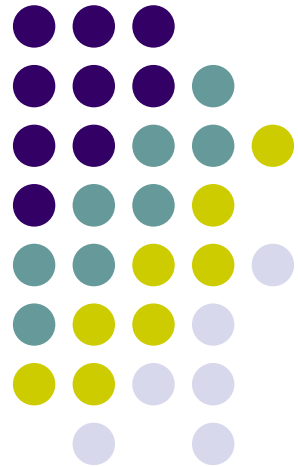
Hašovací funkce:
SHA-3 & Blue Midnight Wish

(On Blue Midnight Wish Decomposition)

Vlastimil Klima [1] and Danilo Gligoroski [2]

[1] Nezávislý kryptolog - konzultant, Praha
v.klima@volny.cz, http://cryptography.hyperlink.cz
[2] Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering Norwegian University of Science and TechnologyTechnology - NTNU, NORWAY



SantaCrypt 2009, December 3 – 4, 2009, Hotel Olympik, Prague, Czech Republic

Obsah

- Poděkování
  - doc. Tůmovi, doc. Matyášovi a Mgr. Vondruškovi – „**Za výchovu a vzdělávání nových kryptologů**“
- O soutěži SHA-3
  - predikce finalistů
  - průběžně články v ezinu Crypto-Worldu a na Crypto-World news (http://crypto-world.info/news/)
- O BMW-n
  - vnitřek
  - doporučení a návody k útokům

SHA-3

- Vývoj: 0 (11/2007), 64 (10/2008), 51 (12/2008),14 (07/2009), nejbližší akce: 5 (08/2010) – výběr 5 finalistů

Kdo budou finalisté ?

Tým BLUE MIDNIGHT WISH:
Danilo Gligoroski
Vlastimil Klima
Svein Johan Knapskog
Mohamed El-Hadedy
Jørn Amundsen
Stig Frode Mjølsnes

Zásadní požadavek:
bezpečnost a rychlost
(z nich se nedá ***nic*** slevit)
další požadavky:
„cena“ HW a SW realizace
(z nich se dá vybírat)

Rozpor **mezi bezp. a rychlostí a nové technologické řešení**

		64-bit, 256 bit speed cycles/bytes
1	Blue Midnight Wish	7.55
2	Skein	7.6
3	Shabal	8.03
4	BLAKE	8.19
5	Keccak	10
6	CubeHash	11
7	SIMD	11
8	Luffa	13.4
9	SHA-256	15.34
10	JH	16.8
11	Grøstl	22.2
12	Hamsi	25
13	SHAvite-3	26.7
14	Fugue	28
15	ECHO	28.5

		64-bit, 512 bit speed cycles/bytes
1	Blue Midnight Wish	3.88
2	Skein	6.1
3	Shabal	8.03
4	BLAKE	9.29
5	CubeHash	11
6	SIMD	12
7	SHA-512	12.59
8	JH	16.8
9	Keccak	20
10	Luffa	23.2
11	Hamsi	25
12	Grøstl	30.5
13	SHAvite-3	38.2
14	ECHO	53.5
15	Fugue	56

BMW*n*

- BMW224
- BMW256
- BMW384
- BMW512
- Rozdíly:
  - „žádné“
  - w =32/64
  - krácení

  výstupu

Algorithm: Blue Midnight Wish

Input: Message M of length l bits, and the message digest size n.
Output: A message digest $Hash$, that is n bits long.

1. Preprocessing
   (a) Pad the message M.
   (b) Parse the padded message into N, m-bit message blocks, $M^{(1)}$, $M^{(2)}, \ldots, M^{(N)}$.
   (c) Set the initial value of the double pipe $H^{(0)}$.
2. Hash computation

   For $i = 1$ to N

   {

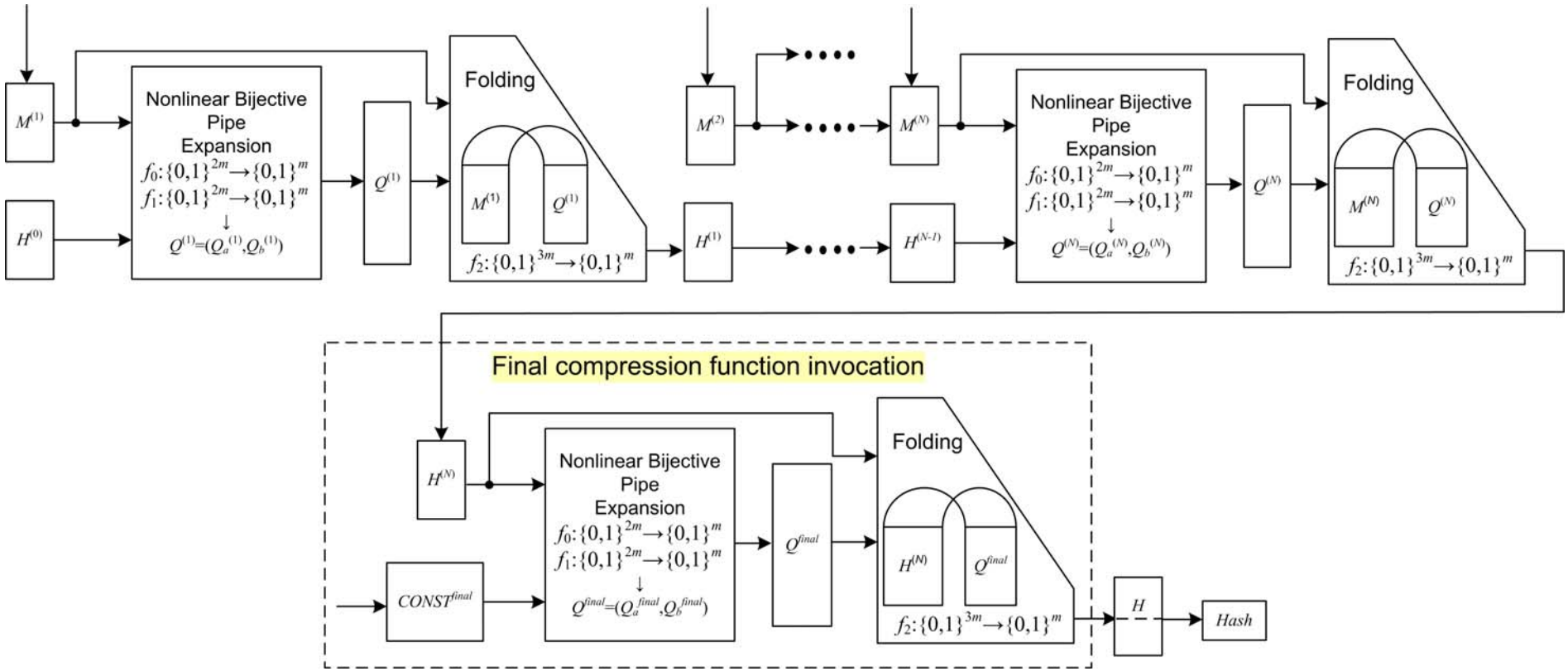
   $H^{(i)} = f(M^{(i)}, H^{(i-1)});$

   }
3. Finalization

   $H^{final} = f(H^{(N)}, CONST^{final});$
4. $Hash$ =Take_n_Least_Significant_Bits(H^{final}).
5. Where the compression function f is defined as follows:
   $Q_a = f_0(M, H);$
   $Q_b = f_1(M, H, Q_a);$
   $newH = f_2(M, Q_a, Q_b);$
   $f(M, H) = newH;$

Table 1: A generic description of the Blue Midnight Wish hash algorithm

Některé principy: Dvojitá pumpa, zobecnění D-M zesílení, finalizace



DPxJmulti (m=2n, QP=4n, f2=6n) F+DP=min2*c
NC=C(2n(DPitm))

Používané operace a funkce

BMW224/BMW256

$$s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{19}(x)$$
$$s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^8(x) \oplus ROTL^{23}(x)$$
$$s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{12}(x) \oplus ROTL^{25}(x)$$
$$s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{15}(x) \oplus ROTL^{29}(x)$$
$$s_4(x) = SHR^1(x) \oplus x$$
$$s_5(x) = SHR^2(x) \oplus x$$
$$r_1(x) = ROTL^3(x)$$
$$r_2(x) = ROTL^7(x)$$
$$r_3(x) = ROTL^{13}(x)$$
$$r_4(x) = ROTL^{16}(x)$$
$$r_5(x) = ROTL^{19}(x)$$
$$r_6(x) = ROTL^{23}(x)$$
$$r_7(x) = ROTL^{27}(x)$$

$$AddElement(j) = \left(ROTL^{((j \bmod 16)+1)}(M_j^{(i)}) + ROTL^{((j+3 \bmod 16)+1)}(M_{j+3}^{(i)}) - ROTL^{((j+10 \bmod 16)+1)}(M_{j+10}^{(i)}) + K_{j+16} \right) \oplus H_{j+7}^{(i)}$$

$$\begin{aligned} expand_1(j) = {} & s_1(Q_{j-16}^{(i)}) + s_2(Q_{j-15}^{(i)}) + s_3(Q_{j-14}^{(i)}) + s_0(Q_{j-13}^{(i)}) \\ & + s_1(Q_{j-12}^{(i)}) + s_2(Q_{j-11}^{(i)}) + s_3(Q_{j-10}^{(i)}) + s_0(Q_{j-9}^{(i)}) \\ & + s_1(Q_{j-8}^{(i)}) + s_2(Q_{j-7}^{(i)}) + s_3(Q_{j-6}^{(i)}) + s_0(Q_{j-5}^{(i)}) \\ & + s_1(Q_{j-4}^{(i)}) + s_2(Q_{j-3}^{(i)}) + s_3(Q_{j-2}^{(i)}) + s_0(Q_{j-1}^{(i)}) \\ & + AddElement(j-16) \end{aligned}$$

$$\begin{aligned} expand_2(j) = {} & Q_{j-16}^{(i)} + r_1(Q_{j-15}^{(i)}) + Q_{j-14}^{(i)} + r_2(Q_{j-13}^{(i)}) \\ & + Q_{j-12}^{(i)} + r_3(Q_{j-11}^{(i)}) + Q_{j-10}^{(i)} + r_4(Q_{j-9}^{(i)}) \\ & + Q_{j-8}^{(i)} + r_5(Q_{j-7}^{(i)}) + Q_{j-6}^{(i)} + r_6(Q_{j-5}^{(i)}) \\ & + Q_{j-4}^{(i)} + r_7(Q_{j-3}^{(i)}) + s_4(Q_{j-2}^{(i)}) + s_5(Q_{j-1}^{(i)}) \\ & + AddElement(j-16) \end{aligned}$$

BMW384/BMW512

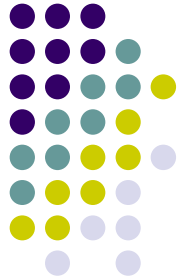
$$s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{37}(x)$$
$$s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^{13}(x) \oplus ROTL^{43}(x)$$
$$s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{19}(x) \oplus ROTL^{53}(x)$$
$$s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{28}(x) \oplus ROTL^{59}(x)$$
$$s_4(x) = SHR^1(x) \oplus x$$
$$s_5(x) = SHR^2(x) \oplus x$$
$$r_1(x) = ROTL^5(x)$$
$$r_2(x) = ROTL^{11}(x)$$
$$r_3(x) = ROTL^{27}(x)$$
$$r_4(x) = ROTL^{32}(x)$$
$$r_5(x) = ROTL^{37}(x)$$
$$r_6(x) = ROTL^{43}(x)$$
$$r_7(x) = ROTL^{53}(x)$$

$$AddElement(j) = \left(ROTL^{((j \bmod 16)+1)}(M_j^{(i)}) + ROTL^{((j+3 \bmod 16)+1)}(M_{j+3}^{(i)}) - ROTL^{((j+10 \bmod 16)+1)}(M_{j+10}^{(i)}) + K_{j+16} \right) \oplus H_{j+7}^{(i)}$$

$$\begin{aligned} expand_1(j) = {} & s_1(Q_{j-16}^{(i)}) + s_2(Q_{j-15}^{(i)}) + s_3(Q_{j-14}^{(i)}) + s_0(Q_{j-13}^{(i)}) \\ & + s_1(Q_{j-12}^{(i)}) + s_2(Q_{j-11}^{(i)}) + s_3(Q_{j-10}^{(i)}) + s_0(Q_{j-9}^{(i)}) \\ & + s_1(Q_{j-8}^{(i)}) + s_2(Q_{j-7}^{(i)}) + s_3(Q_{j-6}^{(i)}) + s_0(Q_{j-5}^{(i)}) \\ & + s_1(Q_{j-4}^{(i)}) + s_2(Q_{j-3}^{(i)}) + s_3(Q_{j-2}^{(i)}) + s_0(Q_{j-1}^{(i)}) \\ & + AddElement(j-16) \end{aligned}$$

$$\begin{aligned} expand_2(j) = {} & Q_{j-16}^{(i)} + r_1(Q_{j-15}^{(i)}) + Q_{j-14}^{(i)} + r_2(Q_{j-13}^{(i)}) \\ & + Q_{j-12}^{(i)} + r_3(Q_{j-11}^{(i)}) + Q_{j-10}^{(i)} + r_4(Q_{j-9}^{(i)}) \\ & + Q_{j-8}^{(i)} + r_5(Q_{j-7}^{(i)}) + Q_{j-6}^{(i)} + r_6(Q_{j-5}^{(i)}) \\ & + Q_{j-4}^{(i)} + r_7(Q_{j-3}^{(i)}) + s_4(Q_{j-2}^{(i)}) + s_5(Q_{j-1}^{(i)}) \\ & + AddElement(j-16) \end{aligned}$$

S-boxy Blue Midnight Wish a SHA-2



$$BMW224/256: \begin{cases} s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{19}(x) \\ s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^8(x) \oplus ROTL^{23}(x) \\ s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{12}(x) \oplus ROTL^{25}(x) \\ s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{15}(x) \oplus ROTL^{29}(x) \end{cases}$$

$$BMW384/512: \begin{cases} s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{37}(x) \\ s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^{13}(x) \oplus ROTL^{43}(x) \\ s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{19}(x) \oplus ROTL^{53}(x) \\ s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{28}(x) \oplus ROTL^{59}(x) \end{cases}$$

SHA-224/256

$$\begin{aligned} \Sigma_0^{256}(x) &= ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \\ \Sigma_1^{256}(x) &= ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x) \\ \sigma_0^{256}(x) &= ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x) \\ \sigma_1^{256}(x) &= ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x) \end{aligned}$$

(návrhová kritéria jsou tajná)

SHA-384/512

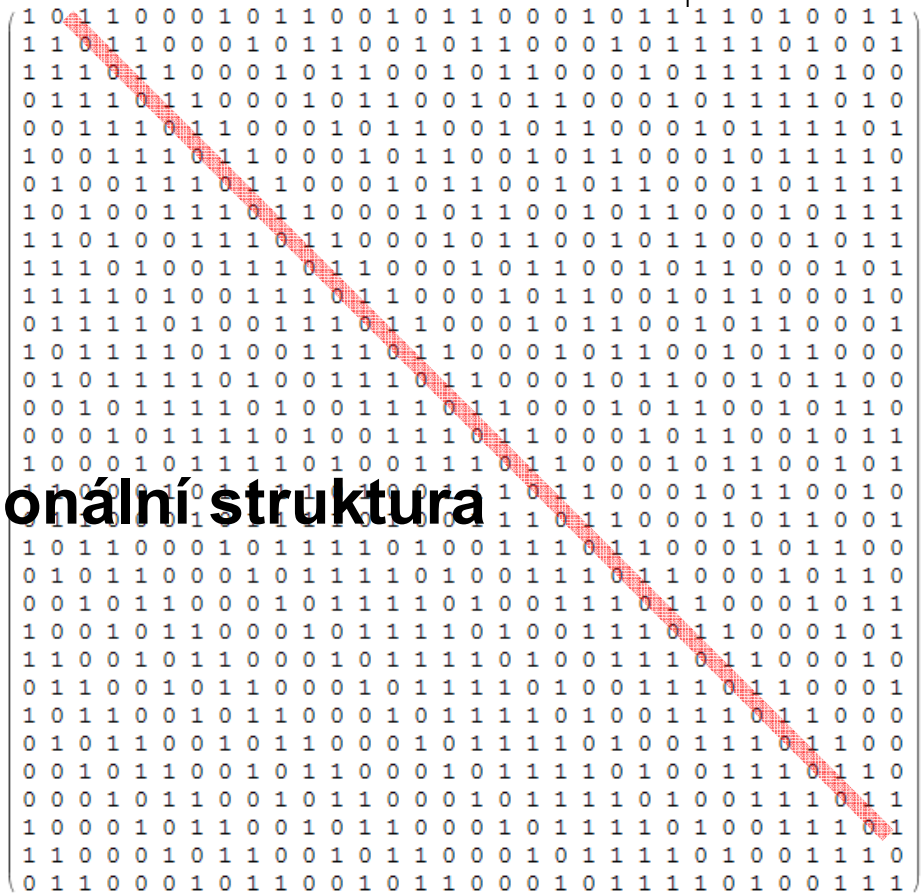
$$\begin{aligned} \Sigma_0^{512}(x) &= ROTR^{28}(x) \oplus ROTR^{34}(x) \oplus ROTR^{39}(x) \\ \Sigma_1^{512}(x) &= ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x) \\ \sigma_0^{512}(x) &= ROTR^1(x) \oplus ROTR^8(x) \oplus SHR^7(x) \\ \sigma_1^{512}(x) &= ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^6(x) \end{aligned}$$

Pozorování u S-boxů SHA-2

$$\Sigma_0^{256}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$$

Inverzní matice (v GF(2))

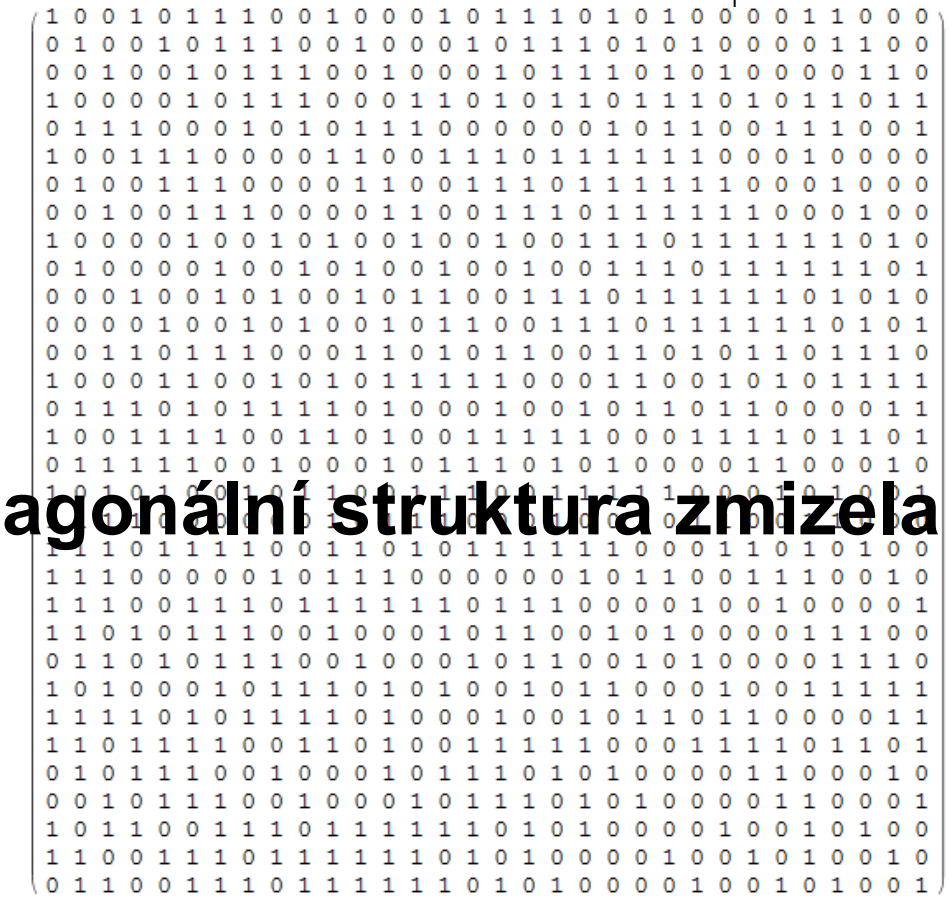
Diagonální struktura



Pozorování u S-boxů SHA-2

$$\sigma_0^{256}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$$

Inverzní matice (v GF(2))



Diagonální struktura zmizela

Pojem výpočetní asymetrie

Definition 1. *For every nonsingular matrix* $\mathbf{S}$ *of order* $n \times n$ *in* $GF(2)$*, let us denote by* $C(\mathbf{S}^{-1})$ *the number of different elements present in the inverse matrix* $\mathbf{S}^{-1}$ *when the inverse is taken in the ring* $\mathbb{Z}_{2^n}(+, *)$.

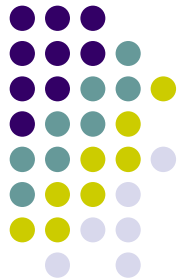
Příklad

$$\mathbf{S} = \begin{pmatrix}
0&0&0&0&0&1&0&1&0&0&1&0&0&1&1&0\\
0&0&0&0&0&0&1&0&1&0&0&1&0&0&1&1\\
1&0&0&0&0&0&0&1&0&1&0&0&1&0&0&1\\
1&1&0&0&0&0&0&0&1&0&1&0&0&1&0&0\\
0&1&1&0&0&0&0&0&0&1&0&1&0&0&1&0\\
0&0&1&1&0&0&0&0&0&0&1&0&1&0&0&1\\
1&0&0&1&1&0&0&0&0&0&0&1&0&1&0&0\\
0&1&0&0&1&1&0&0&0&0&0&0&1&0&1&0\\
0&0&1&0&0&1&1&0&0&0&0&0&0&1&0&1\\
1&0&0&1&0&0&1&1&0&0&0&0&0&0&1&0\\
0&1&0&0&1&0&0&1&1&0&0&0&0&0&0&1\\
1&0&1&0&0&1&0&0&1&1&0&0&0&0&0&0\\
0&1&0&1&0&0&1&0&0&1&1&0&0&0&0&0\\
0&0&1&0&1&0&0&1&0&0&1&1&0&0&0&0\\
0&0&0&1&0&1&0&0&1&0&0&1&1&0&0&0\\
0&0&0&0&1&0&1&0&0&1&0&0&1&1&0&0
\end{pmatrix}$$

$$\mathbf{S}^{-1} = \begin{pmatrix}
16191&60910&46261&48574&12336&7710&53971&50116&62452&57055&19275&56284&771&57826&11565&15420\\
15420&16191&60910&46261&48574&12336&7710&53971&50116&62452&57055&19275&56284&771&57826&11565\\
11565&15420&16191&60910&46261&48574&12336&7710&53971&50116&62452&57055&19275&56284&771&57826\\
57826&11565&15420&16191&60910&46261&48574&12336&7710&53971&50116&62452&57055&19275&56284&771\\
771&57826&11565&15420&16191&60910&46261&48574&12336&7710&53971&50116&62452&57055&19275&56284\\
56284&771&57826&11565&15420&16191&60910&46261&48574&12336&7710&53971&50116&62452&57055&19275\\
19275&56284&771&57826&11565&15420&16191&60910&46261&48574&12336&7710&53971&50116&62452&57055\\
57055&19275&56284&771&57826&11565&15420&16191&60910&46261&48574&12336&7710&53971&50116&62452\\
62452&57055&19275&56284&771&57826&11565&15420&16191&60910&46261&48574&12336&7710&53971&50116\\
50116&62452&57055&19275&56284&771&57826&11565&15420&16191&60910&46261&48574&12336&7710&53971\\
53971&50116&62452&57055&19275&56284&771&57826&11565&15420&16191&60910&46261&48574&12336&7710\\
7710&53971&50116&62452&57055&19275&56284&771&57826&11565&15420&16191&60910&46261&48574&12336\\
12336&7710&53971&50116&62452&57055&19275&56284&771&57826&11565&15420&16191&60910&46261&48574\\
48574&12336&7710&53971&50116&62452&57055&19275&56284&771&57826&11565&15420&16191&60910&46261\\
46261&48574&12336&7710&53971&50116&62452&57055&19275&56284&771&57826&11565&15420&16191&60910\\
60910&46261&48574&12336&7710&53971&50116&62452&57055&19275&56284&771&57826&11565&15420&16191
\end{pmatrix}$$

$C(S^{-1})=16$

Výpočetní asymetrie u S-boxů SHA-2 [GK2009]



Corollary 2.

$$C(\Sigma_0^{256-1}) = 32,\ C(\Sigma_1^{256-1}) = 32,\ C(s_0^{256-1}) = 504 \text{ and } C(s_1^{256-1}) = 121.$$
$$C(\Sigma_0^{512-1}) = 64,\ C(\Sigma_1^{512-1}) = 64,\ C(s_0^{512-1}) = 116 \text{ and } C(s_1^{512-1}) = 2044. \quad \square$$

Maxim. možné hodnoty

Blízké k maximu (523 a 2079)

Vzdálené

S-boxy u Blue Midnight Wish

Hodnota blízká maximu

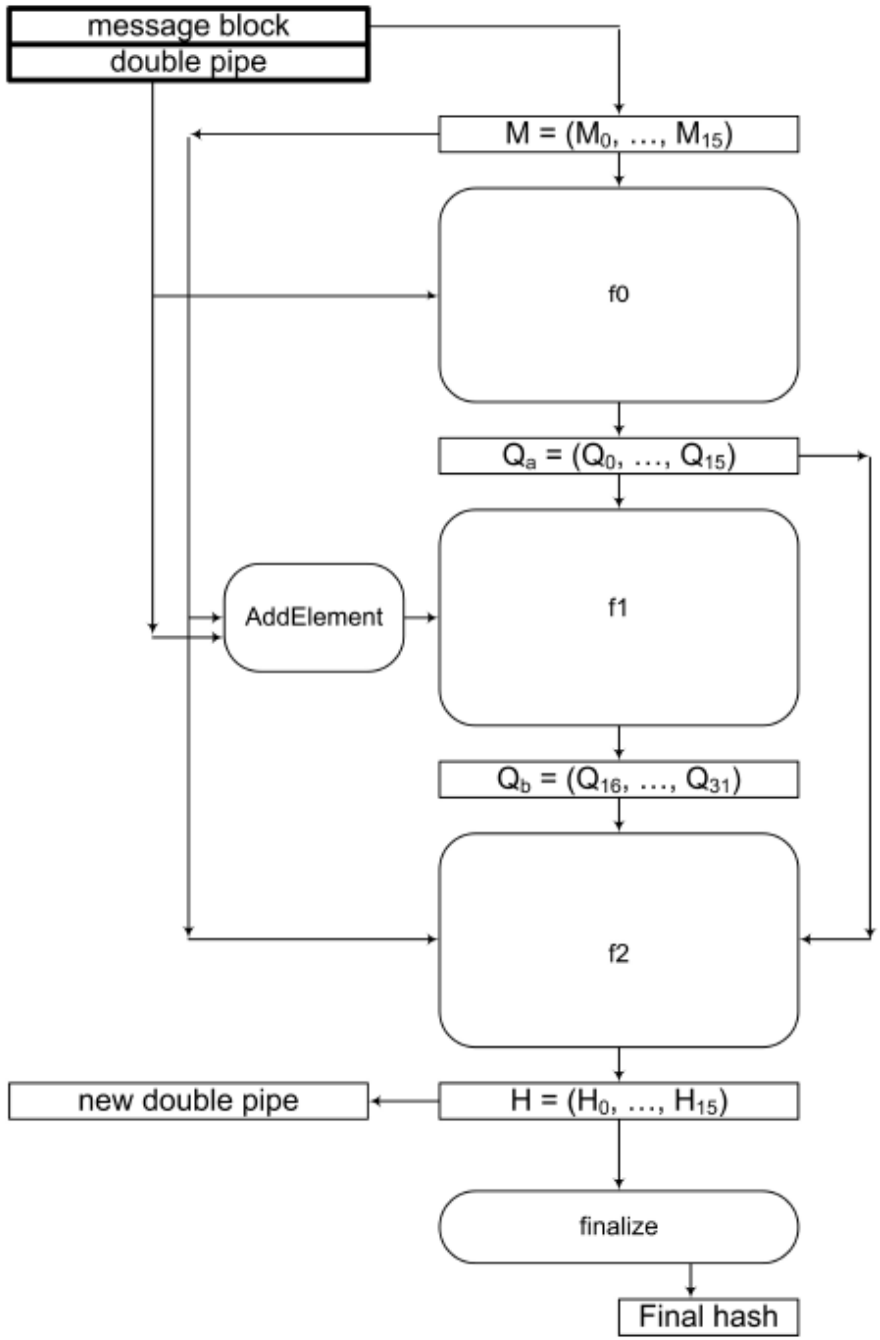
Maximální možná hodnota

$$BMW224/256: \begin{cases} C(\mathbf{s_0}^{-1}) = 524 \\ C(\mathbf{s_1}^{-1}) = 528 \\ C(\mathbf{s_2}^{-1}) = 528 \\ C(\mathbf{s_3}^{-1}) = 528 \end{cases}$$

$$BMW384/512: \begin{cases} C(\mathbf{s_0}^{-1}) = 2080 \\ C(\mathbf{s_1}^{-1}) = 2080 \\ C(\mathbf{s_2}^{-1}) = 2080 \\ C(\mathbf{s_3}^{-1}) = 2080 \end{cases}$$

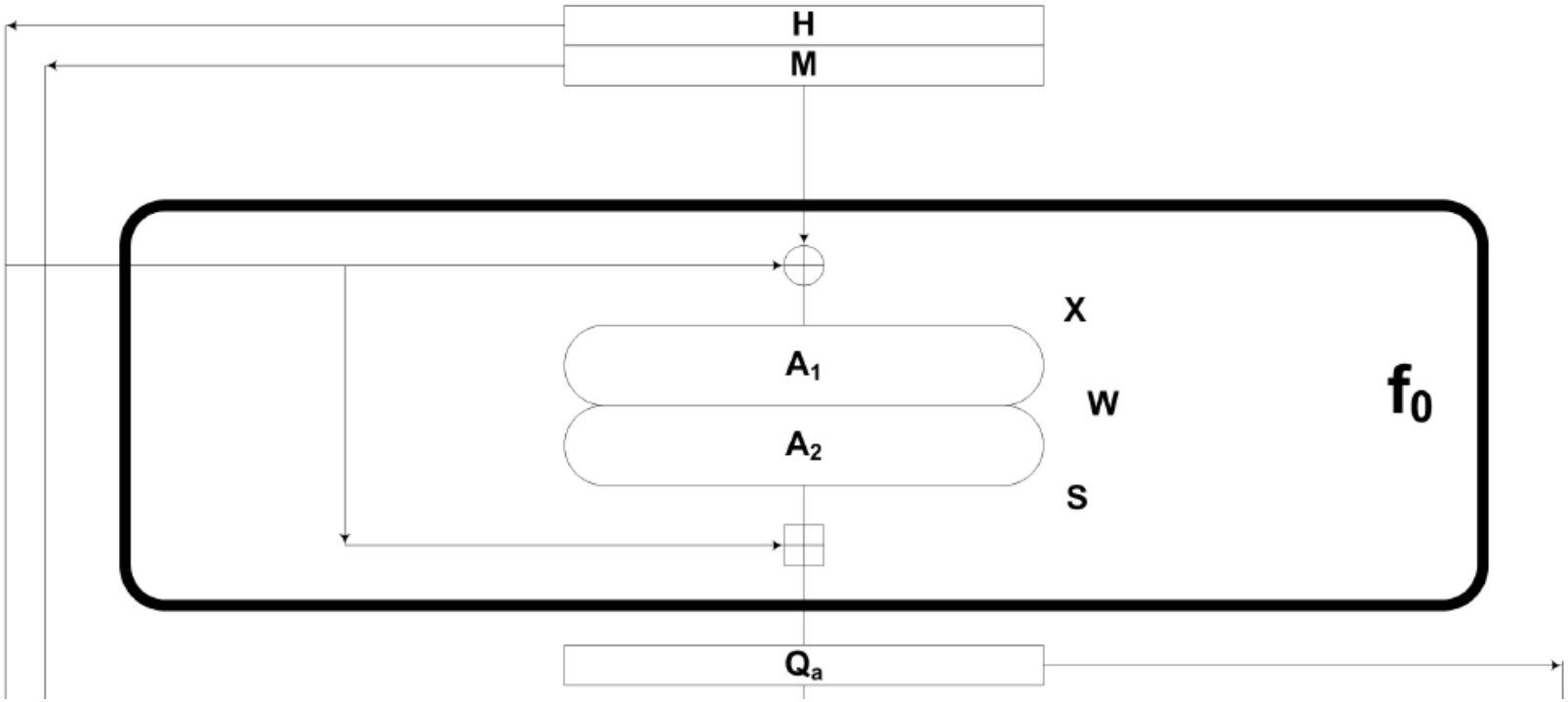
Základní schéma kompresní funkce

- 2 násobná pumpa H
- 4 násobná pumpa Q = (Qa, Qb)
- M, H,..., newH
- hash = ½ H



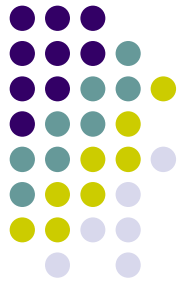
$$Q_a^{(i)} = f_0(M^{(i)}, H^{(i-1)});$$
$$Q_b^{(i)} = f_1(M^{(i)}, H^{(i-1)}, Q_a^{(i)});$$
$$H^{(i)} = f_2(M^{(i)}, Q_a^{(i)}, Q_b^{(i)});$$

$Q_a = f_0(H,M)$ $= A_3(A_2(A_1(A_0(M,H))),H)$



- základní vlastnost: slabá jednosměrná funkce vzhledem k H, bijekce vzhledem k M

f_0



Dílčí funkce:

- xor
- matice
- s-boxy
- +ROTL[1](H)

výstupem je
Qa =(Q0,...Q15)

<u>Vlastnosti:</u>
bijekce nebo
multipermutace,
vzhledem k H
(weak)OWF

$$X = A_0(M, H) = M \oplus H$$

$W = A_1(X)$:

$$\begin{array}{rcccccccccc}
W_0 &=& X_5 &-& X_7 &+& X_{10} &+& X_{13} &+& X_{14} \\
W_1 &=& X_6 &-& X_8 &+& X_{11} &+& X_{14} &-& X_{15} \\
W_2 &=& X_0 &+& X_7 &+& X_9 &-& X_{12} &+& X_{15} \\
W_3 &=& X_0 &-& X_1 &+& X_8 &-& X_{10} &+& X_{13} \\
W_4 &=& X_1 &+& X_2 &+& X_9 &-& X_{11} &-& X_{14} \\
W_5 &=& X_3 &-& X_2 &+& X_{10} &-& X_{12} &+& X_{15} \\
W_6 &=& X_4 &-& X_0 &-& X_3 &-& X_{11} &+& X_{13} \\
W_7 &=& X_1 &-& X_4 &-& X_5 &-& X_{12} &-& X_{14} \\
W_8 &=& X_2 &-& X_5 &-& X_6 &+& X_{13} &-& X_{15} \\
W_9 &=& X_0 &-& X_3 &+& X_6 &-& X_7 &+& X_{14} \\
W_{10} &=& X_8 &-& X_1 &-& X_4 &-& X_7 &+& X_{15} \\
W_{11} &=& X_8 &-& X_0 &-& X_2 &-& X_5 &+& X_9 \\
W_{12} &=& X_1 &+& X_3 &-& X_6 &-& X_9 &+& X_{10} \\
W_{13} &=& X_2 &+& X_4 &+& X_7 &+& X_{10} &+& X_{11} \\
W_{14} &=& X_3 &-& X_5 &+& X_8 &-& X_{11} &-& X_{12} \\
W_{15} &=& X_{12} &-& X_4 &-& X_6 &-& X_9 &+& X_{13}
\end{array}$$

$S = A_2(W)$:

$$\begin{array}{cccc}
S_0 = s_0(W_0) & S_1 = s_1(W_1) & S_2 = s_2(W_2) & S_3 = s_3(W_3) \\
S_4 = s_4(W_4) & S_5 = s_0(W_5) & S_6 = s_1(W_6) & S_7 = s_2(W_7) \\
S_8 = s_3(W_8) & S_9 = s_4(W_9) & S_{10} = s_0(W_{10}) & S_{11} = s_1(W_{11}) \\
S_{12} = s_2(W_{12}) & S_{13} = s_3(W_{13}) & S_{14} = s_4(W_{14}) & S_{15} = s_0(W_{15})
\end{array}$$

$Q_a = A_3(S, H)$:

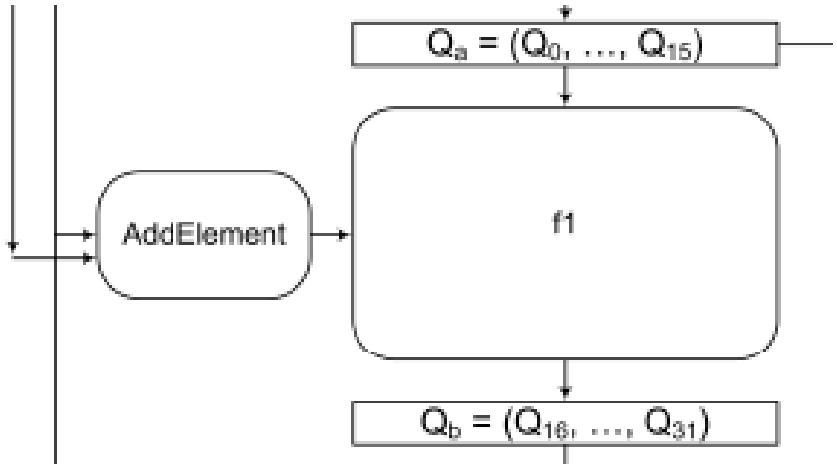
$$\begin{array}{cccc}
Q_0 = S_0 + H_1; & Q_1 = S_1 + H_2; & Q_2 = S_2 + H_3; & Q_3 = S_3 + H_4; \\
Q_4 = S_4 + H_5; & Q_5 = S_5 + H_6; & Q_6 = S_6 + H_7; & Q_7 = S_7 + H_8; \\
Q_8 = S_8 + H_9; & Q_9 = S_9 + H_{10}; & Q_{10} = S_{10} + H_{11}; & Q_{11} = S_{11} + H_{12}; \\
Q_{12} = S_{12} + H_{13}; & Q_{13} = S_{13} + H_{14}; & Q_{14} = S_{14} + H_{15}; & Q_{15} = S_{15} + H_0;
\end{array}$$

(SW) realizace f_0

$$
\begin{array}{lllll}
Q_0 = & H_1 & + & s_0 & (\\
Q_1 = & H_2 & + & s_1 & (\\
Q_2 = & H_3 & + & s_2 & (\\
Q_3 = & H_4 & + & s_3 & (\\
Q_4 = & H_5 & + & s_4 & (\\
Q_5 = & H_6 & + & s_0 & (\\
Q_6 = & H_7 & + & s_1 & (\\
Q_7 = & H_8 & + & s_2 & (\\
Q_8 = & H_9 & + & s_3 & (\\
Q_9 = & H_{10} & + & s_4 & (\\
Q_{10} = & H_{11} & + & s_0 & (\\
Q_{11} = & H_{12} & + & s_1 & (\\
Q_{12} = & H_{13} & + & s_2 & (\\
Q_{13} = & H_{14} & + & s_3 & (\\
Q_{14} = & H_{15} & + & s_4 & (\\
Q_{15} = & H_0 & + & s_0 & (
\end{array}
\begin{array}{lllllllll}
(M_5 \oplus H_5) & - & (M_7 \oplus H_7) & + & (M_{10} \oplus H_{10}) & + & (M_{13} \oplus H_{13}) & + & (M_{14} \oplus H_{14}) \\
(M_6 \oplus H_6) & - & (M_8 \oplus H_8) & + & (M_{11} \oplus H_{11}) & + & (M_{14} \oplus H_{14}) & - & (M_{15} \oplus H_{15}) \\
(M_0 \oplus H_0) & + & (M_7 \oplus H_7) & + & (M_9 \oplus H_9) & - & (M_{12} \oplus H_{12}) & + & (M_{15} \oplus H_{15}) \\
(M_0 \oplus H_0) & - & (M_1 \oplus H_1) & + & (M_8 \oplus H_8) & - & (M_{10} \oplus H_{10}) & + & (M_{13} \oplus H_{13}) \\
(M_1 \oplus H_1) & + & (M_2 \oplus H_2) & + & (M_9 \oplus H_9) & - & (M_{11} \oplus H_{11}) & - & (M_{14} \oplus H_{14}) \\
(M_3 \oplus H_3) & - & (M_2 \oplus H_2) & + & (M_{10} \oplus H_{10}) & - & (M_{12} \oplus H_{12}) & + & (M_{15} \oplus H_{15}) \\
(M_4 \oplus H_4) & - & (M_0 \oplus H_0) & - & (M_3 \oplus H_3) & - & (M_{11} \oplus H_{11}) & + & (M_{13} \oplus H_{13}) \\
(M_1 \oplus H_1) & - & (M_4 \oplus H_4) & - & (M_5 \oplus H_5) & - & (M_{12} \oplus H_{12}) & - & (M_{14} \oplus H_{14}) \\
(M_2 \oplus H_2) & - & (M_5 \oplus H_5) & - & (M_6 \oplus H_6) & + & (M_{13} \oplus H_{13}) & - & (M_{15} \oplus H_{15}) \\
(M_0 \oplus H_0) & - & (M_3 \oplus H_3) & + & (M_6 \oplus H_6) & - & (M_7 \oplus H_7) & + & (M_{14} \oplus H_{14}) \\
(M_8 \oplus H_8) & - & (M_1 \oplus H_1) & - & (M_4 \oplus H_4) & - & (M_7 \oplus H_7) & + & (M_{15} \oplus H_{15}) \\
(M_8 \oplus H_8) & - & (M_0 \oplus H_0) & - & (M_2 \oplus H_2) & - & (M_5 \oplus H_5) & + & (M_9 \oplus H_9) \\
(M_1 \oplus H_1) & + & (M_3 \oplus H_3) & - & (M_6 \oplus H_6) & - & (M_9 \oplus H_9) & + & (M_{10} \oplus H_{10}) \\
(M_2 \oplus H_2) & + & (M_4 \oplus H_4) & + & (M_7 \oplus H_7) & + & (M_{10} \oplus H_{10}) & + & (M_{11} \oplus H_{11}) \\
(M_3 \oplus H_3) & - & (M_5 \oplus H_5) & + & (M_8 \oplus H_8) & - & (M_{11} \oplus H_{11}) & - & (M_{12} \oplus H_{12}) \\
(M_{12} \oplus H_{12}) & - & (M_4 \oplus H_4) & - & (M_6 \oplus H_6) & - & (M_9 \oplus H_9) & + & (M_{13} \oplus H_{13})
\end{array}
\begin{array}{l}
) \\
) \\
) \\
) \\
) \\
) \\
) \\
) \\
) \\
) \\
) \\
) \\
) \\
) \\
) \\
)
\end{array}
$$

f_1

non-linear feedback shift register, střídá funkce ve zpětné vazbě



The function f_1 expands $Q_a = (Q_0, ..., Q_{15})$ to $Q_b = (Q_{16}, ..., Q_{31})$ according to the tunable parameters $ExpandRounds_1$ and $ExpandRounds_2$:

1.1 For $ii = 0$ to $ExpandRounds_1 - 1$
$Q^{(i)}_{ii+16} = expand_1(ii + 16)$

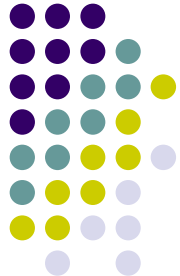
1.2 For $ii = ExpandRounds_1$ to $ExpandRounds_1 + ExpandRounds_2 - 1$
$Q^{(i)}_{ii+16} = expand_2(ii + 16)$

where the functions $expand_1()$ and $expand_2()$ are defined as:

$$\begin{aligned} expand_1(j) = {} & s_1(Q_{j-16}) + s_2(Q_{j-15}) + s_3(Q_{j-14}) + s_0(Q_{j-13}) \\ & + s_1(Q_{j-12}) + s_2(Q_{j-11}) + s_3(Q_{j-10}) + s_0(Q_{j-9}) \\ & + s_1(Q_{j-8}) + s_2(Q_{j-7}) + s_3(Q_{j-6}) + s_0(Q_{j-5}) \\ & + s_1(Q_{j-4}) + s_2(Q_{j-3}) + s_3(Q_{j-2}) + s_0(Q_{j-1}) \\ & + A_{j-16} \end{aligned}$$

$$\begin{aligned} expand_2(j) = {} & Q_{j-16} + r_1(Q_{j-15}) + Q_{j-14} + r_2(Q_{j-13}) \\ & + Q_{j-12} + r_3(Q_{j-11}) + Q_{j-10} + r_4(Q_{j-9}) \\ & + Q_{j-8} + r_5(Q_{j-7}) + Q_{j-6} + r_6(Q_{j-5}) \\ & + Q_{j-4} + r_7(Q_{j-3}) + s_4(Q_{j-2}) + s_5(Q_{j-1}) \\ & + A_{j-16}. \end{aligned}$$

$Qb = Q_{16}, \ldots, Q_{31}$



- NLFSR:

Q[16] = s1(Q[0])+s2(Q[1])+s3(Q[2])+s0(Q[3])+s1(Q[4])+s2(Q[5])+s3(Q[6])+
s0(Q[7])+s1(Q[8])+s2(Q[9])+s3(Q[10])+s0(Q[11])+s1(Q[12])+s2(Q[13])+
s3(Q[14])+s0(Q[15]) +A[0]

Q[17]= s1(Q[1])+s2(Q[2])+s3(Q[3])+s0(Q[4])+s1(Q[5])+s2(Q[6])+s3(Q[7])+
s0(Q[8])+s1(Q[9])+s2(Q[10])+s3(Q[11])+s0(Q[12])+s1(Q[13])+s2(Q[14])+
s3(Q[15]) + s0(Q[16]) + A[1]

Q[18]= Q[2]+r1(Q[3])+Q[4]+r2(Q[5])+Q[6]+r3(Q[7])+Q[8]+r4(Q[9])+
Q[10]+r5(Q[11])+Q[12]+r6(Q[13])+Q[14]+r7(Q[15]) +s5(Q[16])+
s4(Q[17]) + A[2]

Q[19]= Q[3]+r1(Q[4])+Q[5]+r2(Q[6])+Q[7]+r3(Q[8])+Q[9]+r4(Q[10])+Q[11]+
r5(Q[12])+Q[13]+r6(Q[14])+Q[15]+r7(Q[16])+s5(Q[17])+s4(Q[18]) + A[3]

Q[20]= Q[4]+r1(Q[5])+Q[6]+r2(Q[7])+Q[8]+r3(Q[9])+Q[10]+r4(Q[11])+Q[12]+
r5(Q[13])+Q[14]+r6(Q[15])+Q[16]+r7(Q[17])+s5(Q[18])+s4(Q[19]) + A[4]

Q[21]= Q[5]+r1(Q[6])+Q[7]+r2(Q[8])+Q[9]+r3(Q[10])+Q[11]+r4(Q[12)+Q[13]+
r5(Q[14])+Q[15] +r6(Q[16])+Q[17]+r7(Q[18])+s5(Q[19])+s4(Q[20]) + A[5]

.....

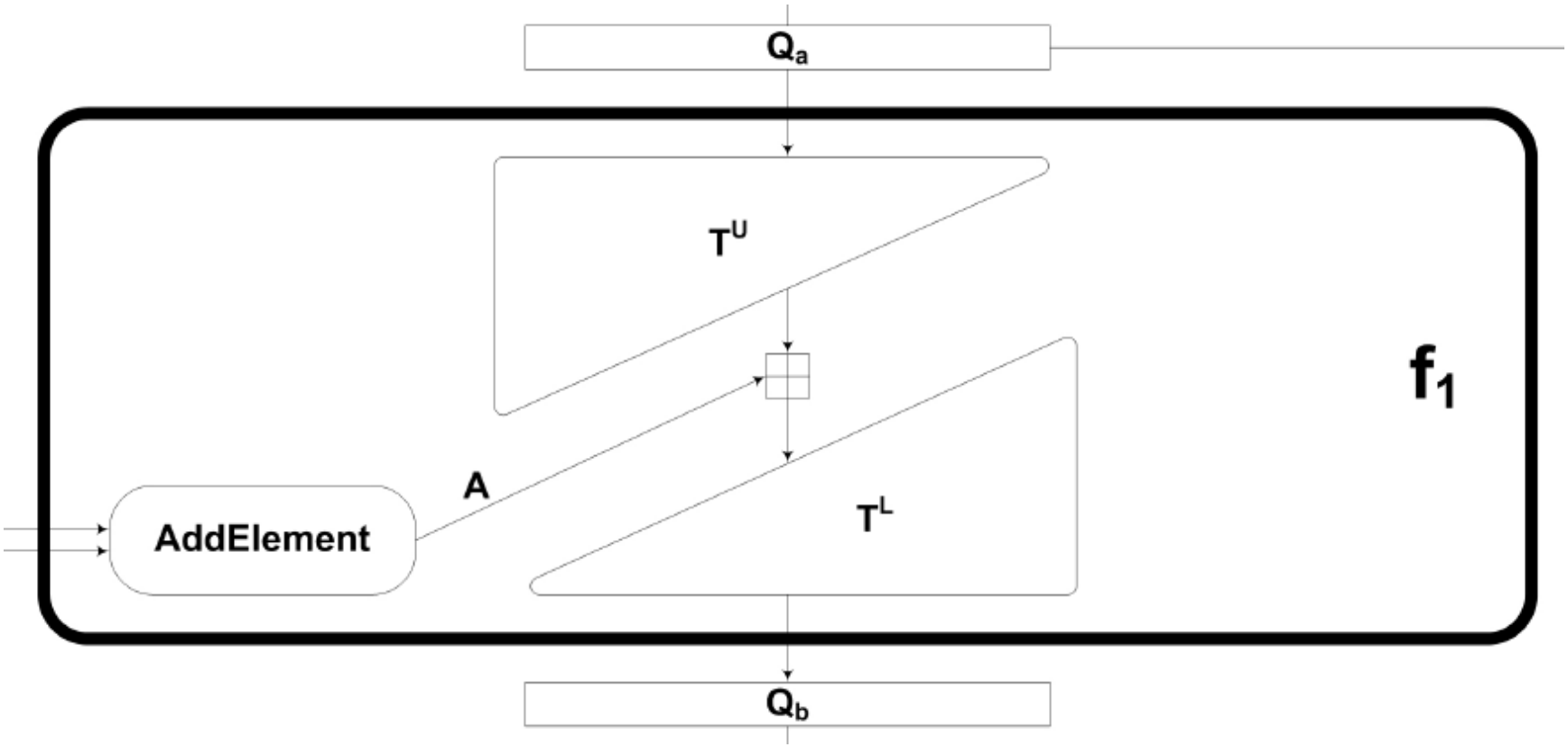
Rozklad Qb

$$
\begin{aligned}
P_0 &= s1(Q_0) + s2(Q_1) + s3(Q_2) + s0(Q_3) + s1(Q_4) + s2(Q_5) + s3(Q_6) + s0(Q_7) + s1(Q_8) + s2(Q_9) + s3(Q_{10}) + s0(Q_{11}) + s1(Q_{12}) + s2(Q_{13}) + \\
&\quad + s3(Q_{14}) + s0(Q_{15}) \\
P_1 &= s1(Q_1) + s2(Q_2) + s3(Q_3) + s0(Q_4) + s1(Q_5) + s2(Q_6) + s3(Q_7) + s0(Q_8) + s1(Q_9) + s2(Q_{10}) + s3(Q_{11}) + s0(Q_{12}) + s1(Q_{13}) + \\
&\quad + s2(Q_{14}) + s3(Q_{15}) \\
P_2 &= Q_2 + r1(Q_3) + Q_4 + r2(Q_5) + Q_6 + r3(Q_7) + Q_8 + r4(Q_9) + Q_{10} + r5(Q_{11}) + Q_{12} + r6(Q_{13}) + Q_{14} + r7(Q_{15}) \\
P_3 &= Q_3 + r1(Q_4) + Q_5 + r2(Q_6) + Q_7 + r3(Q_8) + Q_9 + r4(Q_{10}) + Q_{11} + r5(Q_{12}) + Q_{13} + r6(Q_{14}) + Q_{15} \\
P_4 &= Q_4 + r1(Q_5) + Q_6 + r2(Q_7) + Q_8 + r3(Q_9) + Q_{10} + r4(Q_{11}) + Q_{12} + r5(Q_{13}) + Q_{14} + r6(Q_{15}) \\
P_5 &= Q_5 + r1(Q_6) + Q_7 + r2(Q_8) + Q_9 + r3(Q_{10}) + Q_{11} + r4(Q_{12}) + Q_{13} + r5(Q_{14}) + Q_{15} \\
P_6 &= Q_6 + r1(Q_7) + Q_8 + r2(Q_9) + Q_{10} + r3(Q_{11}) + Q_{12} + r4(Q_{13}) + Q_{14} + r5(Q_{15}) \\
P_7 &= Q_7 + r1(Q_8) + Q_9 + r2(Q_{10}) + Q_{11} + r3(Q_{12}) + Q_{13} + r4(Q_{14}) + Q_{15} \\
P_8 &= Q_8 + r1(Q_9) + Q_{10} + r2(Q_{11}) + Q_{12} + r3(Q_{13}) + Q_{14} + r4(Q_{15}) \\
P_9 &= Q_9 + r1(Q_{10}) + Q_{11} + r2(Q_{12}) + Q_{13} + r3(Q_{14}) + Q_{15} \\
P_{10} &= Q_{10} + r1(Q_{11}) + Q_{12} + r2(Q_{13}) + Q_{14} + r3(Q_{15}) \\
P_{11} &= Q_{11} + r1(Q_{12}) + Q_{13} + r2(Q_{14}) + Q_{15} \\
P_{12} &= Q_{12} + r1(Q_{13}) + Q_{14} + r2(Q_{15}) \\
P_{13} &= Q_{13} + r1(Q_{14}) + Q_{15} \\
P_{14} &= Q_{14} + r1(Q_{15}) \\
P_{15} &= Q_{15}
\end{aligned}
$$

- P = T^U(Qa)
- R = P + A, A = AddElement
- Qb = T^L(R)

$$
\begin{aligned}
Q_{16} &= R_0 \\
Q_{17} &= R_1 + s0(Q_{16}) \\
Q_{18} &= R_2 + s4(Q_{16}) + s5(Q_{17}) \\
Q_{19} &= R_3 + r7(Q_{16}) + s4(Q_{17}) + s5(Q_{18}) \\
Q_{20} &= R_4 + Q_{16} + r7(Q_{17}) + s4(Q_{18}) + s5(Q_{19}) \\
Q_{21} &= R_5 + r6(Q_{16}) + Q_{17} + r7(Q_{18}) + s4(Q_{19}) + s5(Q_{20}) \\
Q_{22} &= R_6 + Q_{16} + r6(Q_{17}) + Q_{18} + r7(Q_{19}) + s4(Q_{20}) + s5(Q_{21}) \\
Q_{23} &= R_7 + r5(Q_{16}) + Q_{17} + r6(Q_{18}) + Q_{19} + r7(Q_{20}) + s4(Q_{21}) + s5(Q_{22}) \\
Q_{24} &= R_8 + Q_{16} + r5(Q_{17}) + Q_{18} + r6(Q_{19}) + Q_{20} + r7(Q_{21}) + s4(Q_{22}) + s5(Q_{23}) \\
Q_{25} &= R_9 + r4(Q_{16}) + Q_{17} + r5(Q_{18}) + Q_{19} + r6(Q_{20}) + Q_{21} + r7(Q_{22}) + s4(Q_{23}) + s5(Q_{24}) \\
Q_{26} &= R_{10} + Q_{16} + r4(Q_{17}) + Q_{18} + r5(Q_{19}) + Q_{20} + r6(Q_{21}) + Q_{22} + r7(Q_{23}) + s4(Q_{24}) + s5(Q_{25}) \\
Q_{27} &= R_{11} + r3(Q_{16}) + Q_{17} + r4(Q_{18}) + Q_{19} + r5(Q_{20}) + Q_{21} + r6(Q_{22}) + Q_{23} + r7(Q_{24}) + s4(Q_{25}) + s5(Q_{26}) \\
Q_{28} &= R_{12} + Q_{16} + r3(Q_{17}) + Q_{18} + r4(Q_{19}) + Q_{20} + r5(Q_{21}) + Q_{22} + r6(Q_{23}) + Q_{24} + r7(Q_{25}) + s4(Q_{26}) + s5(Q_{27}) \\
Q_{29} &= R_{13} + r2(Q_{16}) + Q_{17} + r3(Q_{18}) + Q_{19} + r4(Q_{20}) + Q_{21} + r5(Q_{22}) + Q_{23} + r6(Q_{24}) + Q_{25} + r7(Q_{26}) + s4(Q_{27}) + s5(Q_{28}) \\
Q_{30} &= R_{14} + Q_{16} + r2(Q_{17}) + Q_{18} + r3(Q_{19}) + Q_{20} + r4(Q_{21}) + Q_{22} + r5(Q_{23}) + Q_{24} + r6(Q_{25}) + Q_{26} + r7(Q_{27}) + s4(Q_{28}) + s5(Q_{29}) \\
Q_{31} &= R_{15} + r1(Q_{16}) + Q_{17} + r2(Q_{18}) + Q_{19} + r3(Q_{20}) + Q_{21} + r4(Q_{22}) + Q_{23} + r5(Q_{24}) + Q_{25} + r6(Q_{26}) + Q_{27} + r7(Q_{28}) + s4(Q_{29}) + s5(Q_{30})
\end{aligned}
$$

Rozklad a vlastnosti f_1



- TU,TL,f1 – bijekce a multipermutace

AddElement: rozklad a vlastnosti

$A = AddElement(M, H) = (B(rotM) + K) \oplus ROTL^7(H)$, where K is a constant $K = (16 * 0x05555555, ..., 31 * 0x05555555)$.

dílčí zobrazení

B, rot, xor H: bijekce, multipermutace

B(M) =

$$
\begin{array}{lcl}
M_0 + M_3 - M_{10} \\
M_1 + M_4 - M_{11} \\
M_2 + M_5 - M_{12} \\
M_3 + M_6 - M_{13} \\
M_4 + M_7 - M_{14} \\
M_5 + M_8 - M_{15} \\
M_6 + M_9 - M_0 \\
M_7 + M_{10} - M_1 \\
M_8 + M_{11} - M_2 \\
M_9 + M_{12} - M_3 \\
M_{10} + M_{13} - M_4 \\
M_{11} + M_{14} - M_5 \\
M_{12} + M_{15} - M_6 \\
M_{13} + M_0 - M_7 \\
M_{14} + M_1 - M_8 \\
M_{15} + M_2 - M_9
\end{array}
$$

A =

$$
\begin{array}{lcl}
H_6 \oplus (ROTL^1(M_0) + ROTL^4(M_3) - ROTL^{11}(M_{10}) + K_0) \\
H_7 \oplus (ROTL^2(M_1) + ROTL^5(M_4) - ROTL^{12}(M_{11}) + K_1) \\
H_8 \oplus (ROTL^3(M_2) + ROTL^6(M_5) - ROTL^{13}(M_{12}) + K_2) \\
H_9 \oplus (ROTL^4(M_3) + ROTL^7(M_6) - ROTL^{14}(M_{13}) + K_3) \\
H_{10} \oplus (ROTL^5(M_4) + ROTL^8(M_7) - ROTL^{15}(M_{14}) + K_4) \\
H_{11} \oplus (ROTL^6(M_5) + ROTL^9(M_8) - ROTL^{16}(M_{15}) + K_5) \\
H_{12} \oplus (ROTL^7(M_6) + ROTL^{10}(M_9) - ROTL^1(M_0) + K_6) \\
H_{13} \oplus (ROTL^8(M_7) + ROTL^{11}(M_{10}) - ROTL^2(M_1) + K_7) \\
H_{14} \oplus (ROTL^9(M_8) + ROTL^{12}(M_{11}) - ROTL^3(M_2) + K_8) \\
H_{15} \oplus (ROTL^{10}(M_9) + ROTL^{13}(M_{12}) - ROTL^4(M_3) + K_9) \\
H_0 \oplus (ROTL^{11}(M_{10}) + ROTL^{14}(M_{13}) - ROTL^5(M_4) + K_{10}) \\
H_1 \oplus (ROTL^{12}(M_{11}) + ROTL^{15}(M_{14}) - ROTL^6(M_5) + K_{11}) \\
H_2 \oplus (ROTL^{13}(M_{12}) + ROTL^{16}(M_{15}) - ROTL^7(M_6) + K_{12}) \\
H_3 \oplus (ROTL^{14}(M_{13}) + ROTL^1(M_0) - ROTL^8(M_7) + K_{13}) \\
H_4 \oplus (ROTL^{15}(M_{14}) + ROTL^2(M_1) - ROTL^9(M_8) + K_{14}) \\
H_5 \oplus (ROTL^{16}(M_{15}) + ROTL^3(M_2) - ROTL^{10}(M_9) + K_{15})
\end{array}
$$

f1: $Q_b = T^L(R) = T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H)))$

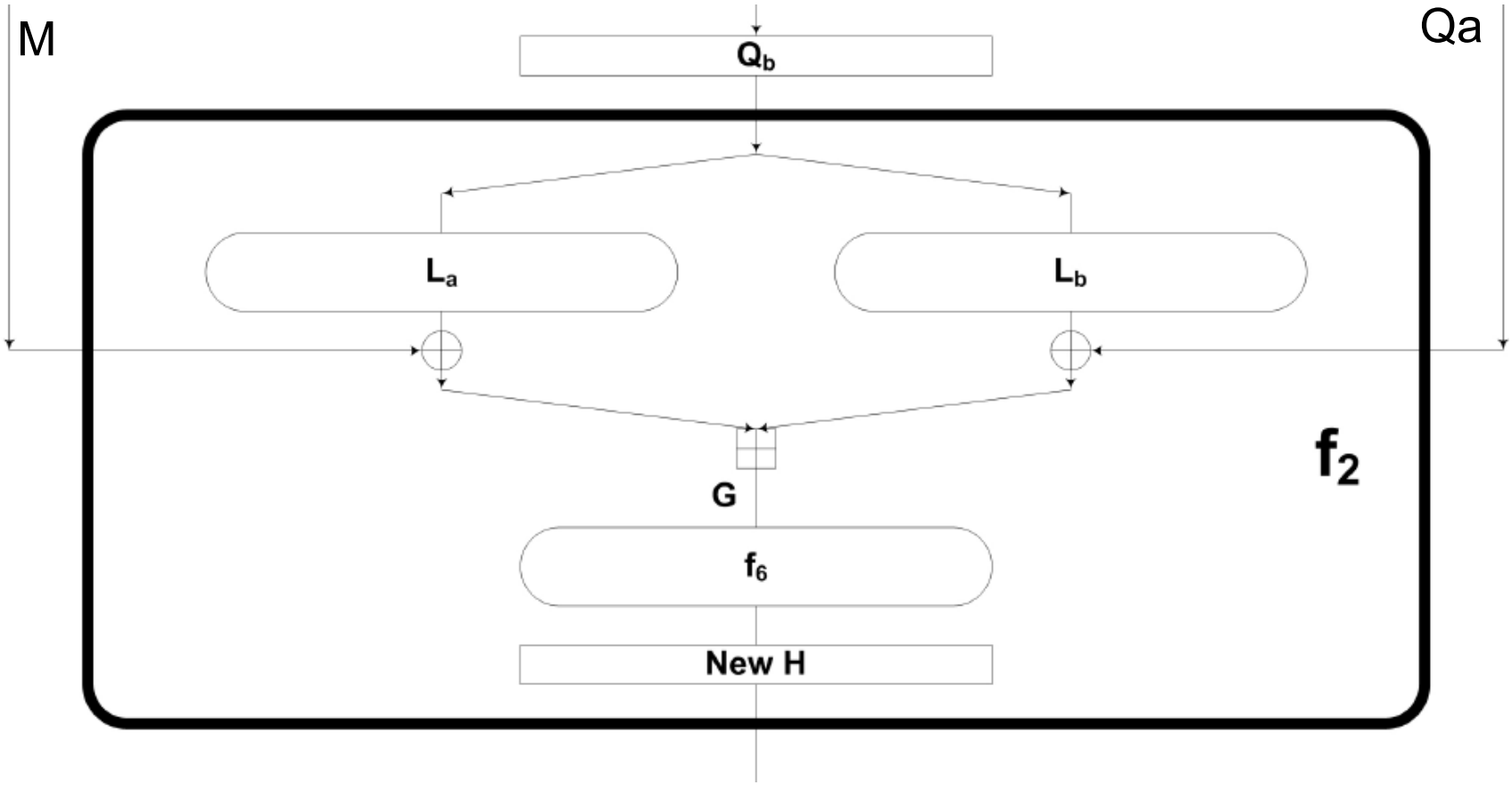
$$
\begin{aligned}
P_0 &= s1(Q_0) + s2(Q_1) + s3(Q_2) + s0(Q_3) + s1(Q_4) + s2(Q_5) + s3(Q_6) + s0(Q_7) + s1(Q_8) + s2(Q_9) + s3(Q_{10}) + s0(Q_{11}) + s1(Q_{12}) + s2(Q_{13}) + \\
&\quad + s3(Q_{14}) + s0(Q_{15}) \\
P_1 &= s1(Q_1) + s2(Q_2) + s3(Q_3) + s0(Q_4) + s1(Q_5) + s2(Q_6) + s3(Q_7) + s0(Q_8) + s1(Q_9) + s2(Q_{10}) + s3(Q_{11}) + s0(Q_{12}) + s1(Q_{13}) + \\
&\quad + s2(Q_{14}) + s3(Q_{15}) \\
P_2 &= Q_2 + r1(Q_3) + Q_4 + r2(Q_5) + Q_6 + r3(Q_7) + Q_8 + r4(Q_9) + Q_{10} + r5(Q_{11}) + Q_{12} + r6(Q_{13}) + Q_{14} + r7(Q_{15}) \\
P_3 &= Q_3 + r1(Q_4) + Q_5 + r2(Q_6) + Q_7 + r3(Q_8) + Q_9 + r4(Q_{10}) + Q_{11} + r5(Q_{12}) + Q_{13} + r6(Q_{14}) + Q_{15} \\
P_4 &= Q_4 + r1(Q_5) + Q_6 + r2(Q_7) + Q_8 + r3(Q_9) + Q_{10} + r4(Q_{11}) + Q_{12} + r5(Q_{13}) + Q_{14} + r6(Q_{15}) \\
P_5 &= Q_5 + r1(Q_6) + Q_7 + r2(Q_8) + Q_9 + r3(Q_{10}) + Q_{11} + r4(Q_{12}) + Q_{13} + r5(Q_{14}) + Q_{15} \\
P_6 &= Q_6 + r1(Q_7) + Q_8 + r2(Q_9) + Q_{10} + r3(Q_{11}) + Q_{12} + r4(Q_{13}) + Q_{14} + r5(Q_{15}) \\
P_7 &= Q_7 + r1(Q_8) + Q_9 + r2(Q_{10}) + Q_{11} + r3(Q_{12}) + Q_{13} + r4(Q_{14}) + Q_{15} \\
P_8 &= Q_8 + r1(Q_9) + Q_{10} + r2(Q_{11}) + Q_{12} + r3(Q_{13}) + Q_{14} + r4(Q_{15}) \\
P_9 &= Q_9 + r1(Q_{10}) + Q_{11} + r2(Q_{12}) + Q_{13} + r3(Q_{14}) + Q_{15} \\
P_{10} &= Q_{10} + r1(Q_{11}) + Q_{12} + r2(Q_{13}) + Q_{14} + r3(Q_{15}) \\
P_{11} &= Q_{11} + r1(Q_{12}) + Q_{13} + r2(Q_{14}) + Q_{15} \\
P_{12} &= Q_{12} + r1(Q_{13}) + Q_{14} + r2(Q_{15}) \\
P_{13} &= Q_{13} + r1(Q_{14}) + Q_{15} \\
P_{14} &= Q_{14} + r1(Q_{15}) \\
P_{15} &= Q_{15}
\end{aligned}
$$

$$
\begin{aligned}
R_0 &= P_0 + A_0 &&= P_0 + (H_6 \oplus (ROTL^1(M_0) + ROTL^4(M_3) - ROTL^{11}(M_{10}) + K_0)) \\
R_1 &= P_1 + A_1 &&= P_1 + (H_7 \oplus (ROTL^2(M_1) + ROTL^5(M_4) - ROTL^{12}(M_{11}) + K_1)) \\
R_2 &= P_2 + A_2 &&= P_2 + (H_8 \oplus (ROTL^3(M_2) + ROTL^6(M_5) - ROTL^{13}(M_{12}) + K_2)) \\
R_3 &= P_3 + A_3 &&= P_3 + (H_9 \oplus (ROTL^4(M_3) + ROTL^7(M_6) - ROTL^{14}(M_{13}) + K_3)) \\
R_4 &= P_4 + A_4 &&= P_4 + (H_{10} \oplus (ROTL^5(M_4) + ROTL^8(M_7) - ROTL^{15}(M_{14}) + K_4)) \\
R_5 &= P_5 + A_5 &&= P_5 + (H_{11} \oplus (ROTL^6(M_5) + ROTL^9(M_8) - ROTL^{16}(M_{15}) + K_5)) \\
R_6 &= P_6 + A_6 &&= P_6 + (H_{12} \oplus (ROTL^7(M_6) + ROTL^{10}(M_9) - ROTL^1(M_0) + K_6)) \\
R_7 &= P_7 + A_7 &&= P_7 + (H_{13} \oplus (ROTL^8(M_7) + ROTL^{11}(M_{10}) - ROTL^2(M_1) + K_7)) \\
R_8 &= P_8 + A_8 &&= P_8 + (H_{14} \oplus (ROTL^9(M_8) + ROTL^{12}(M_{11}) - ROTL^3(M_2) + K_8)) \\
R_9 &= P_9 + A_8 &&= P_9 + (H_{15} \oplus (ROTL^{10}(M_9) + ROTL^{13}(M_{12}) - ROTL^4(M_3) + K_9)) \\
R_{10} &= P_{10} + A_{10} &&= P_{10} + (H_0 \oplus (ROTL^{11}(M_{10}) + ROTL^{14}(M_{13}) - ROTL^5(M_4) + K_{10})) \\
R_{11} &= P_{11} + A_{11} &&= P_{11} + (H_1 \oplus (ROTL^{12}(M_{11}) + ROTL^{15}(M_{14}) - ROTL^6(M_5) + K_{11})) \\
R_{12} &= P_{12} + A_{12} &&= P_{12} + (H_2 \oplus (ROTL^{13}(M_{12}) + ROTL^{16}(M_{15}) - ROTL^7(M_6) + K_{12})) \\
R_{13} &= P_{13} + A_{13} &&= P_{13} + (H_3 \oplus (ROTL^{14}(M_{13}) + ROTL^1(M_0) - ROTL^8(M_7) + K_{13})) \\
R_{14} &= P_{14} + A_{14} &&= P_{14} + (H_4 \oplus (ROTL^{15}(M_{14}) + ROTL^2(M_1) - ROTL^9(M_8) + K_{14})) \\
R_{15} &= P_{15} + A_{15} &&= P_{15} + (H_5 \oplus (ROTL^{16}(M_{15}) + ROTL^3(M_2) - ROTL^{10}(M_9) + K_{15}))
\end{aligned}
$$

$$
\begin{aligned}
Q_{16} &= R_0 \\
Q_{17} &= R_1 + s0(Q_{16}) \\
Q_{18} &= R_2 + s4(Q_{16}) + s5(Q_{17}) \\
Q_{19} &= R_3 + r7(Q_{16}) + s4(Q_{17}) + s5(Q_{18}) \\
Q_{20} &= R_4 + Q_{16} + r7(Q_{17}) + s4(Q_{18}) + s5(Q_{19}) \\
Q_{21} &= R_5 + r6(Q_{16}) + Q_{17} + r7(Q_{18}) + s4(Q_{19}) + s5(Q_{20}) \\
Q_{22} &= R_6 + Q_{16} + r6(Q_{17}) + Q_{18} + r7(Q_{19}) + s4(Q_{20}) + s5(Q_{21}) \\
Q_{23} &= R_7 + r5(Q_{16}) + Q_{17} + r6(Q_{18}) + Q_{19} + r7(Q_{20}) + s4(Q_{21}) + s5(Q_{22}) \\
Q_{24} &= R_8 + Q_{16} + r5(Q_{17}) + Q_{18} + r6(Q_{19}) + Q_{20} + r7(Q_{21}) + s4(Q_{22}) + s5(Q_{23}) \\
Q_{25} &= R_9 + r4(Q_{16}) + Q_{17} + r5(Q_{18}) + Q_{19} + r6(Q_{20}) + Q_{21} + r7(Q_{22}) + s4(Q_{23}) + s5(Q_{24}) \\
Q_{26} &= R_{10} + Q_{16} + r4(Q_{17}) + Q_{18} + r5(Q_{19}) + Q_{20} + r6(Q_{21}) + Q_{22} + r7(Q_{23}) + s4(Q_{24}) + s5(Q_{25}) \\
Q_{27} &= R_{11} + r3(Q_{16}) + Q_{17} + r4(Q_{18}) + Q_{19} + r5(Q_{20}) + Q_{21} + r6(Q_{22}) + Q_{23} + r7(Q_{24}) + s4(Q_{25}) + s5(Q_{26}) \\
Q_{28} &= R_{12} + Q_{16} + r3(Q_{17}) + Q_{18} + r4(Q_{19}) + Q_{20} + r5(Q_{21}) + Q_{22} + r6(Q_{23}) + Q_{24} + r7(Q_{25}) + s4(Q_{26}) + s5(Q_{27}) \\
Q_{29} &= R_{13} + r2(Q_{16}) + Q_{17} + r3(Q_{18}) + Q_{19} + r4(Q_{20}) + Q_{21} + r5(Q_{22}) + Q_{23} + r6(Q_{24}) + Q_{25} + r7(Q_{26}) + s4(Q_{27}) + s5(Q_{28}) \\
Q_{30} &= R_{14} + Q_{16} + r2(Q_{17}) + Q_{18} + r3(Q_{19}) + Q_{20} + r4(Q_{21}) + Q_{22} + r5(Q_{23}) + Q_{24} + r6(Q_{25}) + Q_{26} + r7(Q_{27}) + s4(Q_{28}) + s5(Q_{29}) \\
Q_{31} &= R_{15} + r1(Q_{16}) + Q_{17} + r2(Q_{18}) + Q_{19} + r3(Q_{20}) + Q_{21} + r4(Q_{22}) + Q_{23} + r5(Q_{24}) + Q_{25} + r6(Q_{26}) + Q_{27} + r7(Q_{28}) + s4(Q_{29}) + s5(Q_{30})
\end{aligned}
$$

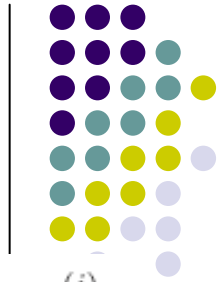
f_2: Rozklad a vlastnosti

- La, Lb jsou blízké bijekci, L = La xor Lb je bijekce
- f6 je bijekce



f2:

$$\begin{aligned} G &= (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)), \\ newH &= f(M,H) = f_6(G). \end{aligned}$$



Význam

XH, XL, f5, La, Lb

$$\begin{aligned} XL &= Q_{16}^{(i)} \oplus Q_{17}^{(i)} \oplus \ldots \oplus Q_{23}^{(i)} \\ XH &= XL \oplus Q_{24}^{(i)} \oplus Q_{25}^{(i)} \oplus \ldots \oplus Q_{31}^{(i)} \end{aligned}$$

$$\begin{aligned}
H_0 &= (SHL^5(XH) \oplus SHR^5(Q_{16}) \oplus M_0) + (XL \oplus Q_{24} \oplus Q_0) \\
H_1 &= (SHR^7(XH) \oplus SHL^8(Q_{17}) \oplus M_1) + (XL \oplus Q_{25} \oplus Q_1) \\
H_2 &= (SHR^5(XH) \oplus SHL^5(Q_{18}) \oplus M_2) + (XL \oplus Q_{26} \oplus Q_2) \\
H_3 &= (SHR^1(XH) \oplus SHL^5(Q_{19}) \oplus M_3) + (XL \oplus Q_{27} \oplus Q_3) \\
H_4 &= (SHR^3(XH) \oplus Q_{20} \oplus M_4) + (XL \oplus Q_{28} \oplus Q_4) \\
H_5 &= (SHL^6(XH) \oplus SHR^6(Q_{21}) \oplus M_5) + (XL \oplus Q_{29} \oplus Q_5) \\
H_6 &= (SHR^4(XH) \oplus SHL^6(Q_{22}) \oplus M_6) + (XL \oplus Q_{30} \oplus Q_6) \\
H_7 &= (SHR^{11}(XH) \oplus SHL^2(Q_{23}) \oplus M_7) + (XL \oplus Q_{31} \oplus Q_7) \\
H_8 &= ROTL^9(H_4) + (XH \oplus Q_{24} \oplus M_8) + (SHL^8(XL) \oplus Q_{23} \oplus Q_8) \\
H_9 &= ROTL^{10}(H_5) + (XH \oplus Q_{25} \oplus M_9) + (SHR^6(XL) \oplus Q_{16} \oplus Q_9) \\
H_{10} &= ROTL^{11}(H_6) + (XH \oplus Q_{26} \oplus M_{10}) + (SHL^6(XL) \oplus Q_{17} \oplus Q_{10}) \\
H_{11} &= ROTL^{12}(H_7) + (XH \oplus Q_{27} \oplus M_{11}) + (SHL^4(XL) \oplus Q_{18} \oplus Q_{11}) \\
H_{12} &= ROTL^{13}(H_0) + (XH \oplus Q_{28} \oplus M_{12}) + (SHR^3(XL) \oplus Q_{19} \oplus Q_{12}) \\
H_{13} &= ROTL^{14}(H_1) + (XH \oplus Q_{29} \oplus M_{13}) + (SHR^4(XL) \oplus Q_{20} \oplus Q_{13}) \\
H_{14} &= ROTL^{15}(H_2) + (XH \oplus Q_{30} \oplus M_{14}) + (SHR^7(XL) \oplus Q_{21} \oplus Q_{14}) \\
H_{15} &= ROTL^{16}(H_3) + (XH \oplus Q_{31} \oplus M_{15}) + (SHR^2(XL) \oplus Q_{22} \oplus Q_{15})
\end{aligned}$$

Hash jako H8,..., H15:

$$\begin{aligned}
H_8 &= ROTL^9((SHR^3(XH) \oplus Q_{20} \oplus M_4) + (XL \oplus Q_{28} \oplus Q_4)) + (XH \oplus Q_{24} \oplus M_8) + (SHL^8(XL) \oplus Q_{23} \oplus Q_8) \\
H_9 &= ROTL^{10}((SHL^6(XH) \oplus SHR^6(Q_{21}) \oplus M_5) + (XL \oplus Q_{29} \oplus Q_5)) + (XH \oplus Q_{25} \oplus M_9) + (SHR^6(XL) \oplus Q_{16} \oplus Q_9) \\
H_{10} &= ROTL^{11}((SHR^4(XH) \oplus SHL^6(Q_{22}) \oplus M_6) + (XL \oplus Q_{30} \oplus Q_6)) + (XH \oplus Q_{26} \oplus M_{10}) + (SHL^6(XL) \oplus Q_{17} \oplus Q_{10}) \\
H_{11} &= ROTL^{12}((SHR^{11}(XH) \oplus SHL^2(Q_{23}) \oplus M_7) + (XL \oplus Q_{31} \oplus Q_7)) + (XH \oplus Q_{27} \oplus M_{11}) + (SHL^4(XL) \oplus Q_{18} \oplus Q_{11}) \\
H_{12} &= ROTL^{13}((SHL^5(XH) \oplus SHR^5(Q_{16}) \oplus M_0) + (XL \oplus Q_{24} \oplus Q_0)) + (XH \oplus Q_{28} \oplus M_{12}) + (SHR^3(XL) \oplus Q_{19} \oplus Q_{12}) \\
H_{13} &= ROTL^{14}((SHR^7(XH) \oplus SHL^8(Q_{17}) \oplus M_1) + (XL \oplus Q_{25} \oplus Q_1)) + (XH \oplus Q_{29} \oplus M_{13}) + (SHR^4(XL) \oplus Q_{20} \oplus Q_{13}) \\
H_{14} &= ROTL^{15}((SHR^5(XH) \oplus SHL^5(Q_{18}) \oplus M_2) + (XL \oplus Q_{26} \oplus Q_2)) + (XH \oplus Q_{30} \oplus M_{14}) + (SHR^7(XL) \oplus Q_{21} \oplus Q_{14}) \\
H_{15} &= ROTL^{16}((SHR^1(XH) \oplus SHL^5(Q_{19}) \oplus M_3) + (XL \oplus Q_{27} \oplus Q_3)) + (XH \oplus Q_{31} \oplus M_{15}) + (SHR^2(XL) \oplus Q_{22} \oplus Q_{15})
\end{aligned}$$

f

$$
\begin{array}{lllllllllllllll}
Q_0 = & H_1 & + & s_0 & (& (M_5 \oplus H_5) & - & (M_7 \oplus H_7) & + & (M_{10} \oplus H_{10}) & + & (M_{13} \oplus H_{13}) & + & (M_{14} \oplus H_{14}) &) \\
Q_1 = & H_2 & + & s_1 & (& (M_6 \oplus H_6) & - & (M_8 \oplus H_8) & + & (M_{11} \oplus H_{11}) & + & (M_{14} \oplus H_{14}) & - & (M_{15} \oplus H_{15}) &) \\
Q_2 = & H_3 & + & s_2 & (& (M_0 \oplus H_0) & + & (M_7 \oplus H_7) & + & (M_9 \oplus H_9) & - & (M_{12} \oplus H_{12}) & + & (M_{15} \oplus H_{15}) &) \\
Q_3 = & H_4 & + & s_3 & (& (M_0 \oplus H_0) & - & (M_1 \oplus H_1) & + & (M_8 \oplus H_8) & - & (M_{10} \oplus H_{10}) & + & (M_{13} \oplus H_{13}) &) \\
Q_4 = & H_5 & + & s_4 & (& (M_1 \oplus H_1) & + & (M_2 \oplus H_2) & + & (M_9 \oplus H_9) & - & (M_{11} \oplus H_{11}) & - & (M_{14} \oplus H_{14}) &) \\
Q_5 = & H_6 & + & s_0 & (& (M_3 \oplus H_3) & - & (M_2 \oplus H_2) & + & (M_{10} \oplus H_{10}) & - & (M_{12} \oplus H_{12}) & + & (M_{15} \oplus H_{15}) &) \\
Q_6 = & H_7 & + & s_1 & (& (M_4 \oplus H_4) & - & (M_0 \oplus H_0) & - & (M_3 \oplus H_3) & - & (M_{11} \oplus H_{11}) & + & (M_{13} \oplus H_{13}) &) \\
Q_7 = & H_8 & + & s_2 & (& (M_1 \oplus H_1) & - & (M_4 \oplus H_4) & - & (M_5 \oplus H_5) & - & (M_{12} \oplus H_{12}) & - & (M_{14} \oplus H_{14}) &) \\
Q_8 = & H_9 & + & s_3 & (& (M_2 \oplus H_2) & - & (M_5 \oplus H_5) & - & (M_6 \oplus H_6) & + & (M_{13} \oplus H_{13}) & - & (M_{15} \oplus H_{15}) &) \\
Q_9 = & H_{10} & + & s_4 & (& (M_0 \oplus H_0) & - & (M_3 \oplus H_3) & + & (M_6 \oplus H_6) & - & (M_7 \oplus H_7) & + & (M_{14} \oplus H_{14}) &) \\
Q_{10} = & H_{11} & + & s_0 & (& (M_8 \oplus H_8) & - & (M_1 \oplus H_1) & - & (M_4 \oplus H_4) & - & (M_7 \oplus H_7) & + & (M_{15} \oplus H_{15}) &) \\
Q_{11} = & H_{12} & + & s_1 & (& (M_8 \oplus H_8) & - & (M_0 \oplus H_0) & - & (M_2 \oplus H_2) & - & (M_5 \oplus H_5) & + & (M_9 \oplus H_9) &) \\
Q_{12} = & H_{13} & + & s_2 & (& (M_1 \oplus H_1) & + & (M_3 \oplus H_3) & - & (M_6 \oplus H_6) & - & (M_9 \oplus H_9) & + & (M_{10} \oplus H_{10}) &) \\
Q_{13} = & H_{14} & + & s_3 & (& (M_2 \oplus H_2) & + & (M_4 \oplus H_4) & + & (M_7 \oplus H_7) & + & (M_{10} \oplus H_{10}) & + & (M_{11} \oplus H_{11}) &) \\
Q_{14} = & H_{15} & + & s_4 & (& (M_3 \oplus H_3) & - & (M_5 \oplus H_5) & + & (M_8 \oplus H_8) & - & (M_{11} \oplus H_{11}) & - & (M_{12} \oplus H_{12}) &) \\
Q_{15} = & H_0 & + & s_0 & (& (M_{12} \oplus H_{12}) & - & (M_4 \oplus H_4) & - & (M_6 \oplus H_6) & - & (M_9 \oplus H_9) & + & (M_{13} \oplus H_{13}) &)
\end{array}
$$

$$
\begin{aligned}
P_0 &= s1(Q_0) + s2(Q_1) + s3(Q_2) + s0(Q_3) + s1(Q_4) + s2(Q_5) + s3(Q_6) + s0(Q_7) + s1(Q_8) + s2(Q_9) + s3(Q_{10}) + s0(Q_{11}) + s1(Q_{12}) + s2(Q_{13}) + \\
&\quad + s3(Q_{14}) + s0(Q_{15}) \\
P_1 &= s1(Q_1) + s2(Q_2) + s3(Q_3) + s0(Q_4) + s1(Q_5) + s2(Q_6) + s3(Q_7) + s0(Q_8) + s1(Q_9) + s2(Q_{10}) + s3(Q_{11}) + s0(Q_{12}) + s1(Q_{13}) + \\
&\quad + s2(Q_{14}) + s3(Q_{15}) \\
P_2 &= Q_2 + r1(Q_3) + Q_4 + r2(Q_5) + Q_6 + r3(Q_7) + Q_8 + r4(Q_9) + Q_{10} + r5(Q_{11}) + Q_{12} + r6(Q_{13}) + Q_{14} + r7(Q_{15}) \\
P_3 &= Q_3 + r1(Q_4) + Q_5 + r2(Q_6) + Q_7 + r3(Q_8) + Q_9 + r4(Q_{10}) + Q_{11} + r5(Q_{12}) + Q_{13} + r6(Q_{14}) + Q_{15} \\
P_4 &= Q_4 + r1(Q_5) + Q_6 + r2(Q_7) + Q_8 + r3(Q_9) + Q_{10} + r4(Q_{11}) + Q_{12} + r5(Q_{13}) + Q_{14} + r6(Q_{15}) \\
P_5 &= Q_5 + r1(Q_6) + Q_7 + r2(Q_8) + Q_9 + r3(Q_{10}) + Q_{11} + r4(Q_{12}) + Q_{13} + r5(Q_{14}) + Q_{15} \\
P_6 &= Q_6 + r1(Q_7) + Q_8 + r2(Q_9) + Q_{10} + r3(Q_{11}) + Q_{12} + r4(Q_{13}) + Q_{14} + r5(Q_{15}) \\
P_7 &= Q_7 + r1(Q_8) + Q_9 + r2(Q_{10}) + Q_{11} + r3(Q_{12}) + Q_{13} + r4(Q_{14}) + Q_{15} \\
P_8 &= Q_8 + r1(Q_9) + Q_{10} + r2(Q_{11}) + Q_{12} + r3(Q_{13}) + Q_{14} + r4(Q_{15}) \\
P_9 &= Q_9 + r1(Q_{10}) + Q_{11} + r2(Q_{12}) + Q_{13} + r3(Q_{14}) + Q_{15} \\
P_{10} &= Q_{10} + r1(Q_{11}) + Q_{12} + r2(Q_{13}) + Q_{14} + r3(Q_{15}) \\
P_{11} &= Q_{11} + r1(Q_{12}) + Q_{13} + r2(Q_{14}) + Q_{15} \\
P_{12} &= Q_{12} + r1(Q_{13}) + Q_{14} + r2(Q_{15}) \\
P_{13} &= Q_{13} + r1(Q_{14}) + Q_{15} \\
P_{14} &= Q_{14} + r1(Q_{15}) \\
P_{15} &= Q_{15}
\end{aligned}
$$

$$
\begin{array}{lllllllll}
H_6 & \oplus (& ROTL^1(M_0) & + & ROTL^4(M_3) & - & ROTL^{11}(M_{10}) & + & K_0 \;)) \\
H_7 & \oplus (& ROTL^2(M_1) & + & ROTL^5(M_4) & - & ROTL^{12}(M_{11}) & + & K_1 \;)) \\
H_8 & \oplus (& ROTL^3(M_2) & + & ROTL^6(M_5) & - & ROTL^{13}(M_{12}) & + & K_2 \;)) \\
H_9 & \oplus (& ROTL^4(M_3) & + & ROTL^7(M_6) & - & ROTL^{14}(M_{13}) & + & K_3 \;)) \\
H_{10} & \oplus (& ROTL^5(M_4) & + & ROTL^8(M_7) & - & ROTL^{15}(M_{14}) & + & K_4 \;)) \\
H_{11} & \oplus (& ROTL^6(M_5) & + & ROTL^9(M_8) & - & ROTL^{16}(M_{15}) & + & K_5 \;)) \\
H_{12} & \oplus (& ROTL^7(M_6) & + & ROTL^{10}(M_9) & - & ROTL^1(M_0) & + & K_6 \;)) \\
H_{13} & \oplus (& ROTL^8(M_7) & + & ROTL^{11}(M_{10}) & - & ROTL^2(M_1) & + & K_7 \;)) \\
H_{14} & \oplus (& ROTL^9(M_8) & + & ROTL^{12}(M_{11}) & - & ROTL^3(M_2) & + & K_8 \;)) \\
H_{15} & \oplus (& ROTL^{10}(M_9) & + & ROTL^{13}(M_{12}) & - & ROTL^4(M_3) & + & K_9 \;)) \\
H_0 & \oplus (& ROTL^{11}(M_{10}) & + & ROTL^{14}(M_{13}) & - & ROTL^5(M_4) & + & K_{10} \;)) \\
H_1 & \oplus (& ROTL^{12}(M_{11}) & + & ROTL^{15}(M_{14}) & - & ROTL^6(M_5) & + & K_{11} \;)) \\
H_2 & \oplus (& ROTL^{13}(M_{12}) & + & ROTL^{16}(M_{15}) & - & ROTL^7(M_6) & + & K_{12} \;)) \\
H_3 & \oplus (& ROTL^{14}(M_{13}) & + & ROTL^1(M_0) & - & ROTL^8(M_7) & + & K_{13} \;)) \\
H_4 & \oplus (& ROTL^{15}(M_{14}) & + & ROTL^2(M_1) & - & ROTL^9(M_8) & + & K_{14} \;)) \\
H_5 & \oplus (& ROTL^{16}(M_{15}) & + & ROTL^3(M_2) & - & ROTL^{10}(M_9) & + & K_{15} \;))
\end{array}
$$

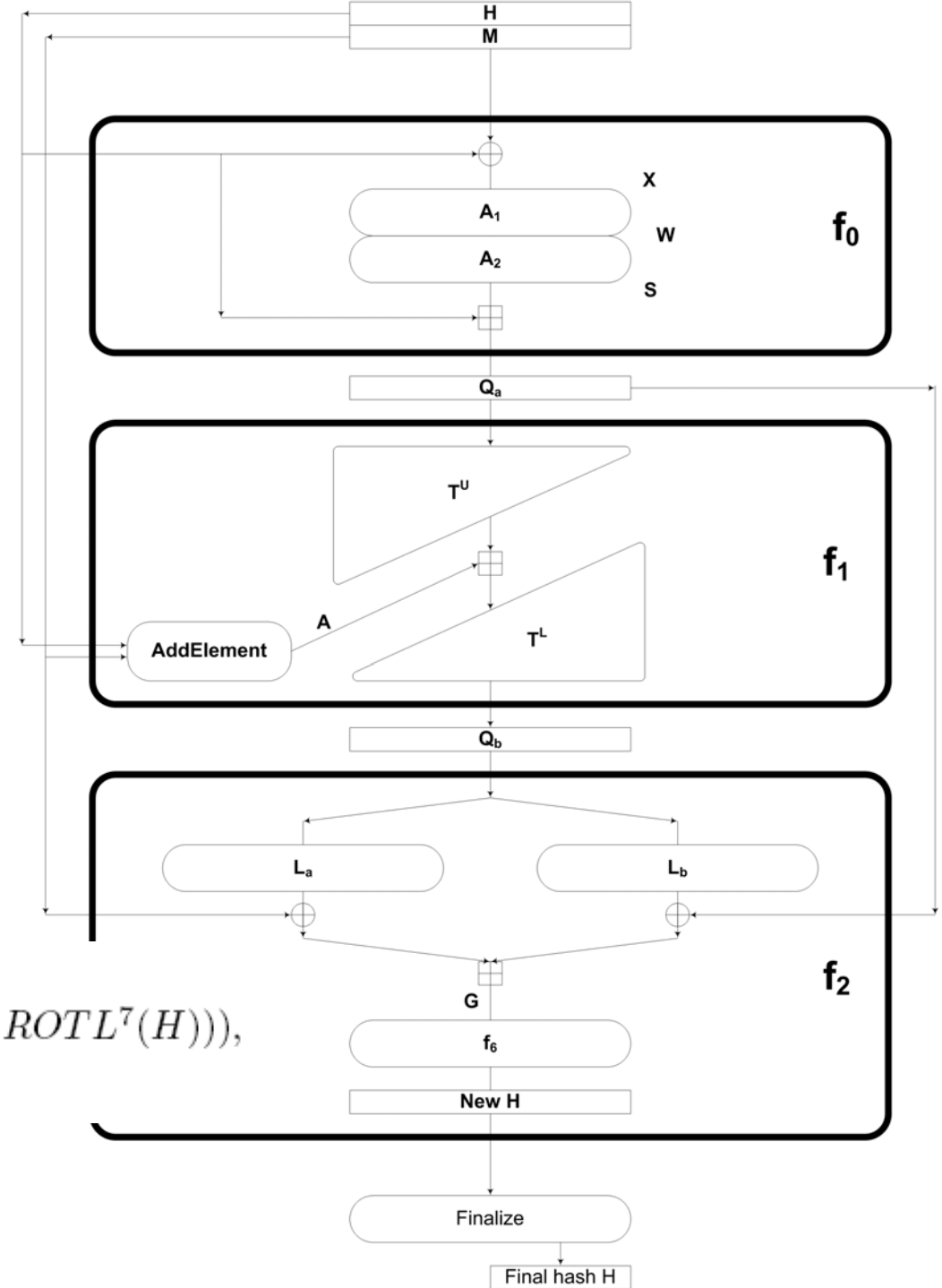
$$
\begin{aligned}
Q_{16} &= R_0 \\
Q_{17} &= R_1 + s0(Q_{16}) \\
Q_{18} &= R_2 + s4(Q_{16}) + s5(Q_{17}) \\
Q_{19} &= R_3 + r7(Q_{16}) + s4(Q_{17}) + s5(Q_{18}) \\
Q_{20} &= R_4 + Q_{16} + r7(Q_{17}) + s4(Q_{18}) + s5(Q_{19}) \\
Q_{21} &= R_5 + r6(Q_{16}) + Q_{17} + r7(Q_{18}) + s4(Q_{19}) + s5(Q_{20}) \\
Q_{22} &= R_6 + Q_{16} + r6(Q_{17}) + Q_{18} + r7(Q_{19}) + s4(Q_{20}) + s5(Q_{21}) \\
Q_{23} &= R_7 + r5(Q_{16}) + Q_{17} + r6(Q_{18}) + Q_{19} + r7(Q_{20}) + s4(Q_{21}) + s5(Q_{22}) \\
Q_{24} &= R_8 + Q_{16} + r5(Q_{17}) + Q_{18} + r6(Q_{19}) + Q_{20} + r7(Q_{21}) + s4(Q_{22}) + s5(Q_{23}) \\
Q_{25} &= R_9 + r4(Q_{16}) + Q_{17} + r5(Q_{18}) + Q_{19} + r6(Q_{20}) + Q_{21} + r7(Q_{22}) + s4(Q_{23}) + s5(Q_{24}) \\
Q_{26} &= R_{10} + Q_{16} + r4(Q_{17}) + Q_{18} + r5(Q_{19}) + Q_{20} + r6(Q_{21}) + Q_{22} + r7(Q_{23}) + s4(Q_{24}) + s5(Q_{25}) \\
Q_{27} &= R_{11} + r3(Q_{16}) + Q_{17} + r4(Q_{18}) + Q_{19} + r5(Q_{20}) + Q_{21} + r6(Q_{22}) + Q_{23} + r7(Q_{24}) + s4(Q_{25}) + s5(Q_{26}) \\
Q_{28} &= R_{12} + Q_{16} + r3(Q_{17}) + Q_{18} + r4(Q_{19}) + Q_{20} + r5(Q_{21}) + Q_{22} + r6(Q_{23}) + Q_{24} + r7(Q_{25}) + s4(Q_{26}) + s5(Q_{27}) \\
Q_{29} &= R_{13} + r2(Q_{16}) + Q_{17} + r3(Q_{18}) + Q_{19} + r4(Q_{20}) + Q_{21} + r5(Q_{22}) + Q_{23} + r6(Q_{24}) + Q_{25} + r7(Q_{26}) + s4(Q_{27}) + s5(Q_{28}) \\
Q_{30} &= R_{14} + Q_{16} + r2(Q_{17}) + Q_{18} + r3(Q_{19}) + Q_{20} + r4(Q_{21}) + Q_{22} + r5(Q_{23}) + Q_{24} + r6(Q_{25}) + Q_{26} + r7(Q_{27}) + s4(Q_{28}) + s5(Q_{29}) \\
Q_{31} &= R_{15} + r1(Q_{16}) + Q_{17} + r2(Q_{18}) + Q_{19} + r3(Q_{20}) + Q_{21} + r4(Q_{22}) + Q_{23} + r5(Q_{24}) + Q_{25} + r6(Q_{26}) + Q_{27} + r7(Q_{28}) + s4(Q_{29}) + s5(Q_{30})
\end{aligned}
$$

$$
\begin{array}{lllllll}
H_0 = & & (SHL^5(XH) \oplus SHR^5(Q_{18}) \oplus M_0) & + & (XL \oplus Q_{24} \oplus Q_0) \\
H_1 = & & (SHR^7(XH) \oplus SHL^8(Q_{17}) \oplus M_1) & + & (XL \oplus Q_{25} \oplus Q_1) \\
H_2 = & & (SHR^5(XH) \oplus SHL^5(Q_{18}) \oplus M_2) & + & (XL \oplus Q_{26} \oplus Q_2) \\
H_3 = & & (SHR^1(XH) \oplus SHL^5(Q_{19}) \oplus M_3) & + & (XL \oplus Q_{27} \oplus Q_3) \\
H_4 = & & (SHR^3(XH) \oplus Q_{20} \oplus M_4) & + & (XL \oplus Q_{28} \oplus Q_4) \\
H_5 = & & (SHL^6(XH) \oplus SHR^6(Q_{21}) \oplus M_5) & + & (XL \oplus Q_{29} \oplus Q_5) \\
H_6 = & & (SHR^4(XH) \oplus SHL^6(Q_{22}) \oplus M_6) & + & (XL \oplus Q_{30} \oplus Q_6) \\
H_7 = & & (SHR^{11}(XH) \oplus SHL^2(Q_{23}) \oplus M_7) & + & (XL \oplus Q_{31} \oplus Q_7) \\
H_8 = & ROTL^9(H_4) & + (XH \oplus Q_{24} \oplus M_8) & + & (SHL^8(XL) \oplus Q_{23} \oplus Q_8) \\
H_9 = & ROTL^{10}(H_5) & + (XH \oplus Q_{25} \oplus M_9) & + & (SHR^8(XL) \oplus Q_{16} \oplus Q_9) \\
H_{10} = & ROTL^{11}(H_6) & + (XH \oplus Q_{26} \oplus M_{10}) & + & (SHL^8(XL) \oplus Q_{17} \oplus Q_{10}) \\
H_{11} = & ROTL^{12}(H_7) & + (XH \oplus Q_{27} \oplus M_{11}) & + & (SHL^4(XL) \oplus Q_{18} \oplus Q_{11}) \\
H_{12} = & ROTL^{13}(H_0) & + (XH \oplus Q_{28} \oplus M_{12}) & + & (SHR^3(XL) \oplus Q_{19} \oplus Q_{12}) \\
H_{13} = & ROTL^{14}(H_1) & + (XH \oplus Q_{29} \oplus M_{13}) & + & (SHR^4(XL) \oplus Q_{20} \oplus Q_{13}) \\
H_{14} = & ROTL^{15}(H_2) & + (XH \oplus Q_{30} \oplus M_{14}) & + & (SHR^7(XL) \oplus Q_{21} \oplus Q_{14}) \\
H_{15} = & ROTL^{16}(H_3) & + (XH \oplus Q_{31} \oplus M_{15}) & + & (SHR^2(XL) \oplus Q_{22} \oplus Q_{15})
\end{array}
$$

Dekompozice celé funkce f

- Jednoduchý popis snad usnadní analýzu a útoky ☺
- BMW ~ Bijections Mounted Widely

$$
\begin{aligned}
Q_a &= A_2 A_1 (M \oplus H) + ROTL^1(H), \\
Q_b &= T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H))), \\
G &= (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)).
\end{aligned}
$$



Analýza

- ssss

Literatura

- on-line na http://cryptography.hyperlink.cz/
- [BMW] Danilo Gligoroski, Vlastimil Klima, Svein J. Knapskog, Mohamed El-Hadedy, Jorn Amundsen, Stig F. Mjolsnes: Cryptographic Hash Function Blue Midnight Wish, 2nd version, Sept. 15, 2009, homepage, the whole submission package, description, presentation at the First SHA-3 Candidate Conference, Feb. 25-28, 2009
- [GK2009] Danilo Gligoroski, Vlastimil Klima: On the Computational Asymmetry of the S-boxes Present in Blue Midnight Wish Cryptographic Hash Function, Information on ICT Innovations 2009, Sept. 28 - 30, 2009, Ohrid, R. Macedonia