ПОСТРОЕНИЕ ВЕРХНИХ ОЦЕНОК СРЕДНИХ ВЕРОЯТНОСТЕЙ ЦЕЛОЧИСЛЕННЫХ ДИФФЕРЕНЦИАЛОВ ДЛЯ РАУНДОВЫХ ФУНКЦИЙ ОПРЕДЕЛЕННОЙ СТРУКТУРЫ

Н. В. Кучинская, Л. В. Ковальчук, Л. В. Скрыпник

Институт специальной связи и защиты информации НТУУ «КПИ»
Киев, Украина
E-mail: n.kuchinska@gmail.com

Получены верхние оценки средних вероятностей целочисленных дифференциалов для раундовых функций в случае нетривиального блока подстановки и оператора сдвига определенной структуры.

Ключевые слова: блочный шифр, разностный криптоанализ, целочисленные дифференциалы.

ВВЕДЕНИЕ

Большинство современных блоковых шифров (AES [1], ГОСТ 28147 [2], «Калина» [3], «Мухомор» [4]) содержат в своей структуре композицию ключевого сумматора, блока подстановки и оператора перестановки, линейного над полем F_2 или его некоторым расширением. Поэтому задача оценивания стойкости таких шифров к линейному, билинейному и различным модификациям разностного криптоанализа [5–10] или сводится к задаче построения верхних оценок средних вероятностей таких композиций, или содержит ее как подзадачу. Последняя полностью решена в следующих случаях:

- если в ключевом сумматоре реализована операция побитового сложения, и при этом входные и выходные разности в раундовом дифференциале рассматриваются относительно этой же операции (см. библиографию, приведенную в работах [5, 7]);

- если в ключевом сумматоре реализована операция сложения по модулю 2^n, а входные и выходные разности в раундовом дифференциале рассматриваются относительно операции побитового сложения [5–10];
- если в ключевом сумматоре реализована операция сложения по модулю 2^n, входные и выходные разности рассматриваются относительно этой же операции (такой дифференциал называют целочисленным [11, 12]), и при этом либо отсутствует оператор перестановки [6], либо отсутствует блок подстановки и оператор перестановки является оператором циклического сдвига [13];
- если в ключевом сумматоре реализована либо операция побитового сложения, либо операция сложения по модулю 2^n, блок подстановки является произвольным, а оператор перестановки является оператором циклического сдвига (величина сдвига взаимнопроста с длиной входа s-блока).

Однако вопрос о построении верхних оценок средних вероятностей целочисленных дифференциалов остается открытым в случае нетривиальных блока подстановки и произвольного оператора перестановки. В данной работе решается задача построения верхних оценок средних вероятностей целочисленных дифференциалов отображений, которые являются композициями сумматора, блока подстановки и оператора циклического сдвига, в случае, когда величина сдвига пропорциональна длине входа *s*-блока.

ПОСТРОЕНИЕ ВЕРХНИХ ОЦЕНОК ВЕРОЯТНОСТЕЙ ЦЕЛОЧИСЛЕННЫХ РАУНДОВЫХ ДИФФЕРЕНЦИАЛОВ

Введем следующие обозначения: $(\forall n \in N)$: $V_n = \{0,1\}^n$ множество n-мерных битовых векторов. Вектора из V_n однозначно соответствуют целым числам от 0 до $2^n - 1$, $n \in N$. Пусть $n = pu$, $p \geq 2$, тогда $(\forall x \in V_n)$: $x = (x^{(p)},...,x^{(1)})$, $x^{(i)} \in V_u$, $i = \overline{1,p}$. Рассмотрим биективное отображение $S : V_n \to V_n$, такое , что $\forall x \in V_n$: $S(x) = (s^{(p)}(x^{(p)}),...,s^{(1)}(x^{(1)}))$, $x^{(i)} \in V_u, i = \overline{1,p}$, где $s^{(i)} : V_u \to V_u$, $i = \overline{1,p}$ – биективные отображения. Такое отображение часто называют блоком подстановки, а отображения $s^{(i)}$ – s-блоками. Обозначим $L_{tu} : V_n \longrightarrow V_n$ отображение сдвига влево на tu бит вектора из V_n, $1 \leq t \leq p-1$. На множестве V_n можно определить следующие подмножества [14]:

$$\Gamma_{tu}(\gamma) = \{\beta \in V_n \mid \exists k \in V_n : L_{tu}(k+\gamma) - L_{tu}(k) = \beta\};$$

$$\Gamma_{tu}^{-1}(\beta) = \{\gamma \in V_n \mid \exists k \in V_n : L_{tu}(k+\gamma) - L_{tu}(k) = \beta\}.$$

Для произвольной функции $F : V_n \times V_n \longrightarrow V_n$ обозначим $F_k(x) := F(k,x)$, $k, x \in V_n$.

В данной работе мы будем рассматривать отображения, которые являются композицией ключевого сумматора, блока подстановки и оператора циклического сдвига: $F_k(x) = L_{tu}(S(x \dotplus k))$. Следуя из определения (например, [7]), средняя (по ключам) вероятность целочисленного дифференциала для отображения $F_k(x)$ будет иметь вид

$$2^{-2n} \sum_{x,k \in V_n} \delta(F_k(x+\alpha) - F_k(x), \beta) = 2^{-2n} \sum_{x,k \in V_n} \delta(L_{tu}(S(x+k+\alpha)) - L_{tu}(S(x+k)), \beta).$$

После выполнения замены переменной $x+k$ на k получим

$$2^{-2n}\sum_{x,k\in V_n}\delta(F_k(x+\alpha)-F_k(x),\beta)=2^{-n}\sum_{k\in V_n}\delta(L_{tu}(S(k+\alpha))-L_{tu}(S(k)),\beta)=$$

$$=2^{-n}\sum_{k\in V_n}\left\{\sum_{\gamma\in V_n}\delta(L_{tu}(S(k)+\gamma)-L_{tu}(S(k),\beta)\times\delta(S(k+\alpha)-S(k),\gamma)\right\}\le$$

$$\le 2^{-n}\sum_{k\in V_n}\sum_{\gamma\in\Gamma_{tu}^{-1}(\beta)}\delta(S(k+\alpha)-S(k),\gamma),$$

поскольку $\delta(L_m(S(k)+\gamma)-L_m(S(k)),\beta)\le 1$.

Воспользуемся леммой 1 из [14] и результатами, представленными в [13], для $\forall tu\in N$, $\forall\beta\in V_n$, $\beta=q\cdot 2^{n-tu}+r$, где $0\le r\le 2^{n-tu}-1$, $0\le q\le 2^{tu}-1$, выполняется следующее соотношение между множествами:

$$\Gamma_{tu}{}^{-1}(\beta)=\Gamma_{n-tu}(\beta)\subset\{\gamma,\gamma+1,\gamma-2^{n-tu},\gamma-2^{n-tu}+1\}=\{\gamma_1,\gamma_2,\gamma_3,\gamma_4\},$$

где $\gamma=\gamma(\beta)=q+r\cdot 2^{tu}=q+\beta\cdot 2^{tu}$. В частности, $|\Gamma_{tu}{}^{-1}(\beta)|\le 4$.

Тогда $\gamma_1=q+r\cdot 2^{tu}$, $\gamma_2=q+1+r\cdot 2^{tu}$, $\gamma_3=q+r\cdot 2^{tu}-2^{n-tu}$, $\gamma_4=q+1+r\cdot 2^{tu}-2^{n-tu}$.
Таким образом,

$$2^{-2n}\sum_{x,k\in V_n}\delta(F_k(x+\alpha)-F_k(x),\beta)\le 2^{-n}\sum_{k\in V_n}\sum_{i=1}^{4}\delta(S(k+\alpha)-S(k),\gamma_i).$$

Рассмотрим случай t =1 (величина сдвига влево равна длине входа s-блока). Для произвольного $x\in V_n$, $x=(x^{(p)},...,x^{(1)})$, $x^{(i)}\in V_u$, $i=\overline{1,p}$, и для введенного ранее отображения $S:V_n\ -\ V_n$ обозначим $\widetilde{x}=(x^{(p)},...,x^{(2)})\in V_{n-u}$;

$$\widetilde{S}:V_{n\text{-}u}\to V_{n\text{-}u},\ \text{где}\ \widetilde{S}(\widetilde{x})=(s^{(p)}(x^{(p)}),...,s^{(2)}(x^{(2)})).$$

Тогда $x=(\tilde{x},x^{(1)})$, $\alpha=(\tilde{\alpha},\alpha^{(1)})$, и соответственно для $0\le q<2^u-1$, $\alpha^{(1)}\ne 0$,
$\gamma_1=(\tilde{\gamma}_1,\gamma_1^{(1)})=(r,q)$, $\gamma_2=(r,q+1)$, $\gamma_3=(r-2^{n-2u},q)$, $\gamma_3=(r-2^{n-2u},q+1)$ и справедлива следующая оценка:

$$2^{-n}\sum_{k\in V_n}\sum_{i=1}^{4}\delta(S(k+\alpha)-S(k),\gamma_i)\le\max_{\alpha^{(1)},q\in V_u\setminus\{0\}}2^{-u}\sum_{k^{(1)}\in V_u}(\delta(S_1(k^{(1)}+\alpha^{(1)})-S_1(k^{(1)}),q)+$$

$$+\delta(S_1(k^{(1)}+\alpha^{(1)})-S_1(k^{(1)}),q+1)).\qquad(1)$$

Заметим, что в случае t =1, если $q=2^u-1$, $\alpha^{(1)}\ne 0$,
$\gamma_1=(\widetilde{\gamma}_1,\gamma_1^{(1)})=(r,2^u-1)$, $\gamma_2=(r+1,0)$, $\gamma_3=(r-2^{n-2u},2^u-1)$, $\gamma_3=(r-2^{n-2u}+1,0)$,
справедлива оценка

$$2^{-n}\sum_{k\in V_n}\sum_{i=1}^{4}\delta(S(k+\alpha)-S(k),\gamma_i)\le\max_{\substack{\alpha\in V_u\setminus\{0\}\\ q=2^u-1}}2^{-u}\sum_{k^{(1)}\in V_u}\delta(S_1(k^{(1)}+\alpha^{(1)})-S_1(k^{(1)}),q).\qquad(2)$$

Заметим, что для случая $\alpha^{(1)}=0$ построены верхние оценки средних вероятностей и проведены статистические исследования в [14].

Рассмотрим случай $t=p-1$, $p>2$, $0\le r\le 2^u-1$, $0\le q\le 2^{(p-1)u}-1$. Для произвольного $x\in V_n$, $x=(x^{(p)},...,x^{(1)})$, $x^{(i)}\in V_u$, $i=\overline{1,p}$, и для введенного ранее ото-

бражения $S: V_n \longrightarrow V_n$ обозначим $\tilde{\tilde{x}} = (x^{(p-1)},...,x^{(1)}) \in V_{n-u}$; $\tilde{\tilde{S}}: V_{n-u} \to V_{n-u}$, где $\tilde{\tilde{S}}(\tilde{\tilde{x}}) = (s^{(p-1)}(x^{(p-1)}),...,s^{(1)}(x^{(1)}))$. Можем записать $x = (x^{(p)}, \tilde{\tilde{x}})$, $\alpha = (\alpha^{(p)}, \tilde{\tilde{\alpha}})$, и соответственно для $\gamma_1 = q + r \cdot 2^{(p-1)u}$, $\gamma_2 = q + 1 + r \cdot 2^{(p-1)u}$, $\gamma_3 = q + r \cdot 2^{(p-1)u} - 2^u$, $\gamma_4 = q + 1 + r \cdot 2^{(p-1)u} - 2^u$, $\alpha^{(p)} \neq 0$ и $0 \le q < 2^{(p-1)u} - 1$, выполняется неравенство:

$$2^{-n} \sum_{k \in V_n} \sum_{i=1}^{4} \delta(S(k+\alpha) - S(k), \gamma_i) \le$$

$$\le \max_{\substack{\alpha^{(p)}, r \in V_u \setminus \{0\} \\ v,\tau,\varepsilon \in \{0,1\}}} 2^{-u} \sum_{k^{(p)} \in V_u} (2)^{-|\varepsilon(q)|} \Big\{ \delta(S_p(k^{(p)} + \alpha^{(p)} + v) - S_p(k^{(p)}) - \tau, r) + \tag{4}$$

$$+ \delta(S_p(k^{(p)} + \alpha^{(p)} + v) - S_p(k^{(p)}) - \tau, r - \varepsilon(q)) \Big\}$$

$$\varepsilon(q) = \begin{cases} 0, & 2^u \le q \le 2^{(p-1)u} - 1 \\ 1, & 0 \le q \le 2^u - 1 \\ -1, & q = 2^{(p-1)u} - 1, \tilde{\tilde{\alpha}} = 0 \end{cases}, \qquad v(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) = \begin{cases} 0, \tilde{\tilde{k}} + \tilde{\tilde{\alpha}} < 2^{(p-1)u} \\ 1, \textit{иначе} \end{cases}$$

$$\text{и } \tau(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) = \begin{cases} 0, S(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) < S(\tilde{\tilde{k}}) \\ 1, \textit{иначе} \end{cases}.$$

В результате статистических исследований распределений полученных параметров для 8-битных s-блоков, в частности, были найдены подстановки с наименьшими возможными значениями данных параметров. Например, исходя из полученных результатов, верхние оценки средних вероятностей целочисленных раундовых дифференциалов отображения, при надлежащем выборе s-блоков, могут принимать значения не более 0.035 в случае (1) и не более 0.015 в случае (2).

Полученные результаты позволяют строить верхние оценки средних вероятностей целочисленных разностных характеристик блоковых шифров, в структуру которых входят указанные отображения. При этом средняя вероятность разностной характеристики будет зависеть как от количества раундов, так и от свойств блока подстановки, и наличия дополнительных преобразований в раунде.

Следует заметить, что открытым остается вопрос о влиянии на величину вероятности дифференциала наличия дополнительных преобразований в раунде.

ЛИТЕРАТУРА

1. National Institute of Standards and Technology: The Advanced Encryption Standard (AES). Режим доступа: http://csrc.nist.gov/aes/.

2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Госстандарт СССР, 1989. 28 с.

3. *Горбенко, И. Д.* Перспективний блоковий шифр «Калина» – основні положення та специфікація / Горбенко И. Д., Тоцький О. С., Казьміна С. В. // Прикладна радіоелектроніка. 2007. Т. 6, № 2. С. 195–208.

4. *Горбенко, И. Д.* Перспективний блоковий шифр «Мухомор» – основні положення та специфікація / И. Д. Горбенко, М. Ф. Бондаренко [та ін.] // Прикладна радіоелектроніка. 2007. Т. 6, № 2. С. 147–157.

5. *Kovalchuk, L.* Upper Bounds of Maximum Value of Average Differential and Linear Characteristic Probabilities of Feistel Cipher with Adder Modulo 2^n / L. Kovalchuk, A. Alekseyshuk // Theory of Stochastic Processes. 2006. Vol. 12(28). № 1, 2. P. 20–32.

6. *Ковальчук, Л. В.* Верхние оценки средних вероятностей дифференциальных аппроксимаций булевых отображений/Ковальчук Л. В//Тр. Четвертой Общерос. науч. конф. «Математика и безопасность информационных технологий» (МаБИТ-05), 2–3 ноября 2005. С.163–167.

7. *Ковальчук, Л. В.* Обобщенные марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа / Л. В. Ковальчук // Тр. Пятой Общерос. науч. конф. «Математика и безопасность информационных технологий». (МаБИТ-06), 25–27 октября 2006. С. 595–599.

8. *Олексійчук, А. Н.* Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу / А. Н. Олексійчук, Л. В. Ковальчук, С. В. Пальченко // Захист інформації. 2007. № 2. С. 12–23.

9. *Алексейчук, А.* Оценки практической стойкости блочного шифра «Калина» относительно разностного, линейного билинейного методов криптоанализа / А. Алексейчук, Л. Ковальчук, А. Шевцов, Л. Скрыпник // Тр. Седьмой Общерос. науч. конф. «Математика и безопасность информационных технологий». (МаБИТ-08), 30 октября – 2 ноября 2008. С. 15–20.

10. *Алексейчук, А.* Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах / А. Алексейчук, Л. Ковальчук, Е. Скрынник, А. Шевцов// Прикладная радиоэлектроника. 2008. № 1. С. 203–210.

11. *Wang, X.* How to Break MD5 and Other Hash Functions /X. Wang, H. Yu // Advances in Cryptology EUROCRYPT'05, Lectures Notes in Computer Science 3494, Springer-Verlag, 2005. P. 19–35.

12. *Cotini, S.* Security of the RC6^{TM} Block Cipher /S. Cotini, R. L. Riverst, M. J. B. Robshaw, Y. Lisa Yin // http//www.rsasecurity.com/rsalabs/rc6/.

13. *Berson, T. A.* Differential cryptanalysis mod 2^{32} with applications to MD5/ T. A. Berson // Advanced in Cryptology. – CRYPTO'98 (LNCS 372). 1999. P. 95–103.

14. *Ковальчук, Л. В.* Верхние оценки средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и циклического сдвига / Л. В. Ковальчук, Л. В. Скрыпник, С. В. Пальченко // Тр. Восьмой Общерос. науч. конф. «Математика и безопасность информационных технологий». (МаБИТ-09), 30 октября – 2 ноября 2009.