СПИСОК ЛИТЕРАТУРЫ:

1. Язык разметки подтверждения безопасности (SAML). URL: http://xml.coverpages.org/saml.html.
2. Безопасность Web-сервисов (WS-Security) рабочей группы OASIS. URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.
3. Подпись XML (XML Signature). URL: http://www.w3.org/TR/xmldsig-core/.
4. Шифрование XML (XML Encryption). URL: http://www.w3.org/TR/xmlenc-core/.
5. *Хейн А. А., Климов В. В.* Задача связи сервис-ориентированного приложения и мобильного устройства // VIII Курчатовская молодежная научная школа. Сборник докладов. М., 2011. Часть 3. С. 166–170.

Г. И. Хоруженко

АНАЛИЗ РЕДУЦИРОВАННОГО АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ PRINT-96 ЛИНЕЙНЫМ МЕТОДОМ И МЕТОДОМ СВЯЗАННЫХ КЛЮЧЕЙ

Алгоритм блочного шифрования PRINT предложен на конференции CHES 2010 в двух вариантах — PRINT-48 и PRINT-96 — в зависимости от размеров блока открытого текста и ключа шифрования [1]. При проектировании авторами алгоритма уделено особое внимание компактности и энергопотреблению его аппаратной реализации. К алгоритму PRINT-48 применены методы линейного и разностного анализа в работах [2–4]. Так, в работе [2] приведены классы слабых ключей алгоритма шифрования PRINT-48, для которых существуют линейные характеристики, позволяющие атаковать 28 раундов. В настоящей работе редуцированный 52-раундовый алгоритм PRINT-96 анализируется линейным методом, аналогичным методу, предложенному в работе [2]. Также предлагается атака на основе метода связанных ключей.

Приведем описание алгоритма шифрования PRINT-96. Пусть ключ шифрования имеет вид $k = \left(k^{(0)}, k^{(1)}\right)$, $k^{(0)} \in V_{96}$, $k^{(1)} \in V_2^{32}$. Пусть также заданы преобразования

$$\hat{s} = \left(\underbrace{s,\ldots,s}_{26}\right), s \in S\left(V_3\right),\ h : V_{96} \to V_{96},\ h\left(\left(\alpha_{95},\ldots,\alpha_0\right)\right) = \left(\alpha_{\sigma(95)},\ldots,\alpha_{\sigma(0)}\right),\ \sigma \in S_{96},$$

$$\hat{\pi}_{k^{(1)}} = \left(\pi_{k_{31}^{(1)}},\ldots,\pi_{k_0^{(1)}}\right),\ \pi_{k_i^{(1)}} \in S\left(V_3\right),\ i \in \{0,\ldots,32\}.$$

Таким образом, раундовая функция для j-го раунда имеет вид

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

где $c^{(j)} \in V_{96}$ — константа, зависящая от номера раунда.

При построении линейных характеристик используется следующее утверждение.

Утверждение 1. Для любого s-бокса $s \in S\left(V_3\right)$ существует такое преобразование ρ: {0,1,2,}→{0,1,2,}, что

$$\left|\left\{\alpha \in V_3 \mid \alpha_i = s\left(\alpha\right)_{\rho(i)}\right\}\right| \neq 2^2,\ i \in \{0,1,2\}.$$

Далее, при построении характеристик s-бокс будем представлять в виде системы координатных функций $f_i^{(s)} : V_3 \to \{0,1\}$, $i \in \{0,1,2\}$, причем $p\left\{f_i^{(s)}(\alpha) = \alpha_{\rho(i)}\right\} \neq \frac{1}{2}$, $i \in \{0,1,2\}$, α выбирается из множества V_3 случайно и равновероятно.

В работе под слабыми ключами относительно линейного анализа будем понимать ключи шифрования, для которых определенные биты ключа $k^{(1)}$ являются фиксированными. Для получения классов слабых ключей максимальной мощности будем рассматривать характеристики, повторяющиеся при шифровании с определенным периодом $t < 32$.

В следующем утверждении описываются классы слабых ключей алгоритма шифрования PRINT-96 относительно линейного анализа. Обозначим $w_l(i)=i-3l(mod96)$, $w_l^{-1}(i)=i+3l(mod96)$.

Утверждение 2. Пусть $i \in \{0,...,95\}$, $r \in \{1,...,32\}$, $l_0,...,l_{r-1} \in Z_{32}$. Пусть также найдутся такие числа $n \in N$, $t_0,...,t_{n-1} \in \{0,...,r-1\}$, что справедливы соотношения

1) $0 \le i^{\sigma\omega_{l_{t_0}}\pi\rho_{k^{(1)}_{l_{t_0}}}\omega^{-1}_{l_{t_0}}...\sigma\omega_{l_{t_{j-1}}}\pi\rho_{k^{(1)}_{l_{t_{j-1}}}}} \le 2, j \in \{1,...,n\}$,

2) $i^{\sigma\omega_{l_{t_0}}\pi\rho_{k^{(1)}_{l_{t_0}}}\omega^{-1}_{l_{t_0}}...\sigma\omega_{l_{t_{n-1}}}\pi\rho_{k^{(1)}_{l_{t_{n-1}}}}\omega^{-1}_{l_{t_{n-1}}}} = i$.

Тогда существует класс слабых ключей алгоритма шифрования PRINT-96 мощности $2^{96+2(32-r)}$.

Отметим также, что классы слабых ключей определяются номерами s-боксов и соответствующих им подстановок $\pi_{k_l(1)}$, используемых при построении характеристик.

Оценка трудоемкости атаки линейным методом, аналогично работе [2], определяется следующим образом. Временная сложность равна $T_1(m)=2^{2(m+1)}$, при этом число необходимых пар открытых текстов и соответствующих им шифртекстов также равно $C_1(m)=2^{2(m+1)}$, где $m \in \{1,...,47\}$ — число атакуемых раундов.

Следовательно, наибольшее число атакуемых раундов достигается при наличии 2^{96} текстов, при этом линейная характеристика удовлетворяет 47 раундам. Для проведения атаки на большее число раундов (в частности, на 52 раунда в настоящей работе) в качестве входных данных для характеристики используются нелинейные соотношения.

Приведенные утверждения распространяются и на обобщенный алгоритм шифрования PRINT с произвольными преобразованиями (σ, s, π). Отметим также, что существуют такие (σ, s, π), что невозможно построить линейную характеристику с периодом $t < 32$, и в этом случае настоящая атака оказывается неприменимой.

Обозначим $\sigma=(1,0,\ ...,0) \in V_{96}$. Приведем разностную характеристику для 2 раундов алгоритма PRINT-96 с использованием пары связанных ключей.

Утверждение 3. Пусть a выбирается случайно и равновероятно из множества V_{96}. Пусть также $k,k' \in V_{96} \times V_2^{32}$, такие, что

$k^{(0)} \oplus k'^{(0)} = \delta$, $k^{(1)}_{31} \in \{(1,0),(0,0)\}$.

Тогда

$p\left\{\alpha^{g^{(j)}_k g^{(j+1)}_k} \oplus (\alpha \oplus \delta)^{g^{(j)}_{k'} g^{(j+1)}_{k'}} = \delta\right\} = 2^{-2},\ j \in \{1,...,96\}$.

На основе утверждения 3 возможно построить разностную характеристику на $m = 2 \cdot j, j \in \{1,...,48\}$ раундов с вероятностью $p(m)=2^{-m}$. Приведем оценку временной сложности атаки методом связанных ключей.

Утверждение 4. Пусть $u, m < 96-3^u \in N$, тогда трудоемкость восстановления 3^u-1 битов ключа шифрования $k^{(0)}$ алгоритма PRINT-96 определяется как $T_2(m)=2^m+2^{3^u-1}$ при наличии $C_2(m)=2 \cdot 2^m$ пар открытых текстов и соответствующих им шифртекстов.

СПИСОК ЛИТЕРАТУРЫ:

1. *Knudsen L., Leander G., Poschmann A., Robshaw M.* PRINTcipher: A Block Cipher for IC Printing // S. Mangard and F-X. Standart, editors. Cryptographic Hardware and Embedded Systems – CHES 2010. Vol. 6225 of Lecture Notes in Computer Science. Springer, 2010. P. 16–32.

2. *Agren M., Johanson T.* Linear Cryptanalysis of PRINTcipher – Trails and Samples Everywhere // Cryptology ePrint Archive. Report 2011/423.

3. *Abdelraheem M., Leander G. and Zenner E.* Differential Cryptanalysis of Round-Reduced PRINTcipher: Computing Roots of Permutations // A. Joux, editor. Fast Software Encryption 2011. Lecture Notes in Computer Science. Springer-Verlag, 2011. P. 1–17.
4. *Karakoc F., Demirci H., Harmanc A.* Combined Differential and Linear Cryptanalysis of Reduced-Round PRINTcipher // Selected Areas in Cryptography – SAC 2011. To be published in Lecture Notes in Computer Science. Springer-Verlag, 2011.

Н. Д. Хынг, В. А. Камаев, А. В. Кизим, Д. В. Быков

РАЗРАБОТКА СИСТЕМЫ ДОКУМЕНТООБОРОТА ВОЛГГТУ

В университетах и конкретнее в университете ВолгГТУ каждый день выполняется множество операций подписи договоров, командировок и других видов документов. Использование электронных документов имеет много преимуществ по сравнению с бумажными документами, таких как снижение затрат бумаги, времени ожидания подписи и др. Поэтому разработка системы документооборота для университета является актуальной задачей.

Система позволяет преподавателям, сотрудникам в нашем университете готовить и подписывать документы. Эта система реализована на основе МАС, снижено время подготовки документов для преподавателей, которые могут подписать документы везде, как дома, так и в университете, во время командировки и даже на улице. Система основана на российских стандартах, соответствует российским законам об электронной цифровой подписи. Система реализована на механизме «клиент – сервер», в ней используется стандарт ГОСТ Р 34.10 – 2001 для подписи документов, ГОСТ 28147-89 для шифровки данных и Американский симметричный стандарт RSA для обмена ключом, поэтому документы абсолютно защищены. Архитектура системы показана на рис. 1.

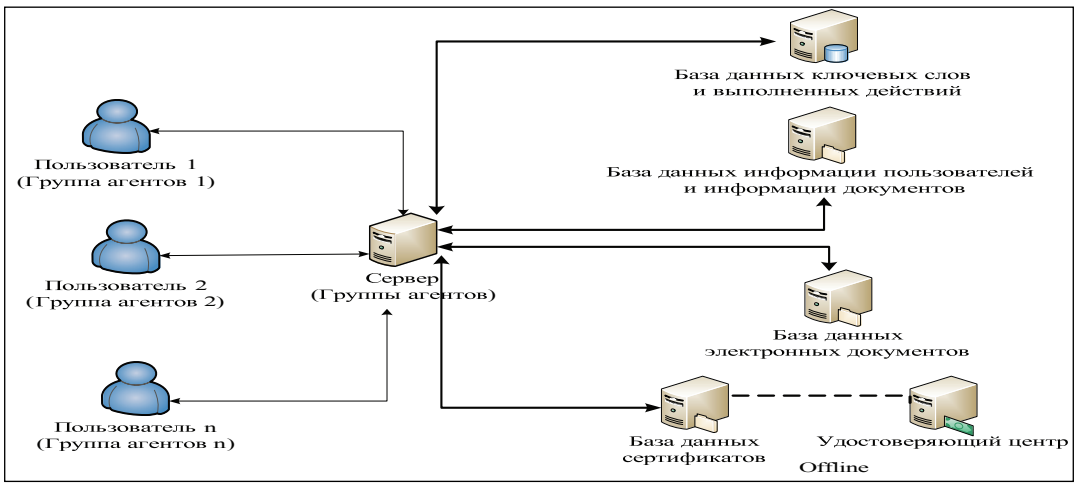

Рис. 1. Архитектура СЭД на основе МАС

Комплекс системы управления электронным документооборотом университета состоит из удостоверяющего центра и программной системы управления электронными документами. Удостоверяющий центр выполняет работу с сертификатами [1]: выпускания, аннулирования сертификатов и др. У каждого пользователя (сотрудник университета) имеется свой сертификат, в котором содержится информация о цифровой подписи владельца. Функциональная структура системы документооборота университета показана на рис. 2.