М. А. Пудовкина, Г. И. Хоруженко

АЛГОРИТМЫ РАЗВЕРТЫВАНИЯ КЛЮЧА БЛОЧНЫХ XSL-ШИФРСИСТЕМ, СТОЙКИЕ ОТНОСИТЕЛЬНО РАЗНОСТНОГО МЕТОДА АНАЛИЗА

Введение

В настоящее время активно развиваются области исследований, связанные с использованием криптографических примитивов в средах с ограниченными ресурсами. Особое внимание уделяется производительности, энергопотреблению, компактности реализации, что зачастую ведет к снижению стойкости относительно известных методов анализа.

В данной работе предлагается метод оценки стойкости XSL-шифрсистем к разностному методу анализа. В качестве примера рассматриваются AES-подобные шифрсистемы с измененным алгоритмом развертывания ключа (АРК), вместо оригинального АРК используется более быстрый и компактный с точки зрения аппаратной реализации.

1. Основные обозначения и определения

Обозначим: N— множество натуральных чисел; V_n — векторное пространство размерности n, $\alpha=(\alpha_{n-1}, ...,\alpha_0)\in V_n$; $\alpha = (\tilde{\alpha}_{d-1}, ...,\tilde{\alpha}_0)\in V_n$, $\tilde{\alpha}_i\in V_m$, $i\in\{0, ..., d-1\}$; S (X) — симметрическая группа, заданная на множестве X; $x\oplus y$ — побитовое сложение векторов $x, y\in V_n$; K — ключевое множество.

Положим $n, m, d, r\in N$, $n = md$, $h\in GL_n(2)$. Пусть $s_i\in S(V_m)$ и $s_i^{(j)}: V_m\to\{0,1\}$ — j-я координатная функция подстановки s_i, $i\in\{0,...,d-1\}$, $j\in\{0,...,m-1\}$. Пусть также $\gamma=(\gamma_{n-1}, ..., \gamma_0)$. Определим s-бокс $s: V_n\to V_n$ как

$$s=(s_{d-1},...,s_0),$$

$$s(\gamma)=\left(s_{d-1}\left(\gamma_{dm-1},..., \gamma_{d(m-1)}\right),...,s_0\left(\gamma_{m-1},...,\gamma_0\right)\right).$$

В настоящей работе рассматривается XSL-шифрсистема A.Длина блока текста шифрсистемы A равна n, ключа шифрования — n', число раундов — r.

Обозначим: $\alpha^{(0)} = (\alpha_{n-1}^{(0)}, ..., \alpha_0^{(0)})\in V_n$ — блок открытого текста; $\alpha^{(i)}\in V$ — блок промежуточного шифртекста; $k\in V_{n'}$ — ключ шифрования, $k^{(i)}\in V_n$ — раундовый ключ. Определим раундовую функцию $g_{k^{(i)}}: V_n\to V_n$ следующим образом

$$\alpha^{(i)} = g_{k^{(i)}}^{(A)}\left(\alpha^{(i-1)}\right)= h\left(s\left(\alpha^{(i-1)}\oplus k^{(i)}\right)\right),$$

где i — номер раунда $i\in\{1,\dots,r\}$.

Функция зашифрования $f_k: V_n\to V_n$ имеет вид $f_k=\prod_{i=1}^{r} g_{k^{(i)}}$.

Алгоритм развертывания ключа задан следующим образом:

$$k^{(i)} = k\mathbf{a}_i\oplus c_i,$$

где $\mathbf{a}_i$ — матрица размера $n\times n'$ над полем $GF(2)$, c_i — константа, зависящая от номера раунда, $c_i\in V_n$, $i\in\{1,\dots,r\}$.

Определим также функции $f_k^{(i,j)}=\prod_{t=i}^{j} g_{k^{(t)}}$ и $f'^{(i,j)}_{(k'^{(i)},...,k'^{(j)})}=\prod_{t=i}^{j} g_{k'^{(t)}}$, $k'^{(t)}\in V_n$, $t\in\{i,...,j\}$.

Отметим, что в данной работе оценка стойкости относительно линейного и разностного анализа проводится в предположении независимости раундовых ключей [1].

2. Разностный метод анализа

Разностный метод анализа предложен в работе [2]. Основная идея заключается в применении разностных характеристик шифрсистемы для вычисления битов раундовых ключей. В настоящем разделе рассматривается атака из оригинальной работы [2].

Пусть $\alpha^{(i)} \in_U V_n$ — промежуточный шифртекст шифрсистемы A, выбранный случайно и равновероятно, $\delta^{(t)} \in V_n$, $t \in \{i,..., j\}$, $\alpha'^{(i)} = \alpha^{(i)} \oplus d^{(i)}$. Под разностной характеристикой δ шифрсистемы A будем пониматьупорядоченный набор пар вида

$$d = \left(\left(\delta^{(i)}, p^{(i)}\right), \left(\delta^{(i+1)}, p^{(i+1)}\right) ..., \left(\delta^{(j)}, p^{(j)}\right)\right),$$

где

$$p^{(t)} = P\left\{\delta^{(t)} = f_k^{(t-1,t)}\left(\alpha^{(i)}\right) \oplus f_k^{(t-1,t)}\left(\alpha'^{(t-1)}\right)\right\}.$$

В работе будем рассматривать нетривиальные разностные характеристики, для которых справедливо соотношение $\prod_{t=i}^{j} p^{(t)} < 1$. Отметим, что в случае $\prod_{t=i}^{j} p^{(t)} = 1$ можно отличить шифрсистему от случайной подстановки, однако эта атака не рассматривается в настоящей работе.

Приведем описание атаки из работы [2] в обозначениях, принятых в настоящей работе. Атака состоит из двух этапов. На первом этапе определяется множество пар открытых и соответствующих им шифртекстов, для которых справедлива заданная разностная характеристика. На втором этапе восстанавливается часть ключа шифрования.

Обозначим $u(d) = \min\limits_{t \in \{0,...,r\}} \left\{t \mid \left(p^{(t)} < 1\right) \vee \left(p^{(r-t)} < 1\right)\right\}$. В зависимости от свойств разностной характеристики при атаке на шифрсистему возможны два случая: $u(d) = 0$ и $u(d) > 0$.

Рассмотрим случай $u(d) = 0$. При этом справедлив алгоритм, приведенный в работе [3]. Приведем алгоритм атаки на основе разностного метода анализа в случае $u(d) = 0$.

Алгоритм 1. *Атака на основе разностного метода анализа в случае* $u(d) = 0$.

Вход: d — разностная характеристика, Θ — множество пар открытых и соответствующих им шифртекстов вида

$$\theta = \left(\left(\alpha^{(0)}, \alpha^{(0)} \oplus \delta^{(0)}\right), \left(f_k\left(\alpha^{(0)}\right), f_k\left(\alpha^{(0)} \oplus \delta^{(0)}\right)\right)\right).$$

Этап 1. *Построение множества пар открытых и соответствующих им шифртекстов, удовлетворяющих разностной характеристике.*

1. Положить $\Lambda := \varnothing$.

2. Для всех $\theta \in \Theta$ выполнить:

2.1. Если $f_k\left(\alpha^{(0)}\right) \oplus f_k\left(\alpha^{(0)} \oplus \delta^{(0)}\right) = \delta^{(r)}$, то положить $\Lambda := \Lambda \cup \{\theta\}$.

Этап 2. *Восстановление битов ключа шифрования.*

1. Положить $H := \varnothing$.

2. Для всех $i \in \{0,..., d-1\}, \tilde{k} \in V_m$ положить $\lambda_{\tilde{k}}^{(i)} := 0$.

3. Для всех $i \in \{0,..., d-1\}$ выполнить:

3.1. Если $\tilde{\delta}_i^{(r)} \neq (0,...,0)$, то для всех $\tilde{k} \in V_m$ и $\theta \in \Lambda$ выполнить:

3.1.1. Положить $k := \left(0,...,0,\tilde{k},\underbrace{0,...,0}_{i}\right)$.

3.1.2. Если выполнено соотношение

$$\left(f_\kappa^{(r-1,r)}\right)^{-1}\left(f_k^{(0,r)}\left(\alpha^{(0)}\right)\right) \oplus \left(f_\kappa^{(r-1,r)}\right)^{-1}\left(f_k^{(0,r)}\left(\alpha^{(0)} \oplus \delta^{(0)}\right)\right) = \delta^{(r-1)},$$

то положить $\lambda_{\tilde{\kappa}}^{(i)} := \lambda_{\tilde{\kappa}}^{(i)} + 1$.

3.2. Положить $H := H \cup \left\{\left(\left\{\tilde{\kappa} \mid \lambda_{\tilde{\kappa}}^{(i)} = \max\limits_{\tilde{\kappa} \in V_m}\left\{\lambda_{\tilde{\kappa}}^{(i)}\right\}\right\}, i\right)\right\}$.

Выход: множество H кандидатов в раундовый ключ $k^{(r)}$.

Трудоемкость атаки при использовании заданной разностной характеристики $T_d^{(0)}$ оценивается как

$$T_d^{(0)} \leq 2 \cdot |\Theta| + 2 \cdot d2^m + 2^{n_0^{(0)}}$$

операций шифрования, где $n_0^{(0)}$ — количество битов ключа шифрования, которые не удалось восстановить с помощью описанной атаки. Вероятность успеха при этом оценивается, например,

по формуле, представленной в работе [3]. В настоящей работе оценка стойкости к разностному анализу проводится исключительно исходя из трудоемкости атаки.

Отметим, что использование разностной характеристики d шифрсистемы A для атаки возможно, если выполнено следующее соотношение:

$$\forall t \in [0, r]: p^{(t)} \in \left(2^{-n}, 1\right]. \qquad (1)$$

В утверждении 1 доказывается, что трудоемкость восстановления ключа шифрования в первом случае будет всегда меньше трудоемкости атаки методом полного перебора, независимо от АРК.

Утверждение 1. *Пусть существует такая разностная характеристика*

$$d = \left(\left(\delta^{(0)}, p^{(0)}\right), \left(\delta^{(1)}, p^{(1)}\right) \ldots, \left(\delta^{(r)}, p^{(r)}\right)\right)$$

шифрсистемы A, что выполнено условие (1) и $u(d) = 0$. *Тогда трудоемкость восстановления ключа шифрования разностным методом оценивается как* $T_d < 2^{n'}$.

Доказательство следует из описания алгоритма 1.

Рассмотрим случай $u(d) > 0$. В утверждении 2 доказана невозможность различения ложных и истинных битов ключа на основе разностей $\delta^{(0)} \to \delta^{(1)}$ и $\delta^{(r-1)} \to \delta^{(r)}$ в этом случае.

Утверждение 2.*Пусть для разностной характеристики* d *справедливо соотношение* $p^{(0)} = p^{(r)} = 1$. *Тогда в результате выполнения алгоритма 1 будут получены значения* $\lambda_{\tilde{\kappa}}^{(i)}$, *для которых справедливо соотношение*

$$\lambda^{(i)}_{(0,\ldots,0,0)} = \lambda^{(i)}_{(0,\ldots,0,1)} = \ldots = \lambda^{(i)}_{(1,\ldots,1,1)} = |\Theta|.$$

Доказательство. Рассмотрим векторы $\tilde{k}, \tilde{k}' \in V_m$, которым исходя из описания алгоритма 1 ставятся в соответствие раундовые ключи шифрования $k, k' \in V_n$. Поскольку $p^{(r)} = 1$, то для любых векторов $\alpha^{(r)}$, $\kappa \in V_n$ справедливо соотношение

$$\left(f_\kappa^{(r-1,r)}\right)^{-1}\left(\alpha^{(r)}\right) \oplus \left(f_\kappa^{(r-1,r)}\right)^{-1}\left(\alpha^{(r)} \oplus \delta^{(r)}\right) = \delta^{(r-1)}$$

Следовательно, для любых $\tilde{k}, \tilde{k}' \in V_n$ верны равенства:

$\lambda^{(i)}_{\tilde{\kappa}} = \lambda^{(i)}_{\tilde{\kappa}'}$, $\lambda^{(i)}_{\tilde{\kappa}} = |\Theta|$

и справедливо соотношение

$\lambda^{(i)}_{(0,\ldots,0,0)} = \lambda^{(i)}_{(0,\ldots,0,1)} = \ldots = \lambda^{(i)}_{(1,\ldots,1,1)} = |\Theta|$.

Утверждение доказано.

Для восстановления битов ключа в этом случае необходимо использовать другие разности – $\delta^{(u(d))}$ или $\delta^{(r-u(d))}$, следовательно,значения промежуточных шифртекстов $\alpha^{(u(d))}$ или $\alpha^{(r-u(d))}$ необходимо вычислить.Для этого при проведении атаки опробуются необходимые биты раундовых ключей. Приведем алгоритм 2 атаки на основе разностного метода анализа в случае $u(d) > 0$.

Алгоритм 2.*Атака на основе разностного метода анализа в случае* $u(d) > 0$.

Вход: d – разностная характеристика, Θ – множество пар открытых и соответствующим им шифртекстов вида

$$\theta = \left(\left(\alpha^{(0)}, \alpha^{(0)} \oplus \delta^{(0)}\right), \left(f_k\left(\alpha^{(0)}\right), f_k\left(\alpha^{(0)} \oplus \delta^{(0)}\right)\right)\right)$$

Этап 1. *Построение множества пар открытых и соответствующих им шифртекстов, удовлетворяющих разностной характеристике.*

3. Положить $\Lambda := \varnothing$.

4. Для всех $\theta \in \Theta$ выполнить:

4.1. Если $f_k\left(\alpha^{(0)}\right) \oplus f_k\left(\alpha^{(0)} \oplus \delta^{(0)}\right) = \delta^{(r)}$, то положить $\Lambda := \Lambda \cup \{\theta\}$.

Этап 2. *Восстановление битов ключа шифрования.*

4. Положить $H := \varnothing$.

5. Для всех $i \in \{0,\ldots,d-1\}, \kappa^{(i)} \in K^{(\delta^{(i)})}$ положить $\lambda_{\kappa^{(i)}}^{(i)} := 0$.

6. Для всех $i \in \{0,\ldots,d-1\}$ выполнить:

6.1. Если $\tilde{\delta}_i^{(r-u(d))} \neq (0,\ldots,0)$, то для всех $\kappa^{(i)} \in K^{(\delta^{(i)})}$ и $\theta \in \Lambda$ выполнить:

6.1.1. Если выполнено соотношение

$$\left(f_{\kappa^{(i)}}^{(r-u(d),r)}\right)^{-1}\left(f_k^{(0,r)}\left(\alpha^{(0)}\right)\right) \oplus \left(f_{\kappa^{(i)}}^{(r-u(d),r)}\right)^{-1}\left(f_k^{(0,r)}\left(\alpha^{(0)} \oplus \delta^{(0)}\right)\right) = \delta^{(r-d(u)-1)},$$

то положить $\lambda_{\kappa^{(i)}}^{(i)} := \lambda_{\kappa^{(i)}}^{(i)} + 1$.

6.2. Положить $H := H \cup \left\{\left(\left\{\kappa^{(i)} \mid \lambda_{\kappa^{(i)}}^{(i)} = \max_{\kappa^{(i)} \in K^{(\delta^{(i)})}} \left\{\lambda_{\kappa^{(i)}}^{(i)}\right\}\right\}, i\right)\right\}$.

Выход: множество H.

Трудоемкость атаки при использовании заданной разностной характеристики $T_d^{(1)}$ оценивается как

$$T_d^{(1)} = 2 \cdot |\Theta| + \sum_{i=0}^{d-1} \left|K^{(\delta^{(i)})}\right| + 2 \cdot d 2^m + 2^{n_0^{(1)}}$$

операций шифрования, где $n_0^{(1)}$ — количество битов ключа шифрования, которые не удалось восстановить с помощью описанной атаки. Вероятность успеха вычисляется аналогично случаю $u(d) = 0$.

Отметим, что в данном случае трудоемкость атаки, в отличие от предыдущего случая, определяется в том числе и свойствами АРК. В утверждении 3 приводятся условия для АРК, разностной характеристики и параметров шифрсистемы, при которых трудоемкость $T_d^{(1)}$ атаки на основе разностного метода больше наперед заданного значения T_0.

Утверждение 3. *Пусть для любого* $\tilde{\delta}_j^{(r-u(d))} \in V_m$ *справедливо соотношение*

$$\left|B_{im}\left(f_k^{(r-u(d),r)}\right) \cup B_{im+1}\left(f_k^{(r-u(d),r)}\right) \cup \ldots \cup B_{(i+1)m}\left(f_k^{(r-u(d),r)}\right)\right| \geq \log_2 T_0,$$

тогда

$T_d^{(1)} > T_0$.

Доказательство. Рассмотрим произвольную разность $\tilde{\delta}_j^{(r-u(d))}$. Мощность множества $K^{(\delta^{(i)})}$ определяется из соотношения

$$\left|K^{(\delta^{(i)})}\right| = 2^{\left|B_{im}\left(f_k^{(r-u(d),r)}\right) \cup B_{im+1}\left(f_k^{(r-u(d),r)}\right) \cup \ldots \cup B_{(i+1)m}\left(f_k^{(r-u(d),r)}\right)\right|}.$$

В силу произвольности выбора разности $\tilde{\delta}_j^{(r-u(d))}$ имеем

$$T_d^{(1)} > \left|K^{(\delta^{(r-u(d))})}\right| \geq T_0.$$

Утверждение доказано.

Вследствие отсутствия на данный момент подхода, позволяющего строить множество разностных характеристик для заданной шифрсистемы и реализуемого на практике, предлагается для противодействия атакам на основе разностного метода оценить необходимое число раундов и вследствие этого не накладывать ограничений на АРК.

В настоящей работе предлагается оценивать необходимое число раундов $r_{\max}$ на основе минимального числа активных s-боксов для заданного числа раундов. Далее приводятся соответствующие оценки $r_{\max}$ для некоторых AES-подобных шифрсистем.

3. Построение АРК для AES-подобных шифрсистем

Предложенные методы оценки стойкости АРК относительно линейного [4] и разностного методов анализа применены к двум типам АРК (АРК-1 и АРК-2)для шифрсистем AES, SQUARE, CRYPTON. Для описываемых далее АРК положим $n' = n$.

АРК первого типа задаются следующими соотношениями:

$k^{(1)} = k \oplus c^{(1)}$,

$k^{(i+1)} = h\left(k^{(i)}\right) \oplus c^{(i+1)}, i \in \{1,...,r-1\}$.

АРК-1 представляет интерес с точки зрения оптимизации аппаратной реализации алгоритма шифрования, поскольку в данном случае линейное преобразование, используемое в раундовой функции, также применяется и для вычисления раундовых ключей.

Пусть $l \in \left\{1,...,\left\lfloor \frac{n}{8} \right\rfloor - 1\right\}$. АРК второго типа задается следующими соотношениями:

$k^{(i)} = \left(k_{(n-1+8li) \bmod n},...,k_{(1+8li) \bmod n}, k_{(8li) \bmod n}\right) \oplus c^{(i)}, i \in \{1,...,r\}$.

АРК-2 представляет интерес с точки зрения оптимизации как аппаратной реализации, так и программной реализации, поскольку в основе имеет вычислительно простую операцию циклического сдвига.

В таблице 1 представлены результаты оценки стойкости шифрсистем с описанными АРК к линейному и разностному методам анализа.

Таблица 1. Оценка стойкости AES-подобных шифрсистем с АРК-1 и АРК-2

Алгоритм шифрования	Разностный анализ, $r_{\max}$	АРК-1	АРК-2
AES	4	+	$l \in \{3,5,11,13\}$
SQUARE	4	+	$l \in \{2,6,14\}$
CRYPTON	4	+	$l \in \{2,8,11\}$

В результате проведенных экспериментов установлено, что указанные в таблице AES-подобные шифрсистемы являются стойкими относительно линейного и разностного алгоритмов шифрования для числа раундов $r \geq 4$ при использовании АРК-1, а также при использовании АРК-2 для определенных значений параметра l.

СПИСОКЛИТЕРАТУРЫ:

1. *Knudsen L.* Practically secure Feistel cipher // Vol 809 of Lecture Notes in Computer Science. Springer, 1994. P. 211–221.
2. *Biham E., Shamir A.* A Differential Cryptanalysis of the Data Encryption Standard // Springer-Verlag, 1993.
3. *Selcuk A. A.* On Probability of Success in Linear and Differential Cryptanalysis // Journal of Cryptology. 2008. №1 Vol. 21. P. 131–147.
4. *Хоруженко Г. И.* Алгоритмы развертывания ключа блочных XSL-шифрсистем, стойкие относительно линейного метода анализа // Системы высокой доступности. 2013. Т. 3 (в печати).

REFERENCES:

1. *Knudsen L.* Practically secure Feistel cipher // Vol 809 of Lecture Notes in Computer Science. Springer, 1994. P. 211–221.
2. *Biham E., Shamir A.* A Differential Cryptanalysis of the Data Encryption Standard // Springer-Verlag, 1993.
3. *Selcuk A. A.* On Probability of Success in Linear and Differential Cryptanalysis // Journal of Cryptology. 2008. №1 Vol. 21. P. 131–147.
4. *KhoruzhenkoG. I.*AlgoritvyrazvertyvaniaykluychablochnikhXSL-chifrsistem, stoiykieotnosatel`nolineynogometodaanaliza // Sistemyvysokoydostupnosti. 2013. T. 3 (v pechati).