ПОДСЕКЦИЯ 4.3
«МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ»

УДК 519.719.2

О КЛАССАХ СЛАБЫХ КЛЮЧЕЙ

Абылахатов Аскар
Магистрант ЕНУ имени Л.Н.Гумилев , Нур-Султан, Казахстан
Научный руководитель – К.М. Сулейменов

Введение

В данной 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 [1-3].

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.

Постановка задачи

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 множество X; $\|\alpha\|$ – вес Хеминга вектора α; $\oplus$ - операция покоординатного по модулю два сложения векторов из V_t; $GL_n(2)$ – полная линейная группа преобразований пространства

$$V_n;\ m, d, p \in \mathbb{N},\ n = md;$$

$$\hat{s} = (s, \dots, s),\ s \in S(V_m);\ \alpha^g = \alpha g -$$

образ элемента $\alpha \in X$ при действий на него подстановкой

$$\alpha \in S(X);\ \alpha^G = \{\alpha^G | g \in G\},\ G \subseteq S(X);$$

линейное преобразование $t \in GL_n(2)$ в стандартном базисе задается подстановочной матрицей h, где

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

Далее, действие -бокса $\hat{s}$ на вектор

$$\alpha = (\alpha_{n-1}, \dots, \alpha_1, \alpha_0) \in V_m^d$$

определяется формулой

$$\alpha^{\hat{s}} = \alpha_{d-1}^{s}, \dots, \alpha_0^{s},$$

поэтому рассматриваем $\hat{s}$ как постановку на V_n .

Поскольку каждый вектор

$$\alpha = (\alpha_{n-1}, \dots, \alpha_1, \alpha_0) \in V_n$$

можно рассматривать двоичную запись числа

$$\widetilde{\alpha} = 2^n \alpha_{n-1} + 2\alpha_1 + \alpha_0,$$

мы в работе будем отождествлять вектор α с числом $\widetilde{\alpha}$.

Приведём описание алгоритма развертывания ключа шифрсистемы GPRINT.

Рассмотрим

$$\kappa^{(0)} \in V_n, \kappa^{(1)} = (\kappa_{d-1}^{(1)}, \dots, \kappa_0^{(1)}) \in V_p^d$$

ключа шифрования

$$\kappa = \left(\kappa^{(0)}, \kappa^{(1)}\right) \in V_n \times V_p^d.$$

Раундовым ключом в каждом раунде является ключ шифрование κ.

Раундовая функция алгоритма шифрование GPRINT на j-м раунде

$$g_\kappa^{(j)}: V_n \to V_n$$

имеет вид

$$\alpha^{g_\kappa^{(j)}} = \left(\left(\alpha \oplus \kappa^{(0)}\right)^h \oplus \mathrm{c}^{(j)}\right)^{\hat{p}_{\kappa^1}\hat{s}},$$

Шифрсистема PRINT-48 является частным случаем шифрсистемы GPRINT. Для PRINT-48 имеем n = 48, m = 3, d = 16, p = 2, l=n – число раундов, подстановка σ есть

$$i^\sigma = \begin{cases} 3i - 2 \ (mod\ n-1), & i \in \{1, \dots, n-2\}, \\ n-1, & i = n-1, \end{cases}$$

Преобразование $\rho_{\mathrm{к}}$ для $\kappa \in V_2$ задаётся равенством

$$(\beta_2, \beta_1, \beta_0)^{\rho_{\mathrm{к}}} \begin{cases} (\beta_2, \beta_1, \beta_0), & \mathrm{к} = (0,0), \\ (\beta_1, \beta_2, \beta_0), & \mathrm{к} = (0,1), \\ (\beta_2, \beta_0, \beta_1), & \mathrm{к} = (1,0), \\ (\beta_0, \beta_1, \beta_2), & \mathrm{к} = (1,1), \end{cases}$$

$$\mathrm{s} = (0)(1)(2,3,6,5,4,7),$$

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

где

$$\gamma_5^{(j)}, \dots, \gamma_0^{(j)} \in V_6, j = 1, \dots, n\,.$$

Заметим, что преобразование $\rho_{\mathrm{к}}$ для любого $\kappa \in V_2$ осуществляет перестановку координат векторов из V_3.

Таким образом, в отличие от шифрсистем PRINT-48, шифрсистема GPRINT использует произвольные s-бокс, подстановки σ, $\rho_к$ и длину n блока открытого текста.

Пусть

$$a(u) = (a_{\delta\varepsilon}(u))$$

разностная матрица подстановки $u \in S(V_m)$

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

Список использованной 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 3. Y., Vikkelsoe C. PRESENT - An ultra-lightweight block cipher. // CHES 2007. — Lect. Notes Comput. Sci., 2007. — V. 4727. — P. 450–466.
4. Bulygin S., Walter M. Study of the invariant coset attack on PRINTcipher: more weak keys with practical key recovery. — 2012. —https://eprint.iacr.org/2012/.