On Impossible Truncated Differentials of Generalized Feistel and Skipjack Ciphers

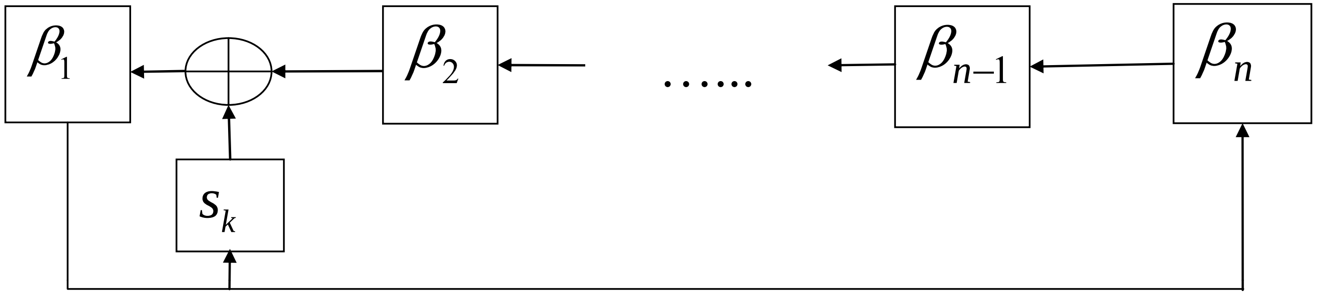
Marina Pudovkina

Moscow Engineering-Physics Institute

Description of generalized Feistel ciphers

$$g^{(1)}_{s_K}:(\beta_1,\beta_2,\dots,\beta_n)\rightarrow(\beta_2\oplus s_k(\beta_1),\beta_3,\dots,\beta_n,\beta_1),$$

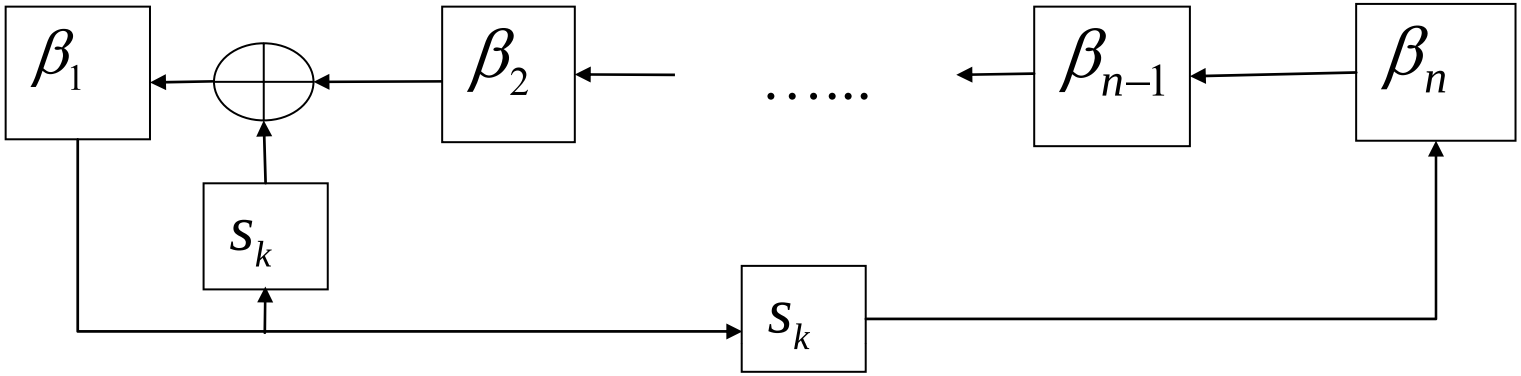
where $(\beta_1,\beta_2,\dots,\beta_n)\in \mathrm{V}_m^n$, $s_k:V_m\rightarrow V_m$ depends on a round key k



Description of generalized Skipjack ciphers

$$g_{s_K}^{(2)}:(\beta_1,\beta_2,\dots,\beta_n)\to(\beta_2\oplus s_k(\beta_1),\beta_3,\dots,\beta_n,s_k(\beta_1))$$

where $(\beta_1,\beta_2,\dots,\beta_n)\in \mathrm{V}_m^n$, $s_k:V_m\to V_m$ depends on a round key k



The Conjecture from ASIACRYPT'2000 (J. Sung, S. Lee, J. Lim, S. Hong and S. Park)

- *Conjecture* [1]. If $l \geq n^2$, there does not exist an impossible truncated differential of generalized Feistel and Skipjack ciphers.

[1] *Sung J., Lee S., Lim J., Hong S., Park S.*, Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis, ASIACRYPT'2000, LNCS 1976, pp. 274–288, 2000

- It was noticed.

[1] {The conjecture can be proved by a computer programming if *n* is small enough, say less than 32. However, since we could not find a general rule of proof, we just do conjecture it in the case that m is large}

We get nontrivial mathematical proofs of the following

- **Hypothesis 1.** There exist generalized Feistel ciphers such that for any $l \geq n^2$ there does not exist any nontrivial impossible truncated differential.

- **Hypothesis 2.** There exist generalized Skipjack ciphers with bijective round functions such that for any $l \geq n^2$ there does not exist any nontrivial impossible truncated differential.

We also prove

- **Corollary 1.** For any $l < n^2$ there exists a generalized Feistel cipher (a generalized Skipjack cipher) such that there exists a nontrivial impossible truncated differential.

- For example, for any $l < n^2$ there exists the following impossible differential

$$(0,\ldots,0,\alpha)\cancel{\xrightarrow{l}}(0,\ldots,0,\beta),\alpha \neq \beta$$

Our Main result (Theorem 1)

There exist generalized Feistel ciphers $g^{(1)}_{s_{\kappa(l)}} = g^{(1)}_{s_{\kappa_1}} \ldots g^{(1)}_{s_{\kappa_l}}$ such that for any $l \geq n^2$, arbitrary nonzero differences $\theta, \theta' \in \left(V_m^n\right)$, and an arbitrary vector $\alpha \in V_m^n$ there exists a key $k(l) = (k_1, \ldots, k_l)$ for which we have

$$g^{(1)}_{s_{\kappa(l)}}(\alpha) \oplus g^{(1)}_{s_{\kappa(l)}}(\alpha \oplus \theta) = \theta',$$

i.e.

$$\theta \xrightarrow{l} \theta'.$$

We prove the *Conjecture* presented by *Sung J., Lee S., Lim J., Hong S., Park S.* Hong

- The proof follows from **Hypothesis 1, Hypothesis 2, Corollary 1, Theorem 1**.

- The proofs of the **Hypotheses, Theorem 1** are based on properties of transitions matrices of generalized Feistel and Skipjack ciphers.

Thank you for your attention!