Prototype of Russian Hash Function "Stribog"

Oleksandr Kazymyrov

Department of Informatics, University of Bergen,
P.O.Box 7803, N-5020 Bergen, Norway
Oleksandr.Kazymyrov@uib.no

May 9, 2012

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.

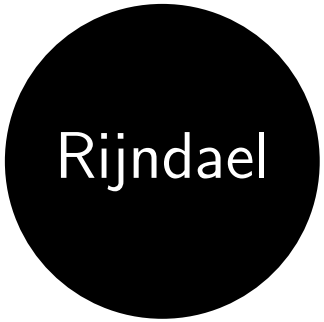
Motivation

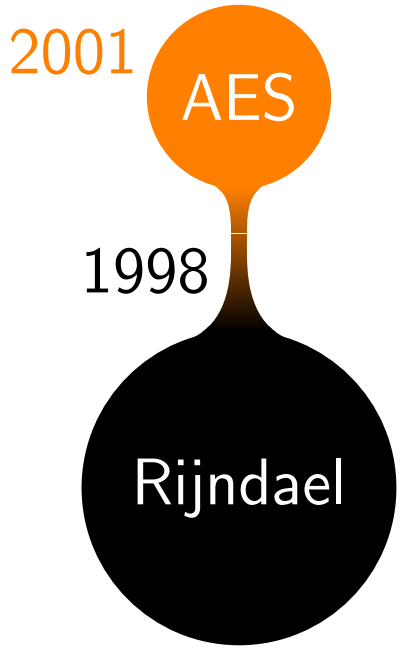
- GOST 34.11-94 was theoretically broken in 2008.
  - The complexities $O(2^{192})/O(2^{69})$ for preimage and second preimage attacks.
- Increasing performance. Stribog is 20% faster than GOST 34.11-94.

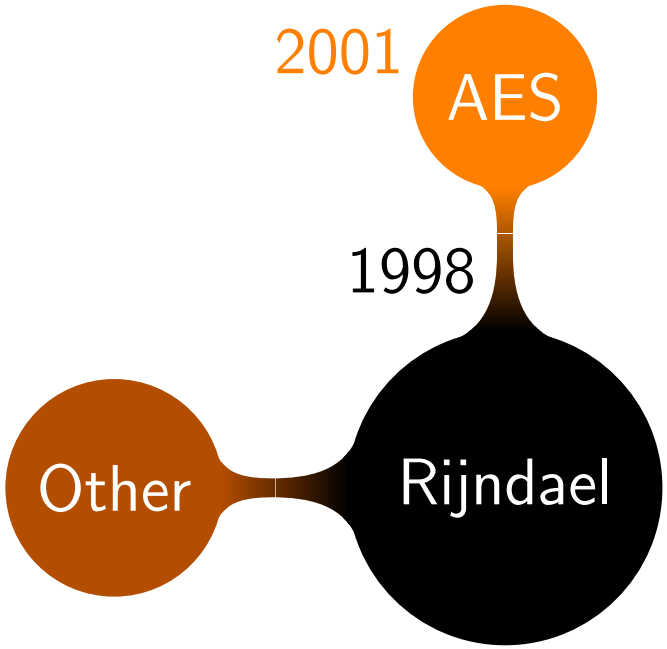
Motivation

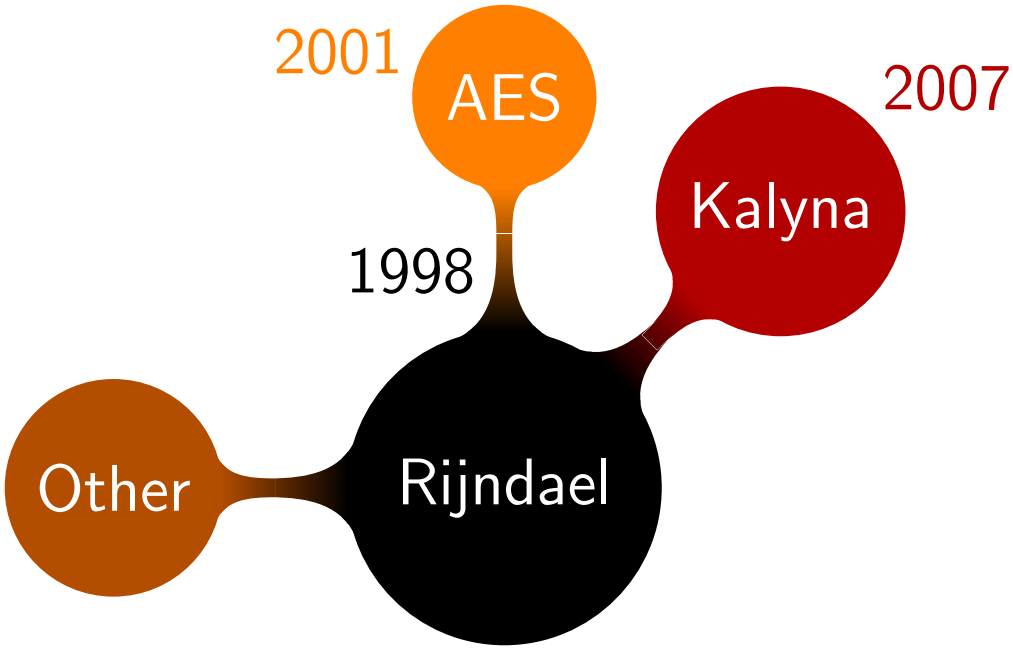
- GOST 34.11-94 was theoretically broken in 2008.
  - The complexities $O(2^{192})/O(2^{69})$ for preimage and second preimage attacks.
- Increasing performance. Stribog is 20% faster than GOST 34.11-94.
- Opposite to SHA-3.

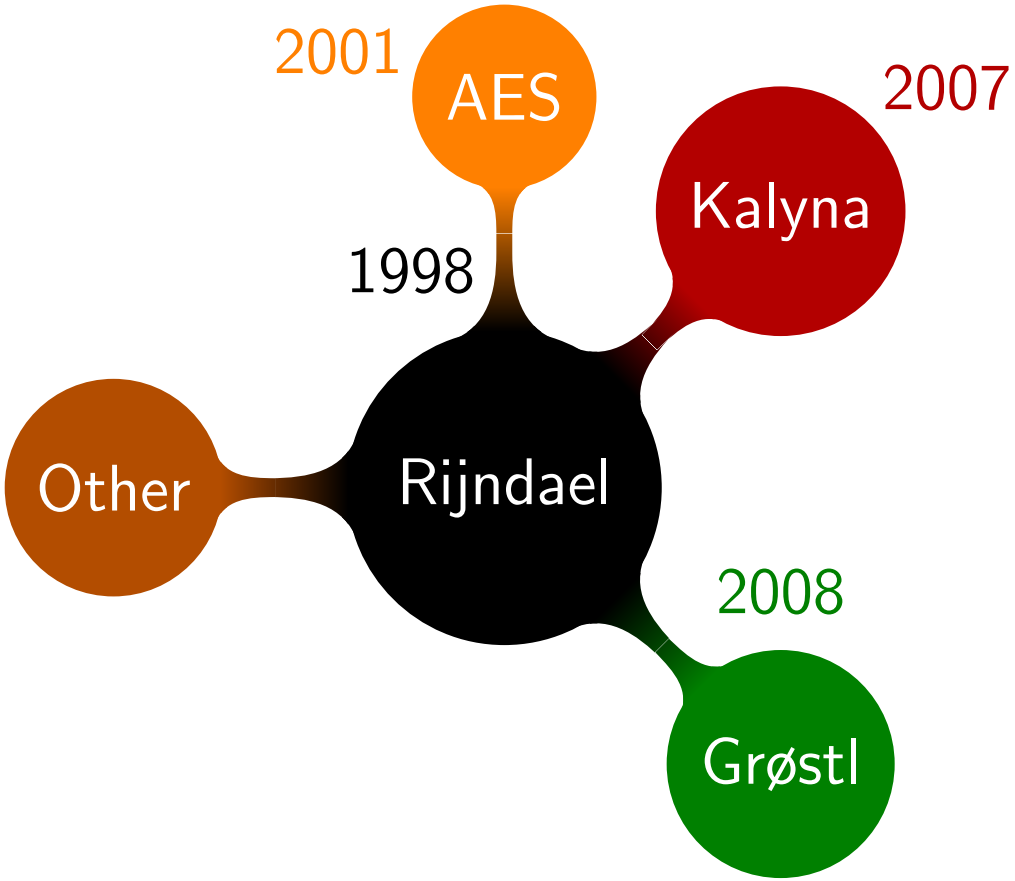
1998

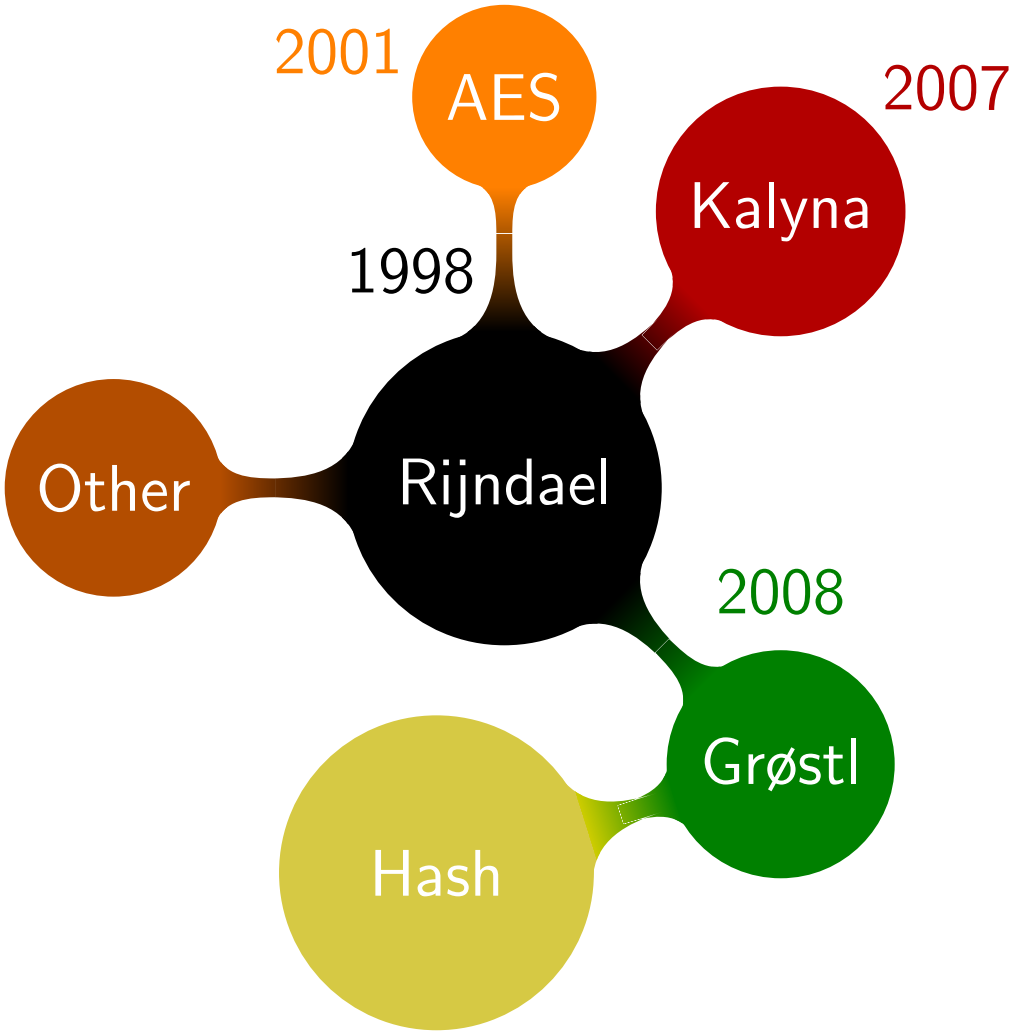


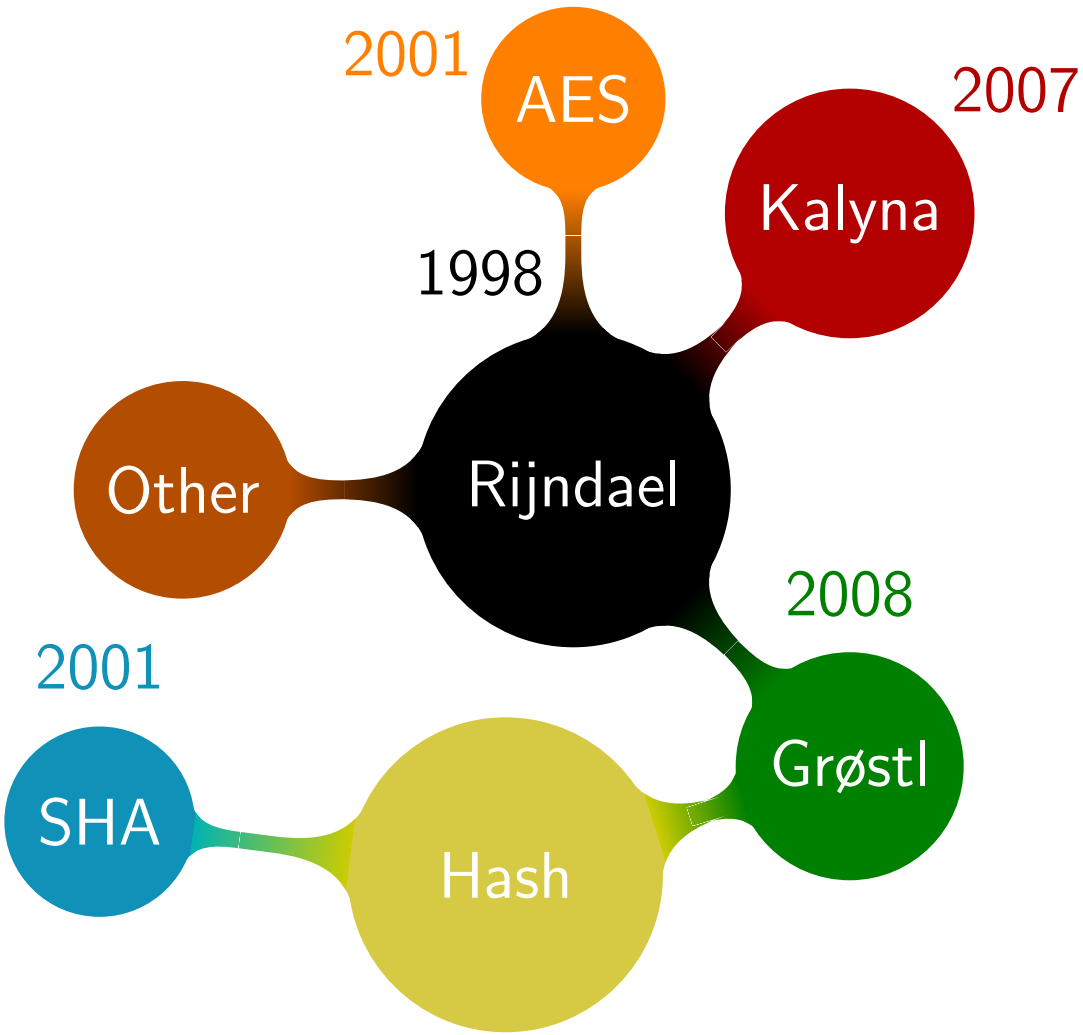

2001
AES
1998
Rijndael

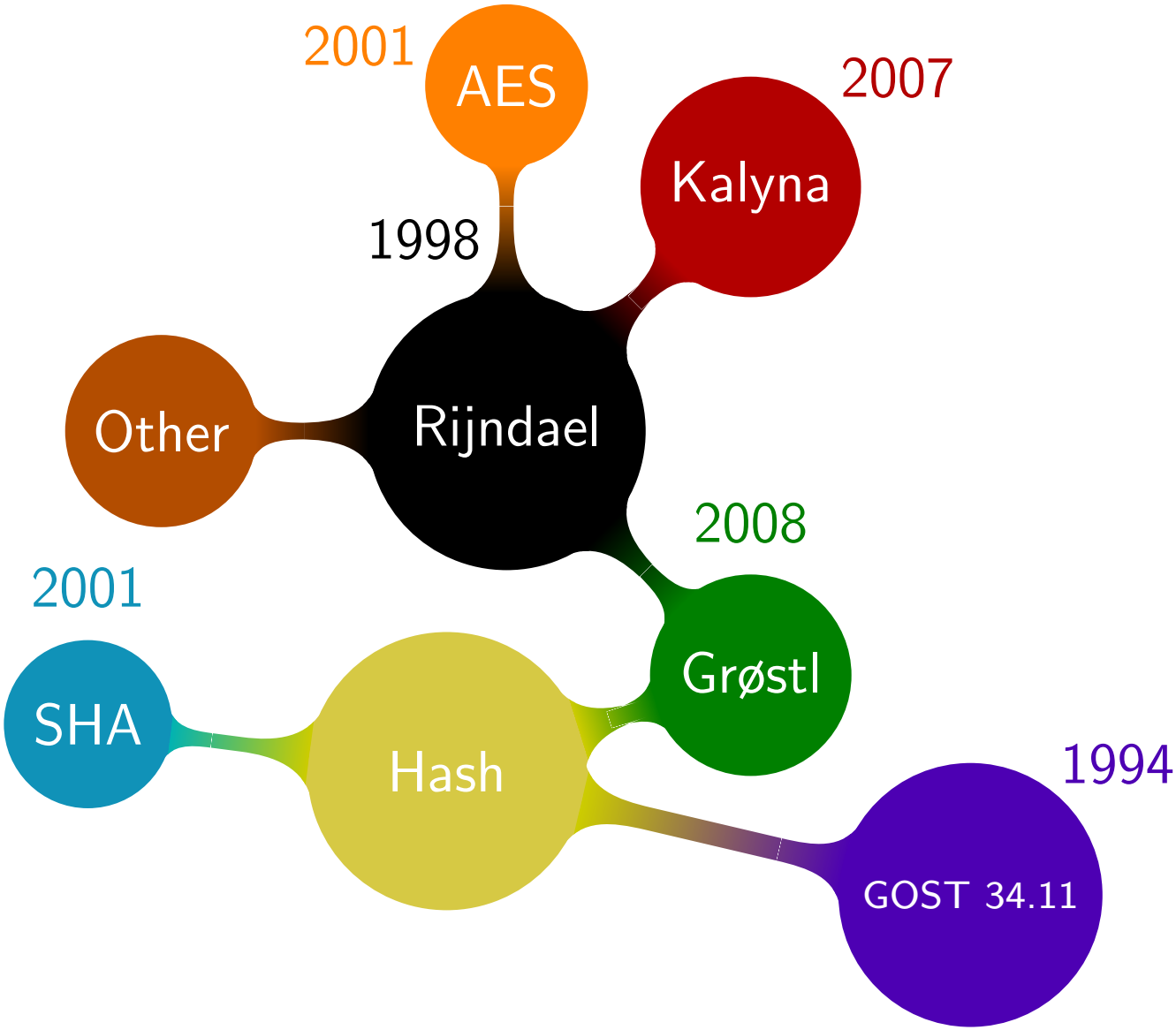

2001
AES
1998
Other
Rijndael

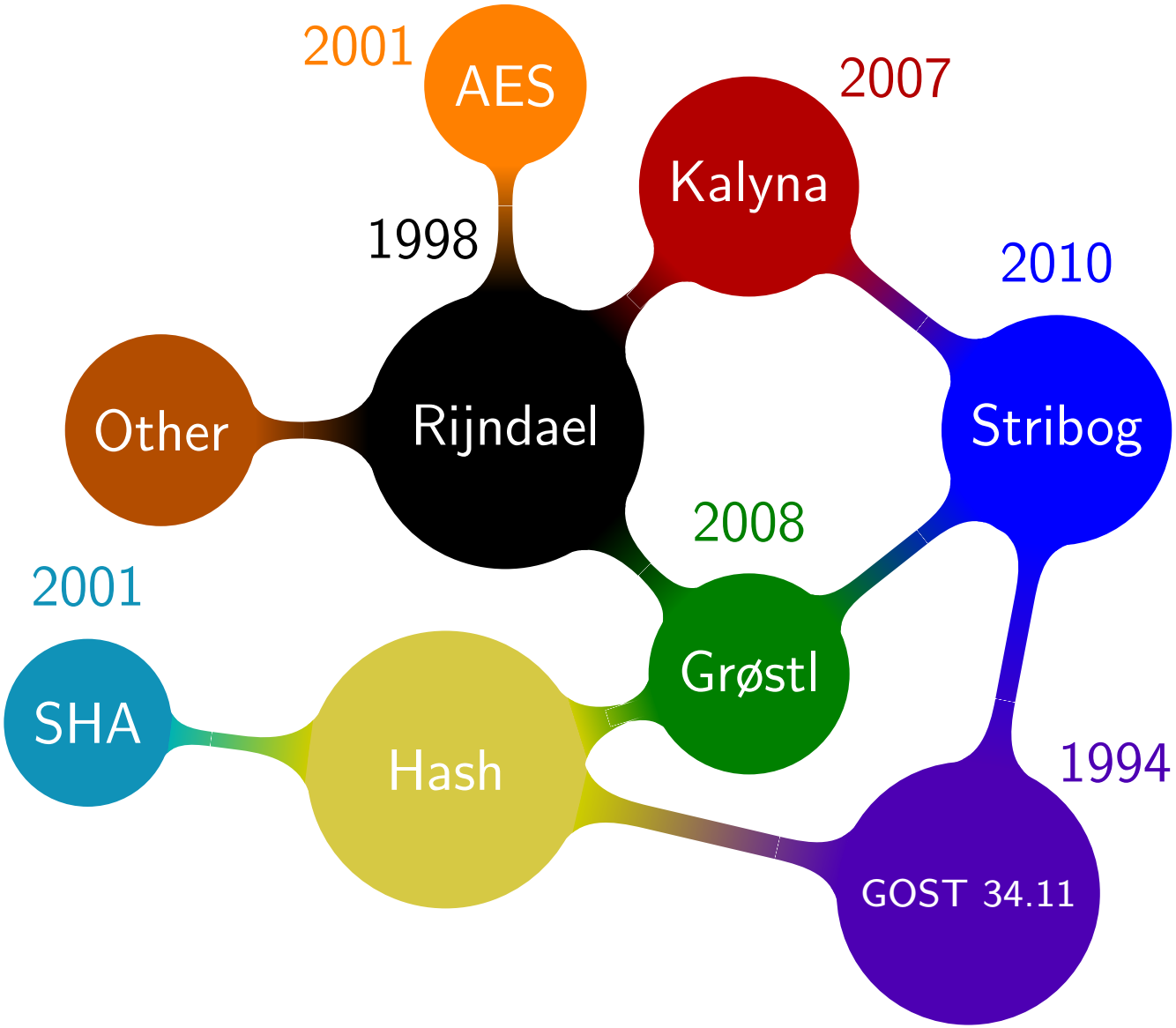

2001
AES
2007
Kalyna
1998
Other
Rijndael


2001
AES
2007
Kalyna
1998
Other
Rijndael
2008
Grøstl


2001
AES
2007
Kalyna
1998
Other
Rijndael
2008
Grøstl
Hash


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


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

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

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

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

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}

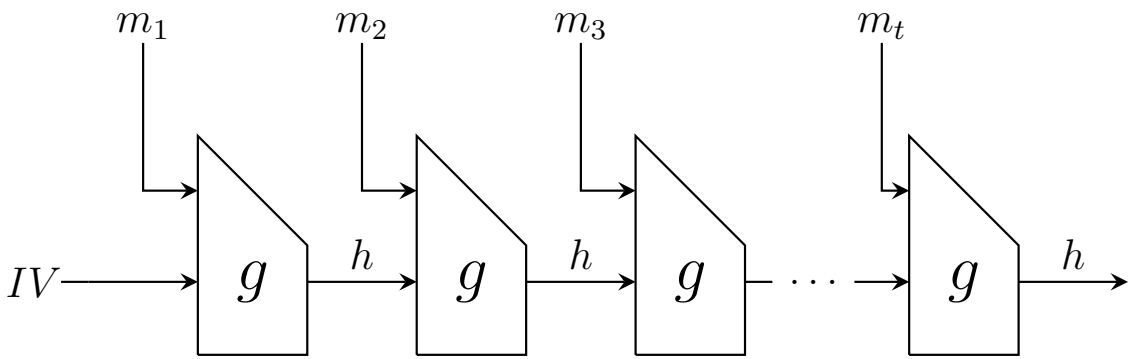
Stribog

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}

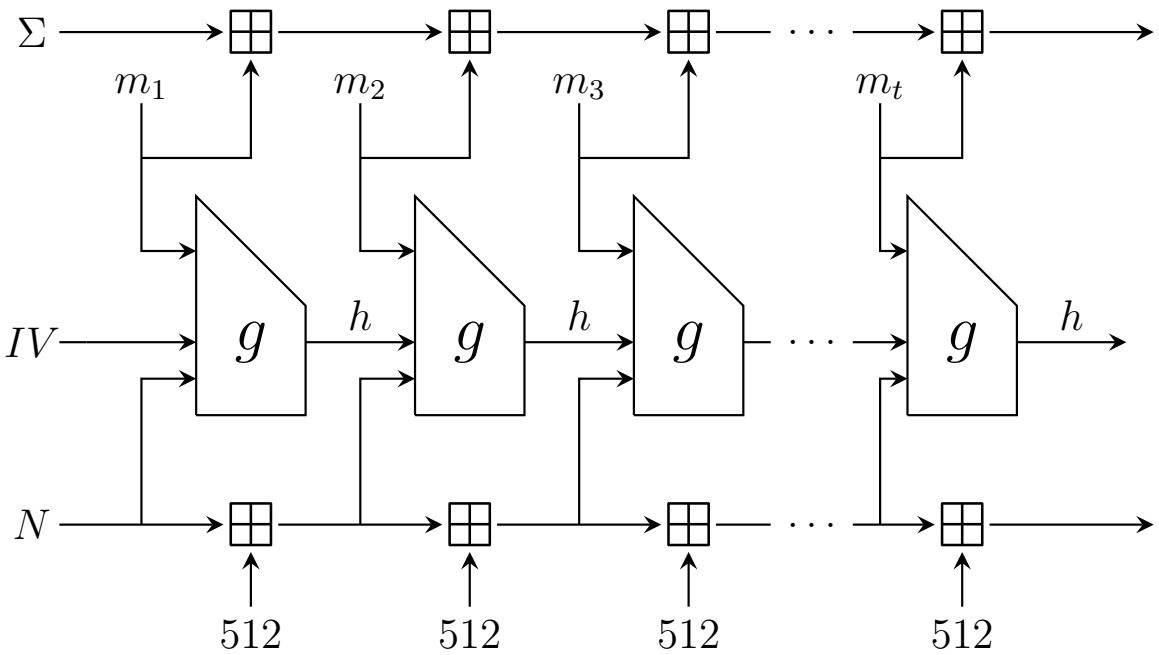
$$A = a_0||a_1||\ldots||a_{63}$$

Outline

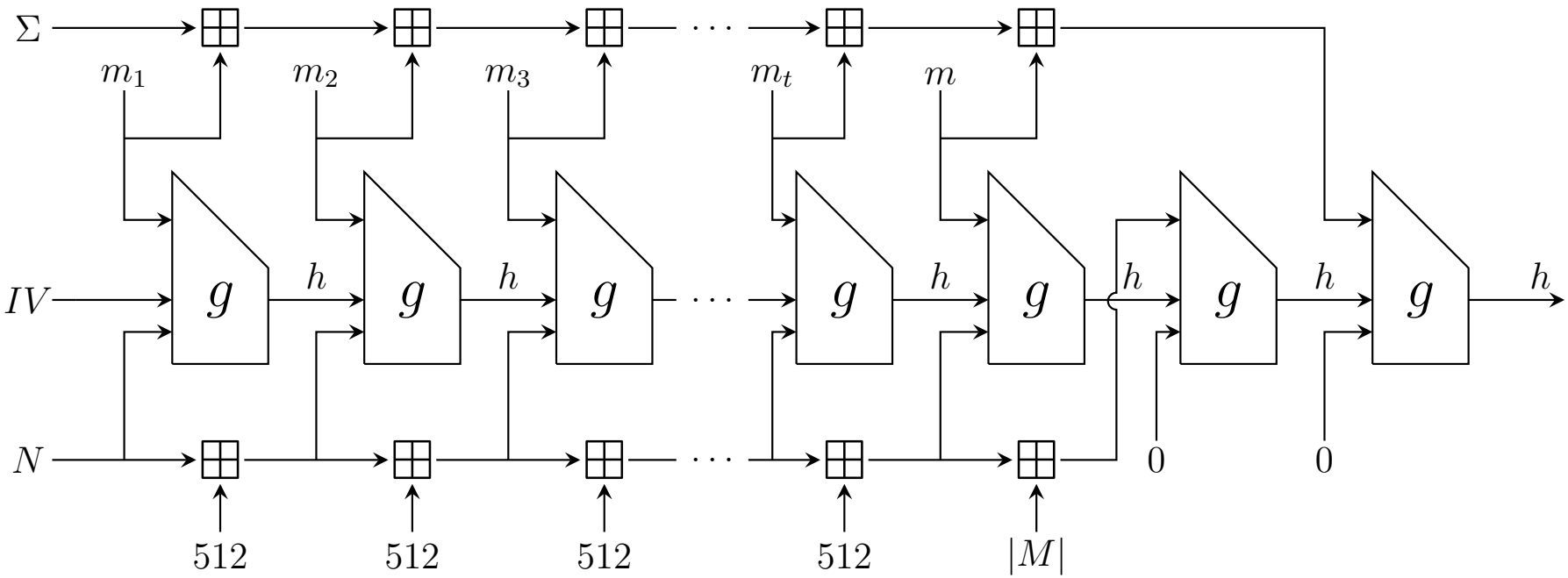
Merkle-Damgård Scheme



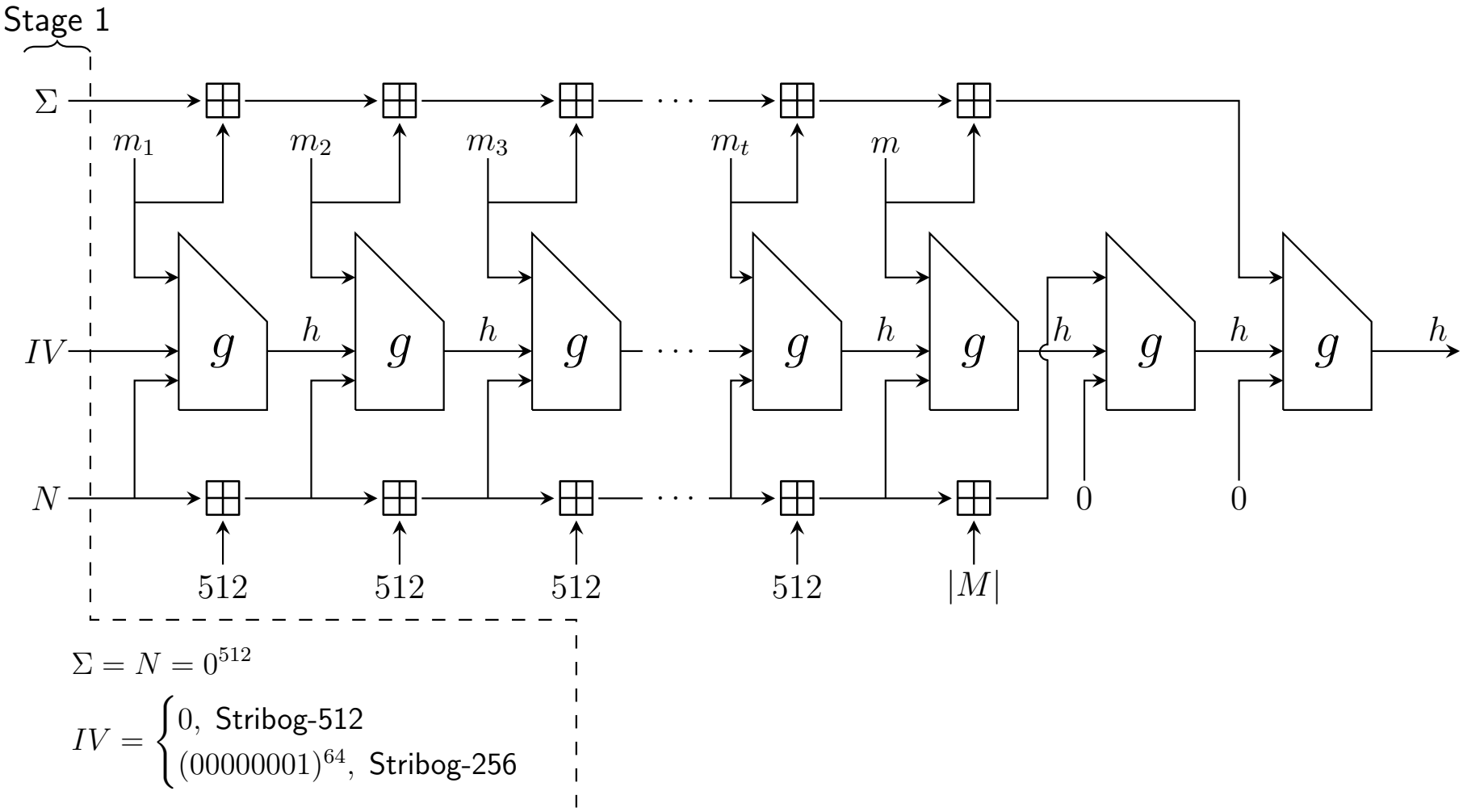
Modification of Merkle-Damgård Scheme



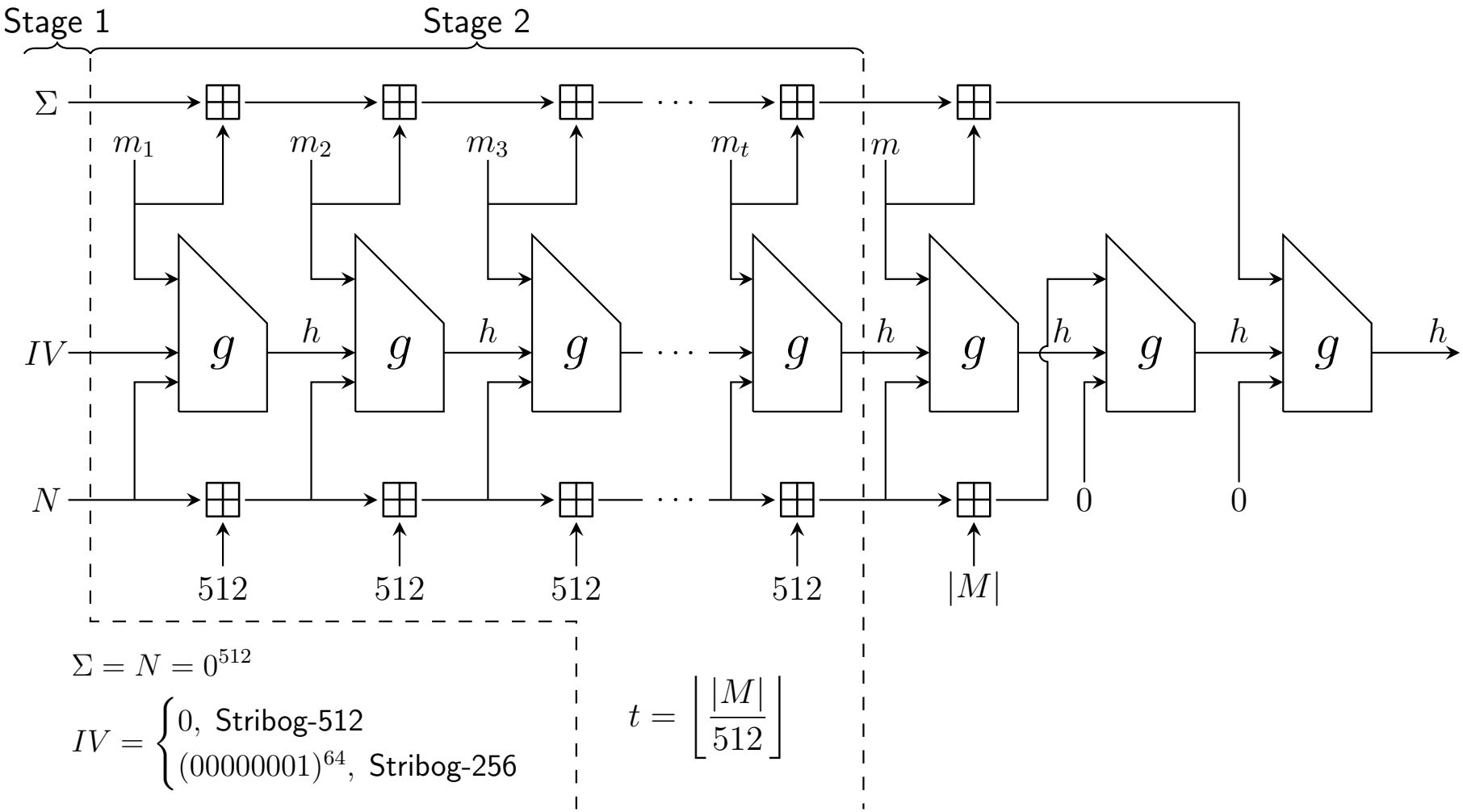
Hash Function Stribog



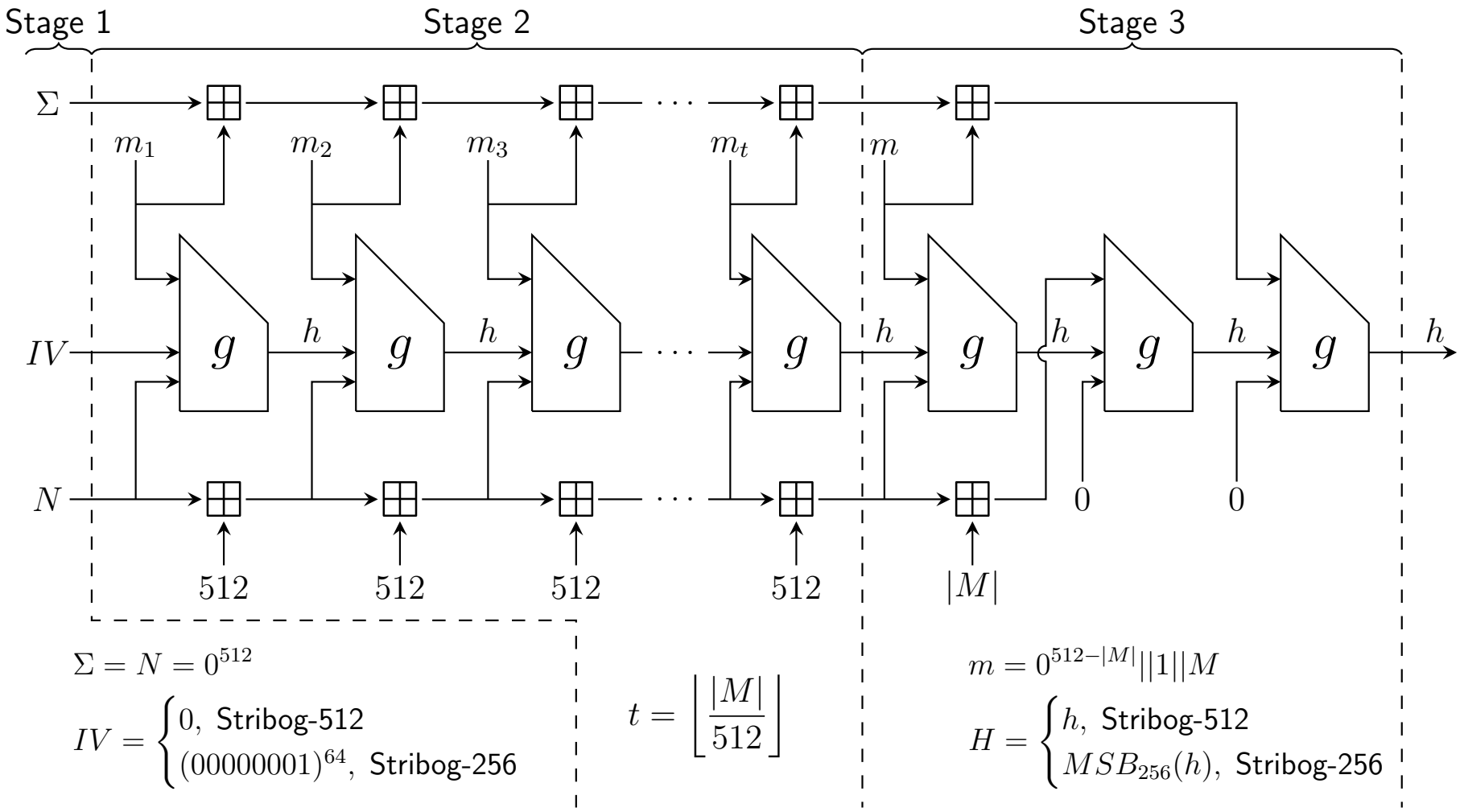
Hash Function Stribog. Stage 1



Hash Function Stribog. Stage 2

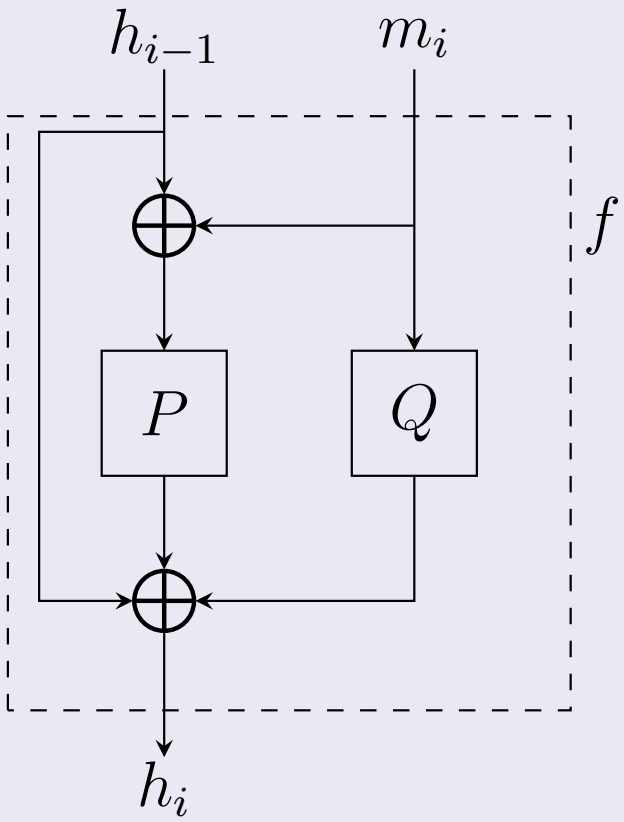


Hash Function Stribog. Stage 3

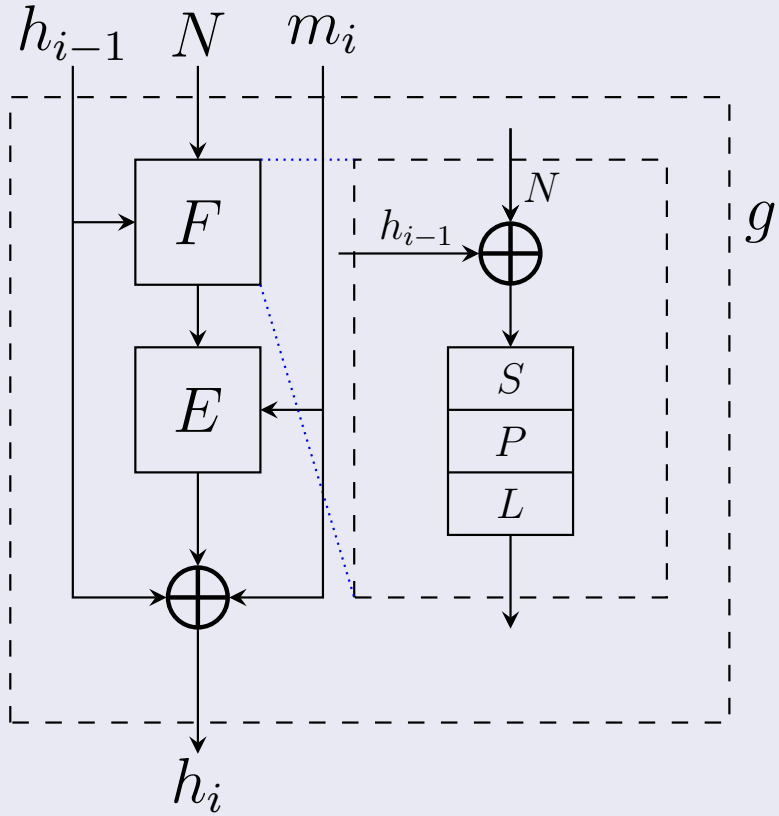


Compression Function Construction

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

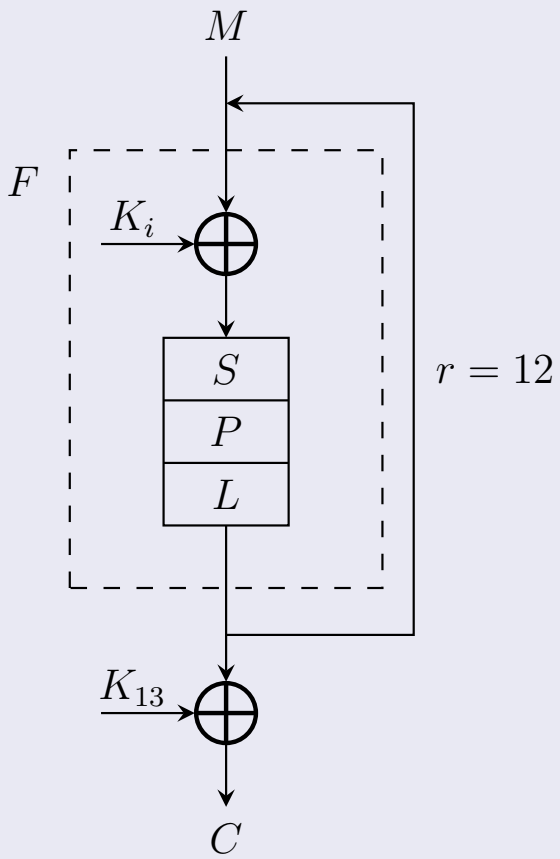
$$E(K, m) = X[K_{13}] \circ \prod_{i=1}^{12} L \circ P \circ S \circ X[K_i]$$

KeySchedule function

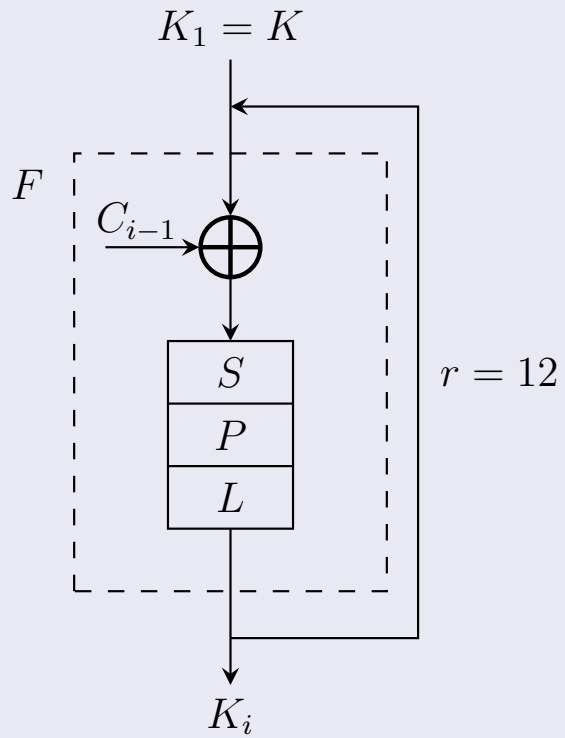
$$K_i = L \circ P \circ S(K_{i-1} \oplus C_{i-1}),\ K_1 = K,\ i \in \{2, \ldots, 13\}.$$

Representation of E

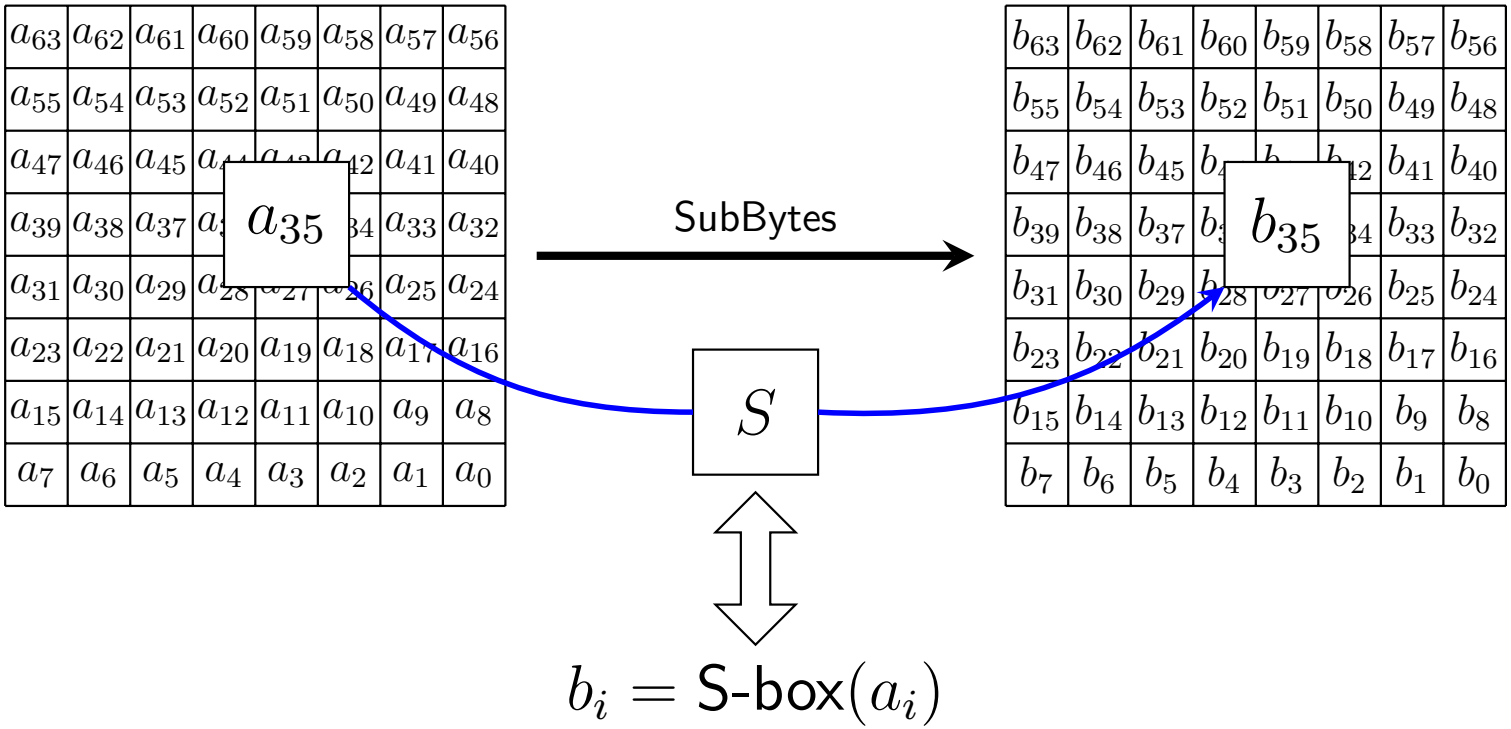
StribogT BC



Key Schedule



SubBytes Transformation



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

S-box of Stribog

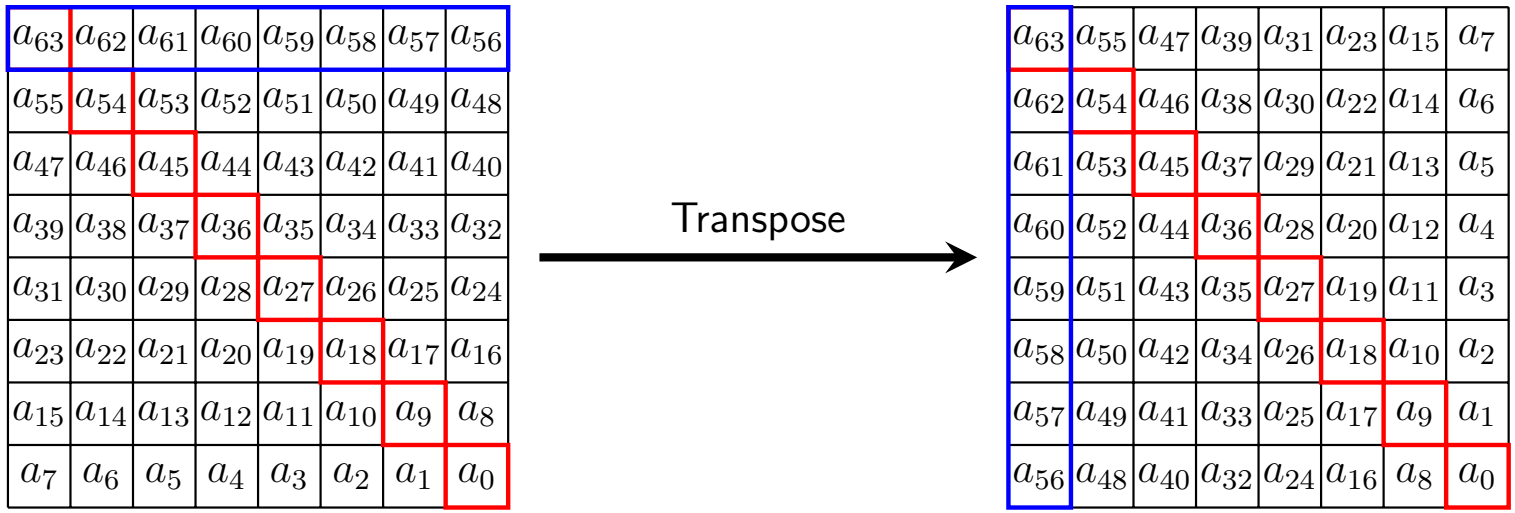
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	FC	EE	DD	11	CF	6E	31	16	FB	C4	FA	DA	23	C5	04	4D
1	E9	77	F0	DB	93	2E	99	BA	17	36	F1	BB	14	CD	5F	C1
2	F9	18	65	5A	E2	5C	EF	21	81	1C	3C	42	8B	01	8E	4F
3	05	84	02	AE	E3	6A	8F	A0	06	0B	ED	98	7F	D4	D3	1F
4	EB	34	2C	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

Characteristics	Stribog	AES
Boolean Functions		
Balanced	True	True
Nonlinearity	100	112
AI	96	32
SSI	258688	133120
PC	0	0
CI	0	0
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
AI	3(441)	2(39)

Transposition

Transposition transformation has a form

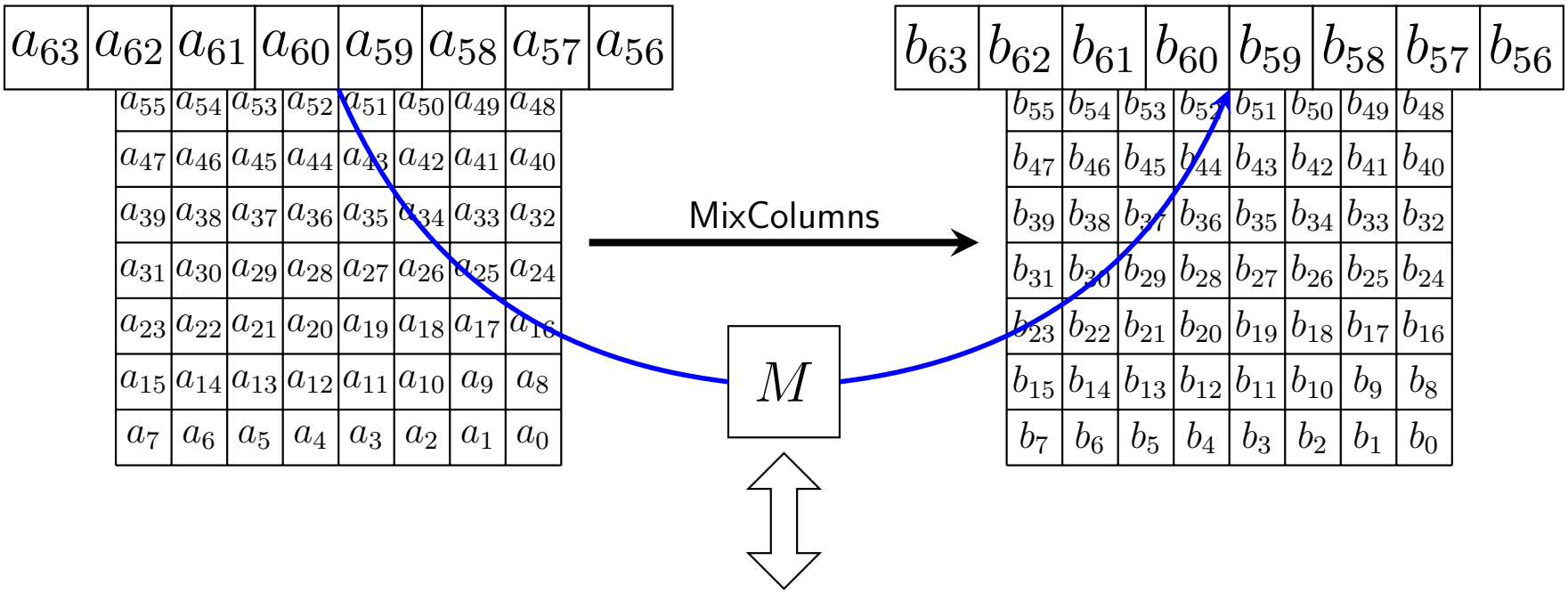


a_{63}	a_{62}	a_{61}	a_{60}	a_{59}	a_{58}	a_{57}	a_{56}
a_{55}	a_{54}	a_{53}	a_{52}	a_{51}	a_{50}	a_{49}	a_{48}
a_{47}	a_{46}	a_{45}	a_{44}	a_{43}	a_{42}	a_{41}	a_{40}
a_{39}	a_{38}	a_{37}	a_{36}	a_{35}	a_{34}	a_{33}	a_{32}
a_{31}	a_{30}	a_{29}	a_{28}	a_{27}	a_{26}	a_{25}	a_{24}
a_{23}	a_{22}	a_{21}	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}

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

MixColumns transformation has a form

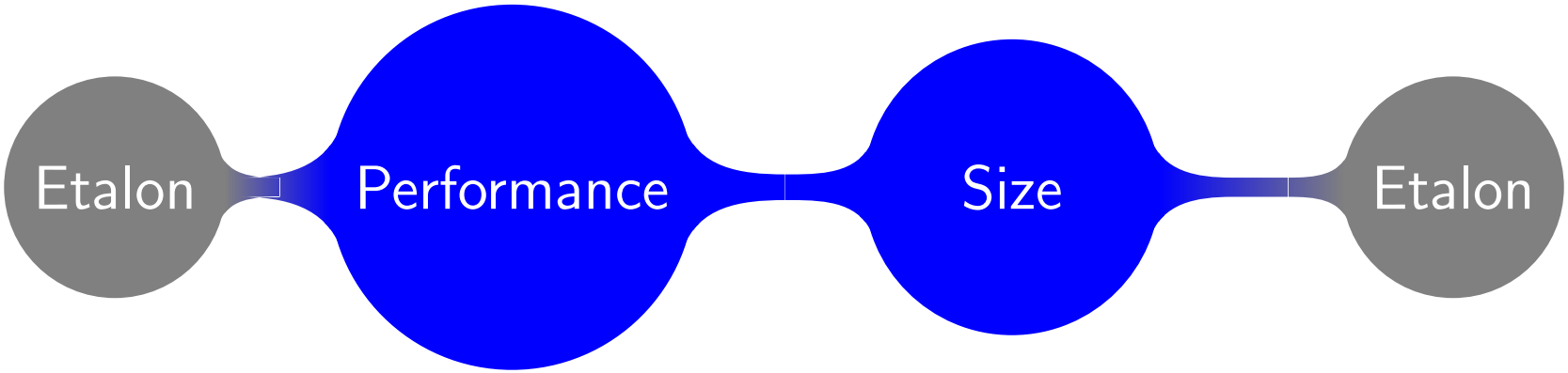


Multiplying the vector by the constant 64×64 matrix M in $\mathbb{F}_2$

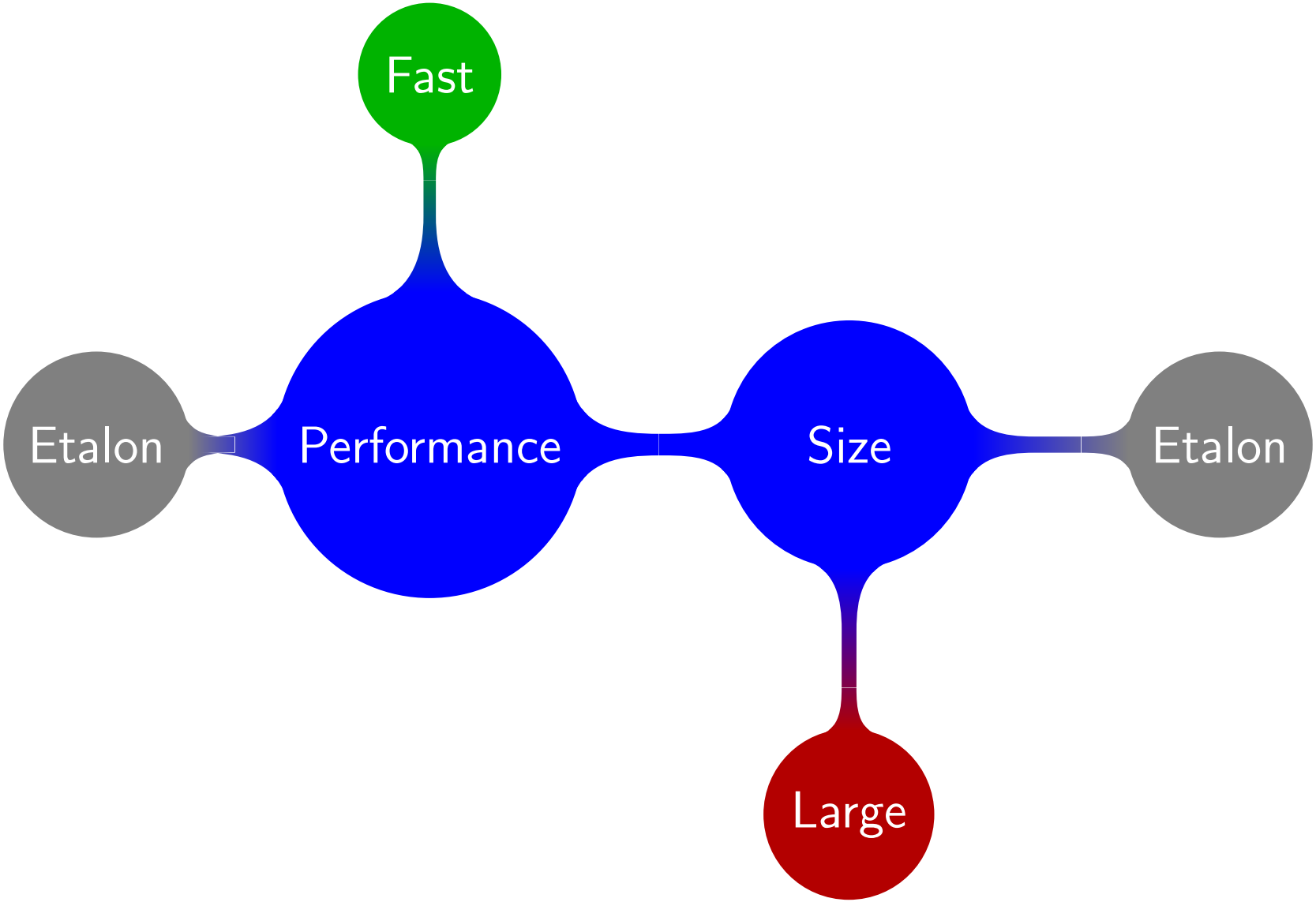
$$B = A \cdot M$$

Outline

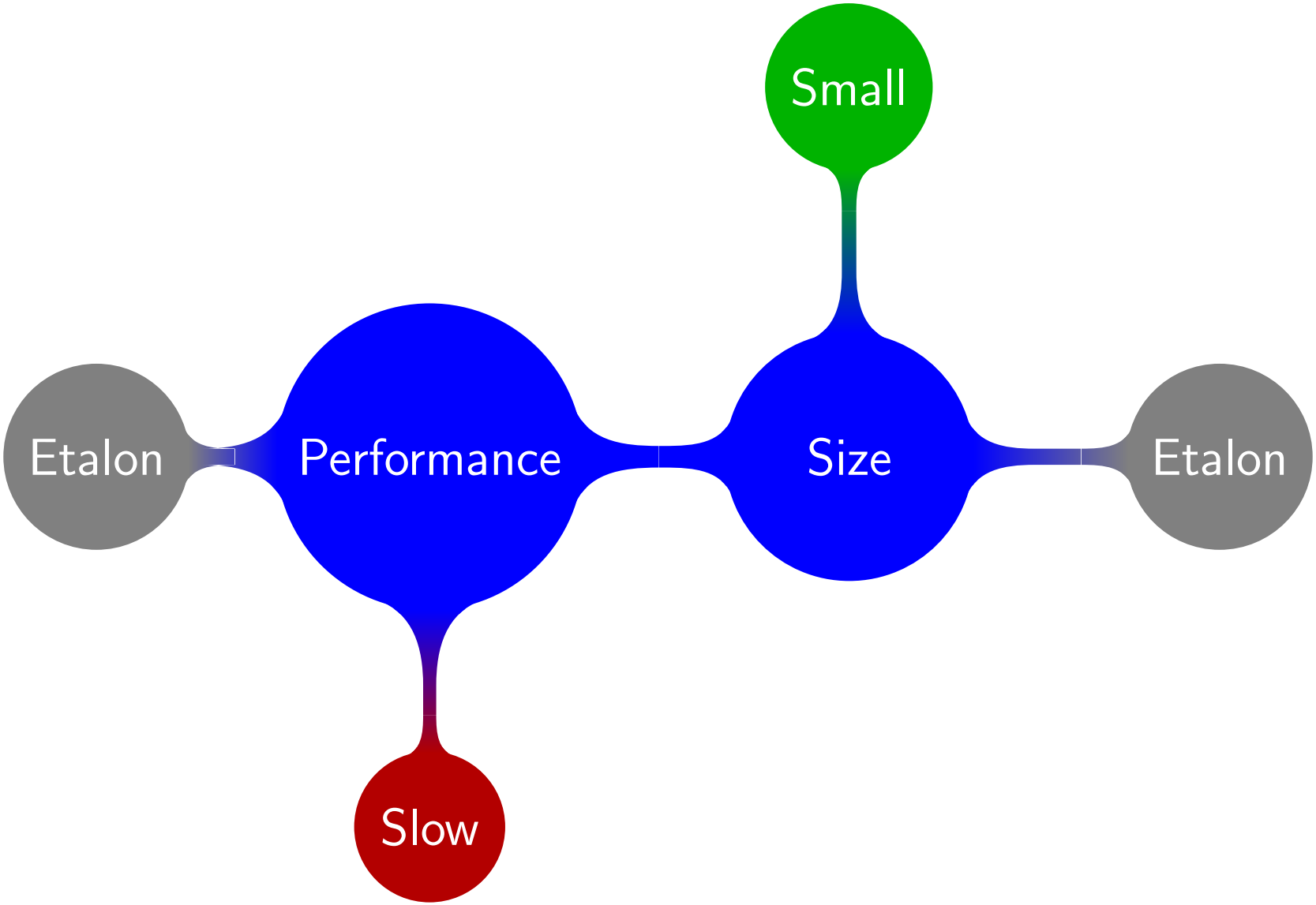
Implementation Features



Implementation Features



Implementation Features

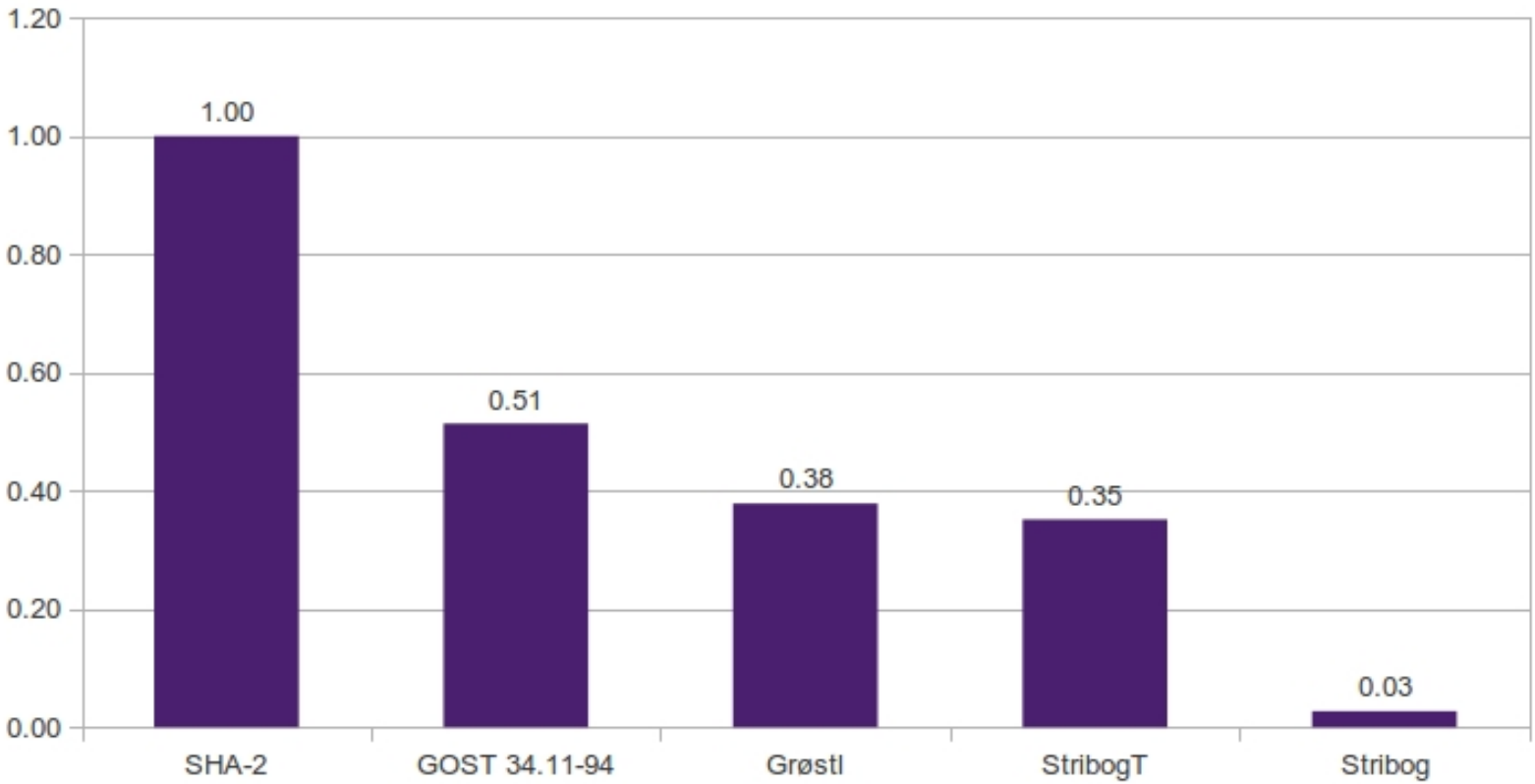


Performance

Algorithm	Performance Mbits/s
SHA-2	74
GOST 34.11-94	38
Grøstl	28
StribogT	26
Stribog	2

Stribog with table implementation is 30% slower than GOST 34.11-94.

Performance



Comments for Performance

	Stribog BC	AES
Performance	140 Mbits/s	490 Mbits/s
Number of F	12	10
Number of lookup tables	64	16
Number of lookup tables (total)	768	160
Optimized	64 bit	32 bit

CPU: Intel T2050 1.60GHz **RAM:** 2GB
OS: Linux i686 **GCC:** version 4.6.3

Conclusions

- Stribog is evolution of GOST 34.11-94.

Conclusions

- Stribog is evolution of GOST 34.11-94.
- It is planned to replace the existing standard 34.11-94.

Conclusions

- Stribog is evolution of GOST 34.11-94.
- It is planned to replace the existing standard 34.11-94.
  - It leads to the replacement of the standard 34.10-01.

Conclusions

- Stribog is evolution of GOST 34.11-94.
- It is planned to replace the existing standard 34.11-94.
  - It leads to the replacement of the standard 34.10-01.
- Is Stribog 20% faster than GOST 34.11-94?

Conclusions

- Stribog is evolution of GOST 34.11-94.
- It is planned to replace the existing standard 34.11-94.
  - It leads to the replacement of the standard 34.10-01.
- Is Stribog 20% faster than GOST 34.11-94?
  - No, it is 30% slower on x86_32.

Conclusions

- Stribog is evolution of GOST 34.11-94.
- It is planned to replace the existing standard 34.11-94.
  - It leads to the replacement of the standard 34.10-01.
- Is Stribog 20% faster than GOST 34.11-94?
  - No, it is 30% slower on x86_32.
- Several mistakes in appendix (test vectors).

Conclusions

- Stribog is evolution of GOST 34.11-94.
- It is planned to replace the existing standard 34.11-94.
  - It leads to the replacement of the standard 34.10-01.
- Is Stribog 20% faster than GOST 34.11-94?
  - No, it is 30% slower on x86_32.
- Several mistakes in appendix (test vectors).
  - Appendices are for reference purposes only and are not part of the standard.

What is Stribog?

"Stribog in the Slavic pantheon, is the god and spirit of the winds, sky and air; he is said to be the ancestor (grandfather) of the winds of the eight directions."

– Wikipedia

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`.