ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

УДК 519.719

О ШИФРСИСТЕМЕ GPRINT

Абылахатов Аскар
abylakhatov@gmail.com
Магистрант ЕНУ им. Л. Н. Гумилева, г. Астана, Казахстан
Научный руководитель – К. Сулейменов

Шифрсистема PRINT предложена на конференции CHES-2010 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 . 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.

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. 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

Описание шифрсистемы Gprint и основные обозначение

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; α — вес Хемминга вектора α; $\oplus$ — операция покоординатного по модулю два сложения векторов из V_{t}; $GL_n(2)$ — полная линейная группа преобразований пространства

$$V_n;\ m,d,p\ \in\ \mathbb{N}, n\ =\ md;$$
$$\hat{s}\ =\ (\underbrace{s,\ldots,s}_{d}), s \in S(V_m);\ \alpha^{\mathrm{g}}\ =\ \alpha\mathrm{g}$$

— образ элемента $\alpha \in X$ при действии на него подстановкой

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

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

$$(a_{n-1},\ldots,a_0)\boldsymbol{h}\ =\ (a_{(n-1)^\sigma},\ldots,a_{0^\sigma}),\ \ \sigma\ \in\ S(\{0,\ldots,n\ -\ 1\}).$$

Далее, действие -бокса $\hat{s}$ на вектор $\alpha\ =\ (\alpha_{\,d-1},\ldots,\alpha_{\,0})\ \in\ V_m^d$ определяется формулой $\alpha^{\hat{s}}\ =(a_{d-1}^{s},\ldots,a_0^{s})$, поэтому мы рассматриваем $\hat{s}$ как подстановку на V_{n}.

Поскольку каждый вектор $\alpha\ =\ (\alpha_{\,n-1},\ldots,\alpha_{\,1},\alpha_{\,0})\ \in V_n$ можно рассматр- ивать как двоичную запись числа $\tilde{\alpha}\ =\ 2^{n-1}\alpha_{n-1}+\ldots+2\alpha_1+\alpha_0$, мы в работе будем отождествлять вектор α с числом $\tilde{\alpha}$.

Приведем описание алгоритма развертывания ключа шифрсистемы GPRINT. Рассмотрим два подблока

$$k^{(0)} \in V_n, k^{(1)} = \left(k_{d-1}^{(1)}, \ldots, k_0^{(1)}\right) \in V_p^d$$

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 $\hat{p}_{k^{(1)}} : V_n \to V_n$ следующим образом:

$$(\beta_{d-1}, \ldots, \beta_0)^{\hat{p}_{k^{(1)}}} = (\rho_{k_{d-1}^{(1)}}(\beta_{d-1}), \ldots, \rho_{k_0^{(1)}}(\beta_0)),$$

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

$$(\gamma_{m-1}, \ldots, \gamma_0)^{\rho_k} = (\gamma_{(m-1)^{\overline{\rho_k}}}, \ldots, \gamma_{0^{\overline{\rho_k}}}), \overline{\rho_k} \in S(\{0, \ldots, m-1\}).$$

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 $\mathrm{g}_k^{(j)} : V_\mathrm{n} \to V_\mathrm{n}$ имеет вид

$$\alpha^{\mathrm{g}_k^{(j)}} = \left(\left(\alpha \bigoplus k^{(0)}\right)^h \bigoplus c^{(j)}\right)^{\hat{\rho}_{k^{(1)}\hat{s}}}$$

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

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

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

Преобразование ρ_k *для* $k \in V_2$ задается равенством

$$(\beta_2, \beta_1, \beta_0)^{\rho_k} = \begin{cases} (\beta_2, \beta_1, \beta_0), \text{если } k = (0,0) \\ (\beta_1, \beta_2, \beta_0), \text{если } k = (0,1) \\ (\beta_2, \beta_0, \beta_1), \text{если } k = (1,0) \\ (\beta_0, \beta_1, \beta_2), \text{если } k = (1,1) \end{cases}$$

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

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

где $\left(\gamma_5^{(j)}, \ldots, \gamma_0^{(j)}\right) \in V_6, \ j = 1, \ldots, n.$

Заметим, что преобразование ρ_k для любого $k \in V_2$ осуществляет перестановку координат векторов из V_3.

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

Пусть $a(u) = \left(a_{\delta\varepsilon}(u)\right)$ — 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 $\delta, \varepsilon \in V_m$.

Список использованных источников

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.

ӘОЖ 004.056.5

ҚОРҒАНЫС ТҮРЛЕНДІРУЛЕРІНІҢ АЛГЕБРАЛЫҚ АЛГОРИТМДЕРІ

Ануарбеков Алмас Маратович
anuarbekovalmas7@gmail.com
Л.Н.Гумилев атындағы ЕҰУ механика-математика факультетінің криптология мамандығының 1-курс магистранты
Ғылыми жетекшісі – Қозыбаев Д.Х.

Қазіргі әлемде ақпарат қауіпсіздігі өте маңызды рөл атқарады. Хабарлар тасымалданатын байланыс арналары көбінесе қорғалмаған болып келеді және осы арнаға қатынас құру құқығы бар кез келген адам хабарларды қолға түсіре алады. Сондықтан тораптарда ақпаратқа біраз шабуылдар жасау мүмкіндігі бар. Бұзушы - тиым салынған операцияларды қателескендіктен, білместіктен орындауға әрекет жасаған немесе ол үшін саналы түрде әртүрлі мүмкіншіліктерді, әдістерді және құралдарды қолданатын тұлға. Ақпаратты қорғау құралдары- мемлекеттік құпия болып табылатын мәліметтерді қорғауға арналған техникалық, криптографиялық, бағдарламалық және басқа да құралдар, олар жүзеге асырылған құралдар, сондайақпарат қорғаудың тиімділігін бақылау құралдары.

Ақпаратты қорғауды қамтамасыз етудің маңызды механизмдерінің бірі ақпаратты түрлендіру болып табылады. Ақпаратты қорғау алгоритмдерін оңтайландыру мәселелері компьютерлік желілердегі ақпарат ағындарының ұлғаюына әкелетін жад құрылғыларының көлемінің және процессор өнімділігінің жылдам өсуімен сипатталатын қазіргі заманғы компьютерлік техниканың дамуының тұрақты тенденцияларына байланысты маңыздырақ болып отыр. Трансформация алгоритмдерінің ең маңызды параметрлері түрлендірудің тұрақтылығы мен жылдамдығы болып табылады. Қауіпсіздіктің осы деңгейінде ақпаратты қорғау алгоритмдерінің жылдамдығының артуы, әсіресе автоматтандырылған басқару жүйелерінің ішінде бөлінген есептеу желілерінің жұмысын айтарлықтай жақсартуға мүмкіндік береді.

Бұл мәселеге ең математикалық қатал тәсіл криптология шеңберінде. Шеннонның классикалық жұмысына сәйкес оқиғаның ықтималдығы криптограмманың ашу қабілеттілігінің өлшемі ретінде пайдаланылады: «белгілі криптограмманы ескере отырып, ашық мәтіннің таңдалған бағасы шынайы ашық мәтінмен сәйкес келді». Бірақ бұл