Prototype of Russian Hash Function "Stribog"

Oleksandr Kazymyrov

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

Spring 2013

Outline

Motivation

- GOST 34.11-94 was theoretically broken in 2008.
  - The complexities $O(2^{192})/O(2^{69})$ for preimage and second preimage attacks.

Motivation

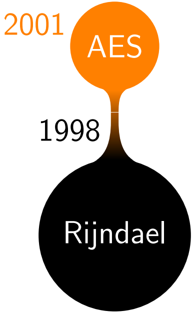
- GOST 34.11-94 was theoretically broken in 2008.
  - The complexities $O(2^{192})/O(2^{69})$ for preimage and second preimage attacks.
- Increasing performance. Stribog is 20% faster than GOST 34.11-94.

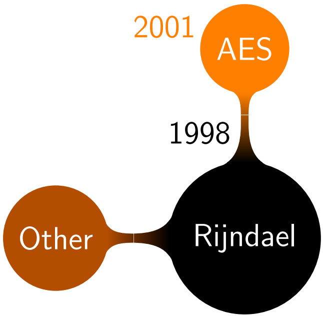
Motivation

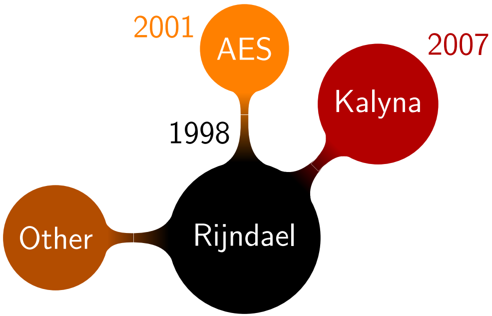
- GOST 34.11-94 was theoretically broken in 2008.
  - The complexities $O(2^{192})/O(2^{69})$ for preimage and second preimage attacks.
- Increasing performance. Stribog is 20% faster than GOST 34.11-94.
- Opposite to SHA-3 (Keccak).

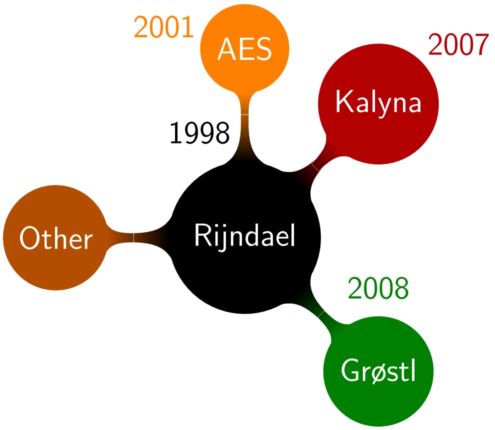
1998

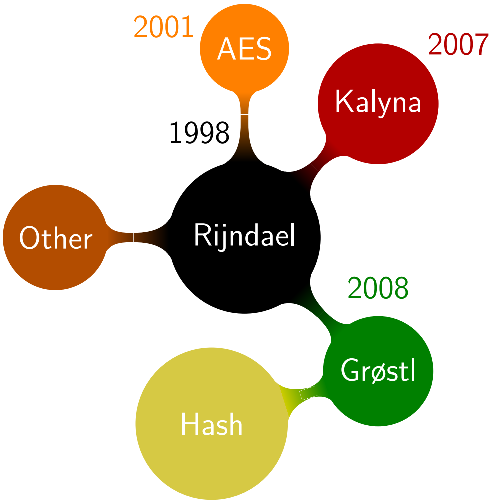
Rijndael

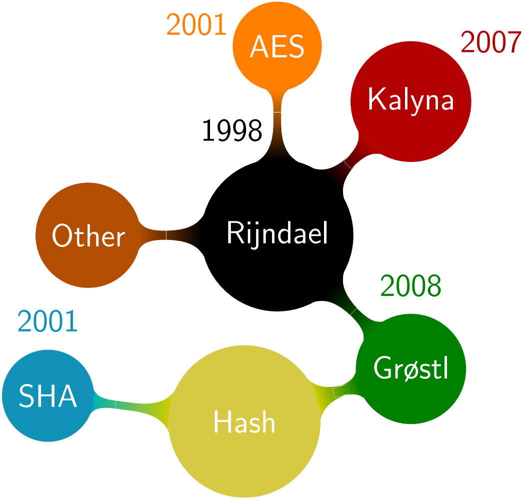

2001
AES
1998
Rijndael

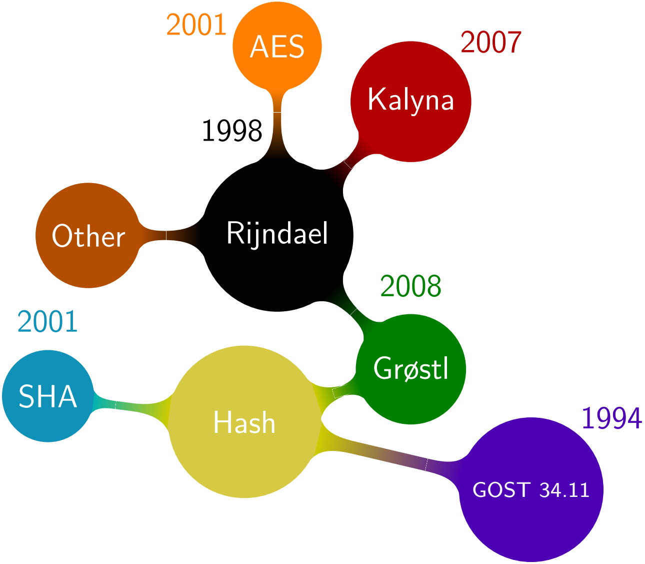

2001
AES
1998
Other
Rijndael

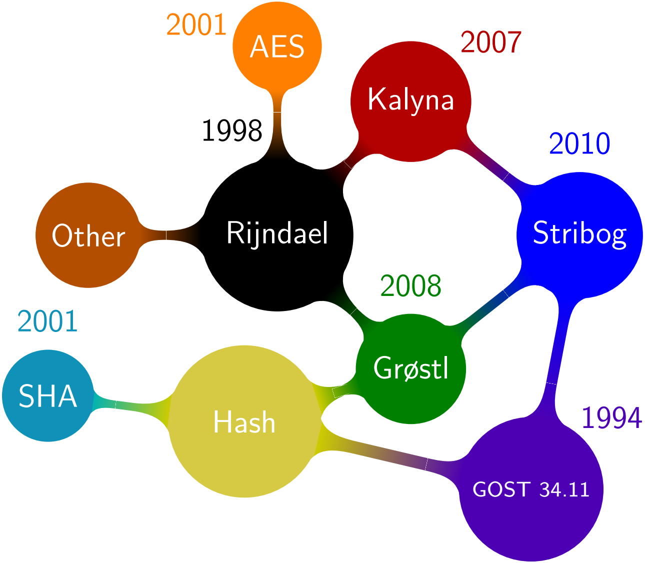

2001
AES
2007
Kalyna
1998
Other
Rijndael


2001
AES
2007
Kalyna
1998
Other
Rijndael
2008
Grøstl


2001
AES
2007
Kalyna
1998
Other
Rijndael
2008
Grøstl
Hash


2001
AES
2007
Kalyna
1998
Rijndael
Other
2008
Grøstl
2001
SHA
Hash


2001
AES
2007
Kalyna
1998
Rijndael
Other
2008
Grøstl
2001
SHA
Hash
1994
GOST 34.11


2001
AES
2007
Kalyna
1998
2010
Other
Rijndael
Stribog
2008
2001
Grøstl
SHA
Hash
1994
GOST 34.11

Basic Operations and Functions

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}

$$\Updownarrow$$

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

Stribog

b_{63}	b_{62}	b_{61}	b_{60}	b_{59}	b_{58}	b_{57}	b_{56}
b_{55}	b_{54}	b_{53}	b_{52}	b_{51}	b_{50}	b_{49}	b_{48}
b_{47}	b_{46}	b_{45}	b_{44}	b_{43}	b_{42}	b_{41}	b_{40}
b_{39}	b_{38}	b_{37}	b_{36}	b_{35}	b_{34}	b_{33}	b_{32}
b_{31}	b_{30}	b_{29}	b_{28}	b_{27}	b_{26}	b_{25}	b_{24}
b_{23}	b_{22}	b_{21}	b_{20}	b_{19}	b_{18}	b_{17}	b_{16}
b_{15}	b_{14}	b_{13}	b_{12}	b_{11}	b_{10}	b_9	b_8
b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0

$$\Updownarrow$$

$$B = b_{63}||b_{62}||\dots||b_0$$

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}

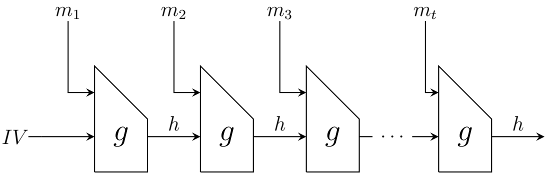
Stribog

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}

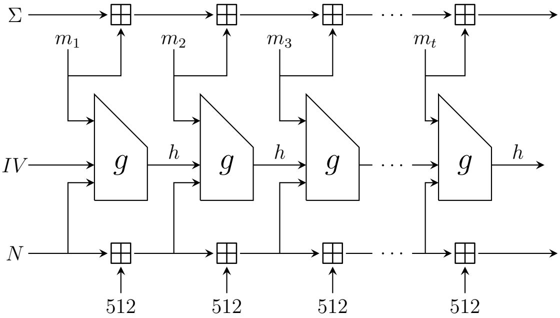
$$A = a_0||a_1||\dots||a_{63}$$

Outline

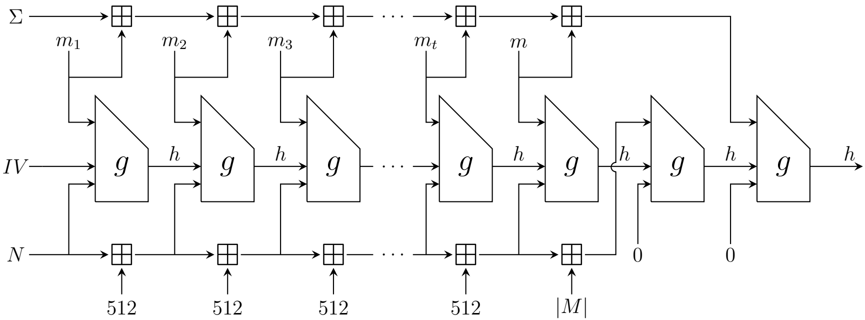
Merkle-Damgård Scheme



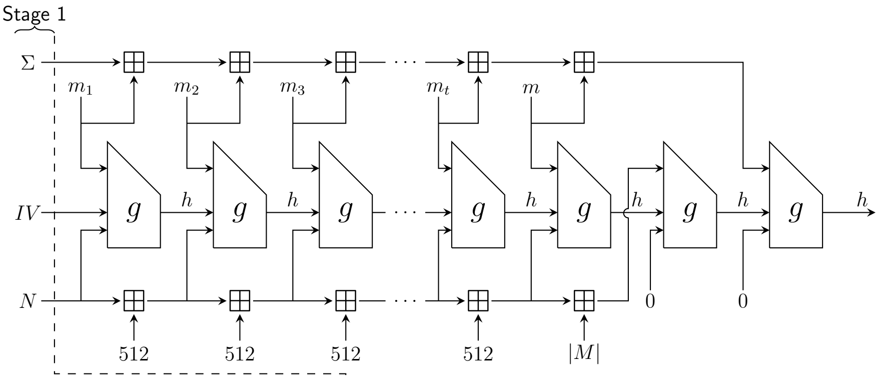
Modification of Merkle-Damgård Scheme



Hash Function Stribog



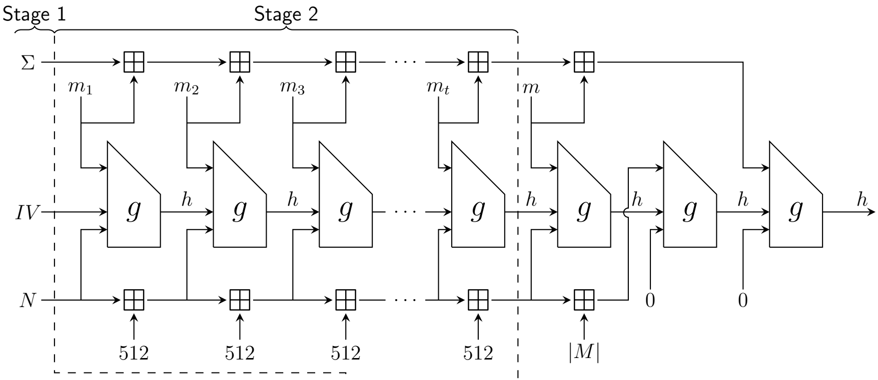
Hash Function Stribog. Stage 1



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

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

Hash Function Stribog. Stage 2

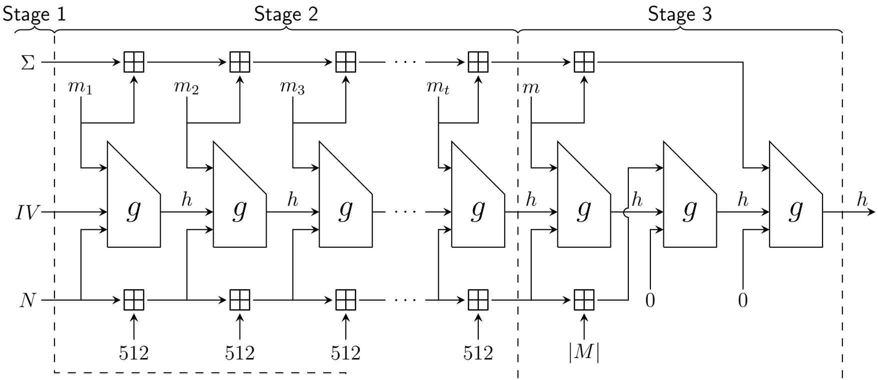


$$\Sigma = N = 0^{512}$$

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

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

Hash Function Stribog. Stage 3



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

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

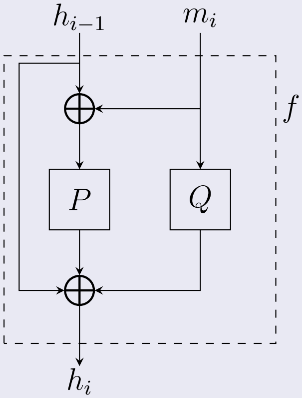
$$t = \left\lfloor \frac{|M|}{512} \right\rfloor$$

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

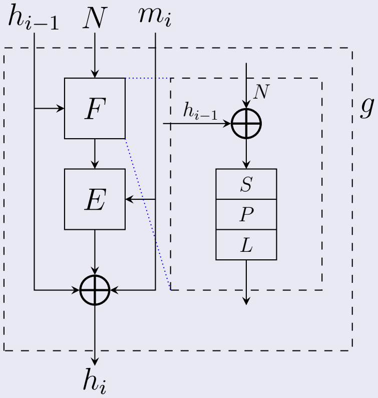
$$H = \begin{cases} h, & \text{Stribog-512} \\ MSB_{256}(h), & \text{Stribog-256} \end{cases}$$

Compression Function Construction

Grøstl



Stribog



Design of E

Compression function $g_N : \mathbb{F}_2^{512} \times \mathbb{F}_2^{512} \mapsto \mathbb{F}_2^{512}$, $N \in \mathbb{F}_2^{512}$ is defined as follows

$$g_N(h, m) = E(L \circ P \circ S(h \oplus N), m) \oplus h \oplus m, \quad h, m \in \mathbb{F}_2^{512}$$

where

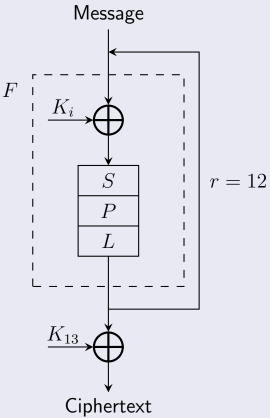
$$E(K, m) = X[K_{13}] \circ \prod_{i=1}^{12} L \circ P \circ S \circ X[K_i]$$

KeySchedule function

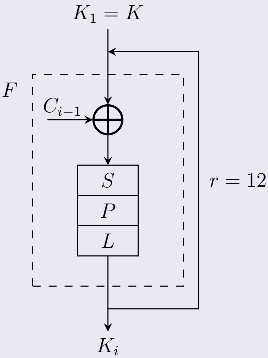
$$K_i = L \circ P \circ S(K_{i-1} \oplus C_{i-1}),\ K_1 = K,\ i \in \{2, \ldots, 13\}.$$

Representation of E

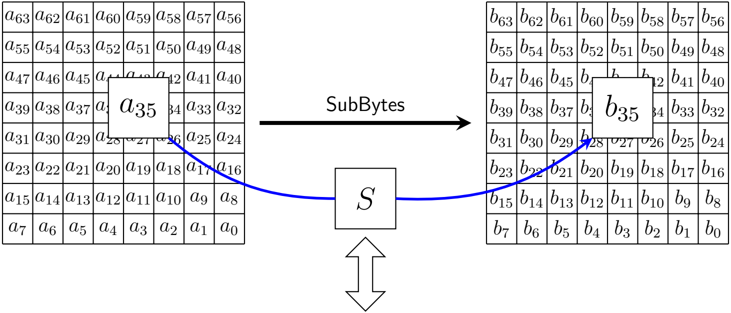
Block Cipher of Stribog



Key Schedule



SubBytes Transformation



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

S-box of Stribog

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

S-box Characteristics

Properties	Stribog	AES
Vectorial Boolean Function		
Balancedness	True	True
Nonlinearity	100	112
Absolute Indicator	96	32
SSI	258688	133120
PC	0	0
CI	0	0
Algebraic Degree	7	7
Resiliency	0	0
SAC	False	False
Substitution		
Bijection	True	True
MDT	8	4
MLT	28	16
Cycles	252:243, 46:13	43:27, 242:87, 99:59, 124:81, 143:2
Algebraic Immunity	3(441)	2(39)

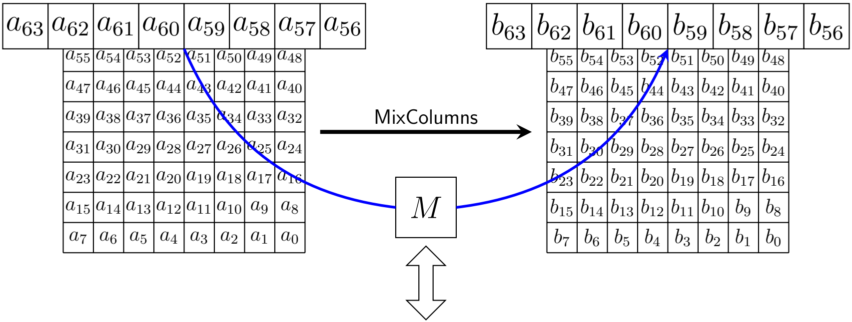
Transposition

Transposition transformation has a form

$$
\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
a_{63} & a_{62} & a_{61} & a_{60} & a_{59} & a_{58} & a_{57} & a_{56} \\ \hline
a_{55} & a_{54} & a_{53} & a_{52} & a_{51} & a_{50} & a_{49} & a_{48} \\ \hline
a_{47} & a_{46} & a_{45} & a_{44} & a_{43} & a_{42} & a_{41} & a_{40} \\ \hline
a_{39} & a_{38} & a_{37} & a_{36} & a_{35} & a_{34} & a_{33} & a_{32} \\ \hline
a_{31} & a_{30} & a_{29} & a_{28} & a_{27} & a_{26} & a_{25} & a_{24} \\ \hline
a_{23} & a_{22} & a_{21} & a_{20} & a_{19} & a_{18} & a_{17} & a_{16} \\ \hline
a_{15} & a_{14} & a_{13} & a_{12} & a_{11} & a_{10} & a_{9} & a_{8} \\ \hline
a_{7} & a_{6} & a_{5} & a_{4} & a_{3} & a_{2} & a_{1} & a_{0} \\ \hline
\end{array}
\xrightarrow{\text{Transpose}}
\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
a_{63} & a_{55} & a_{47} & a_{39} & a_{31} & a_{23} & a_{15} & a_{7} \\ \hline
a_{62} & a_{54} & a_{46} & a_{38} & a_{30} & a_{22} & a_{14} & a_{6} \\ \hline
a_{61} & a_{53} & a_{45} & a_{37} & a_{29} & a_{21} & a_{13} & a_{5} \\ \hline
a_{60} & a_{52} & a_{44} & a_{36} & a_{28} & a_{20} & a_{12} & a_{4} \\ \hline
a_{59} & a_{51} & a_{43} & a_{35} & a_{27} & a_{19} & a_{11} & a_{3} \\ \hline
a_{58} & a_{50} & a_{42} & a_{34} & a_{26} & a_{18} & a_{10} & a_{2} \\ \hline
a_{57} & a_{49} & a_{41} & a_{33} & a_{25} & a_{17} & a_{9} & a_{1} \\ \hline
a_{56} & a_{48} & a_{40} & a_{32} & a_{24} & a_{16} & a_{8} & a_{0} \\ \hline
\end{array}
$$

MixColumns

MixColumns transformation has a form



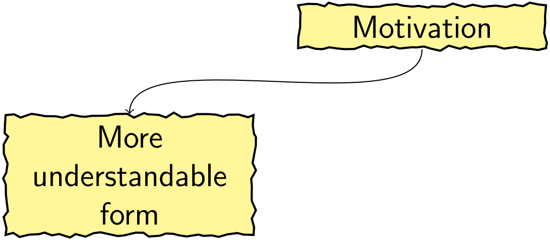
Multiplying the vector by the constant 64×64 matrix M over $\mathbb{F}_2$

$$B = A \cdot M$$

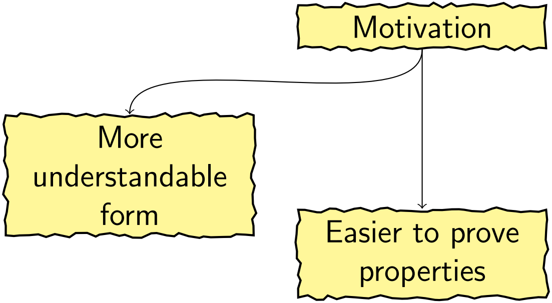
Outline

Motivation

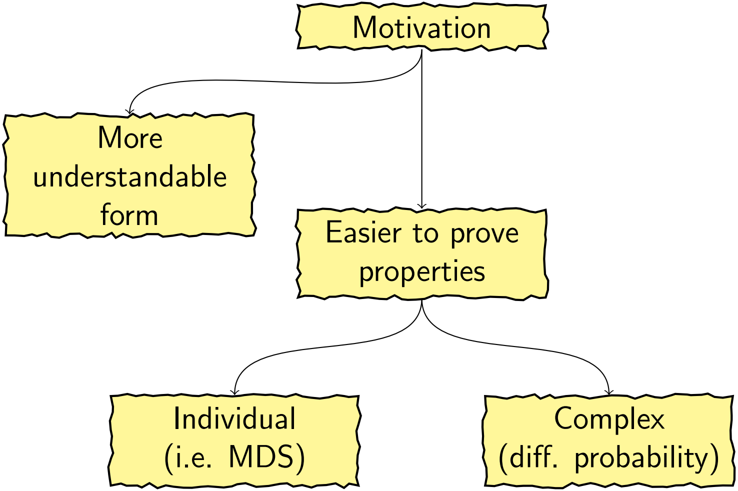
Motivation



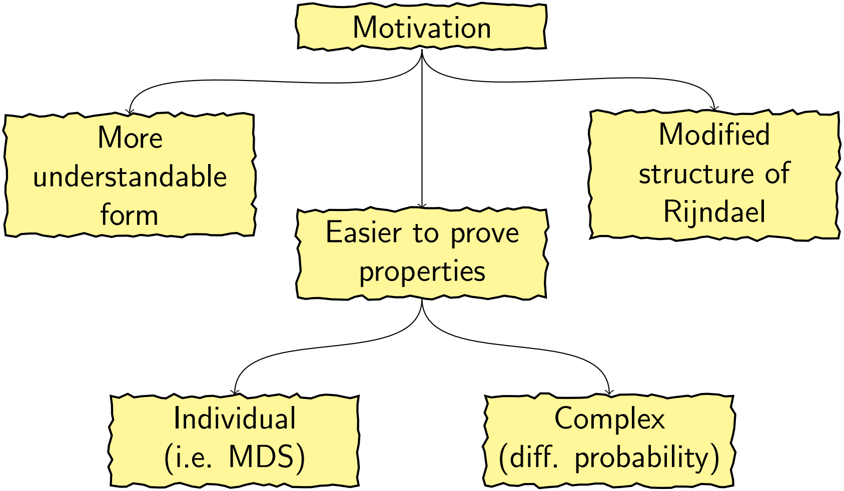
Motivation


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/AES)
- Reverse output bits

$$
\begin{tikzcd}
B_0, B_1, \ldots, B_{63} \arrow[d, leftrightarrow] & & B'_0, B'_1, \ldots, B'_{63} \arrow[d, leftrightarrow] \\
b_0, b_1, \ldots, b_{511} \arrow[rr, leftrightarrow, "\text{(Inv)ReverseBits}"] & & b_{511}, b_{510}, \ldots, b_0
\end{tikzcd}
$$

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

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

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

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

$$\mathbb{F}_{2^n} \underset{hard}{\overset{easy}{\rightleftarrows}} \mathbb{F}_2$$

Representation of MixColumns

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 on a matrix

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

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

Representation of MixColumns

Let $L : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ be a linear function of the form

$$L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i}.$$

Representation of MixColumns

Let $L : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ be a linear function of the form

$$L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i}.$$

Proposition [5]

Any linear function $L : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ can be converted to a matrix with the complexity $O(n)$.

Representation of MixColumns

Let $L : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ be a linear function of the form

$$L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i}.$$

Proposition [5]

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

The main steps of 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 8×8 submatrices to the element of the filed
    2. check MDS property of the resulting matrix

Representation of MixColumns

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

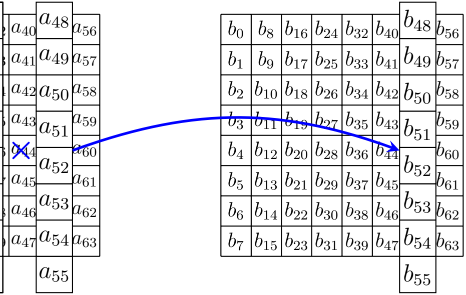
1. for every irreducible polynomial (30)
    1. convert each 8×8 submatrices to the element of the filed
    2. check MDS property of the resulting matrix

Hint

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

MixColumns

71	05	09	B9	61	A2	27	0E
04	88	5B	B2	E4	36	5F	65
5F	CB	AD	0F	BA	2C	04	A5
E5	01	54	BA	0F	11	2A	76
D4	81	1C	FA	39	5E	15	24
05	71	5E	66	17	1C	D0	02
2D	F1	E7	28	55	A0	4C	9A
0E	02	F6	8A	15	9D	39	71



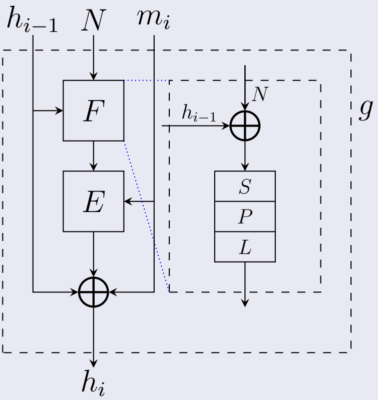
$\Updownarrow$

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

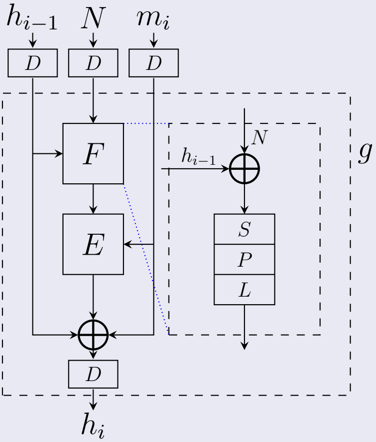
$$B = G \cdot A$$

Modified Compression Function

Original Function



Modified Function



Conclusions

- Stribog is based on GOST 34.11-94 as well as on AES.

Conclusions

- Stribog is based on GOST 34.11-94 as well as on AES.
- It is planned to replace existing standard 34.11-94 in 2013.

Conclusions

- Stribog is based on GOST 34.11-94 as well as on AES.
- It is planned to replace existing standard 34.11-94 in 2013.
- Is Stribog 20% faster than GOST 34.11-94?

Conclusions

- Stribog is based on GOST 34.11-94 as well as on AES.
- It is planned to replace existing standard 34.11-94 in 2013.
- Is Stribog 20% faster than GOST 34.11-94?
  - No, it is slower.

Conclusions

- Stribog is based on GOST 34.11-94 as well as on AES.
- It is planned to replace existing standard 34.11-94 in 2013.
- Is Stribog 20% faster than GOST 34.11-94?
    - No, it is slower.
- More details on github.

References

F. Mendel, N. Pramstaller, C. Rechberger, M. Kontak, and J. Szmidt. Cryptanalysis of the GOST hash function. In D. Wagner, editor, *Advances in Cryptology CRYPTO 2008*, volume 5157 of *LNCS*, pages 162–178.

Matuhin D.V., Shyshkin V.A., Rudskoy V.I.: Prospective hashing algorithm. RusCrypto'2010, 2010. (In Russian).

GOST 34.11-20__, Information technology. Cryptographic data security. Hash function. Prototype (version 1). `http://infotecs.ru/laws/gost/proj/gost3411.pdf`. (In Russian).

R. Oliynykov, I. Gorbenko, V. Dolgov, V. Ruzhentsev, Results of Ukrainian National Public Cryptographic Competition, Tatra Mt. Math. Publ. 47 2010, 99–113. `http://www.sav.sk/journals/uploads/0317154006ogdr.pdf`.