Hashovací funkce a SHA–3

Martin Heller

Katedra matematiky, FJFI ČVUT v Praze

18. dubna 2011

Konstrukce hashovacích funkcí

- chceme zpracovávat vstupy libovolné délky a dostat výstup délky pevně dané (např. 256 bitů)
- vstup budeme zpracovávat po blocích, z nich zkonstruujeme výsledný hash

Konstrukce hashovacích funkcí

- chceme zpracovávat vstupy libovolné délky a dostat výstup délky pevně dané (např. 256 bitů)
- vstup budeme zpracovávat po blocích, z nich zkonstruujeme výsledný hash

Jednosměrná kompresní funkce

- kompresní funkce – $f : \mathrm{M} \times \mathrm{K} \to \mathrm{O}$
- požadavky:
  - snadný výpočet
  - obtížná inverze (preimage)
  - obtížné nalezení jiné zprávy se stejným výsledkem (second preimage)
  - obtížné nalezení kolizí
- může vyhovovat dobrá bloková šifra

Jednosměrná kompresní funkce

- kompresní funkce – $f : \mathrm{M} \times \mathrm{K} \to \mathrm{O}$
- požadavky:
  - snadný výpočet
  - obtížná inverze (preimage)
  - obtížné nalezení jiné zprávy se stejným výsledkem (second preimage)
  - obtížné nalezení kolizí
- může vyhovovat dobrá bloková šifra

Jednosměrná kompresní funkce

- kompresní funkce – $f : \mathrm{M} \times \mathrm{K} \to \mathrm{O}$
- požadavky:
  - snadný výpočet
  - obtížná inverze (preimage)
  - obtížné nalezení jiné zprávy se stejným výsledkem (second preimage)
  - obtížné nalezení kolizí
- může vyhovovat dobrá bloková šifra

Jednosměrná kompresní funkce

- kompresní funkce – $f : \mathrm{M} \times \mathrm{K} \to \mathrm{O}$
- požadavky:
  - snadný výpočet
  - obtížná inverze (preimage)
  - obtížné nalezení jiné zprávy se stejným výsledkem (second preimage)
  - obtížné nalezení kolizí
- může vyhovovat dobrá bloková šifra

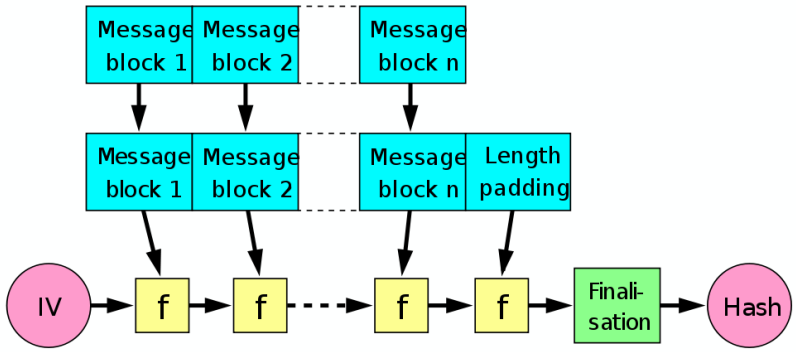
Jednosměrná kompresní funkce

- kompresní funkce – $f : \mathrm{M} \times \mathrm{K} \to \mathrm{O}$
- požadavky:
  - snadný výpočet
  - obtížná inverze (preimage)
  - obtížné nalezení jiné zprávy se stejným výsledkem (second preimage)
  - obtížné nalezení kolizí
- může vyhovovat dobrá bloková šifra

Jednosměrná kompresní funkce

- kompresní funkce – $f : \mathrm{M} \times \mathrm{K} \to \mathrm{O}$
- požadavky:
  - snadný výpočet
  - obtížná inverze (preimage)
  - obtížné nalezení jiné zprávy se stejným výsledkem (second preimage)
  - obtížné nalezení kolizí
- může vyhovovat dobrá bloková šifra

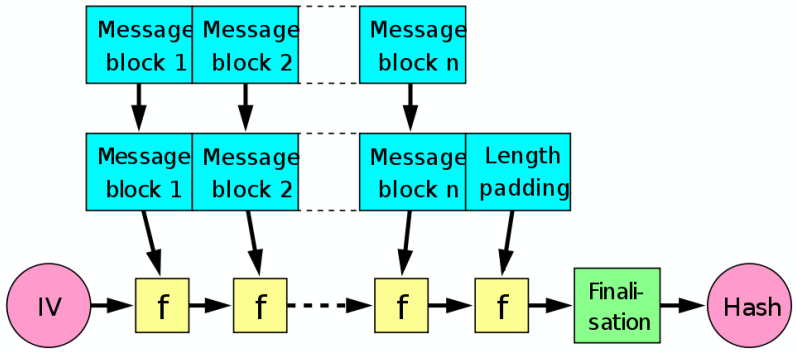
Merkle-Damgårdova konstrukce



Slabiny

- známe-li H(X), snadno získáme H(pad(X) Y)
- length extension
- multicollision

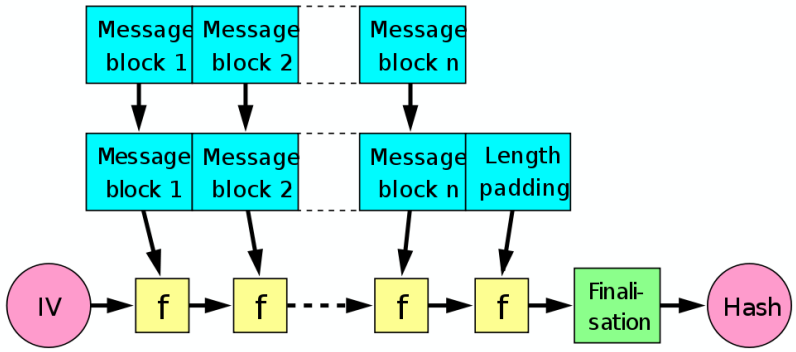
Merkle-Damgårdova konstrukce



Slabiny

- známe-li H(X), snadno získáme H(pad(X) Y)
- length extension
- multicollision

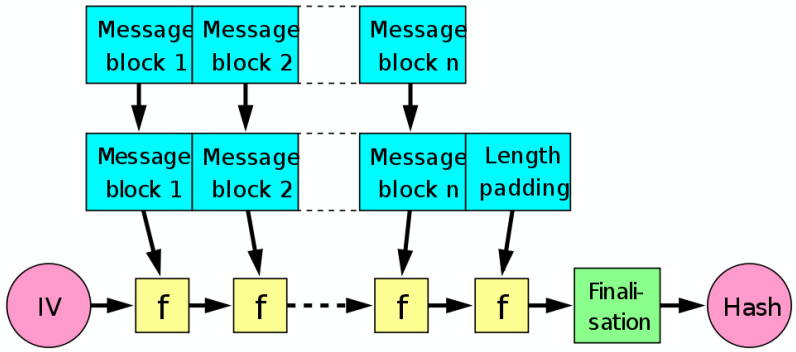
Merkle-Damgårdova konstrukce



Slabiny

- známe-li H(X), snadno získáme H(pad(X) Y)
- length extension
- multicollision

Merkle-Damgårdova konstrukce



Slabiny

- známe-li H(X), snadno získáme H(pad(X) Y)
- length extension
- multicollision

Útoky proti hashovacím funkcím

- preimage
- second preimage
- collision – birthday attack
- distinguishing attack

Útoky proti hashovacím funkcím

- preimage
- second preimage
- collision – birthday attack
- distinguishing attack

Útoky proti hashovacím funkcím

- preimage
- second preimage
- collision – birthday attack
- distinguishing attack

Útoky proti hashovacím funkcím

- preimage
- second preimage
- collision – birthday attack
- distinguishing attack

SHA–3

- soutěž vyhlášena NIST v r. 2007
- náhrada SHA–1 a SHA–2
- požadavky:
  - bezpečnost
  - rychlost, prostorová nenáročnost
  - odlišnost od SHA–2

SHA–3

- soutěž vyhlášena NIST v r. 2007
- náhrada SHA–1 a SHA–2
- požadavky:
  - bezpečnost
  - rychlost, prostorová nenáročnost
  - odlišnost od SHA–2

SHA–3

- soutěž vyhlášena NIST v r. 2007
- náhrada SHA–1 a SHA–2
- požadavky:
  - bezpečnost
  - rychlost, prostorová nenáročnost
  - odlišnost od SHA–2

SHA–3

- soutěž vyhlášena NIST v r. 2007
- náhrada SHA–1 a SHA–2
- požadavky:
  - bezpečnost
  - rychlost, prostorová nenáročnost
  - odlišnost od SHA–2

SHA–3

- soutěž vyhlášena NIST v r. 2007
- náhrada SHA–1 a SHA–2
- požadavky:
  - bezpečnost
  - rychlost, prostorová nenáročnost
  - odlišnost od SHA–2

Výběr finalistů

- 3 kola, mezi nimi veřejná diskuse
- 14 kandidátů do 2. kola

	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

- 5 kandidátů do 3. kola (finále)
  BLAKE, Grostl, JH, Keccak,Skein

Výběr finalistů

- 3 kola, mezi nimi veřejná diskuse
- 14 kandidátů do 2. kola

	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

- 5 kandidátů do 3. kola (finále)
  BLAKE, Grostl, JH, Keccak,Skein

Výběr finalistů

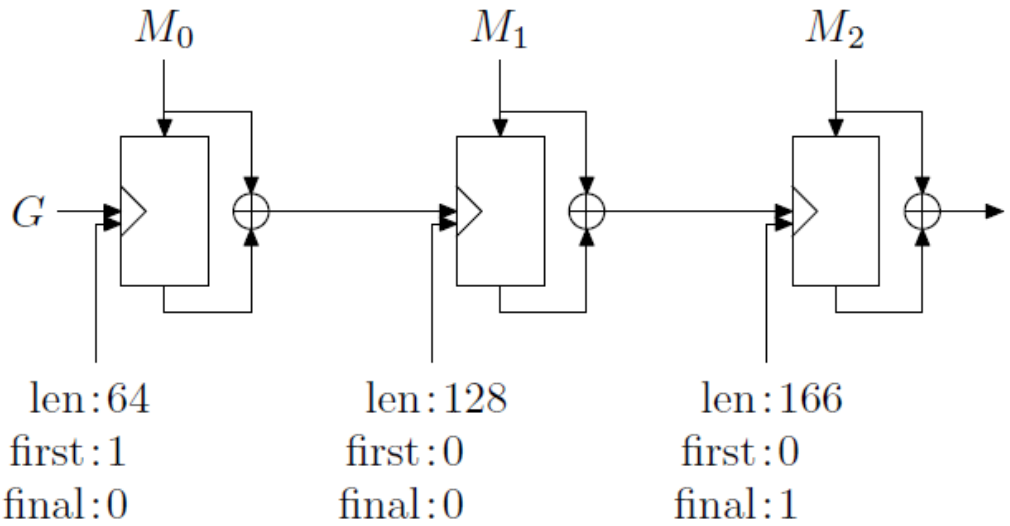
- 3 kola, mezi nimi veřejná diskuse
- 14 kandidátů do 2. kola

	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

- 5 kandidátů do 3. kola (finále)
  BLAKE, Grostl, JH, Keccak,Skein

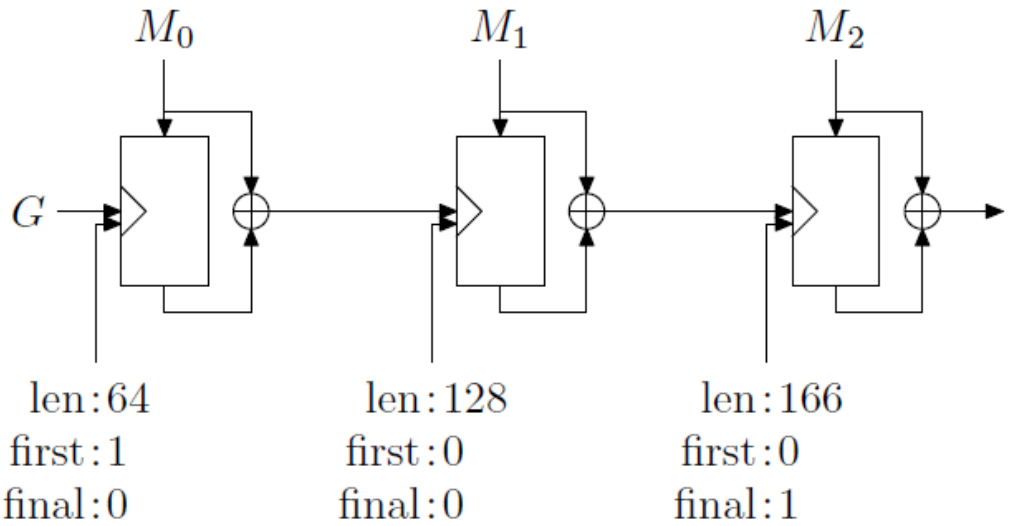
Skein

- spoluautorem Bruce Schneier
- zřejmě favorit soutěže
- založen na šifře Threefish, nepoužívá S-boxy
- narrow-pipe, Unique Block Iteration



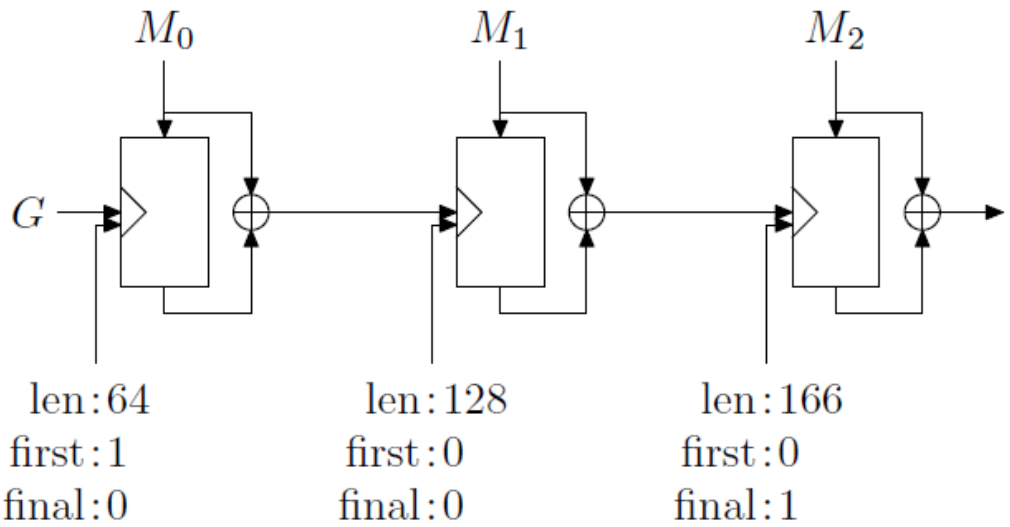
Skein

- spoluautorem Bruce Schneier
- zřejmě favorit soutěže
- založen na šifře Threefish, nepoužívá S-boxy
- narrow-pipe, Unique Block Iteration



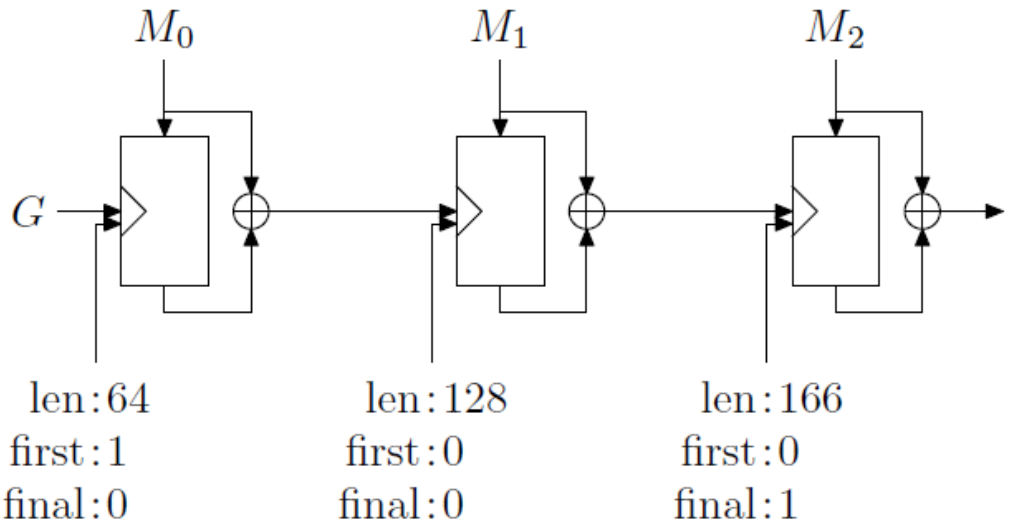
Skein

- spoluautorem Bruce Schneier
- zřejmě favorit soutěže
- založen na šifře Threefish, nepoužívá S-boxy
- narrow-pipe, Unique Block Iteration



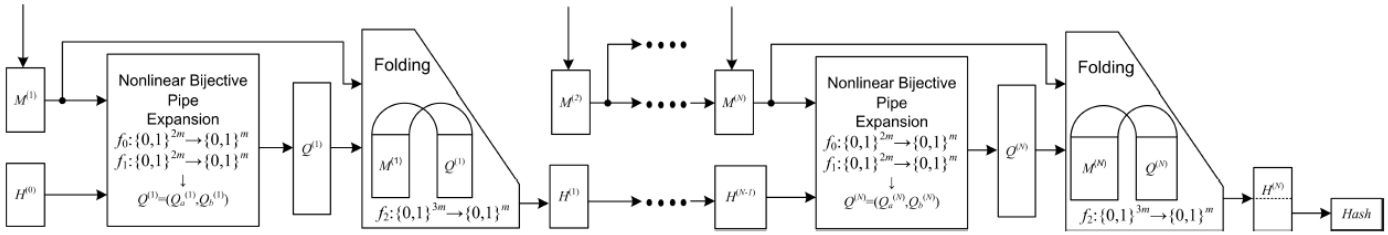
Skein

- spoluautorem Bruce Schneier
- zřejmě favorit soutěže
- založen na šifře Threefish, nepoužívá S-boxy
- narrow-pipe, Unique Block Iteration



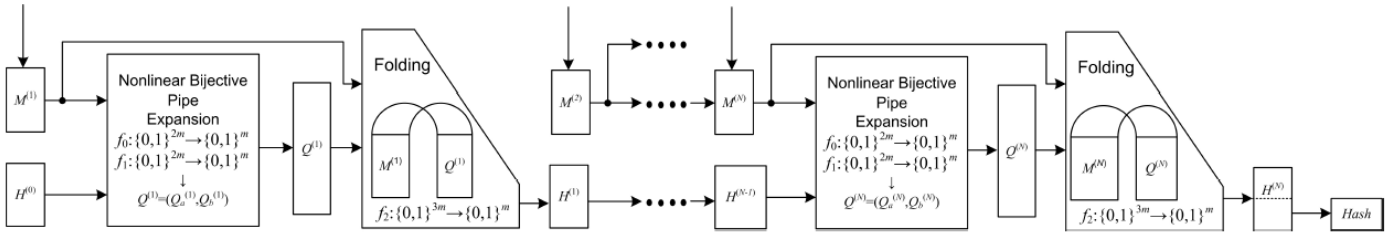
Blue Midnight Wish

- spoluautorem český kryptolog Vlastimil Klíma
- nejrychlejší z kandidátů 2. kola
- nepostoupil do finále
- wide-pipe



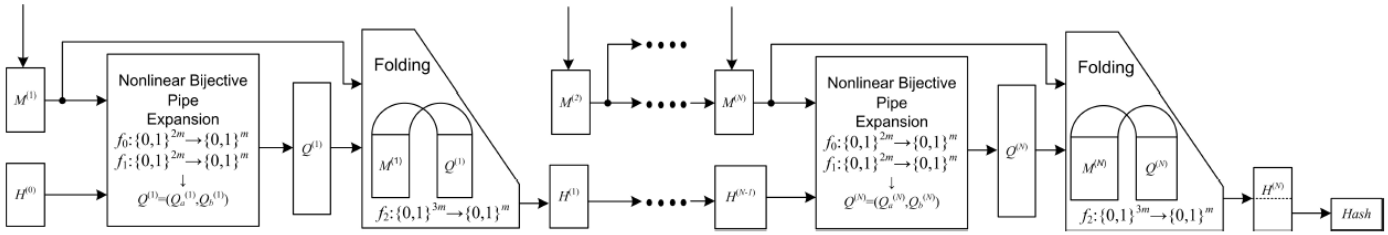
Blue Midnight Wish

- spoluautorem český kryptolog Vlastimil Klíma
- nejrychlejší z kandidátů 2. kola
- nepostoupil do finále
- wide-pipe



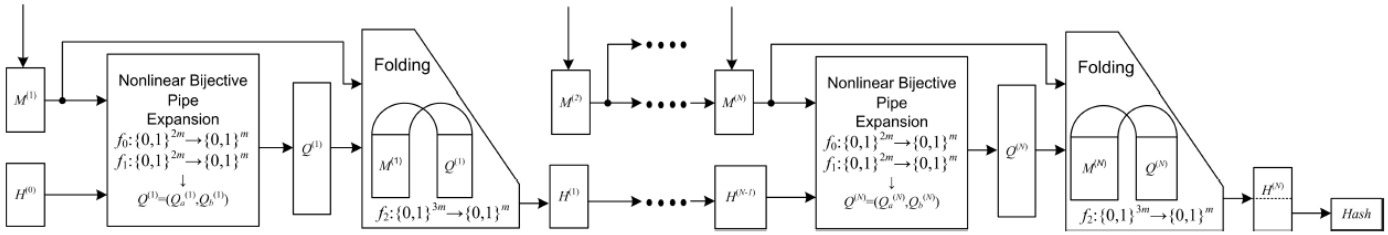
Blue Midnight Wish

- spoluautorem český kryptolog Vlastimil Klíma
- nejrychlejší z kandidátů 2. kola
- nepostoupil do finále
- wide-pipe



Blue Midnight Wish

- spoluautorem český kryptolog Vlastimil Klíma
- nejrychlejší z kandidátů 2. kola
- nepostoupil do finále
- wide-pipe



Literatura


M. S. Turan a kol., *Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition*, NIST Interagency Report 7764, 2011.


N. Ferguson a kol., *The Skein Hash Function Family*, Version 1.3, 2010.


D. Gligoroski, V. Klíma a kol., *Blue Midnight Wish*, Norwegian University of Science and Technology, Trondheim, Norway, 2008.


Wikipedia `http://en.wikipedia.org`