Кафедра 42
Криптология и дискретная математика
Тел. 324-7334; факс. 323-9137; e-mail: kaf42@mail.ru.
Факультет "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Атаки на основе метода связанных ключей

Пудовкина М.

Содержание

- *Пудовкина М.,* Атака на алгоритмы блочного шифрования с «рекуррентным» алгоритмом развёртывания ключа.

- *Пудовкина М., Хоруженко Г.*, Атака на алгоритм шифрования ГОСТ 28147-89 на основе метода связанных ключей;

(на 18-связанных ключах бумерангом – конец ноября 2009 г., компьютерное моделирование – первая половина декабря 2009, 4-связанных январь 2010)

Часть I. Предположения АРК

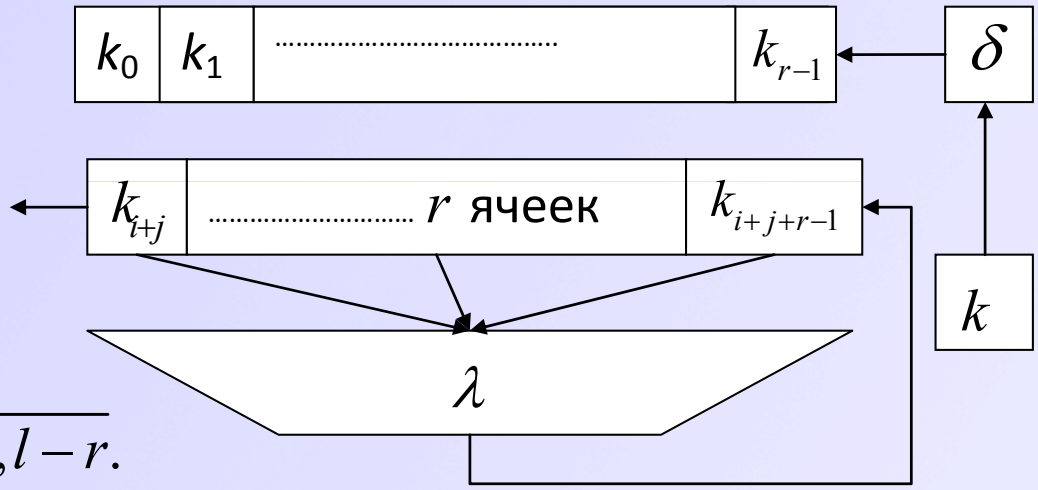
- l — число раундов; ключевое множество $K = V_d$;
- Функция зашифрования $g_k : V_n \to V_n$ и алгоритм развёртывания ключа $\varphi^* = (\delta, \varphi)$ такие, что существуют $r \in \mathbb{N}, r \le l,$ и отображения $\lambda : V_n^r \to V_n, \delta : K \to V_n^r, \varphi : V_n^r \to V_n^l$:

1. $(r-1)\cdot n < d \le r \cdot n;$
2. $\delta(k) = (k_0, \ldots, k_{r-1});$
3. Для любого $i \in \mathbb{N}_0$

$$(k_i, \ldots, k_{i+l-1}) = \varphi(k_i, \ldots, k_{i+r-1}),$$

где

$$k_{i+l+j} = \lambda(k_{i+j}, \ldots, k_{i+r-1+j}), j = \overline{0, l-r}.$$



4. раундовая функция на всех раундах не зависит от номера раунда;
5. $g_k \ne g_{k'}$ для любых различных $k, k' \in V_n$.

(6) Существует такая функция $\psi : V_n \times V_n \to V_n$, что для всех $k, \alpha \in V_n$ выполняется равенство $k = \psi(\alpha, \beta)$, где $\beta = \alpha^{g_k}$.

- Первая в открытой литературе атака на основе метода связанных ключей была применена к алгоритму блочного шифрования LOKI и независимо предложена в работах [Knu92], [Bih94].
- Алгоритм развёртывания ключа LOKI удовлетворяет свойству: для любого ключа шифрования $k \in K$ существует такой $k^{(1)} \in K$, что если

$$\varphi^*(k) = (k_0, \ldots, k_{l-1}),$$

то $\varphi^*(k^{(1)}) = (k_1, \ldots, k_{l-1}, k_0)$.

- Если функция зашифрования блочного алгоритма вдобавок удовлетворяет условиям 4–6, то к нему применяется стандартная сдвиговая атака.

Случай $r \geq 2$. АРК удовлетворяет условия 1–6

$$\vec{k} = (k_0, \ldots, k_{r-1}, k_r, \ldots, k_{l-1}) = \varphi(k_0, \ldots, k_{r-1}).$$

Два связанных ключа: $k^{(i)} = (k_i, \ldots, k_{i+r-1}), k^{(i+1)} = (k_{i+1}, \ldots, k_{i+r})$

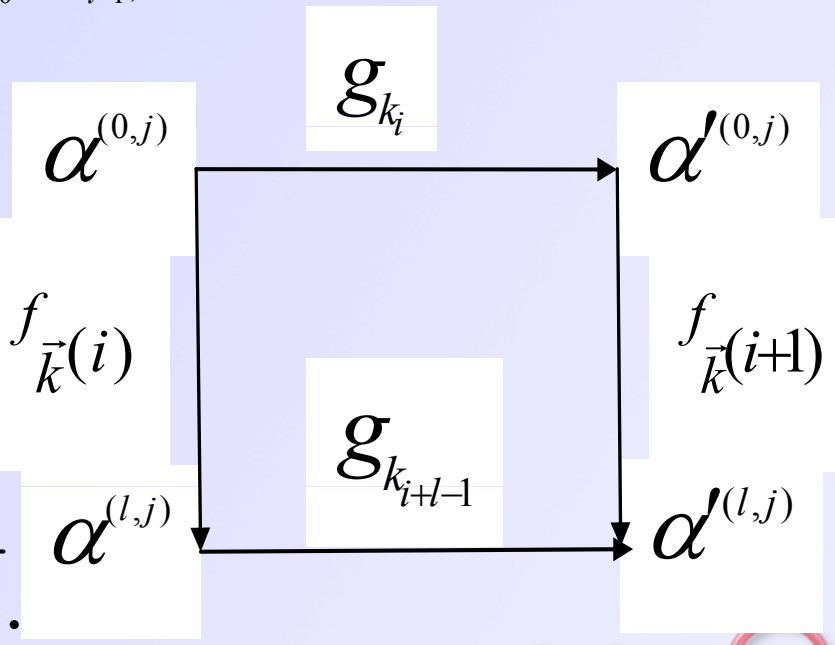
Расширенные ключи: $\vec{k}^{(i)} = (k_i, \ldots, k_{i+l-1}) = \varphi(k^{(i)}), \vec{k}^{(i+1)} = \varphi(k^{(i+1)}).$

$$f_{(k_0,\ldots,k_{i-1})} = g_{k_0} g_{k_1} \ldots g_{k_{i-1}}, \alpha^{(i)} = f_{(k_0,\ldots,k_{i-1})} \alpha^{(0)} = \alpha^{g_{k_0} g_{k_1} \cdots g_{k_{i-1}}}.$$

Опробование ключа $k_i \in V_n$.

Для каждого $k_i \in V_n$ вычисляем:

1. $\alpha^{(l,j)} = f_{\vec{k}^{(i)}}(\alpha^{(0,j)}), j = \overline{1, n_o}.$
2. $\alpha'^{(0,j)} = g_{k_i}(\alpha^{(0,j)}), j = \overline{1, n_o}.$
3. $\alpha'^{(l,j)} = f_{\vec{k}^{(i+1)}}(\alpha'^{(0,j)}), \ j = \overline{1, n_o}.$
4. $k_{i+l-1,j} = \psi(\alpha^{(l,j)}, \alpha'^{(l,j)}), j = \overline{1, n_o}.$



Оценка трудоёмкости

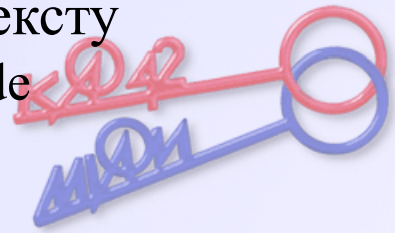
- Трудоёмкость атаки (например, [CiePQ99]):

Тип атаки	число пар откр. и шифр. текстов	число э.о.
по известн. открыт. тексту	$c_1 2^{n/2+1}$	$c_2 2^{n}$
по извес. откр. тексту для схемы Фейстеля	$c_1 2^{n/2+1}$	$c_2 2^{n/2}$
по подобр. откр. тексту для схемы Фейстеля	$c_1 2^{n/4+1}$	$c_2 2^{n/2}$

- [CiePQ99] Для любого ключа шифрования $k \in K$ существует $k^{(1)} \in K$: если $\varphi^*(k) = (k_0, ..., k_{l-1})$, то $\varphi^*(k^{(1)}) = (k_1, ..., k_{l-1}, k_l)$ для некоторого $k_l \in V_n$.

Только для схемы Фейстеля по известному открытому тексту

[CPQ99] *Ciet M., Piret G., Quisquater J.-J.*, Related-Key and Slide Attacks: Analysis, Connections, and Improvements, http://www.dice.ucl.ac.be/~crypto.



Оценка трудоёмкости

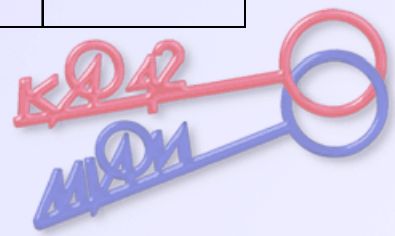
- Если ключ k_i истинный, то $k_{i+l-1} = k_{i+l-1,1} = k_{i+l-1,2} = \ldots = k_{i+l-1,n_o}$,

  и с вероятностью 1 выполняются соотношения

$$\psi(\alpha^{(l,1)}, \alpha'^{(l,1)}) = \ldots. = \psi(\alpha^{(l,n_o)}, \alpha'^{(l,n_o)}). \qquad (1)$$

Если ключ k_i ложный, то вероятность выполнения соотношения (1) равна $2^{-n(n_o-1)}$.

число открыт. текстов	число зашифр	число элемен. операц.	вер. ош. 1 рода	вероятн. ошибки 2 рода	чис. связ. кл.
2	$2^{n+2}r$	$2^{n+2} \cdot r$	0	$1-\left(1-2^{-n}\right)^r$	$r+1$
4	$2^{n+3}r$	$2^{n+2} \cdot r$	0	$1-\left(1-2^{-3n}\right)^r$	$r+1$

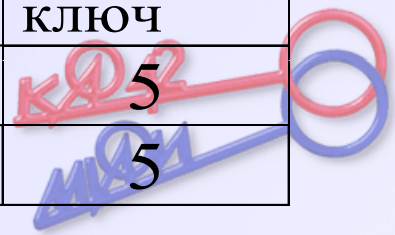


Трудоёмкость для схемы Фейстеля

число откр. текст	чис. заш.	число э.о.	вер. ошиб. 1 рода	вер. ошиб. 2 рода	чис. связ. ключ.
2	$2^{n/2+2} r$	$2^{n/2+2} \cdot r$	0	$1-\left(1-2^{-n/2}\right)^r$	$r+1$
4	$2^{n/2+3} r$	$2^{n/2+2} \cdot r$	0	$1-\left(1-2^{-3n/2}\right)^r$	$r+1$

Трудоёмкость атаки
на 25 раундовый алгоритм блочного
шифрования алгоритм ГОСТ 28147-89

число откр. текст.	число зашиф.	число элем. опер.	вер. ошиб. 1 рода	вер. ошиб. 2 рода	число связан ключ
1	2^{35}	$2^{35}+4$	0	2^{-30}	5
2	2^{36}	$2^{36}+4$	0	2^{-62}	5



АРК удовлетворяет условия 1–5

числ откр тек.	число зашиф.	число элем. операц.	вер ошиб. 1 рода	вероятн. ошибки 2 рода	число связ. ключ.
2	$2^{n+2}r$	$2^{2n+1}\cdot r$	0	$1-\left(1-2^{-n}\right)^{r}$	$r+1$
4	$2^{n+3}r$	$2^{2n+2}\cdot r$	0	$1-\left(1-2^{-3n}\right)^{r}$	$r+1$

Часть II. Определение 31-бита k_1 методами бумеранга и связанных ключей алгоритма ГОСТ 28147-89

- Алгоритм развёртывания ключа $k = (k_1, \ldots, k_8)$

$$\varphi : k \to (k_1, \ldots, k_8, k_1, \ldots, k_8, k_1, \ldots, k_8, k_8, \ldots, k_1)$$

- 4 связанных ключа

$$k, k', k'', k''' \in V_{256} : k \oplus k' = k'' \oplus k''' = (\varepsilon_{31}, \vec{0}, \varepsilon_{31}, \vec{0}, \varepsilon_{31}, \vec{0}, \varepsilon_{31}, \vec{0}, \varepsilon_{31}, \vec{0})$$

$$k \oplus k'' = k' \oplus k''' = (\varepsilon_{31}, \vec{0}, \vec{0}, \vec{0}, \vec{0}, \vec{0}, \vec{0}, \vec{0})$$

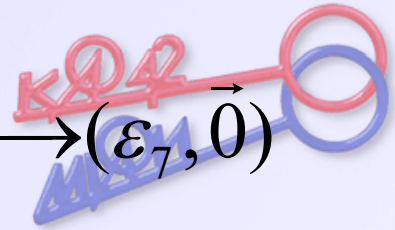
- Четверки открытых текстов

$$\alpha^{(0)}, \alpha'^{(0)}, \beta^{(0)}, \beta'^{(0)} \in V_{64} : \alpha^{(0)} \oplus \alpha'^{(0)} = \beta^{(0)} \oplus \beta'^{(0)} = (\vec{0}, \varepsilon_{31})$$

$$: \alpha^{(32)} \oplus \beta^{(32)} = \alpha'^{(32)} \oplus \beta'^{(32)} = (\varepsilon_7, \vec{0})$$

- Разностные соотношения: $f_{(\kappa_1, \ldots, \kappa_{32})} = f^{(1)}_{(\kappa_1, \ldots, \kappa_{24})} f^{(2)}_{(\kappa_{25}, \ldots, \kappa_{32})}$

$$(\vec{0}, \varepsilon_{31}) \xrightarrow{f^{(1)}_{(\kappa_1, \ldots, \kappa_{24})}, 1} (\vec{0}, \varepsilon_{31}), (\vec{0}, \vec{0}) \xrightarrow{f^{(2)}_{(\kappa_{25}, \ldots, \kappa_{32})}, 1/2^3} (\varepsilon_7, \vec{0})$$



Нахождение усечённым разностным методом k_2 ,..., k_8

- *Youngdai Ko, Seokhie Hong, Wonil Lee, Sangjin Lee, Jongin Lim*. Related Key Differential Attacks on 26 rounds of XTEA and full rounds of GOST, Fast Software Encryption 11th International Workshop, FSE 2004, 2004
- Пара связанных ключей

$$k, k' : k \oplus k' = (\varepsilon_{31}, \vec{0}, \varepsilon_{31}, \vec{0}, \varepsilon_{31}, \vec{0}, \varepsilon_{31}, \vec{0}, \varepsilon_{31}, \vec{0})$$

- Разность на входе $\delta^{(0)} = (\vec{0}, \varepsilon_{31})$
- Пары открытых текстов

$$\alpha^{(0)} = (\alpha_1^{(0)}, \alpha_0^{(0)}), \alpha'^{(0)} = \alpha^{(0)} \oplus \delta^{(0)}$$

Разностная характеристика для 1-30 раундов

$$\kappa = \varphi(k),\ \kappa' = \varphi(k'), \alpha^{(i)} = f_{(\kappa_1,\ldots,\kappa_i)}(\alpha^{(0)}),\ \alpha'^{(i)} = f_{(\kappa'_1,\ldots,\kappa'_i)}(\alpha'^{(0)})$$

- Разностное соотношение 1-24 раунд

$$P\left\{\alpha^{(25)} \oplus \alpha'^{(25)} = (\vec{0}, \varepsilon_{31})\right\} = 1,$$

где $\alpha^{(0)} \oplus \alpha'^{(0)} = (\vec{0}, \varepsilon_{31}), \alpha^{(0)} \in_U V_{32}.$

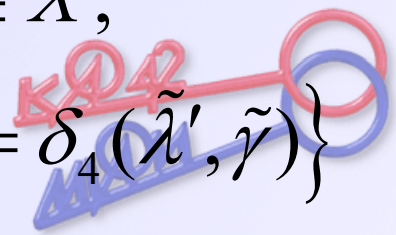
- Разностное соотношение 1-30 раунд

$$P\left\{\alpha^{(30)} \oplus \alpha'^{(30)} \in (\tilde{0}\tilde{X}\tilde{X}\tilde{0}\tilde{X}\tilde{X}\tilde{0}\tilde{X}, \tilde{\varepsilon}_3\tilde{X}\tilde{X}\tilde{0}\tilde{X}\tilde{X}\tilde{X}\tilde{X})\right\} =$$

$$= p_3 p_6 p_1 p_4 p_7 \cdot 3/4,$$

где $\tilde{\nu} \in V_4, \quad \tilde{X} = \{0\} \times V_3, \quad \tilde{\gamma}, \tilde{\lambda} \in_U V_4, \tilde{\lambda} \oplus \tilde{\lambda}' \in \tilde{X},$

$$p_i = P\left\{(\tilde{\lambda} + \tilde{\gamma})^{\tilde{s}} \oplus (\tilde{\lambda}' + \tilde{\gamma})^{\tilde{s}} \in V_3 \times \{0\} \mid \delta_4(\tilde{\lambda}, \tilde{\gamma}) = \delta_4(\tilde{\lambda}', \tilde{\gamma})\right\}$$



Основные этапы атака на ГОСТ 28147-89

- **Вход**: $\alpha'^{(0,i)} = (\vec{0}, \varepsilon_{31}) \oplus \alpha^{(0,i)}, \beta'^{(0,i)} = (\vec{0}, \varepsilon_{31}) \oplus \beta^{(0,i)}, i = \overline{1, n^{(0)}},$
$\left(\alpha^{(0,i)}, \alpha'^{(0,i)}\right), \left(\beta^{(0,i)}, \beta'^{(0,i)}\right).$
- I. Методами бумеранга и связанных ключей находим 31-бит $(k_{1,30}, .., k_{1,0})$ раундового ключа k_1 .
- II. Для всех $k_1 \in \left\{k_1^{(0)}, k_1^{(0)} \oplus \varepsilon_{31}\right\}, k_1^{(0)} = (0, k_{1,30}, .., k_{1,0})$ и $i = \overline{0,6}$ выполняем:

i.1. Расшифровывая $\alpha^{(32-i,j)}$ на k_{i+1} находим $\alpha^{(31-i,j)}, j = \overline{1, n^{(0)}}$.

i.2. Усечённым разностным методом находим k_{i+2}.

- III. На найденных ключах $(k_1^{(0)}, ..., k_8^{(0)}), (k_1^{(1)}, ..., k_8^{(1)})$ шифруем открытых текстов и проверяем равенство соответствующим шифртекстами. Истинным ключом считается ключ на котором все открытых текстов равны соответствующим шифртекстам.
- **Выход**: ключ шифрования k.

Оценка трудоёмкости нахождения ключа шифрования

- Число связанных ключей – 4.
- Трудоёмкость этапа I не больше, чем 2^{30} ≈ 1 час на ноутбуке с процессором AMD Turion, 2.00 ГГц.
- Трудоёмкость этапа II оценивается как $7*2^{45}$ зашифрований.
- Число открытых текстов – 2^{26}.
- Вероятность успеха –0,8.

Спасибо за внимание!