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

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

JSC Institute of Information Technologies,
State Service of Special Communication and Information Protection of Ukraine,
V.N.Karazin Kharkiv National University
Kharkiv National University of Radio Electronics
Ukraine

November 24th, 2015
NISK 2015
Ålesund, Norway

ІНСТИТУТ
ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ

1804
COGNOSCERE DOCERE ERUDIRE
Харківський національний університет
імені В.Н. Каразіна

My path: 2009-2015

Outline

- Second generation of block ciphers in the post-Soviet states
- The new Ukrainian block cipher Kalyna
- Performance comparison with other ciphers
- Other sections of the Ukrainian national standard DSTU 7624:2014
- Conclusions

The block cipher GOST 28147-89

Advantages

- a well known and researched cipher, adopted as the national standard in 1990
- acceptable encryption speed
- appropriate for lightweight cryptography
- "good" S-boxes provide practical strength

Disadvantages

- theoretically broken
- huge classes of weak keys
- special S-boxes allow practical ciphertext-only attacks
- significantly slower performance in comparison to modern block ciphers like AES

Replacements for GOST 28147-89 in Belarus

Belarus: STB 34.101.31-2011

- the block length is 128 bits; the key length is 128, 192 or 256 bits
- 8-round Feistel network with a Lai-Massey scheme
- a single byte S-box with good cryptographic properties
- no key schedule like in GOST
- no cryptanalytical attacks better than exhaustive search are known
- faster than GOST, but slower than AES

Replacements for GOST 28147-89 in Russia

Russia: GOST R 34.12-2015

- the block cipher Magma
  - GOST 28147-89 with fixed substitutions
- the block cipher Kuznyechik
  - the block length is 128 bits; the key length is 256 bits
  - 9 rounds of Rijndael-like transformation
  - single byte S-box (common with "Stribog")
  - non-circulant MDS matrix of 16x16 size over $GF(2^8)$ (different from "Stribog")
  - key schedule based on a Feistel network and involves round transformations
  - no cryptanalytical attacks better than exhaustive search are known
  - faster than GOST, slower* than AES

Replacements for GOST 28147-89 in Ukraine

Ukraine: DSTU 7624:2014

- normal, high and ultra high security level
  - the block and key length 128, 256 and 512 bits
- Rijndael-like SPN structure
- four different S-boxes (not CCZ-equivalent) with optimized cryptographic properties
- 8x8 MDS matrix over $GF(2^8)$
- a new construction of Key Schedule based on the round function
- faster than GOST, faster* than AES

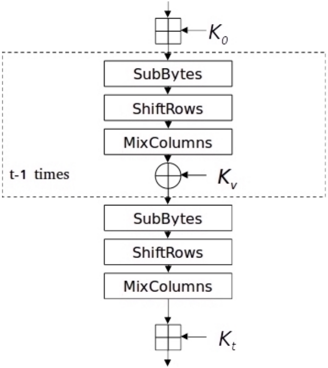
Kalyna: supported block and key lengths

l \ k	128	256	512	c
128	10	14	-	2
256	-	14	18	4
512	-	-	18	8

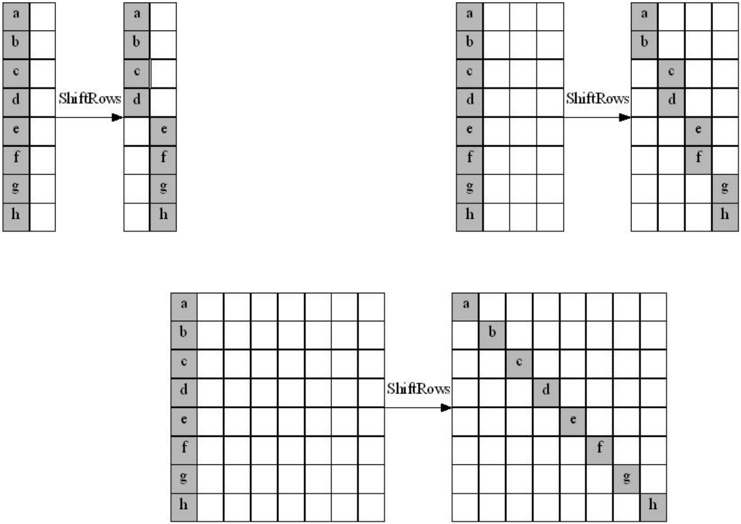
l: the block size; k: the key length;
t: the number of rounds; c: the number of columns

Kalyna: high-level 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: permutation of elements



Kalyna: properties of S-boxes

Property	S-box			
	1	2	3	4
Nonlinearity	104			
Min. algebraic degree of Boolean functions	7			
Max. value of difference distribution table	8			
Max. value of linear approximation table	24			
Algebraic immunity	3			
Number of cycles	4	4	6	4
Minimal cycle length	6	8	4	4

The best known byte permutations with algebraic immunity is equivalent to 3.

Kalyna: linear transformation

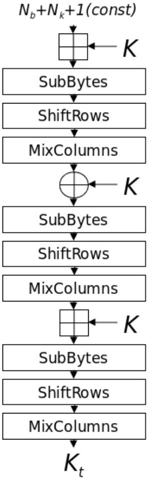
$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 01 \cdot a_0 \oplus 01 \cdot a_1 \oplus 05 \cdot a_2 \oplus 01 \cdot a_3 \oplus 08 \cdot a_4 \oplus 06 \cdot a_5 \oplus 07 \cdot a_6 \oplus 04 \cdot a_7 \\ 04 \cdot a_0 \oplus 01 \cdot a_1 \oplus 01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

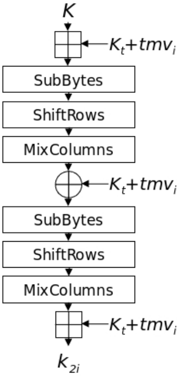
- the brunch number is 9 (the MDS matrix)
- effective software and software-hardware implementations

Requirements to Kalyna's Key Schedule

- 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 (the use of transformations from the round function)

Kalyna: Key Schedule





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

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

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

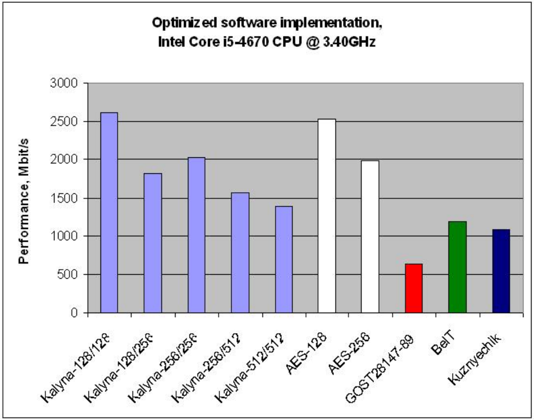
$$\Xi^{(K,K_\sigma,i)} = \eta_l^{(\varphi_i(K_\sigma))} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \kappa_l^{(\varphi_i(K_\sigma))} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(\varphi_i(K_\sigma))}$$

Cryptanalytic attack against Kalyna

Kalyna is resistant to known cryptanalytic methods (based on public information):

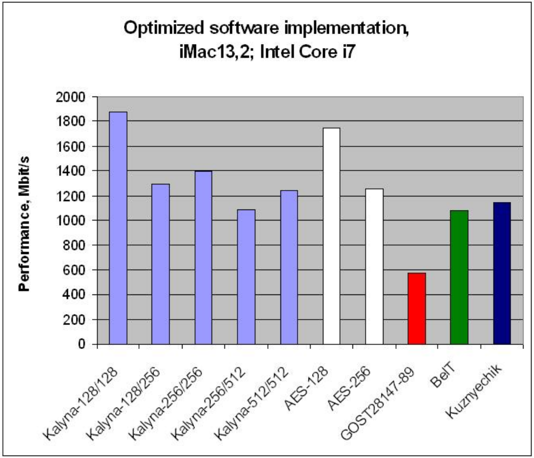
- Kalyna-128/128: from 6^{th} round (out of 10)
- Kalyna-128/256: from 10^{th} round* (out of 14)
- Kalyna-256/256: from 7^{th} round (out of 14)
- Kalyna-256/512: from 10^{th} round* (out of 18)
- Kalyna-512/512: from 9^{th} round (out of 18)

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



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

NIST STS of Kalyna's output sequences

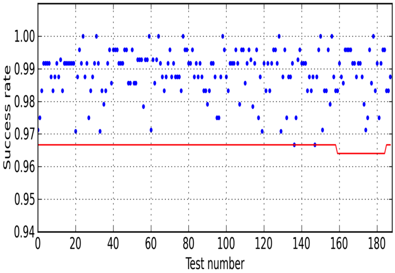


Figure: Even round keys

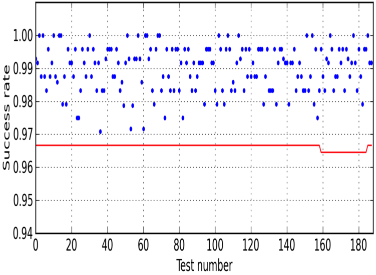


Figure: CTR encryption

DSTU 7624:2014: modes of operation

#	Description	Name	Property
1	Electronic Codebook	ECB	confidentiality
2	Counter	CRT	confidentiality
3	Cipher Feedback	CFB	confidentiality
4	Cipher-based Message Authentication Code	CMAC	integrity
5	Cipher Block Chaining	CBC	confidentiality
6	Output Feedback	OFB	confidentiality
7	Galois Counter Mode	GCM	confidentiality and integrity
	Galois Message Authentication Code	GMAC	integrity
8	Counter with CBC-MAC	CCM	confidentiality and integrity
9	XEX-based tweaked-codebook mode with ciphertext stealing	XTS	confidentiality
10	Key Wrap	KW	confidentiality and integrity

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, CCM, XTS, KW
- 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 Kalyna block cipher 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
- a 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.

Title

Figure: Kalyna / Viburnum / Krossvedslekta