On group generated by ciphers based on Feistel network

V. Antipkin, D. Pasko

TC-26

Sufficient conditions on XSL cipher to generate the alternating group

- A.S. Maslov «On sufficient conditions to generate the alternating group by SA-permutations». National Academy of Sciences of Belarus. Trudy Instituta Matematiki, 15:2 (2007), 58-68, In Russian.

Feistel network. The group generated by cipher round.

- A function $g_k^F: V_{2mn} \to V_{2mn}$ of a cipher based on Feistel network:

$$g_k^F(a, b) = (F(a, k) \oplus b, a).$$

- The particular Feistel network based cipher is determined by the round function $F: V_{mn} \times X \to V_{mn}$, X - a set of keys.
- Let R_F be the group generated by g_k^F

$$R_F = \langle g_k^F | k \in X \rangle.$$

We suppose that round keys k are independent.

- When $R_F = A_{2^{2mn}}$?

The round function F

- $k = (k_1, \ldots, k_l) \in V_{mn}^l$.
- Let's consider the round function $F(x, k) = F_k(x)$ of the following form

$$F_k(x) = Q\pi_{k_l} SL(x).$$

- $Q: V_{mn} \times V_{mn}^{l-1} \to V_{mn}$.
- $\pi_{k_l}(x) = x \oplus k_l$.
- $S(x) = (s_1(x_1), \ldots, s_n(x_n))$, $x = (x_1, \ldots, x_n) \in V_{mn}$, s_i - a permutation of V_m, $i \in \overline{1, n}$.
- $L: V_{mn} \to V_{mn}$ - a non-singular linear transformation.
- We call a transformation of the form $\pi_k SL$ an XSL-transformation.

More notations

- For $a = (a_1, \dots, a_n) \in V_{mn}$ denote $N(a)$ the set on non-zero $a_1, \dots, a_n$.
- Let matrix L be constructed of m × m blocks $L = \|L_{ij}\| \in GL_{mn}(2)$. For L we construct the "diffusion graph" Γ_L with the set of nodes $\{1, \dots, n\}$ and edges $i \to j$ such that L_{ij} is non-singular.
- $M_i(L)$ - the set of indexes of non-singular blocks in i^{th} row of matrix L.

Main result

- **Theorem 2.** *Let permutation $s_i, i \in \overline{1,n}$ of transformation S satisfies the following condition: for any $a_1, a_2 \in V_m$, $a_1 \neq a_2$, vectors*

$$(s_i(a_1 \oplus k_1) \oplus s_i(a_1 \oplus k_2), s_i(a_2 \oplus k_1) \oplus s_i(a_2 \oplus k_2)),\ k_1, k_2 \in V_m$$

generate the vector space V_{2m}, and one of the following conditions hold:

1) for $\forall a_1, a_2 \in V_{mn}$, $a_1 \neq a_2$, there are $k_1, \dots, k_{l-1} \in V_{mn}$, such that

$$|N(a_1 \oplus a_2)| < \left|N\left({a_1}^{Q_{(k_1,\dots,k_{l-1})}} \oplus {a_2}^{Q_{(k_1,\dots,k_{l-1})}}\right)\right|$$

when $|N(a_1 \oplus a_2)| < n$ and

$$|N(a_1 \oplus a_2)| = \left|N\left({a_1}^{Q_{(k_1,\dots,k_{l-1})}} \oplus {a_2}^{Q_{(k_1,\dots,k_{l-1})}}\right)\right|$$

when $|N(a_1 \oplus a_2)| = n$;

2) for $\forall a_1, a_2 \in V_{mn}$, $a_1 \neq a_2$, there are $k_1, \dots, k_{l-1} \in V_{mn}$ such that

$$N(a_1 \oplus a_2) \subseteq N\left({a_1}^{Q_{(k_1,\dots,k_{l-1})}} \oplus {a_2}^{Q_{(k_1,\dots,k_{l-1})}}\right),$$

and transformation L satisfies the condition: the oriented graph Γ_L is strongly connected and the greatest common divisor of its cycles' length is equal to 1.

Then the group R_F equals to the alternating group $A_{2^{2mn}}$.

- In case 2 may be $Q_{(k_1,\dots,k_{l-1})}(x) = x$.

Example of case 1 of theorem 2

- **Statement 2.** *Let function $Q_{(k_1,\dots,k_{l-1})}$ can be represented if the following form*

$$Q_{(k_1,\dots,k_{l-1})} = {Q'}_{(k_1,\dots,k_{l-2})}\pi_{k_{l-1}}S'L',$$

where ${Q'}_{(k_1,\dots,k_{l-2})}: V_{mn} \to V_{mn}$, *and the following conditions hold:*

1) for any $a_1, a_2 \in V_{mn}$, $a_1 \neq a_2$, there are $(k_1,\dots,k_{l-2}) \in V_{mn}^{l-2}$ such that

$$\left|N\left({a_1}^{Q'_{(k_1,\dots,k_{l-2})}} \oplus {a_2}^{Q'_{(k_1,\dots,k_{l-2})}}\right)\right| \geq |N(a_1 \oplus a_2)|;$$

2) L' satisfies the condition: any block ${L'}_{i\,j}$ either null or non-singular, and for any $l \in \overline{1,n-1}$ and pairwise different $i_1,\dots,i_l \in \overline{1,n}$ inequality $\left|\bigcup_{j=1}^{l} M_{i_j}\right| > l$;

3) $S' = (s'_1,\dots,s'_n)$ satisfies the condition: $|M_i(L)| < \frac{1}{p_{s'_i}}$, where

$$p_{s'_i} = \max_{a,b \in V_m\{0\}} |\{x \in V_m | s(x \oplus a) \oplus s(x) = b\}|, i \in \overline{1,n}.$$

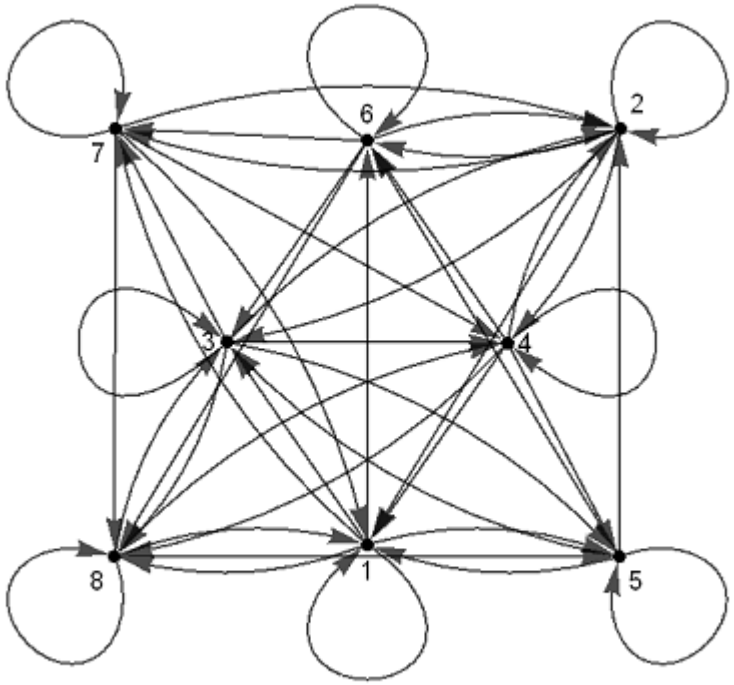
Then $Q_{(k_1,\dots,k_{l-1})}$ satisfies case 1 of theorem 2.

- May be ${Q'}_{(k_1,\dots,k_{l-2})}(x) = x$.

Example 1: MIBS

- Block size: 64 bits, $n = 8$, $m = 4$, round function $F_k(x) = \pi_k SL(x)$.
- Matrix L is tensor product of non-singular binary 8×8-matrix and identity 4×4-matix, permutations $s_1, \dots, s_n$ are all equal.
- Case 2 of theorem 2: $Q_{(k_1,\dots,k_{l-1})}(x) = x$.
- Condition $< \left(a_1^{\pi_{k_1} S} \oplus a_1^{\pi_{k_2} S}, a_2^{\pi_{k_1} S} \oplus a_2^{\pi_{k_2} S}\right) | k_1, k_2 \in V_4 >= V_8$ for all $a_1, a_2 \in V_4$ was confirmed using PC.
- Graph Γ_L is strongly connected and, since it has a loop, it's cycles length GCD is equal to 1.
- $R_F = A_{2^{64}}$

MIBS graph Γ_L



Example 2: Camelia

- Block size: 128 bits, $n = 8$, $m = 8$, round function $F_k(x) = \pi_k SL(x)$.
- There are two additional transformations after every 6 rounds: FL for the left half of the block, and FLI for the right part of the block – ignore them!
- The structure of Camelia is similar to MIBS, and it also satisfies case 2 of theorem 2 with $Q_{(k_1,\ldots,k_{l-1})}(x) = x$.

Example 3: E2

- Block size: 128 bits, $n = 8$, $m = 8$, round function $F_k(x) = \pi_{k_1} SL \pi_{k_2} SL(x)$.
- Permutations $s_1, \dots, s_n$ are all the same.
- Matrix L is tensor product of non-singular binary 8×8-matrix and identity 8×8-matix
- Transformation IT before the first round and transformation FT after the last round – ignore them!
- Statement 2 and case 1 of theorem 2 with $Q'_{(k_1,\dots,k_{l-2})}(x) = x$.
- Condition $< \left(a_1^{\pi_{k_1} s} \oplus a_1^{\pi_{k_2} s}, a_2^{\pi_{k_1} s} \oplus a_2^{\pi_{k_2} s}\right) | k_1, k_2 \in V_8 >= V_{16}$ for all $a_1, a_2 \in V_{16}$ was confirmed using PC.
- $p_s = \frac{10}{256}$, so $25.6 = p_s^{-1} > \max\limits_{i \in \overline{1,n}} |M_i(L)| = 6$.
- The overall number of block columns of matrix L with at least one non-null block in any $l \in \overline{1, n-1}$ block rows is more then l.
- $R_F = A_{2^{128}}$.

Conclusion

- Using the results obtained by A.S. Maslov for groups generated by round functions of XSL ciphers, we investigate the groups generated by the cipher round based of Feistel network with the round function containing one or more XSL transformations.
- We obtain the sufficient conditions when this group equals to alternating group.
- This conditions are mostly easy to check. For example, the conditions on linear transformations are satisfied for MDS matrices, which are often used in block ciphers. The conditions on permutations in practically significant cases are easy to check using PC.

Thank you for your attention!