A New Encryption Standard of Ukraine: The Block Cipher "Kalyna" (DSTU 7624:2014)

Roman Oliynykov,
Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev,
Yurii Gorbenko and Viktor Dolgov

JSC Institute of Information Technologies,
V.N.Karazin Kharkiv National University,
Kharkiv National University of Radio Electronics
Ukraine
roliynykov@gmail.com

July 8th, 2015
Central European Conference on Cryptology
Klagenfurt, Austria

Outline

- The block cipher GOST 28147-89 and its replacements in post-Soviet countries
- The new Ukrainian block cipher "Kalyna"
  - General structure
  - Component properties
  - Key schedule
  - Cryptographic strength
- Performance comparison with other ciphers
- Other components of the Ukrainian national standard DSTU 7624:2014
- Conclusions

Block cipher GOST 28147-89

Advantages

- a well known and researched cipher, adopted as national standard in 1990
- acceptable encryption speed (cf.TripleDES)
- appropriate for lightweight cryptography
- good S-boxes provide practical strength

Disadvantages

- theoretically broken
- huge classes of weak keys
- special S-boxes (non-bijective) allows practical ciphertext-only attacks
- encryption speed significantly slower in comparison to modern block ciphers like AES

GOST 28147-89 is withdrawn in Belarussia (legacy-only application) and will be replaced in Russia (will remain as additional 64-bit algorithm); GOST 28147-89 was refused to be included to ISO/IEC 18033-3

Replacements for GOST 28147-89 in Belarussia

Belarussia: STB 34.101.31-2011 (BelT)

- block length is 128 bits; key length is 128, 192 or 256 bits
- 8-rounds Feistel network with Lai-Massey scheme
- a single byte S-box with good cryptographic properties
- no key schedule like in GOST (encryption key shorter than 256 bits is padded by zeros)
- no cryptanalytical attacks better than exhaustive search are known
- faster than GOST, slower than AES

Replacements for GOST 28147-89 in Russia

Russia: draft standard "Kuznyechik" ("Grasshopper")

- block length is 128 bits; key length is 256 bits
- 9 rounds of Rijndael-like transformation
- single byte S-box (common with the new Russian hash GOST 34.11-2012 "Stribog")
- non-circulant MDS matrix of 16x16 size over $GF(2^8)$ (different from that in "Stribog")
- key schedule based on a Feistel network and involves round transformation (like in CS-cipher)
- no cryptanalytical attacks faster than exhaustive search are known
- faster than GOST, slower than AES

GOST 28147-89 will be used as an additional legacy cipher in the new Russian standard

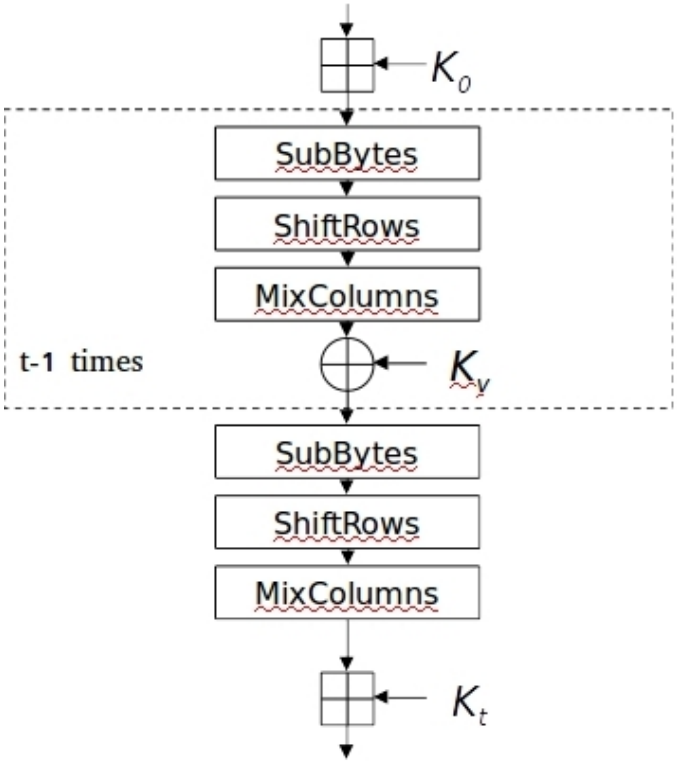
Block cipher "Kalyna"

- normal, high and ultra high security level (block and key length 128, 256 and 512 bits)
- transparent construction and conservative design
- Rijndael-like SPN structure
- four different S-boxes (not CCZ-equivalent) with optimized cryptographic properties
- 8x8 MDS matrix over $GF(2^8)$
- one set of look-up tables for ECB encryption in software implementation (better performance of encryption and decryption for CTR, CFB, CMAC, OFB, GCM, GMAC, CCM modes of operation)
- a new construction of key schedule based on the round function
- effective in software and software-hardware implementations, common look-up tables with the hash function "Kupyna" (DSTU 7564:2014)

"Kalyna": supported block and key length

#	Block size (l)	Key length (k)	Rounds (t)
1	128	128	10
2		256	14
3	256	256	14
4		512	18
5	512	512	18

Block cipher "Kalyna": structure



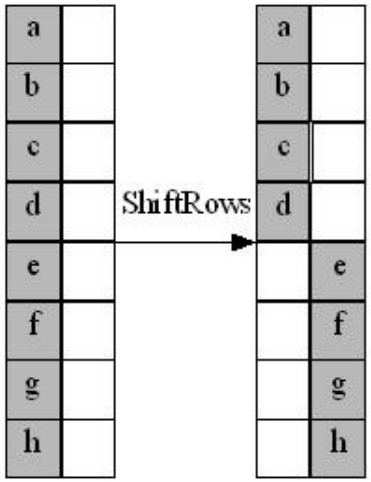
$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi_l' \circ \prod_{\nu=1}^{t-1} (\kappa_l^{(K_\nu)} \circ \psi_l \circ \tau_l \circ \pi_l') \circ \eta_l^{(K_0)}$$

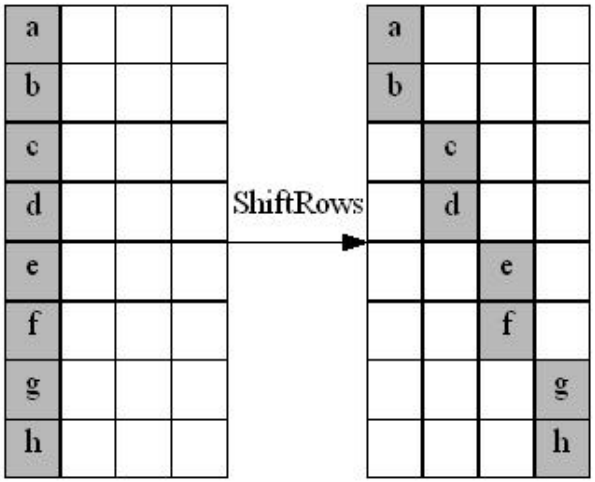
"Kalyna": characteristics of S-boxes

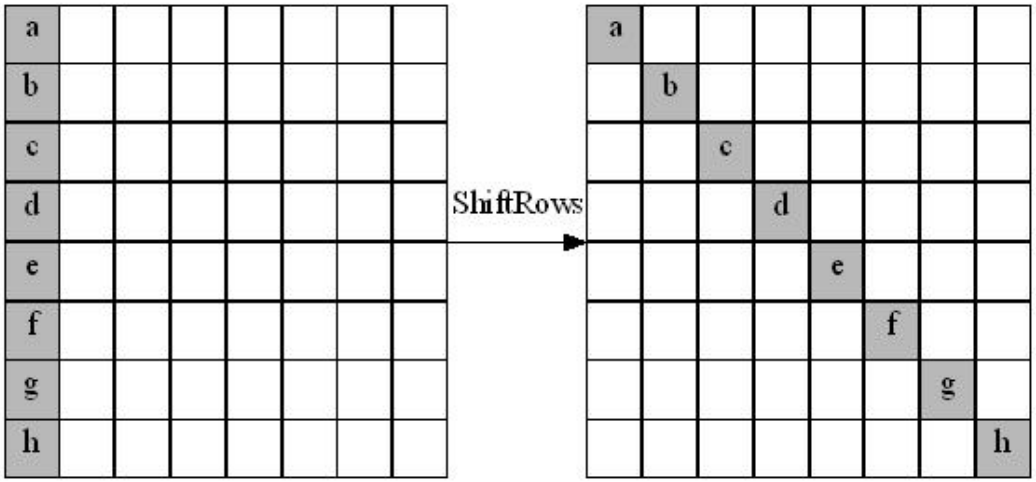
Characteristic	S-box			
	1	2	3	4
Non-linearity of Boolean functions	104			
Min. algebraic degree of Boolean functions	7			
Max. value of difference distribution table	8			
Max. value of linear approximation table	24			
Overdefined system degree	3			
Number of cycles	4	4	6	4
Minimal cycle length	6	8	4	4

Non-linearity is the best known for S-boxes with 3^{rd} degree of overdefined system (the highest among S-boxes of Crypton, Safer+, Skipjack, SNOW, Twofish, Whirlpool, S, Anubis, Stribog/Kuznyechik, STB)

"Kalyna" ShiftRows: 128,256 and 512-bit block







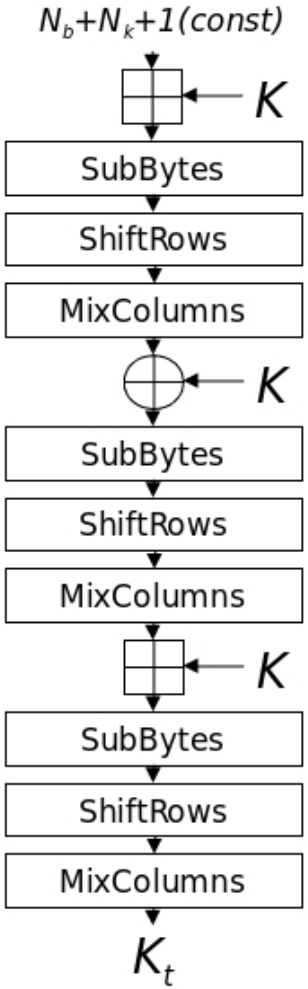
Linear transformation of "Kalyna": MDS matrix

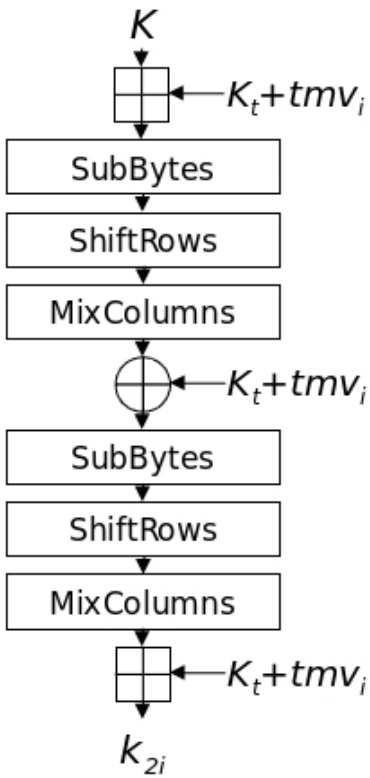
$$
\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix}
01 \cdot a_0 \oplus 01 \cdot a_1 \oplus 05 \cdot a_2 \oplus 01 \cdot a_3 \oplus 08 \cdot a_4 \oplus 06 \cdot a_5 \oplus 07 \cdot a_6 \oplus 04 \cdot a_7 \\
04 \cdot a_0 \oplus 01 \cdot a_1 \oplus 01 \cdot a_2 \oplus 05 \cdot a_3 \oplus 01 \cdot a_4 \oplus 08 \cdot a_5 \oplus 06 \cdot a_6 \oplus 07 \cdot a_7 \\
07 \cdot a_0 \oplus 04 \cdot a_1 \oplus 01 \cdot a_2 \oplus 01 \cdot a_3 \oplus 05 \cdot a_4 \oplus 01 \cdot a_5 \oplus 08 \cdot a_6 \oplus 06 \cdot a_7 \\
06 \cdot a_0 \oplus 07 \cdot a_1 \oplus 04 \cdot a_2 \oplus 01 \cdot a_3 \oplus 01 \cdot a_4 \oplus 05 \cdot a_5 \oplus 01 \cdot a_6 \oplus 08 \cdot a_7 \\
08 \cdot a_0 \oplus 06 \cdot a_1 \oplus 07 \cdot a_2 \oplus 04 \cdot a_3 \oplus 01 \cdot a_4 \oplus 01 \cdot a_5 \oplus 05 \cdot a_6 \oplus 01 \cdot a_7 \\
01 \cdot a_0 \oplus 08 \cdot a_1 \oplus 06 \cdot a_2 \oplus 07 \cdot a_3 \oplus 04 \cdot a_4 \oplus 01 \cdot a_5 \oplus 01 \cdot a_6 \oplus 05 \cdot a_7 \\
05 \cdot a_0 \oplus 01 \cdot a_1 \oplus 08 \cdot a_2 \oplus 06 \cdot a_3 \oplus 07 \cdot a_4 \oplus 04 \cdot a_5 \oplus 01 \cdot a_6 \oplus 01 \cdot a_7 \\
01 \cdot a_0 \oplus 05 \cdot a_1 \oplus 01 \cdot a_2 \oplus 08 \cdot a_3 \oplus 06 \cdot a_4 \oplus 07 \cdot a_5 \oplus 04 \cdot a_6 \oplus 01 \cdot a_7
\end{bmatrix}
$$

Requirements to "Kalyna" key schedule

- each round key depends non-linear on each encryption key bit non-linear dependence of each round key bit on each encryption key bit
- protection from cryptanalytic attacks aimed to key schedule
- high computation complexity of obtaining encryption key having one or several round keys (one-way transformation, additional protection from side-channel attacks)
- key agility is less than three
- possibility to generate round keys in direct and reverse order
- implementation simplicity (application of transformations from the round function only)

"Kalyna" key schedule





$k_{2i+1} = k_{2i} <<< (2 \cdot N_b + 3)$

$tmv_0 = 0x01000100..0100$
$tmv_{i+2} = tmv_i << 1$

$$\Theta^{(K)} = \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\alpha)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \kappa_l^{(K_\omega)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\alpha)}$$

$$\Xi^{(K,K_\sigma,i)} = \eta_l^{(\varphi_i(K_\sigma))} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \kappa_l^{(\varphi_i(K_\sigma))} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(\varphi_i(K_\sigma))}$$

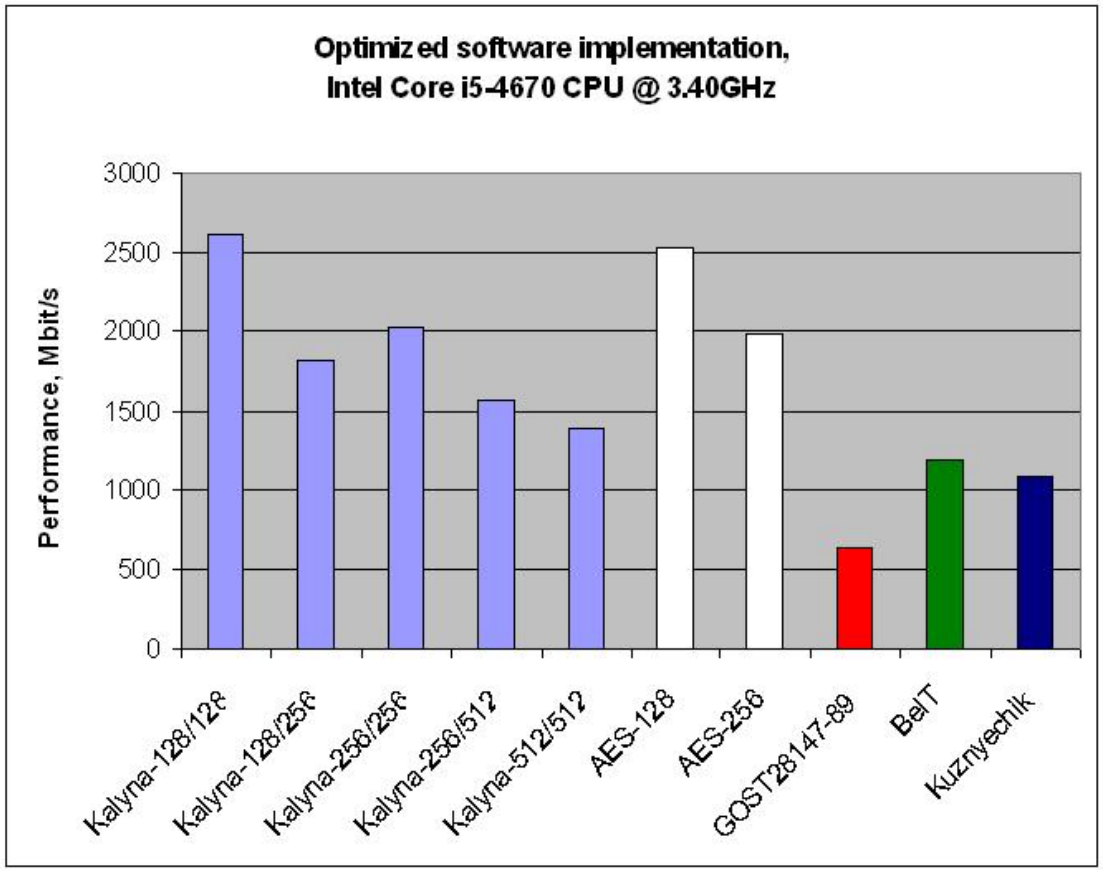
Cryptographic strength of "Kalyna"

Block cipher provides strength to considered methods of cryptanalysis:

- for 128-bit block: after 5^{th} round (out of 10 or 14, depending on the key length)
- for 256-bit block: after 6^{th} round (out of 14 or 18)
- for 512-bit block: after 8^{th} round (out of 18)

"Kalyna" performance comparison with other block ciphers

(Intel Core i5, 64-bit Linux, gcc v4.9.2, best compiler optimization)



https://github.com/Roman-Oliynykov/ciphers-speed/

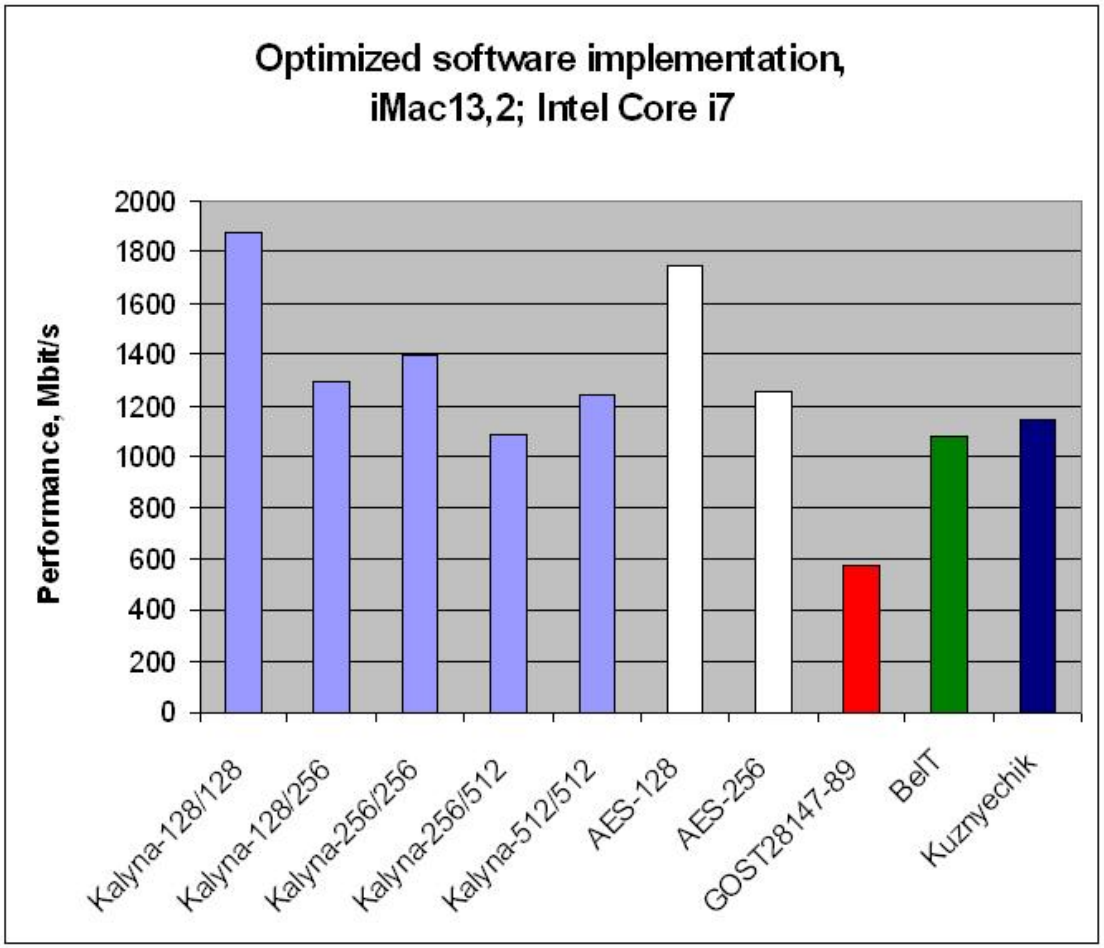
"Kalyna" performance comparison with other block ciphers

(Intel Core i5, 64-bit Linux, gcc v4.9.2, best compiler optimization)

#	Block cipher	Performance, Mbit/s
1	Kalyna-128/128	2611.77
2	Kalyna-128/256	1809.70
3	Kalyna-256/256	2017.97
4	Kalyna-256/512	1560.89
5	Kalyna-512/512	1386.46
6	AES-128	2525.89
7	AES-256	1993.53
8	GOST 28147-89	639.18
9	STB 34.101.31-2011 (BelT)	1188.83
10	Kuznyechik	1081.08

"Kalyna" performance comparison with other block ciphers

(iMac 13.2, Intel Core i7, best compiler optimization)



https://github.com/Roman-Oliynykov/ciphers-speed/

"Kalyna" performance comparison with other block ciphers

(iMac 13.2, Intel Core i7, best compiler optimization)

#	Block cipher	Performance, Mbit/s
1	Kalyna-128/128	1874.39
2	Kalyna-128/256	1295.55
3	Kalyna-256/256	1392.48
4	Kalyna-256/512	1088.88
5	Kalyna-512/512	1243.49
6	AES-128	1747.09
7	AES-256	1257.43
8	GOST 28147-89	576.10
9	STB 34.101.31-2011 (BelT)	1080.02
10	Kuznyechik	1146.31

DSTU 7624:2014 also includes

- Ten modes of operation for the new block cipher
  - ISO 10116: ECB, CBC, CFB, OFB, CTR
  - additional modes, simplified/improved comparing to NIST SP 800-38: GCM/GMAC (securing IP-traffic), CCM (confidentiality & integrity), XTS (on-the-fly encryption of information storage), KW (key data protection)
- Test vectors (including not aligned to the block length and, for some modes, byte length)
- Requirements to implementation:
  - general concepts paying developer's attention to take steps for prevention of side-channel attacks, timing attacks, CRIME/BREACH specific vulnerabilities, etc.
  - limits on the total number of invocation of the block cipher during the encryption key lifetime
  - message replay prevention
- etc.

Conclusions

The new block cipher "Kalyna" provides

- normal, high and ultra high security level
- transparent construction and conservative design
- fast and effective software and software-hardware implementations on modern 64-bit platforms
- optimized construction for better performance on encryption and decryption for CTR, CFB, CMAC, OFB, GCM, GMAC, CCM modes of operation
- new construction of key schedule based on the round transformation
- common look-up tables with the hash function "Kupyna" (the new Ukrainian standard DSTU 7564:2014)

Besides the block cipher, the new Ukrainian standard DSTU 7624:2014 defines ten modes of operation, test vectors, requirements for implementation, limits on protected information amount for a single key application, etc.