Securitatea Sistemelor Informatice

- Curs 8.1 -
SHA-3

Adela Georgescu

Facultatea de Matematică și Informatică
Universitatea din București
Anul universitar 2022-2023, semestrul I

Exemple de funcții hash

- MD5
  - output pe 128 biți
  - propusă în 1991 și considerată rezistentă la coliziuni o perioadă de timp
  - 2004 - atac pentru găsirea de coliziuni + coliziuni explicite
  - astăzi se pot găsi coliziuni în mai puțin de un minut pe un calculator desktop

Exemple de funcții hash

- SHA-1

Exemple de funcții hash

- SHA-1
  - face parte din seria de algoritmi standardizați SHA (Secure Hash Algorithm) si a fost standardul aprobat de NIST până în 2011

Exemple de funcții hash

- SHA-1
  - face parte din seria de algoritmi standardizați SHA (Secure Hash Algorithm) si a fost standardul aprobat de NIST până în 2011
  - output pe 160 biti

Exemple de funcții hash

- SHA-1
  - face parte din seria de algoritmi standardizați SHA (Secure Hash Algorithm) si a fost standardul aprobat de NIST până în 2011
  - output pe 160 biti
  - 2005 - atac teoretic pentru găsirea coliziunilor; necesită 2^{69} evaluări ale funcției hash

Exemple de funcții hash

- SHA-1
  - face parte din seria de algoritmi standardizați SHA (Secure Hash Algorithm) si a fost standardul aprobat de NIST până în 2011
  - output pe 160 biti
  - 2005 - atac teoretic pentru găsirea coliziunilor; necesită 2^{69} evaluări ale funcției hash
  - 2017 - prima coliziune practică - 2^{63} evaluări ale funcției hash

Exemple de funcții hash

- SHA-1
  - face parte din seria de algoritmi standardizați SHA (Secure Hash Algorithm) si a fost standardul aprobat de NIST până în 2011
  - output pe 160 biti
  - 2005 - atac teoretic pentru găsirea coliziunilor; necesită 2^{69} evaluări ale funcției hash
  - 2017 - prima coliziune practică - 2^{63} evaluări ale funcției hash
  - atac pentru găsirea de *coliziuni cu prefix* - aprox. 2^{67} evaluari

Exemple de funcții hash

- SHA-1
  - face parte din seria de algoritmi standardizați SHA (Secure Hash Algorithm) si a fost standardul aprobat de NIST până în 2011
  - output pe 160 biti
  - 2005 - atac teoretic pentru găsirea coliziunilor; necesită 2^{69} evaluări ale funcției hash
  - 2017 - prima coliziune practică - 2^{63} evaluări ale funcției hash
  - atac pentru găsirea de *coliziuni cu prefix* - aprox. 2^{67} evaluari
  - *coliziuni cu prefix* - pornind de la prefixele P si P', se cere găsirea mesajelor $M \neq M'$ cu $H(P||M) = H(P'||M')$
  - în practică, acestea sunt mai periculoase, pot duce la diverse atacuri incluzând generarea de certificate digitale false și atacuri asupra TLS, SSH

Exemple de funcții hash

- SHA-2

Exemple de funcții hash

- SHA-2
  - prezintă două versiuni: SHA-256 și SHA-512 în funcție de lungimea output-ului

Exemple de funcții hash

- SHA-2
  - prezintă două versiuni: SHA-256 și SHA-512 în funcție de lungimea output-ului
  - nu se cunosc vulnerabilități; atât SHA-2 cât și SHA-3 sunt sigur de folosit acolo unde rezistența la coliziuni este necesară

Competiția SHA-3

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

Competiția SHA-3

- Atacurile asupra MD5 si SHA-1 au impus necesitatea unei noi funcții hash;
- 2 noiembrie 2007 - NIST anunță competiția publică SHA-3;

Competiția SHA-3

- Atacurile asupra MD5 si SHA-1 au impus necesitatea unei noi funcții hash;
- 2 noiembrie 2007 - NIST anunță competiția publică SHA-3;
- 31 octombrie 2008 - se primesc 64 de propuneri din toată lumea;

Competiția SHA-3

- Atacurile asupra MD5 si SHA-1 au impus necesitatea unei noi funcții hash;
- 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, Grϕstl, JH, Keccak and Skein;

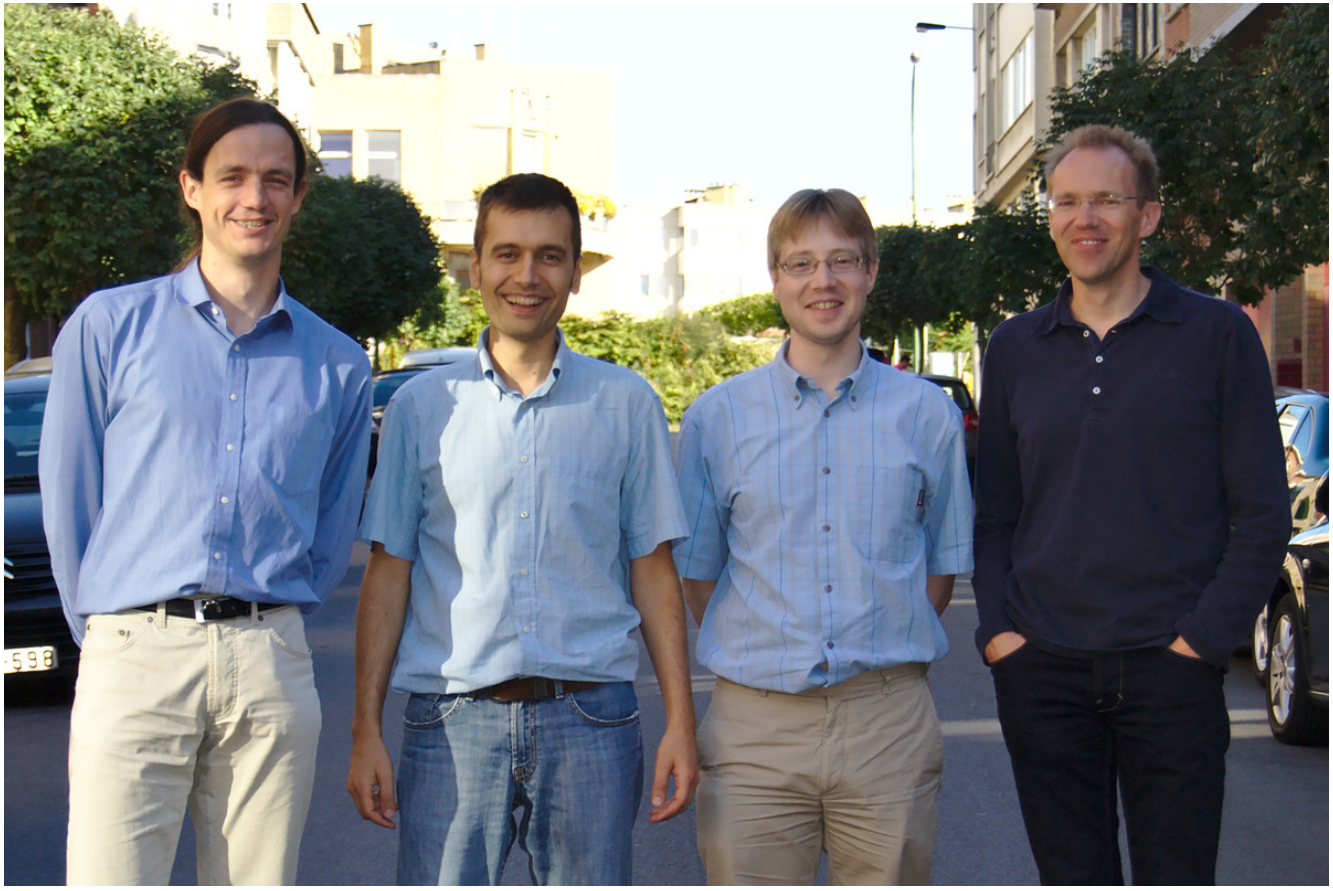
Competiția SHA-3

- 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

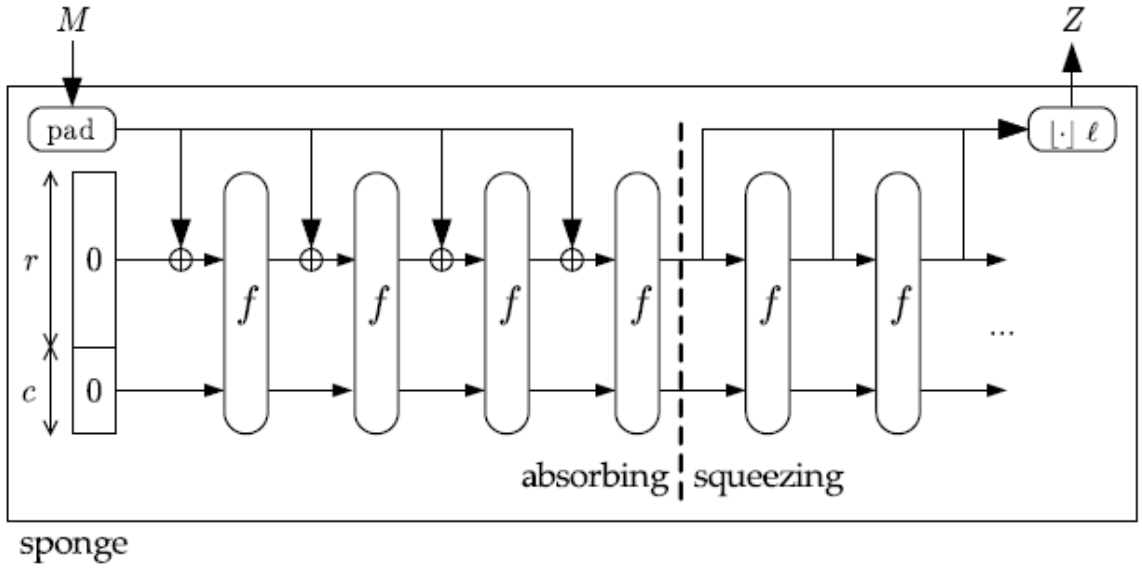
- A fost gândit să difere complet de construcțiile existente (AES, SHA-2);

Keccak

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

Keccak

- A fost gândit să difere complet de construcțiile existente (AES, SHA-2);
- Folosește sponge functions:
- Principala componentă este permutarea f care acceptă blocuri de 1600 biți.



[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

Tabelul de mai jos din standardul NIST (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf) ofera o comparatie d.p.d.v. al securitatii cu SHA-1 si SHA-2.

Function	Output Size	Security Strengths in Bits		
		Collision	Preimage	2nd Preimage
SHA-1	160	< 80	160	$160 - L(M)$
SHA-224	224	112	224	$\min(224, 256 - L(M))$
SHA-512/224	224	112	224	224
SHA-256	256	128	256	$256 - L(M)$
SHA-512/256	256	128	256	256
SHA-384	384	192	384	384
SHA-512	512	256	512	$512 - L(M)$
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	d	$\min(d/2, 128)$	$\geq \min(d, 128)$	$\min(d, 128)$
SHAKE256	d	$\min(d/2, 256)$	$\geq \min(d, 256)$	$\min(d, 256)$

Important de reținut!

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