Low-Weight and Hi-End: Draft Russian Encryption Standard

Vasily Shishkin, Denis Dygin, Ivan Lavrikov,
Grigory Marshalko, Vladimir Rudskoy and Dmitry Trifonov

WORKSHOP ON CURRENT TRENDS IN CRYPTOLOGY
Moscow, Russia

6 June 2014

Outline

Outline

Current standard ("Swiss army knife"?)

GOST 28147-89

- S-boxes are not defined
- modes of operation in the same standard
- cryptographic research shows theoretical weaknesses
- block length imposes some restrictions (e.g. on amount of data to be encrypted)

Current standard ("Swiss army knife"?)

GOST 28147-89

- S-boxes are not defined
- modes of operation in the same standard
- cryptographic research shows theoretical weaknesses
- block length imposes some restrictions (e.g. on amount of data to be encrypted)

BUT ...

- no doubt about practical security
- long-term thorough cryptanalysis
- extremely lightweight-friendly

Improvement of the standard

- two standards: one for block ciphers and another for modes of operation
  (following the structure of ISO/IEC system of cryptographic standards)
- draft standard for modes of operation include ECB, CBC, CTR, OFB, CFB, CMAC.
- GOST 28147-89 algorithm with explicitly defined S-boxes (S-boxes values can be found here http://www.tc26.ru/)
- addition of another block cipher with 128-bit block
  - mainly software oriented
  - with as large security margin as possible
- timeline: standard draft in 2014, acting standard in 2015

Outline

Main Design Principles

- no known attacks
- only well examined constructions and transformations are used as building blocks
- the best performance and the highest security margin (something contradictory...)
- nothing extra: each transformation provides certain cryptographical properties

The Name

We try to follow current trends in everything

- Rijndael [’rɛinda:l]
- Keccak [’kætʃæk]

The Name

We try to follow current trends in everything

- Rijndael [’rɛinda:l]
- Keccak [’kætʃæk]

so, current trend is to produce difficult to pronounce name

- Kuznyechik [ku:zn’etʃik]

meaning just ’grasshopper’ in Russian

Main Details

First presented in 2013:
http://www.ruscrypto.ru/accotiation/archive/rc2013/

- 256-bit key length
- SP-network (XSL-cipher)
- 8-bit S-boxes
- number of rounds is high enough to provide significant security margin
- key schedule (Feistel network): utilize same mappings as round transformation

The spice: linear mapping

- current state-of-the-art: MDS linear mappings
- BUT: too slow on general purpose platforms

The spice: linear mapping

- current state-of-the-art: MDS linear mappings
- BUT: too slow on general purpose platforms

Solution

- theoretical results provide a way to construct MDS mapping which can be implemented by LSFR
- less memory needed (to store & to implement)
- more flexibility in software implementations
- some results show much higher speeds
- * thanks to Alexander Nechaev for pointing on these results

Closer look: basic structure

- 9 rounds and final addition of whitening key
- number of rounds is 1,5 times less than for AES-256

$$E_{K_1,\ldots,K_{10}} = X[K_{10}]LSX[K_9]\ldots LSX[K_2]LSX[K_1],$$

$$K_i \in V_{128},\ i = 1,\ldots,10$$

Closer look: key schedule

- 32 Feistel rounds
- key schedule Feistel round and cipher round transformations are the same (round constants play role of keys)
- values of round constants depend on number of round

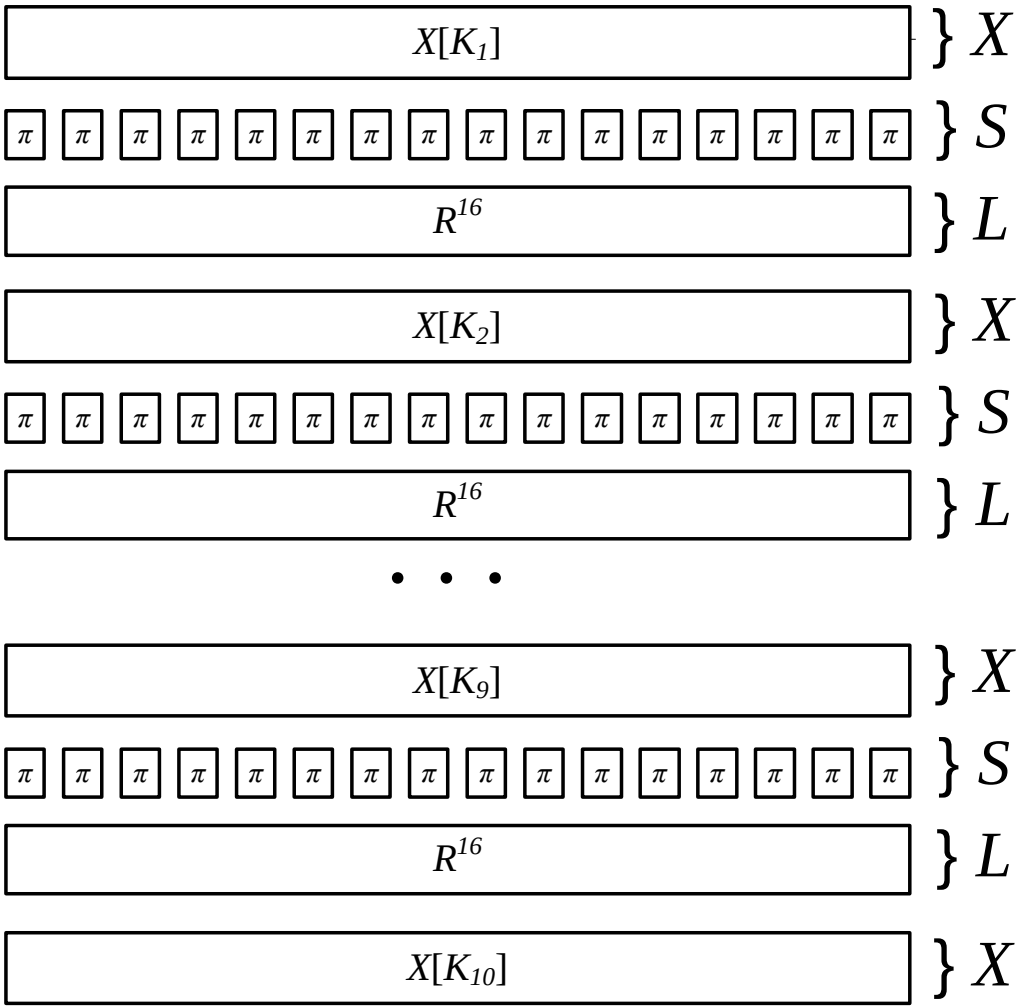
$$K \in V_{256},\ (K_1, K_2) = K,$$

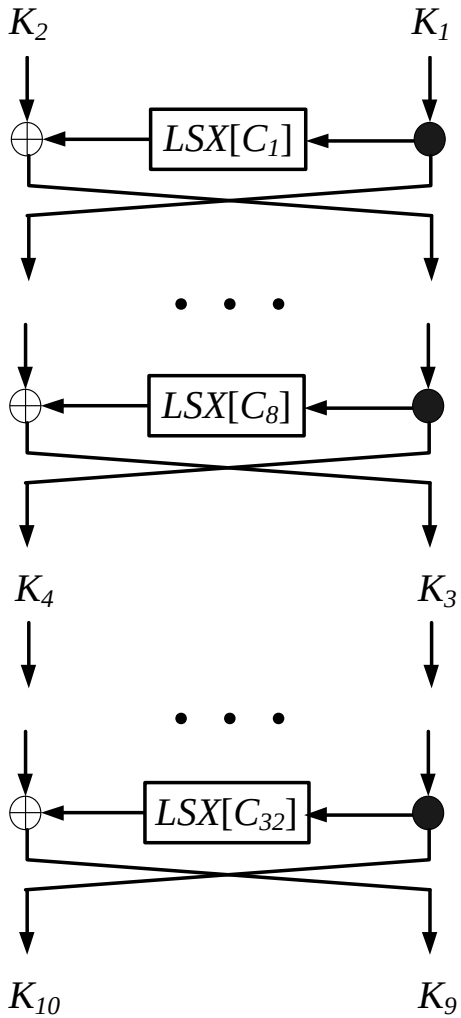
$$(K_{2i+1}, K_{2i+2}) = F[C_{8(i-1)+8}] \dots F[C_{8(i-1)+1}](K_{2i-1}, K_{2i}),$$

$$i = 1, \dots, 4,$$

$$F[C] : V_{128}^2 \to V_{128}^2, \quad F[C](a_1, a_0) = (LSX[C](a_1) \oplus a_0, a_1),$$

$$C_i \in V_{128},\ C_i = L([i]_2), \quad i = 1, \dots, 32$$


$X[K_1]$
X
S
R^{16}
L
$X[K_2]$
X
S
R^{16}
L
$X[K_9]$
X
S
R^{16}
L
$X[K_{10}]$
X


K_2
K_1
$LSX[C_1]$
$LSX[C_8]$
K_4
K_3
$LSX[C_{32}]$
K_{10}
K_9

Closer look: nonlinear mapping

- equal 8-bit S-boxes
- same as in GOST R 34.11-2012

$$S(a) = S(a_{15} \| \ldots \| a_0) = \pi(a_{15}) \| \ldots \| \pi(a_0),$$

where $a = a_{15} \| \ldots \| a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, \ldots, 15$

$$\pi : V_8 \to V_8$$

Closer look: linear mapping

- implemented by LSFR
- coefficients of corresponding linear polynomial have minimum possible binary weight

$$L : V_{128} \to V_{128}, \quad L(a) = R^{16}(a)$$

$$R : V_{128} \to V_{128},$$

$$R(a) = R(a_{15} \| \ldots \| a_0) = l(a_{15}, \ldots, a_0) \| a_{15} \| \ldots \| a_1,$$

where $a = a_{15} \| \ldots \| a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, \ldots, 15$
$l : V_8^{16} \to V_8$ – linear, could be implemented by 16 multiplications by constants in field $GF(2^8)$

P.S.

Thanks to all fellows who were and will be involved in the development process

Thank you for your attention

Questions?