Some Feistel ciphers and two wreath products of symmetric groups

Marina Pudovkina

Moscow Engineering-Physics Institute

Imprimitive groups and iterated block ciphers

Paterson K. G., Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers// FSE'99 – LNCS 1636 – 1999.

Caranti A., Volta F.D., Sala M., Villani F. Imprimitive permutations groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis// Workshop on Coding and Cryptography, UC Cork. – 2005.

$$\Phi_n = \{f_\pi \in S(V_m \times V_m) \mid f_\pi : (\alpha, \beta) \to (\beta, \beta^\pi \oplus \alpha)\}$$

$$n = 2m$$

Some Feistel ciphers and the wreath product $S_{2^{m-1}} wr S_2$

Proposition 1. Let $\pi \in S_{2^{m-1}} wr S_2$, $f_k \in \Phi_n$, $\alpha^{\pi_k} \in \{(\alpha \oplus k)^{\pi}, \alpha^{\pi} \oplus k\}$ for any key $k \in V_m$. Then for any positive integer $l \geq 1$ and for any $k_1, \ldots, k_l \in V_m$ the following are true:

1. $\left(\prod_{j=1}^{l} f_{k_j} \right)^3 \in S_{2^{n-1}} wr S_2$, if $l \not\equiv 0 (\mathrm{mod}\, 3)$,
2. $\left(\prod_{j=1}^{l} f_{k_j} \right)^2 \in S_{2^{n-1}} wr S_2$, if $l \equiv 0 (\mathrm{mod}\, 3)$.

Information on unknown plaintexts without knowledge of the key

Let $g_k = f_{k_1} \dots f_{k_l}$, where f_{k_j} satisfies proposition 1, $k_j \in V_m$, $j \in \{\overline{1,l}\}$, $l \geq 1$.

Let $(\alpha_1, \beta_1), \dots, (\alpha_t, \beta_t)$ be unknown plaintexts of the length $t \geq 1$.

Let $(\alpha_1^{(l)}, \beta_1^{(l)}), \dots, (\alpha_t^{(l)}, \beta_t^{(l)})$ be known ciphertexts, where $(\alpha_i^{(l)}, \beta_i^{(l)}) = (\alpha_i, \beta_i)^{g_k}$, $i = 1, \dots, t$..

Denote by $\alpha \sim_2 \beta$, if $\|\alpha\| \equiv \|\beta\| \pmod 2$.

Proposition 2

For any $i, j \in \{1,\ldots,t\}$ the following are true.

1. if the number of rounds $l \equiv 2(\bmod 3)$, then

$$\beta_i^{(l)} \oplus \beta_j^{(l)} \sim_2 \alpha_i \oplus \alpha_j$$

$$\beta_i^{(l)} \oplus \beta_j^{(l)} \oplus \alpha_i^{(l)} \oplus \alpha_j^{(l)} \sim_2 \beta_i \oplus \beta_j,$$

2. if the number of rounds $l \equiv 1(\bmod 3)$, then

$$\alpha_i^{(l)} \oplus \alpha_j^{(l)} \sim_2 \beta_i \oplus \beta_j$$

$$\beta_i^{(l)} \oplus \beta_j^{(l)} \oplus \alpha_i^{(l)} \oplus \alpha_j^{(l)} \sim_2 \alpha_i \oplus \alpha_j,$$

3. if the number of rounds $l \equiv 0(\bmod 3)$, then

$$\alpha_i^{(l)} \sim_2 \alpha_i, \; \beta_i^{(l)} \sim_2 \beta_i.$$

Some Feistel ciphers and the wreath product $S_2 wr S_{2^{m-1}}$

Let $\overline{a} = a_1 a_2, \ldots,$

$$a_i = \begin{cases} 1, \text{ если } i \equiv 1,2 (\mathrm{mod} 3), \\ 0, \text{если } i \equiv 0 (\mathrm{mod} 3), \end{cases}$$

where $a_i = a_{i-1} \oplus a_{i-2},\ a_0 = 0, a_1 = 1,\ i = 2,3,\ldots$

Proposition 3. Let $\pi \in S_2 wr S_{2^{m-1}}$, $f_k \in \Phi_n$, $\alpha^{\pi_k} \in \{(\alpha \oplus k)^{\pi}, \alpha^{\pi} \oplus k\}$ for any key $k \in V_m$. Then

1. $\pi_k \in S_2 \int S_{2^{m-1}}$ for any key $k \in V_m$.

Proposition 3

$$2.\ (\alpha,\beta)^{\prod_{i=1}^{l} f_{k_i \oplus \theta_i}} = (\alpha^{(l)} \oplus \sum_{i=1}^{l-1} a_{l-i}\theta_i, \beta^{(l)} \oplus \sum_{i=1}^{l} a_{l-i+1}\theta_i),$$

where $(\alpha,\beta)^{\prod_{i=1}^{l} f_{k_i}} = (\alpha^{(l)}, \beta^{(l)})$ and $\theta_i \in \{\vec{0}, \vec{1}\}$, $1 \le i \le l$.

The complexity of the brute-force attack is

$$2^{ml}.$$

The complexity of the attack based on proposition 3 is

$$2^{l(m-1)}.$$