A New Standard of Ukraine: The Kupyna Hash Function (DSTU 7564:2014)

Roman Oliynykov,
Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev,
Oleksandr Kuznetsov, Yurii Gorbenko, Artem Boiko,
Oleksandr Dyrda, Viktor Dolgov and Andrii Pushkaryov

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

Outline

- Retrospective
- The new Ukrainian hash function Kupyna
- Performance comparison with other ciphers
- Conclusions

Retrospective

- theoretical attacks on the previous hash standard GOST 34.311:2009 (GOST 34.311-95)
  - its computational inefficiency in modern platforms
- 256-bit length of a hash value is insufficient for some applications
- replacement in the other post-Soviet states
  - the Belarusian standard STB 34.101.31-2011 defines a hash function
  - GOST R 34.11-2012 ("Streebog") is the new hash function in Russia

Theoretical weaknesses of GOST 34.311:2009

- Complexities of cryptanalytic attacks less than brute-force:
  - pre-image attacks 2^{192}
  - a collision attack 2^{105}
- Cryptanalytic attacks are theoretical
  - memory complexity is 2^{75}

The requirements for the prospective hash function

- the lengths of hash values are 256, 384 and 512 bits
  - supporting lengths from 8 to 512 bits with the 8-bit step
- no limitations on processing messages
- support of the additional mode message authentication code (MAC)
- a conservative approach to the development
  - the use of well-proven constructions
- optimized for modern 64-bit platforms
  - effective in 32-bit implementations
- performance better than GOST 34.311:2009

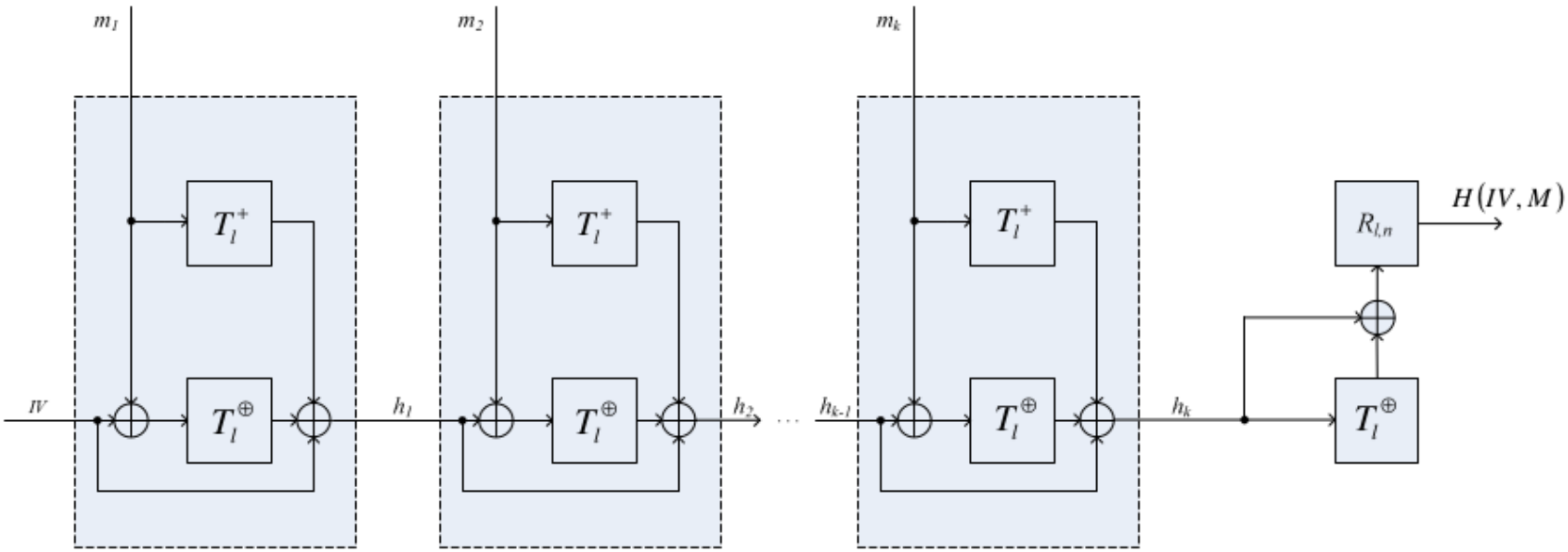
Kupyna: parameters

Table: General parameters for Kupyna

Hash code length (n)	Internal state size (l)	Number of rounds (t)	Rows of the state matrix (c)
$8 \leq n \leq 256$	512	10	8
$256 < n \leq 512$	1024	14	16

Kupyna: high-level structure

$$l = \begin{cases} 512, & \text{if } 8 \leq n \leq 256; \\ 1024, & \text{if } 256 < n \leq 512. \end{cases} \qquad IV = \begin{cases} 1 \ll 510, & \text{if } l = 512; \\ 1 \ll 1023, & \text{if } l = 1024. \end{cases}$$



Kupyna: $T_l^{\oplus}$ and T_l^{+}

$$T_l^{\oplus} = \prod_{\nu=0}^{t-1} \left(\psi \circ \tau^{(l)} \circ \pi' \circ \kappa_\nu^{(l)} \right) \quad T_l^{+} = \prod_{\nu=0}^{t-1} \left(\psi \circ \tau^{(l)} \circ \pi' \circ \eta_\nu^{(l)} \right)$$

- based on the block cipher Kalyna defined in DSTU 7624:2014
- both $T_l^{\oplus}$ and T_l^{+} are pseudorandom functions
- differ in
  - round constants
  - operations of mixing round constants ($mod 2^{64}$, XOR)

Kupyna: constants

$$T_l^{\oplus} : C^i = \begin{bmatrix} 00 \oplus i & 10 \oplus i & 20 \oplus i & 30 \oplus i & 40 \oplus i & 50 \oplus i & \ldots & \text{f}0 \oplus i \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \end{bmatrix}$$

$$T_l^{+} : C^i = \begin{bmatrix} \text{f3} & \text{f3} & \text{f3} & \text{f3} & \text{f3} & \text{f3} & \ldots & \text{f3} \\ \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \ldots & \text{f0} \\ \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \ldots & \text{f0} \\ \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \ldots & \text{f0} \\ \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \ldots & \text{f0} \\ \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \ldots & \text{f0} \\ \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \text{f0} & \ldots & \text{f0} \\ \text{f0} \oplus i & \text{e0} \oplus i & \text{d0} \oplus i & \text{c0} \oplus i & \text{b0} \oplus i & a0 \oplus i & \ldots & 00 \oplus i \end{bmatrix}$$

Kupyna: 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

Equivalent to ones defined in DSTU 7624:2014

Kupyna: permutation of bytes

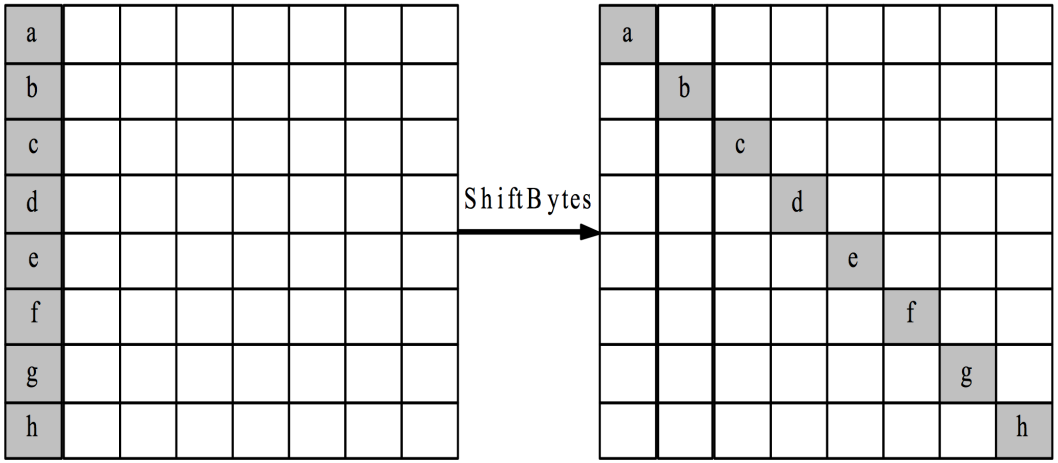


Figure: For $l = 512$

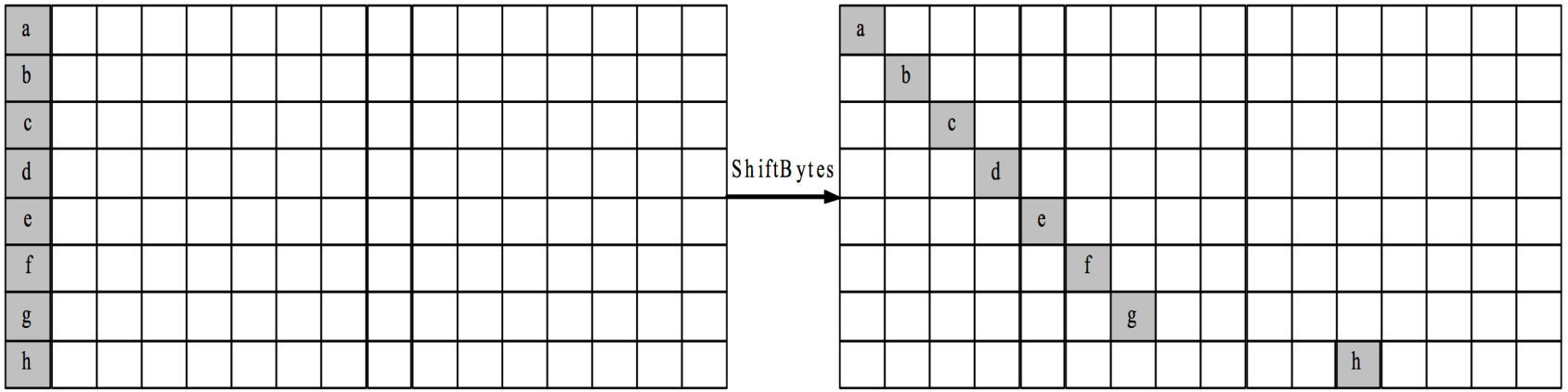


Figure: For $l = 1024$

Kupyna: 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

Transformations from Kalyna

Advantages of using transformations from the block cipher Kalyna

- high and ultra high security level
- high performance of cryptographic transformations
- compact implementation
- the Rijndael-like structure provides pseudorandom properties of permutations even for constant round keys (or their absence at all)

Design principles of the hash function Kupyna

security - performance - compactness

Design principles of the hash function Kupyna

security - performance - compactness

- use proven constructions
- transparency of chosen solutions
- protection from known cryptanalytic methods

Design principles of the hash function Kupyna

security - performance - compactness

- use proven constructions
- transparency of chosen solutions
- protection from known cryptanalytic methods
- focus on modern platforms (64-bit)
  - the effectiveness on existing (32-bit)

Cryptanalytic attack against Kupyna

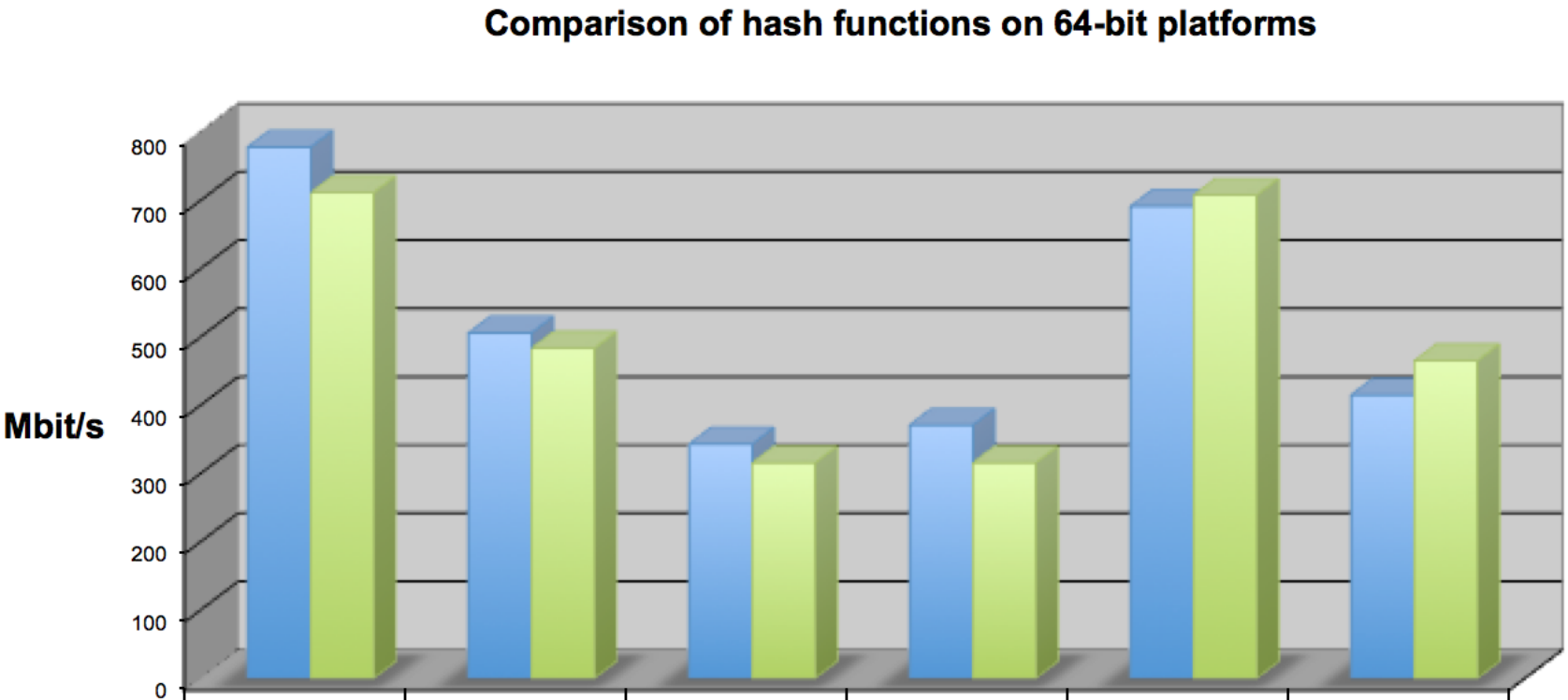
Kupyna is resistant to known cryptanalytic methods (based on public information)

Attack	Kupyna-256	Kupyna-512
Collision	2^{128}	2^{256}
First pre-image	2^{256}	2^{512}
Second pre-image	2^{256}	2^{512}
Fixed points	2^{256}	2^{512}
Length extension	2^{256}	2^{512}

The Ukraine standard DSTU 7564:2014

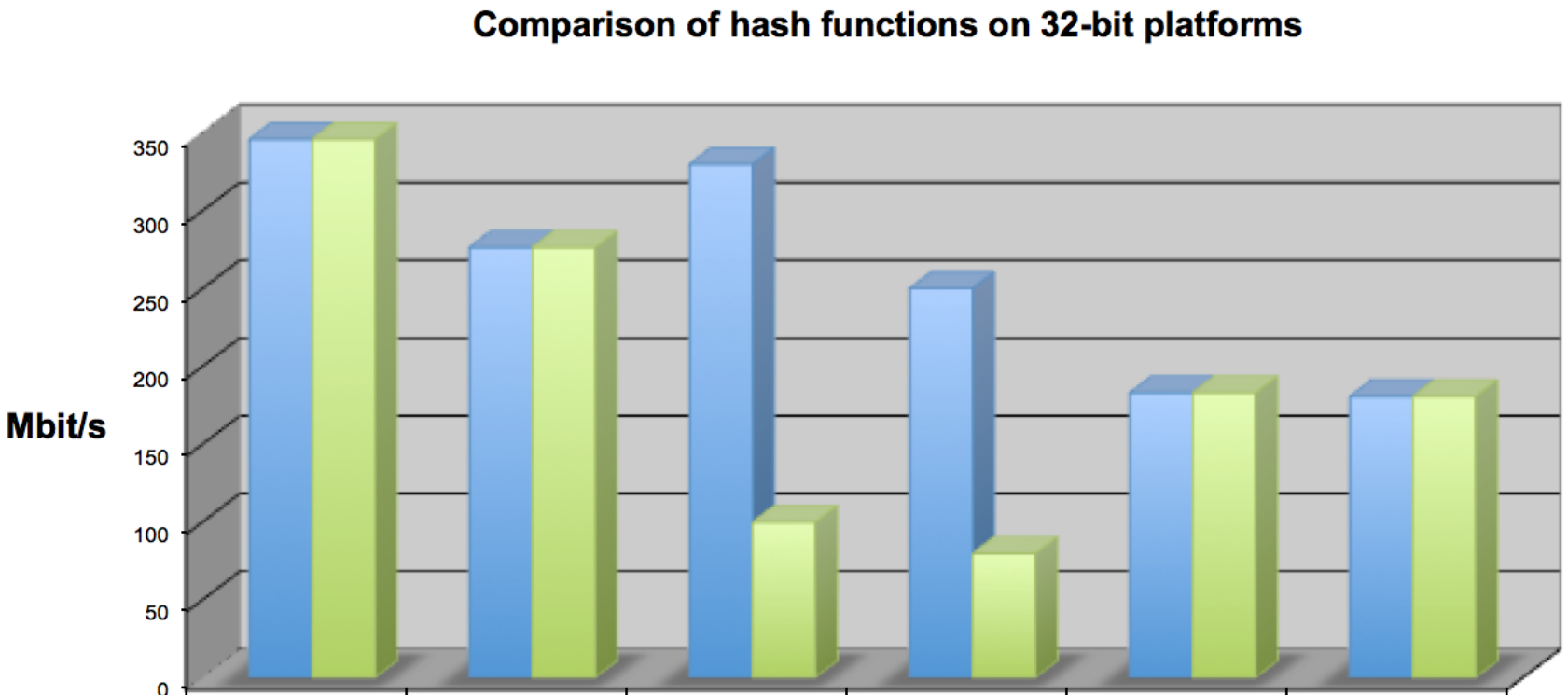
- based on the hash function Kupyna
  - the length of the hash value is flexible
  - predefined recommended parameters
- the message length can vary from 0 (the empty message) to $2^{96} - 1$ bits
- test vectors including not aligned to the block and byte length
- generating of MAC is defined as a mode of operation

Kupyna: performance comparison



	Kupyna-256	Kupyna-512	GOST 34.311-95	Stribog (256,512)	Groestl-256	Groestl-512
Linux 64-bit	778.3093	506.0145	343.2474	371.3182	691.6352	415.3906
Windows 64-bit	711.6397	483.6045	315.8514	316.0483	707.8276	465.3006

Kupyna: performance comparison



	Kupyna-256	Kupyna-512	GOST 34.311-95	Stribog (256,512)	Groestl-256	Groestl-512
Linux 32-bit	346.1454	276.6373	330.1143	250.2085	183.167	180.8638
Windows 32-bit	346.1454	276.6373	100	80	183.167	180.8638

Conclusions

The hash function Kupyna

- provides resistance to known cryptanalytic methods
- based on proven and transparent design principles
- generates hash values that meet the requirements for pseudorandom sequences (NIST STS)
- provides high performance on 64-bit and 32-bit platforms
- allows implement encryption algorithms effectively

Title

Figure: Kupyna / Polygonatum / Kantkonvall