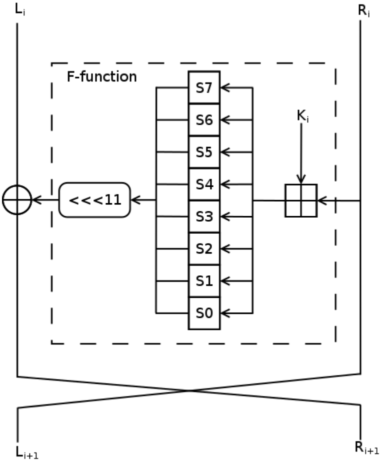
Long-Term Key Recovering of The GOST Cipher

Oleksandr Kazymyrov

Department of Informatics
University of Bergen

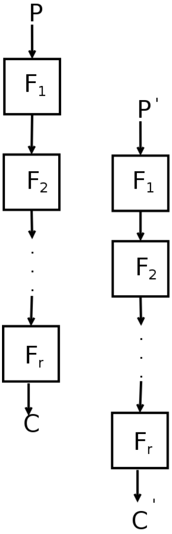
Selmer Center
2011

Cipher GOST 28147



Parameters:
K - session key (256 bit)
S-boxes - long-term key (512 bits)
Input/Output = 64/64 bits
Cipher based on Feistel Network
with $r = 32$ rounds.

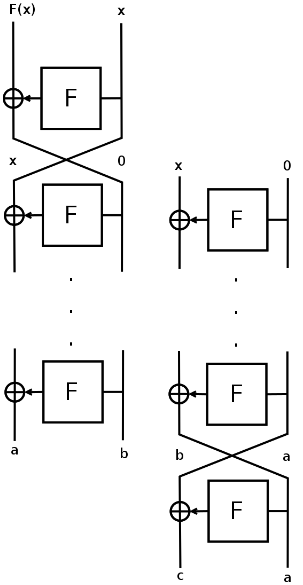
Slide Attack



If $F_1 = F_2 = \ldots = F_r = F$ and $P^{'} = F(P)$, then

$$C^{'} = F(C).$$

Slide Attack on GOST



If session key is equal $K = 0$ and

$$P = (F(x), x) \rightarrow C = (a, b).$$

Then

$$P' = (x, 0) \rightarrow C' = (c, a),$$

where $c = b \oplus F(a)$

Finding Substitutions

Step 1

- Suppose that $x = 0$, then
$$P^{'} = (0, 0) \rightarrow C^{'} = (c, a)$$
- Find $y = \{0, 1, \ldots, 2^{32} - 1\}$ such that
$$P = (y, 0) \rightarrow C = (a, b)$$
- Find $S_i(0)$
$$S_i(0) = y_i \quad i = \{0, 1, \ldots, 7\}$$
$$y_i = ((y \ggg 11) \gg 4i) \wedge F_{16}$$

Finding Substitutions

Step 2

For finding $S_i(u)$ $(u = \{1, 2, \ldots, 15\})$ exhaustive search method is used.
Suppose that $v = S_i(u)$ $(v = \{0, 1, \ldots, 15\})$. Then for all i, u, v let us search values such that $C_R^{'} = C_L$, where $C_R^{'}$, C_L are left and right parts of ciphertext $E(P^{'})$, $E(P)$ respectively and $P^{'} = (u \ll 4i, 0)$, $P = (F(u \ll 4i), u \ll 4i)$.

Finding Substitutions

Step 2 continue

We try to find such parametrs when $S_i(u) = v$.

- Suppose that $x = u \ll 4i$ and for all $v = \{0, 1, \ldots, 15\}$ compute
$$P' = (x, 0) \rightarrow C' = (c, C'_R)$$
$$P = (F(x), x) \rightarrow C = (C_L, b)$$
- If $C'_R = C_L$, then
$$S_i(u) = v$$

Complexity

- The first step requires no more than 2^{32} encryptions.
- The second step requires no more than $2^3(2^4 - 1)2^4 2 = 2^{11}$ encryptions.
- Then total complexity is 2^{32}, because $2^{11} \ll 2^{32}$.

Practical Results

The table below contains information about practical results of finding long-term key in cipher GOST. Time is given in seconds.

Keys	Min	Max	Average
100	0.00	110.00	54.13

Conclusions

Long-term key in cipher GOST doesn't add more security, then session key. The real complexity is no more then 2^{256}.