# Criptografie și Securitate

## - Prelegerea 15.3 -
## SHA - 3

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

# Cuprins

# Competiția SHA-3

- Atacurile asupra MD5, SHA-0, SHA-1 au impus necesitatea unei noi funcții hash;

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

## Announcing the first SHA1 collision

February 23, 2017

Posted by Marc Stevens (CWI Amsterdam), Elie Bursztein (Google), Pierre Karpman (CWI Amsterdam), Ange Albertini (Google), Yarik Markov (Google), Alex Petit Bianco (Google), Clement Baisse (Google)

Cryptographic hash functions like SHA-1 are a cryptographer's swiss army knife. You'll find that hashes play a role in browser security, managing code repositories, or even just detecting duplicate files in storage. Hash functions compress large amounts of data into a small message digest. As a cryptographic requirement for wide-spread use, finding two messages that lead to the same digest should be computationally infeasible. Over time however, this requirement can fail due to attacks on the mathematical underpinnings of hash functions or to increases in computational power.

[https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html]

# Competiția SHA-3

- 2 noiembrie 2007 - NIST anunță competiția publică SHA-3;

# Competiția SHA-3

- 2 noiembrie 2007 - NIST anunță competiția publică SHA-3;
- 31 octombrie 2008 - se primesc 64 de propuneri din toată lumea;

# Competiția SHA-3

- 2 noiembrie 2007 - NIST anunță competiția publică SHA-3;
- 31 octombrie 2008 - se primesc 64 de propuneri din toată lumea;
- decembrie 2008 - rămân 51 de candidați pentru prima rundă (restul sunt eliminați din cauza dosarelor incomplete);

# Competiția SHA-3

- februarie 2009 - are loc prima conferinta la care sunt prezentate 37 de propuneri (dintr-un total de 41, 10 fiind retrase între timp din cauza unor atacuri);

# Competiția SHA-3

- februarie 2009 - are loc prima conferinta la care sunt prezentate 37 de propuneri (dintr-un total de 41, 10 fiind retrase între timp din cauza unor atacuri);
- iulie 2009 - rămân 14 candidați în runda a 2-a;

# Competiția SHA-3

- februarie 2009 - are loc prima conferinta la care sunt prezentate 37 de propuneri (dintr-un total de 41, 10 fiind retrase între timp din cauza unor atacuri);
- iulie 2009 - rămân 14 candidați în runda a 2-a;
- decembrie 2010 - cei 5 candidați în runda finală: BLAKE, Gr$\phi$stl, JH, Keccak and Skein;

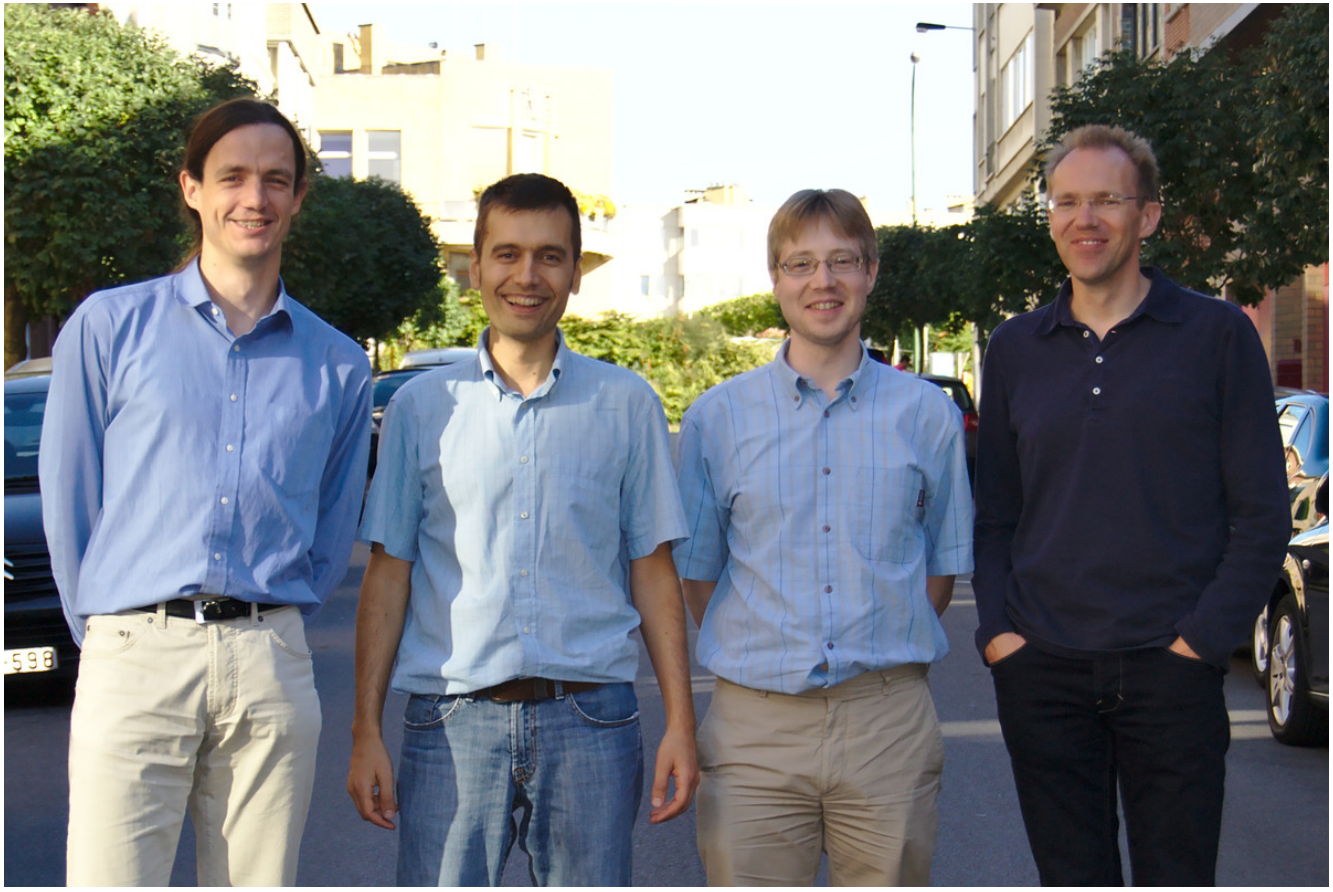
# Competiția SHA-3

- februarie 2009 - are loc prima conferinta la care sunt prezentate 37 de propuneri (dintr-un total de 41, 10 fiind retrase între timp din cauza unor atacuri);
- iulie 2009 - rămân 14 candidați în runda a 2-a;
- decembrie 2010 - cei 5 candidați în runda finală: BLAKE, Grøstl, JH, Keccak and Skein;
- 2 octombrie 2012 - NIST anunță câștigătorul: Keccak.

# Cei 5 finaliști

| | |
|---|---|
| BLAKE | Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Raphael C.-W. Phan |
| Grøstl | Lars Ramkilde Knudsen, Praveen Gauravaram, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläffer, Søren S. Thomsen |
| JH | Hongjun Wu |
| Keccak | Joan Daemen, Guido Bertoni, Michaël Peeters, Gilles Van Assche |
| Skein | Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jesse Walker, Jon Callas |

# Echipa Keccak



[http://keccak.noekeon.org/team.html]

# Criterii de selecție

- Lungimea secvenței de ieșire: $n = 224$, 256, 384 și 512 biți;

# Criterii de selecție

- Lungimea secvenței de ieșire: $n = 224$, 256, 384 și 512 biți;
- Alte dimensiuni ale secvenței de ieșire sunt opționale;

# Criterii de selecție

- Lungimea secvenței de ieșire: $n = 224$, 256, 384 și 512 biți;
- Alte dimensiuni ale secvenței de ieșire sunt opționale;
- Eficientă crescută față de SHA-2;

# Criterii de selecție

- Lungimea secvenței de ieșire: $n = 224, 256, 384$ și 512 biți;
- Alte dimensiuni ale secvenței de ieșire sunt opționale;
- Eficientă crescută față de SHA-2;
- Utilizare în HMAC;

# Criterii de selecție

- Lungimea secvenței de ieșire: $n = 224$, 256, 384 și 512 biți;
- Alte dimensiuni ale secvenței de ieșire sunt opționale;
- Eficientă crescută față de SHA-2;
- Utilizare în HMAC;
- Rezistența la coliziuni, prima și a doua preimagine (conform cu atacurile generice, tradiționale);

# Criterii de selecție

- Lungimea secvenței de ieșire: $n = 224, 256, 384$ și 512 biți;
- Alte dimensiuni ale secvenței de ieșire sunt opționale;
- Eficientă crescută față de SHA-2;
- Utilizare în HMAC;
- Rezistența la coliziuni, prima și a doua preimagine (conform cu atacurile generice, tradiționale);
- Demonstrație de securitate;

# Criterii de selecție

- Lungimea secvenței de ieșire: $n = 224, 256, 384$ și 512 biți;
- Alte dimensiuni ale secvenței de ieșire sunt opționale;
- Eficientă crescută față de SHA-2;
- Utilizare în HMAC;
- Rezistența la coliziuni, prima și a doua preimagine (conform cu atacurile generice, tradiționale);
- Demonstrație de securitate;
- Parametrizabilă, număr de runde variabil;

# Criterii de selecție

- Lungimea secvenței de ieșire: $n = 224, 256, 384$ și 512 biți;
- Alte dimensiuni ale secvenței de ieșire sunt opționale;
- Eficientă crescută față de SHA-2;
- Utilizare în HMAC;
- Rezistența la coliziuni, prima și a doua preimagine (conform cu atacurile generice, tradiționale);
- Demonstrație de securitate;
- Parametrizabilă, număr de runde variabil;
- Simplicitate, claritate.

# Motivație

*"The NIST team praised the Keccak algorithm for its many admirable qualities, including its elegant design and its ability to run well on many different computing devices. The clarity of Keccak's construction lends itself to easy analysis (during the competition all submitted algorithms were made available for public examination and criticism), and Keccak has higher performance in hardware implementations than SHA-2 or any of the other finalists."*

(NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition - `http://www.nist.gov/itl/csd/sha-100212.cfm`)

*"One benefit that KECCAK offers as the SHA-3 winner is its difference in design and implementation properties from that of SHA-2. It seems very unlikely that a single new cryptanalytic attack or approach could threaten both algorithms."*

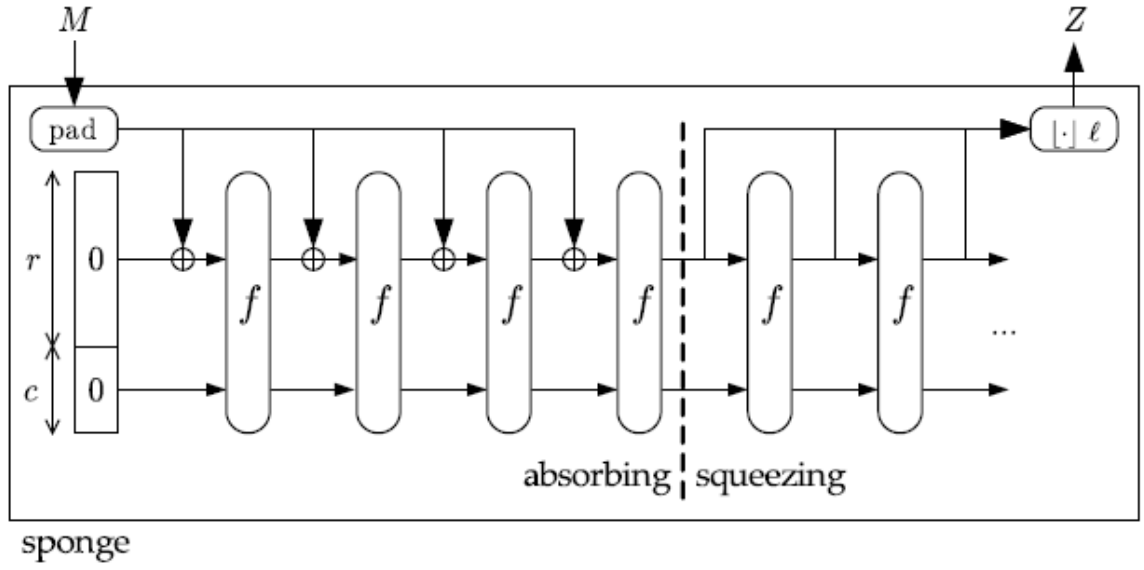
(SHA-3 Selection Announcement - `http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_selection_announcement.pdf`)

# Keccak

- A fost gândit să difere de construcțiile existente (AES, SHA-2);

# Keccak

- A fost gândit să difere de construcțiile existente (AES, SHA-2);
- Folosește sponge functions:




[Cryptographic Sponge Functions - `http://sponge.noekeon.org/CSF-0.1.pdf`]

# Keccak

- Notații:
  - $r = bitrate$
  - $c = capacity$
  - $b = c + r = width$
  - $f =$ o permutare

# Keccak

- Notații:
  - $r = bitrate$
  - $c = capacity$
  - $b = c + r = width$
  - $f =$ o permutare
- Folosește o stare de $b$ biți inițializată la 0;

# Keccak

- Notații:
  - $r$ = *bitrate*
  - $c$ = *capacity*
  - $b = c + r$ = *width*
  - $f$ = o permutare
- Folosește o stare de $b$ biți inițializată la 0;
- Presupune 2 etape:
  1. Absorbing phase: mesajul de intrare se sparge în blocuri de lungime $r$ care se XOR-ează la prima parte a stării, alternând cu aplicarea funcției $f$;
  2. Squeezing phase: partea superioară a stării este returnată la ieșire, alternând cu aplicarea funcției $f$; numărul de iterații depinde de numărul de biți $l$ necesari la ieșire.

# Keccak

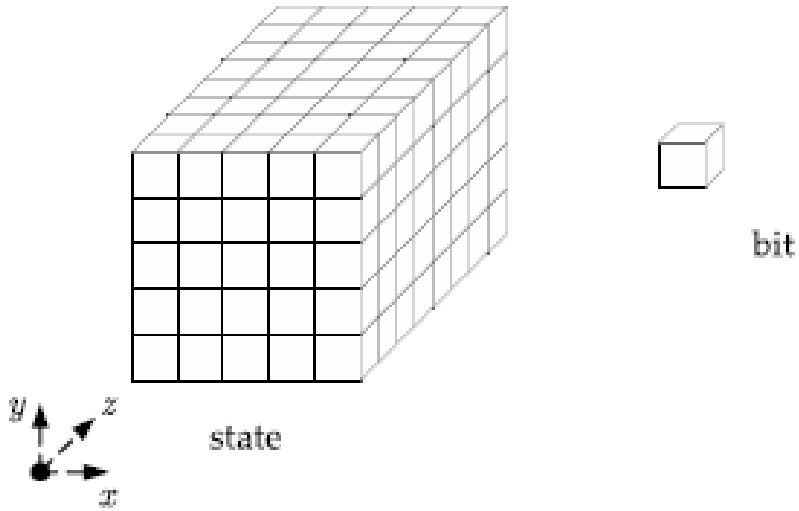
- Pentru implementarea Keccak:
  - $c \leq 512$
  - $600 \leq b \leq 2400$
  - $r = b - c$
  - $f =$ o funcție non-liniară cu bune proprietăți de difuzie;

# Keccak

- Pentru implementarea Keccak:
  - $c \leq 512$
  - $600 \leq b \leq 2400$
  - $r = b - c$
  - $f =$ o funcție non-liniară cu bune proprietăți de difuzie;
- SHA-3:
  - $c = 512$
  - $b = 1600$
  - $r = b - c = 1088$

# Keccak

- Starea este considerată o structură 3D $5 \times 5 \times 2^l$ ($l \in \{1, 2, 4, 8, 16, 32, 64\}$):




[The Keccak Reference - `http://keccak.noekeon.org/Keccak-reference-3.0.pdf`]

# Keccak

- O rundă presupune trecerea stării prin 5 transformări menite să introducă proprietățile necesare (non-liniaritate, difuzie, non-simetrie, etc.):

$$R = \iota \circ \chi \circ \pi \circ \rho \circ \theta$$

# Keccak

- O rundă presupune trecerea stării prin 5 transformări menite să introducă proprietățile necesare (non-liniaritate, difuzie, non-simetrie, etc.):

$$R = \iota \circ \chi \circ \pi \circ \rho \circ \theta$$

- Numărul de runde depinde de parametrul $l$: $12 + 2l$;

# Keccak

- O rundă presupune trecerea stării prin 5 transformări menite să introducă proprietățile necesare (non-liniaritate, difuzie, non-simetrie, etc.):

$$R = \iota \circ \chi \circ \pi \circ \rho \circ \theta$$

- Numărul de runde depinde de parametrul $l$: $12 + 2l$;
- Pentru $b = 1600 = 5 \times 5 \times 2^6 \Rightarrow 12 + 2 * 6 = 24$ runde.

# Important de reținut!

- Keccak este câștigătorul competiției SHA-3
- SHA-2 rămâne în continuare sigură