Algebraic Aspects of the Russian Hash Standard GOST R 34.11-2012

Oleksandr Kazymyrov, Valentyna Kazymyrova

Selmer Center, Department of Informatics,
University of Bergen, Norway
Oleksandr.Kazymyrov@uib.no

CTCrypt 2013

Agenda

Basic Operations and Functions

GOST R 34.11-2012 (Stribog) is based on SP-network block cipher with block and key length equal 512 bits

- SubBytes (S): nonlinear bijective mapping.
- Transposition (P): byte permutation.
- MixColumns (L): linear transformation.
- AddRoundKey (X): addition with the round key using bitwise XOR.

Other basic functions

- $\boxplus$: addition modulo 2^{512}.
- $MSB_s(A)$: getting s most significant bits of vector A.
- $A||B$: concatenation of two vectors A and B.

State Representation

Grøstl

a_0	a_8	a_{16}	a_{24}	a_{32}	a_{40}	a_{48}	a_{56}
a_1	a_9	a_{17}	a_{25}	a_{33}	a_{41}	a_{49}	a_{57}
a_2	a_{10}	a_{18}	a_{26}	a_{34}	a_{42}	a_{50}	a_{58}
a_3	a_{11}	a_{19}	a_{27}	a_{35}	a_{43}	a_{51}	a_{59}
a_4	a_{12}	a_{20}	a_{28}	a_{36}	a_{44}	a_{52}	a_{60}
a_5	a_{13}	a_{21}	a_{29}	a_{37}	a_{45}	a_{53}	a_{61}
a_6	a_{14}	a_{22}	a_{30}	a_{38}	a_{46}	a_{54}	a_{62}
a_7	a_{15}	a_{23}	a_{31}	a_{39}	a_{47}	a_{55}	a_{63}

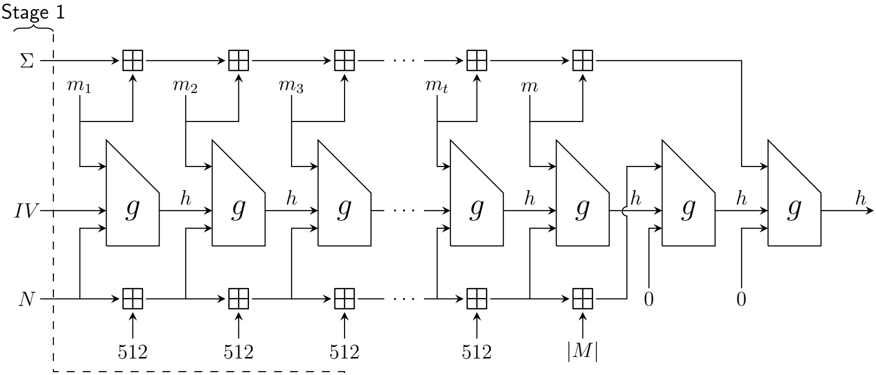
Stribog

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
a_{16}	a_{17}	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}
a_{24}	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}	a_{30}	a_{31}
a_{32}	a_{33}	a_{34}	a_{35}	a_{36}	a_{37}	a_{38}	a_{39}
a_{40}	a_{41}	a_{42}	a_{43}	a_{44}	a_{45}	a_{46}	a_{47}
a_{48}	a_{49}	a_{50}	a_{51}	a_{52}	a_{53}	a_{54}	a_{55}
a_{56}	a_{57}	a_{58}	a_{59}	a_{60}	a_{61}	a_{62}	a_{63}

$$A = a_0||a_1|| \ldots ||a_{63}$$

Agenda

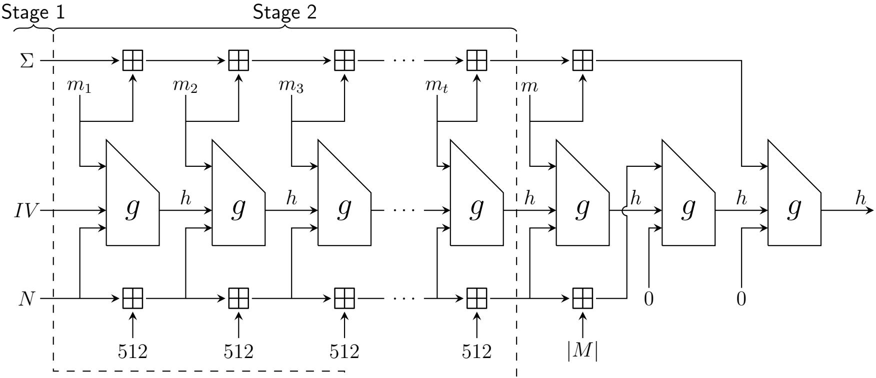
Hash Function Stribog. Stage 1



$\Sigma = N = 0^{512}$

$$IV = \begin{cases} 0, & \text{Stribog-512} \\ (00000001)^{64}, & \text{Stribog-256} \end{cases}$$

Hash Function Stribog. Stage 2

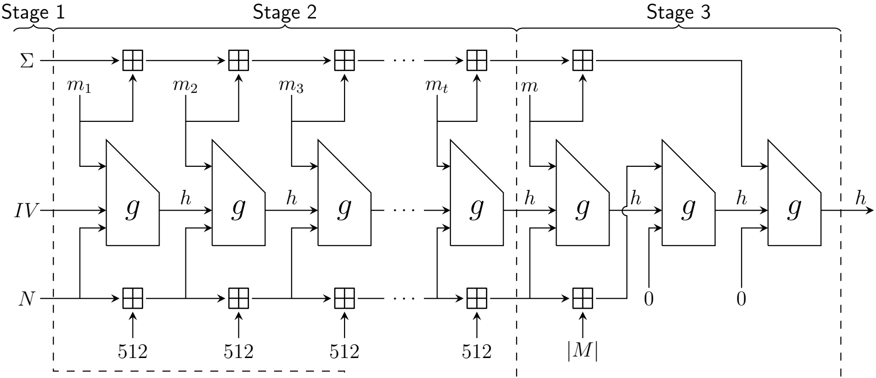


$\Sigma = N = 0^{512}$

$IV = \begin{cases} 0, & \text{Stribog-512} \\ (00000001)^{64}, & \text{Stribog-256} \end{cases}$

$t = \left\lfloor \frac{|M|}{512} \right\rfloor$

Hash Function Stribog. Stage 3



$\Sigma = N = 0^{512}$

$IV = \begin{cases} 0, & \text{Stribog-512} \\ (00000001)^{64}, & \text{Stribog-256} \end{cases}$

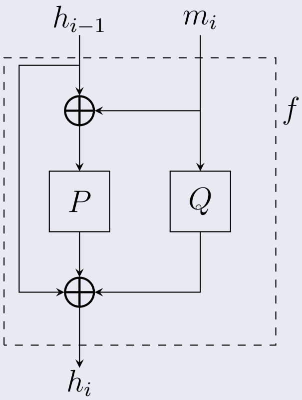
$t = \left\lfloor \frac{|M|}{512} \right\rfloor$

$m = 0^{512-|M|}||1||M$

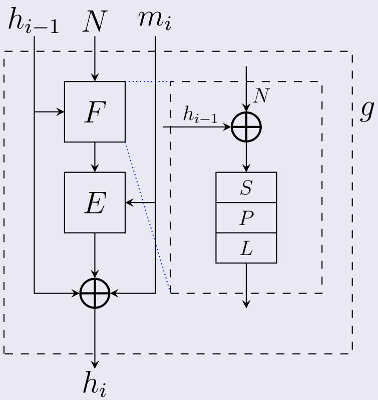
$H = \begin{cases} h, & \text{Stribog-512} \\ MSB_{256}(h), & \text{Stribog-256} \end{cases}$

Construction of the Compression Function g

Grøstl

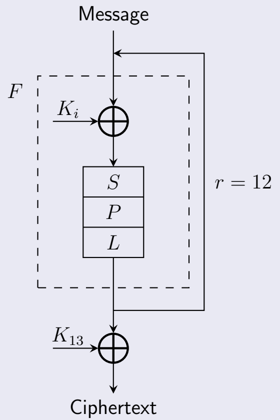


Stribog

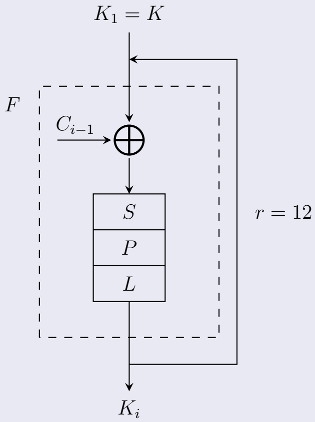


Representation of E

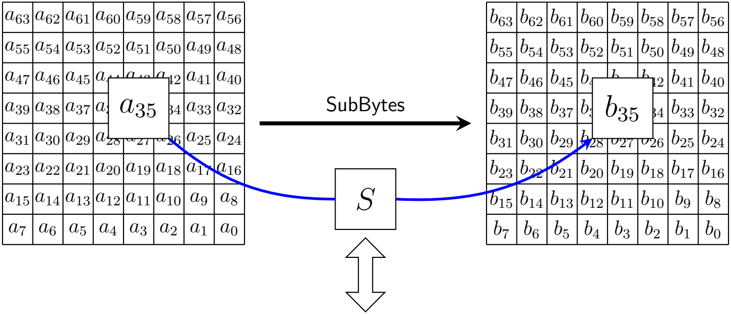
Block Cipher of Stribog



Key Schedule



SubBytes (S)



$$b_i = \text{S-box}(a_i)$$

Transposition (P)

Transposition transformation has a form

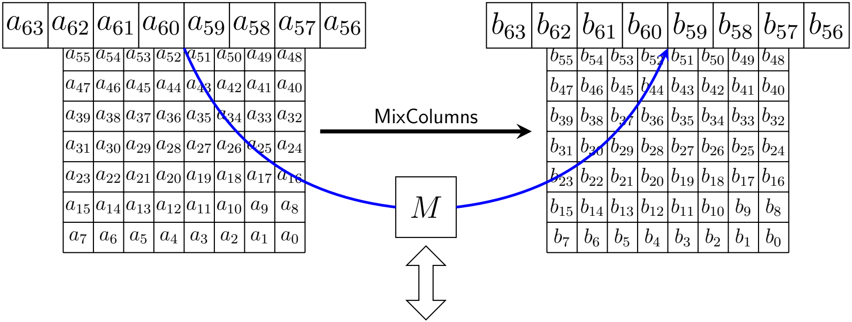
a_{63}	a_{62}	a_{61}	a_{60}	a_{59}	a_{58}	a_{57}	a_{56}
a_{55}	a_{54}	a_{53}	a_{52}	a_{51}	a_{50}	a_{49}	a_{48}
a_{47}	a_{46}	a_{45}	a_{44}	a_{43}	a_{42}	a_{41}	a_{40}
a_{39}	a_{38}	a_{37}	a_{36}	a_{35}	a_{34}	a_{33}	a_{32}
a_{31}	a_{30}	a_{29}	a_{28}	a_{27}	a_{26}	a_{25}	a_{24}
a_{23}	a_{22}	a_{21}	a_{20}	a_{19}	a_{18}	a_{17}	a_{16}
a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8
a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0

Transpose →

a_{63}	a_{55}	a_{47}	a_{39}	a_{31}	a_{23}	a_{15}	a_7
a_{62}	a_{54}	a_{46}	a_{38}	a_{30}	a_{22}	a_{14}	a_6
a_{61}	a_{53}	a_{45}	a_{37}	a_{29}	a_{21}	a_{13}	a_5
a_{60}	a_{52}	a_{44}	a_{36}	a_{28}	a_{20}	a_{12}	a_4
a_{59}	a_{51}	a_{43}	a_{35}	a_{27}	a_{19}	a_{11}	a_3
a_{58}	a_{50}	a_{42}	a_{34}	a_{26}	a_{18}	a_{10}	a_2
a_{57}	a_{49}	a_{41}	a_{33}	a_{25}	a_{17}	a_9	a_1
a_{56}	a_{48}	a_{40}	a_{32}	a_{24}	a_{16}	a_8	a_0

MixColumns (L)

MixColumns transformation has a form



Multiplying the vector by the constant 64×64 matrix M over $\mathbb{F}_2$

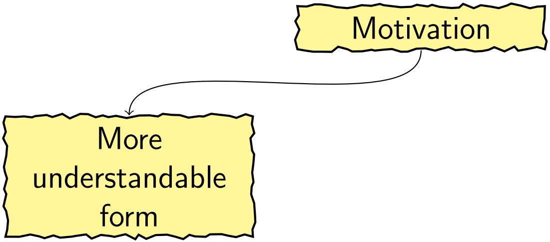
$$B = A \cdot M$$

Agenda

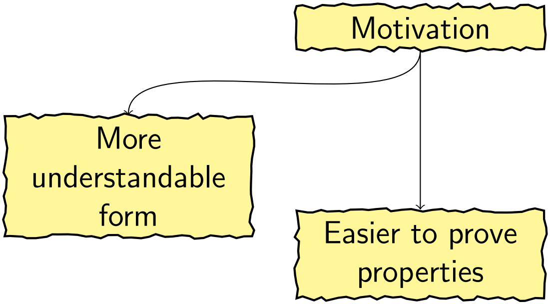
Motivation

Motivation

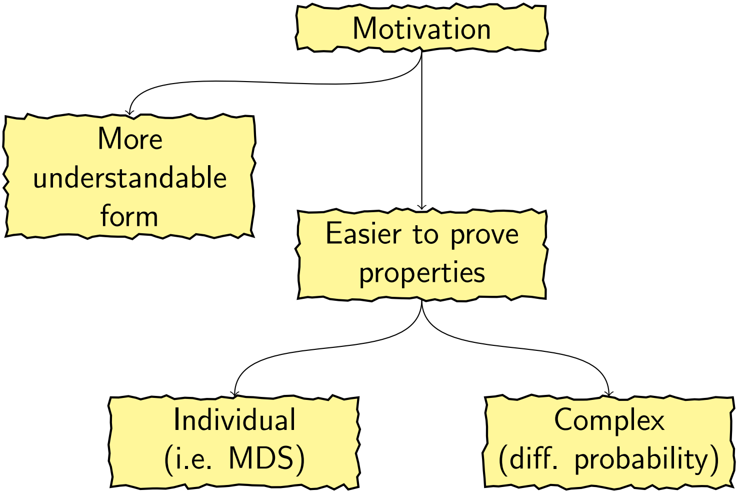
Motivation



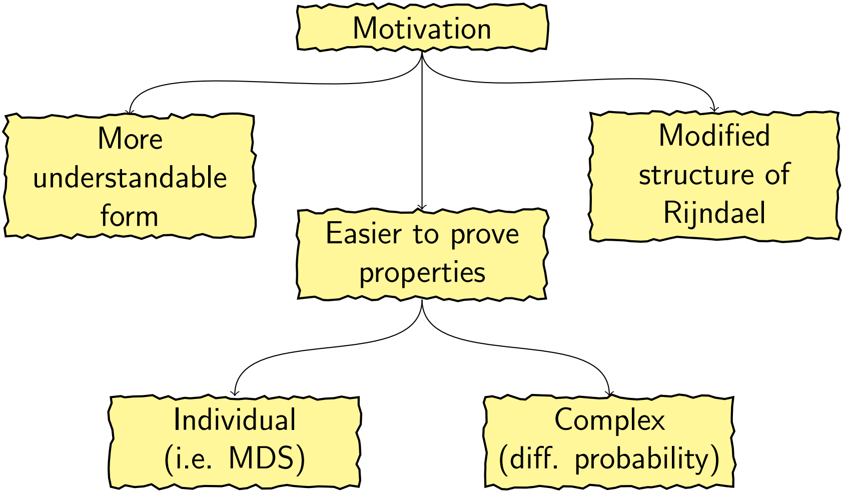
Motivation


Motivation
More understandable form
Easier to prove properties

Motivation


Motivation
More understandable form
Easier to prove properties
Individual (i.e. MDS)
Complex (diff. probability)

Motivation


Motivation
More understandable form
Easier to prove properties
Modified structure of Rijndael
Individual (i.e. MDS)
Complex (diff. probability)

State Representation

Alternative representation

- Reverse input bits
- AES-like transformations (state as in Grøstl)
- Reverse output bits

$$\begin{array}{ccc} B_0, B_1, \ldots, B_{63} & & B'_0, B'_1, \ldots, B'_{63} \\ \updownarrow & & \updownarrow \\ b_0, b_1, \ldots, b_{511} & \xleftrightarrow{\text{ReverseBits}} & b_{511}, b_{510}, \ldots, b_0 \end{array}$$

Transposition and SubBytes Operations

- Transposition is invariant operation.
- Substitution has the form $F(x) = D \circ G \circ D(x)$ for linearized polynomial $D : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$.

Transposition and SubBytes Operations

- Transposition is invariant operation.
- Substitution has the form $F(x) = D \circ G \circ D(x)$ for linearized polynomial $D : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	3F	FB	D7	E0	9F	E5	A8	04	97	07	AD	87	A0	B5	4C	9A
1	DF	EB	4F	0C	81	58	CF	D3	E8	3B	FD	B1	60	31	B6	8B
2	F3	7C	57	61	47	78	08	B4	C9	5E	10	32	C7	E4	FF	67
3	C4	3E	BF	11	D1	26	B9	7D	28	72	39	53	FE	96	C3	9C
4	BB	24	34	CD	A6	06	69	E6	0F	37	70	C1	40	62	98	2E
5	5F	6B	16	D6	3C	1C	1E	A4	8F	14	C8	55	B7	A5	63	F5
6	8C	C2	12	B8	F7	46	59	90	99	0D	6E	1F	F1	AA	51	2D
7	20	9D	73	E7	71	64	4D	36	FA	50	BA	A1	CB	A9	B0	C6
8	77	AF	2C	1A	18	E9	85	8E	EE	F0	0E	D8	21	A2	AE	65
9	23	9E	54	EC	38	1D	89	D9	6C	17	4E	CA	D0	C5	2A	66
A	76	15	13	35	3A	00	DE	D4	74	29	30	FC	56	7A	AC	2F
B	A3	44	5C	9B	80	F9	79	A7	B3	CC	ED	1B	2B	AB	BD	D2
C	88	95	8A	02	5A	CE	94	25	DB	7B	6A	92	75	49	BC	4B
D	5B	6F	45	27	42	41	F6	0B	DD	0A	E2	09	19	BE	01	43
E	68	93	D5	EF	84	22	E3	DA	5D	3D	48	7F	05	F4	7E	03
F	B2	C0	33	91	F2	82	8D	4A	83	52	E1	86	F8	DC	EA	6D

Table : The Substitution F for AES-like Description

Representation of MixColumns (1/4)

The are exist at least three forms:

1. representation over $\mathbb{F}_{2^n}$
2. representation over $\mathbb{F}_2$
    1. matrix form
    2. system of equations

Representation of MixColumns (1/4)

The are exist at least three forms:

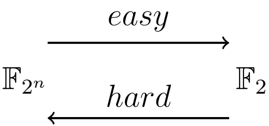
1. representation over $\mathbb{F}_{2^n}$
2. representation over $\mathbb{F}_2$
    1. matrix form
    2. system of equations

$$\mathbb{F}_{2^n} \xrightarrow{\;easy\;} \mathbb{F}_2$$

Representation of MixColumns (1/4)

The are exist at least three forms:

1. representation over $\mathbb{F}_{2^n}$
2. representation over $\mathbb{F}_2$
   1. matrix form
   2. system of equations



Representation of MixColumns (2/4)

Let $L : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ be a linear function of the form

$$L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i}, \quad \delta_i \in \mathbb{F}_{2^n}.$$

Proposition

Any linear function $L : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$ can be converted to a matrix with the complexity $O(n)$.

$$L(x) = \delta x, \quad \delta_i = 0, \text{ for } 1 \leq i \leq n-1.$$

Representation of MixColumns (3/4)

Any multiplication mapping $\mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is a linear transformation of a vector space over $\mathbb{F}_2$ for specified basis.

Multiplication by arbitrary $\delta \in \mathbb{F}_{2^8}$ can be represented as multiplication by a matrix

$$\delta x = \begin{pmatrix} k_{0,0} & \cdots & k_{0,7} \\ k_{1,0} & \cdots & k_{1,7} \\ \vdots & \ddots & \vdots \\ k_{7,0} & \cdots & k_{7,7} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ \ldots \\ x_7 \end{pmatrix}$$

where $x_i, k_{j,s} \in \mathbb{F}_2$.

Representation of MixColumns (3/4)

Any multiplication mapping $\mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is a linear transformation of a vector space over $\mathbb{F}_2$ for specified basis.

Multiplication by arbitrary $\delta \in \mathbb{F}_{2^8}$ can be represented as multiplication by a matrix

$$\delta = \begin{pmatrix} k_{0,0} & \cdots & k_{0,7} \\ k_{1,0} & \cdots & k_{1,7} \\ \vdots & \ddots & \vdots \\ k_{7,0} & \cdots & k_{7,7} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

where $x_i, k_{j,s} \in \mathbb{F}_2$.

Representation of MixColumns (4/4)

The main steps of proposed algorithm for obtaining MDS matrix over $\mathbb{F}_{2^8}$ from 64×64 matrix over $\mathbb{F}_2$

1. for every irreducible polynomial (30)
   1. convert each of 8×8 submatrices to the element of the filed
   2. check MDS property of the resulting matrix

Representation of MixColumns (4/4)

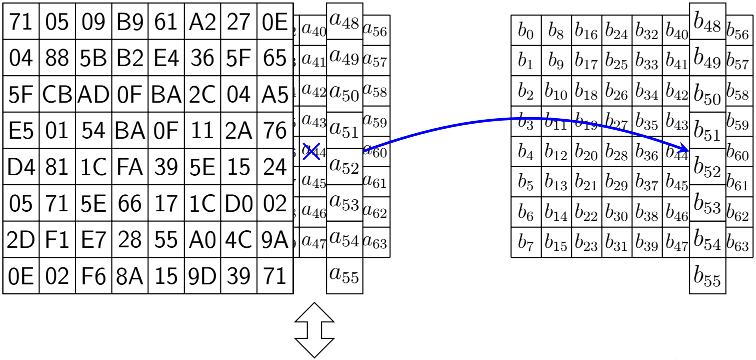
The main steps of proposed algorithm for obtaining MDS matrix over $\mathbb{F}_{2^8}$ from 64×64 matrix over $\mathbb{F}_2$

1. for every irreducible polynomial (30)
    1. convert each of 8×8 submatrices to the element of the filed
    2. check MDS property of the resulting matrix

Hint

It is necessary to transpose matrix of Stribog before applying the algorithm.

MixColumns

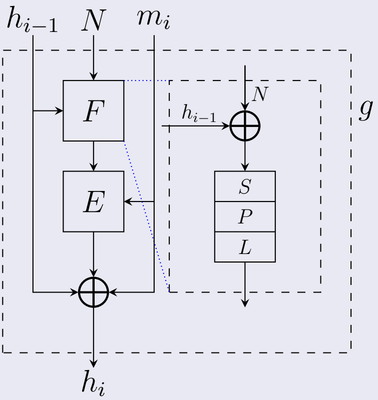


Multiplying the vector by the constant 8×8 matrix G over $\mathbb{F}_{2^8}$ with the primitive polynomial $f(x) = x^8 + x^6 + x^5 + x^4 + 1$

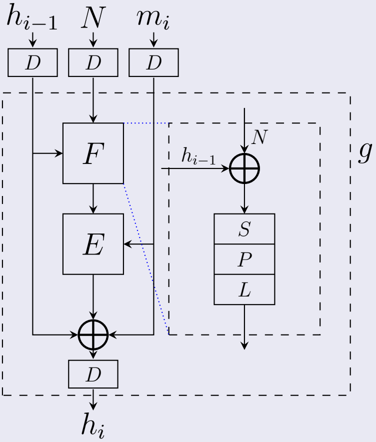
$$B = G \cdot A$$

AES-like Form of Compression Function

Original Function



Modified Function



Agenda

Conclusions

- GOST R 34.11-2012 is based on GOST 34.11-94 as well as on Whirlpool/ Grøstl/AES.

Conclusions

- GOST R 34.11-2012 is based on GOST 34.11-94 as well as on Whirlpool/ Grøstl/AES.
- Performance of GOST R 34.11-2012 is based on the message length.

Conclusions

- GOST R 34.11-2012 is based on GOST 34.11-94 as well as on Whirlpool/ Grøstl/AES.
- Performance of GOST R 34.11-2012 is based on the message length.
- Proposed method has many application fields.

Conclusions

- GOST R 34.11-2012 is based on GOST 34.11-94 as well as on Whirlpool/ Grøstl/AES.
- Performance of GOST R 34.11-2012 is based on the message length.
- Proposed method has many application fields.
- More details on https://github.com/okazymyrov