ISO/IEC JTC 1/SC 27/WG 2
Cryptography and security mechanisms
Convenorship: JISC (Japan)

Document type:	Officer's Contribution
Title:	A Memo on Kuznyechik S-Box
Status:	
Date of document:	2018-09-27
Source:	Project Editor (Vasily Shishkin), Project Co-editor (Grigory Marshalko)
Expected action:	ACT
Action due date:	2018-10-04
No. of pages:	1 + 4
Email of convenor:	t-chika@ipa.go.jp
Committee URL:	https://isotc.iso.org/livelink/livelink/open/jtc1sc27wg2

A Memo on Kuznyechik S-Box

During ballot on 18033-3 DAmd1 (finished in June 2018) comments from some NB were received concerning issues regarding Kuznyechik design rationale and its parameters origins. The goal of this Memo is to provide all relevant information known to the designers of the algorithm.

Kuznyechik has transparent and well studied design. Its design rationale was introduced to WG2 experts in 2016 by presentation (WG2) N1740. Kuznyechik is based on well examined constructions. Each transformation provides certain cryptographic properties. All transformations used as building blocks have transparent origin.

The only transformation used in Kuznyechik which origin may be questioned is the S-box π. This S-box was chosen from Streebog hash-function and it was synthesized in 2007. Note that through many years of cryptanalysis no weakness of this S-box was found. The S-box π was obtained by pseudo-random search and the following properties were taken into account.

1. The differential characteristic

$$p_\pi = \max_{\alpha,\beta \in V_8 \setminus \{0\}} p^\pi_{\alpha,\beta},$$

where $p^\pi_{\alpha,\beta} = \mathcal{P}\{\pi(x \oplus \alpha) \oplus \pi(x) = \beta\}$. The goal was to obtain an S-box for which this characteristic is as small as possible.

2. The linear characteristic

$$\delta_\pi = \max_{\alpha,\beta \in V_8 \setminus \{0\}} |\delta^\pi_{\alpha,\beta}|,$$

where $\delta^\pi_{\alpha,\beta} = 2\mathcal{P}\{x\alpha = \pi(x)\beta\} - 1$, ab – is the scalar product of two boolean vectors of dimension 8, $\mathcal{P}(\dot{})$ – is probability which is calculated when x is chosen at random and independently. The goal was to obtain an S-box for which this characteristic is as small as possible.

3. The non-linearity characteristics

$$\lambda_\pi, \quad \lambda_{\pi^{-1}},$$

where λ_π is the minimum degree among all ANFs representing non-degenerate linear combinations of π's coordinate functions. The goal was to obtain an S-box for which these characteristics are as big as possible (i.e., equal to 7).

4. Let us define characteristics

$$r^\pi_k, \quad k \in \overline{2,3},$$

where r^π_k – is the maximum number of linear independent boolean equations with degree below or equal to k and whose variables are $x_1, \ldots, x_8$ and $y_1, \ldots, y_8$ which satisfy

$$(y_1, \ldots, y_8) = \pi(x_1, \ldots, x_8).$$

The goal was to obtain an S-box for which these characteristics are as small as possible (see [2]).

5. The S-box should not have any fixed points.

Through thorough search current S-box was obtained and its characteristics are as follows.

1. $p_\pi = \frac{8}{128}$;

2. $\delta_\pi = \frac{28}{256}$;

3. $\lambda_\pi = \lambda_{\pi^{-1}} = 7$;

4. r_k^π, $k \in \overline{2,3}$, are as small as possible and are equal to (correspondingly) 0 and 441;

5. π has no fixed points.

No secret structure was enforced during construction of the S-box. At the same time, it is obvious that for any transformation a lot of representations are possible (see, for example, a lot of AES S-box representations). Results of [1] solved a great optimization problem, they are valuable as scientific breakthrough and also provide more flexibility in software/hardware implementation of Kuznyechik as well as other ciphers with 8-bit s-boxes. At the same time further development of results of [1] will make possible to synthesize S-boxes with better cryptographic and implementation characteristics (see for example [3]).

Список литературы

[1] Biryukov Alex, Perrin Léo, Udovenko Aleksei. The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob// IACR Cryptology ePrint Archive. — 2015. — **2015**. — 812.

[2] Courtois Nicolas, Pieprzyk Josef. Cryptanalysis of block ciphers with overdefined systems of equations// Zheng Yuliang, editor, Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings/ Lecture Notes in Computer Science. — v. 2501, Springer. — 2002. — 267–287.

[3] Fomin Denis. New classes of 8-bit permutations based on a butterfly structure// CTCrypt'2018 proceedings. — 2018.