее, последовательно применяются преобразования $\pi^{(s)}$ и $\varrho_{k_{l(t(0))}^{(1)}}$. Условие 2 необходимо для того, чтобы i принадлежало множеству $\{0, \dots, m-1\}$ — области значений данных преобразований, при этом условие 1 гарантирует корректное построение линейной характеристики. Отметим, что на данном этапе значения бит ключа $k_{l(t(0))}^{(1)}$ фиксируются, тем самым однозначно определяя перестановку $\varrho_{k_{l(t(0))}^{(1)}}$. Далее применяется преобразование $v_{l(t(0))}^{-1}$. Таким образом, задана аппроксимация раундовой функции, осуществляющая перестановку τ бит текста.

Перестановка τ удовлетворяет соотношениям

$$\begin{aligned} i^\tau &= i^{\sigma v_{l(t(0))} \pi^{(s)} \varrho_{k_{l(t(0))}}^{(1)} v_{l(t(0))}^{-1}}, \\ i^{\tau^2} &= (i^\tau)^{\sigma v_{l(t(1))} \pi^{(s)} \varrho_{k_{l(t(1))}}^{(1)} v_{l(t(1))}^{-1}}, \\ &\dots \\ i^{\tau^{n_r-1}} &= \left(i^{\tau^{n_r-2}} \right)^{\sigma v_{l(t(n_r-1))} \pi^{(s)} \varrho_{k_{l(t(n_r-1))}}^{(1)} v_{l(t(n_r-1))}^{-1}}, \end{aligned}$$

задающим класс перестановок. Далее предполагается, что τ — произвольная перестановка, принадлежащая этому классу.

Так как один и тот же раундовый ключ применяется во всех раундах алгоритма шифрования, то существует линейная характеристика вида

$$\left(i, i^{\tau^j}, \left(i^\tau, i^{\tau^2}, \dots, i^{\tau^{j-1}} \right) \right),$$

где j — число раундов, $j \in \{1, \dots, n\}$. При этом на каждом раунде фиксируются новые значения бит $k_{l(t(j))}^{(1)}$ ключа, если подстановка s -блока не являлась активной, $j \in \{0, \dots, r-1\}$. Для построения линейной характеристики с наименьшим числом фиксированных бит ключа k необходимо при ее построении использовать наименьшее число подстановок s -блока. Условие 3 определяет периодичность линейной характеристики.

Таким образом, при фиксации rp бит ключа k для $2^{n+p(d-r)}$ ключей шифрования шифрсистемы GPRINT существует линейная характеристика вида

$$\left(i, i, \left(i^\tau, \dots, i^{\tau^{n_r-1}} \right) \right)$$

с периодом n_r . $\square$

Трудоемкость атаки линейным методом оценивается аналогично работе [6]. При проведении атаки используется $2^{2(t+1)}$ шифрований, число пар открытых текстов и соответствующих им шифртекстов также равно $2^{2(t+1)}$, где число атакуемых раундов есть t , $t < \frac{n}{2}$.

Список литературы

1. Knudsen L., Leander G., Poschmann A., Robshaw M.J.B. PRINTcipher: A block cipher for ICPrinting // CHES-2010. — Lect. Notes Comput. Sci., 2010. — V. 6225. — P. 16–32.

2. *Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M. J. B., Seurin Y., Vikkelsoe C.* PRESENT - An ultra-lightweight block cipher. // CHES 2007. — Lect. Notes Comput. Sci., 2007. — V. 4727. — P. 450–466.
3. *Leander G., Abdelraheem M. A., AlKhzaimi H., Zenner E.* A Cryptanalysis of PRINTcipher: The invariant coset attack // CRYPTO-2011. — Lect. Notes Comput. Sci., 2011. — V. 6841. — P. 206–221.
4. *Bulygin S., Walter M.* Study of the invariant coset attack on PRINTcipher: more weak keys with practical key recovery. — 2012. — <http://eprint.iacr.org/2012>.
5. *Abdelraheem M. A., Leander G., Zenner E.* Differential cryptanalysis of round-reduced PRINTcipher: Computing roots of permutations // FSE-2011. — Lect. Notes Comput. Sci., 2011. — V. 6733. — P. 1–17.
6. *Agren M., Johansson T.* Linear Cryptanalysis of PRINTcipher — trails and samples everywhere // INDOCRYPT-2011. — Lect. Notes Comput. Sci., 2011. — V. 7107. — P. 114–133.
7. *Karakoc F., Demirci H., Harmanci A. E.* Combined differential and linear cryptanalysis of reduced-round PRINTcipher // SAC-2011 — Lect. Notes Comput. Sci., 2011 — V. 7118.
8. *Bulygin S., Buchmann J.* Algebraic Cryptanalysis of the round-reduced and side channel analysis of the full PRINTcipher-48 // CANS-2011. — Lect. Notes Comput. Sci., 2011. — V. 7092 — P. 54–75.
9. *Liu B., Gong Z., Qiu W., Zheng D.* On the security of 4-Bit involutive S-Boxes for lightweight designs // ISPEC-2011. — Lect. Notes Comput. Sci., 2011. — V. 6672. — P. 247–256.
10. *Biham E.* On Matsui's linear cryptanalysis. In A. De Santis (Ed.) // Eurocrypt'94. — Lect. Notes Comput. Sci., 1994. — V. 950. — P. 341–355.