Functional Graph Revisited: Updates on (Second) Preimage Attacks on Hash Combiners

Zhenzhen Bao Lei Wang Jian Guo Dawu Gu

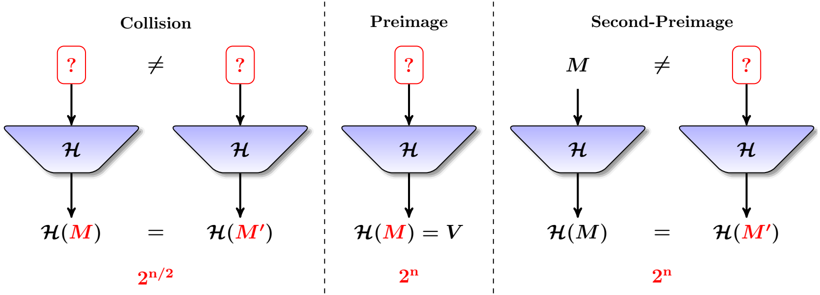
SHANGHAI JIAO TONG UNIVERSITY

NANYANG TECHNOLOGICAL UNIVERSITY

Crypto 2017 August 21
Santa Barbara, CA, USA

Security Requirements for Hash Functions

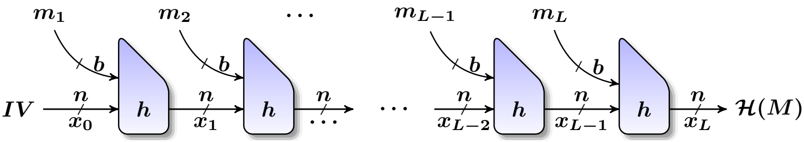
1. **Collision resistance**: It should be computationally difficult to find two messages M and M' such that $\mathcal{H}(M) = \mathcal{H}(M')$.
2. **Preimage resistance**: Given a target V, it should be computationally difficult to find a message M such that $\mathcal{H}(M) = V$.
3. **Second-preimage resistance**: Given a message M, it should be computationally difficult to find another message $M' \neq M$ such that $\mathcal{H}(M') = \mathcal{H}(M)$.



Underlying Construction - Iterative Hash Functions

1. The Merkle-Damgård construction (MD) [Mer90; Dam90]: Padding and dividing $M = m_1 \| m_2 \| \ldots \| m_L$, where m_L is encoded with the length the message $|M|$:

$$x_0 = IV \quad x_i = h(x_{i-1}, m_i) \quad \mathcal{H}(M) = h(x_{L-1}, m_L)$$



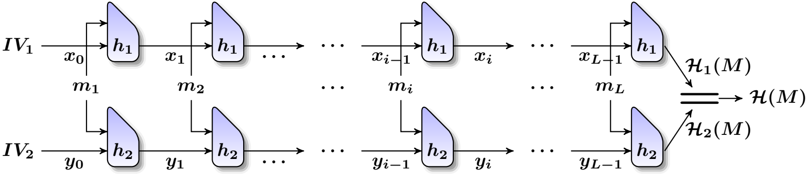
An Approach to Construct a Secure Hash Function - Hash Combiner

Hash Combiner

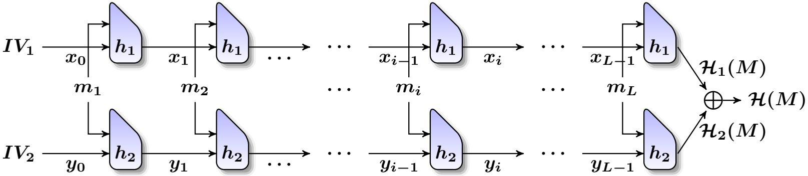
- Security amplification
  the combiner is more secure than its underlying hash functions;
- Security robustness
  the combiner is secure as long as any one of its underlying hash functions is secure

Hash Combiners - Parallel

- Concatenation combiner: $\mathcal{H}(M) = \mathcal{H}_1(M) \| \mathcal{H}_2(M)$

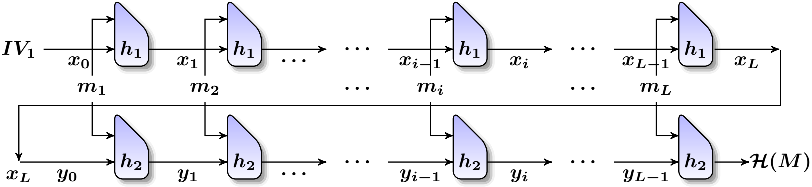


- XOR combiner: $\mathcal{H}(M) = \mathcal{H}_1(M) \oplus \mathcal{H}_2(M)$

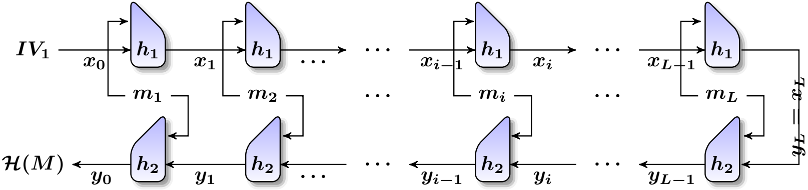


Hash Combiners - Cascade

- Hash Twice: $\mathcal{H}(M) = \mathcal{H}_2(\mathcal{H}_1(IV, M), M)$



- Zipper Hash [Lis07]: $\mathcal{H}(M) = \mathcal{H}_2(\mathcal{H}_1(IV, M), \overleftarrow{M})$



Research on Hash Combiners

Security of classical hash combiners

- Generic attacks: upper bound;
- Security proofs: lower bound;

Research on Hash Combiners

Security of classical hash combiners

- Generic attacks: upper bound; the main focus of this work
- Security proofs: lower bound;

Expected Security of Hash Combiners Before 2004

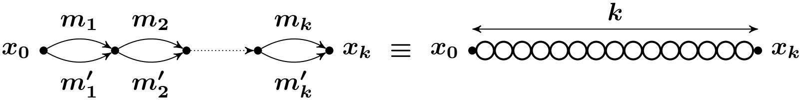
	Digest Size	Collision Resistance	Preimage Resistance	Second Preimage Resistance
Ideal $\mathcal{H}$	n	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \| \mathcal{H}_2$	$2n$	2^n	2^{2n}	2^{2n}
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	n	$2^{n/2}$	2^n	2^n

$\Uparrow$
birthday bound
half of digest size

$\Uparrow$
full digest size

Joux's Multi-collisions (JM [Jou04])

- Get 2^k-multicollision by successively applying birthday attack k times.

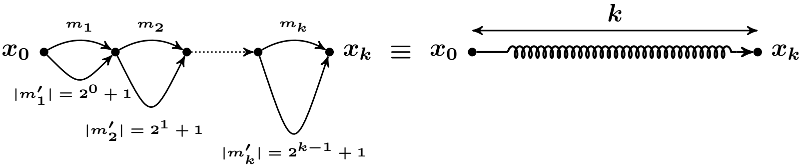


Security Status of MD Hash Combiners in 2004

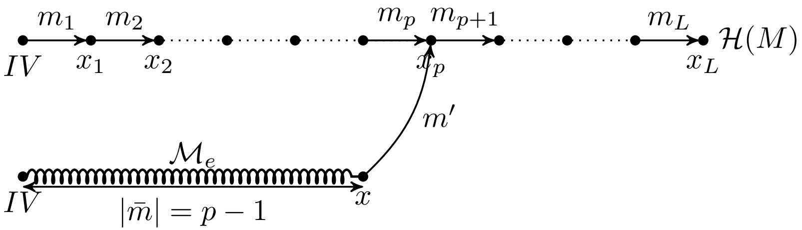
	Collision Resistance	Preimage Resistance	Second Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \| \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD $\mathcal{H}_1 \| \mathcal{H}_2$	([Jou04] JM) $\cancel{2^n}$ $\approx 2^{n/2}$	([Jou04] JM) $\cancel{2^{2n}}$ $\approx 2^n$	([Jou04] JM) $\cancel{2^{2n}}$ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n

Kelsey-Schneier's Expandable Message (EM [KS05])

- Get 2^k-multicollision with length cover the whole range of $[k, k + 2^k - 1]$ by successively applying birthday attack k times.



Second Preimage Attack Using Expandable Message [KS05]



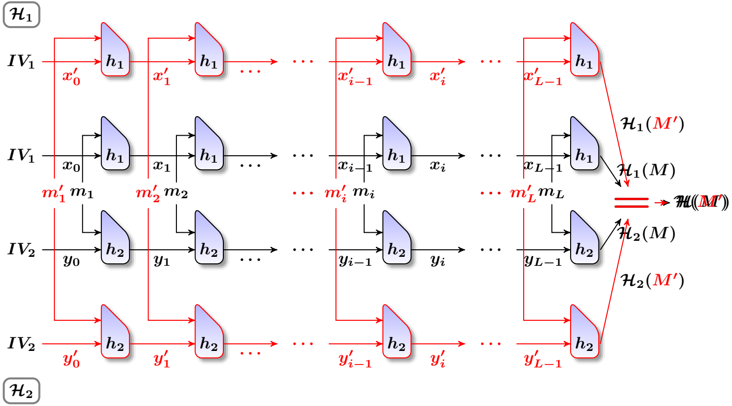
- Step 1: Start from IV, build an expandable message and end up at arbitrary state x.
- Step 2: Start from x and try different m' until $h(x, m') = x_p$ (for each trail $\Pr(succeed) = L/2^n$).
- Step 3: Select message $\bar{m}$ of appropriate length $p-1$ and output $M' = \bar{m}||m'||m_{p+1}|| \ldots ||m_L$.

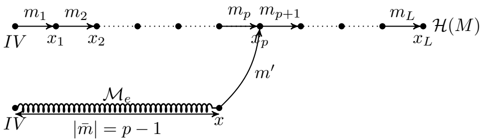
Security Status of MD Hash in 2005

	Collision Resistance	Preimage Resistance	Second Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	([KS05] EM) $\cancel{2^n}$ $2^n/L$
Ideal $\mathcal{H}_1 \| \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD $\mathcal{H}_1 \| \mathcal{H}_2$	([Jou04] JM) $\cancel{2^n}$ $\approx 2^{n/2}$	([Jou04] JM) $\cancel{2^{2n}}$ $\approx 2^n$	([Jou04] JM) $\cancel{2^{2n}}$ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n

A Primary Second Preimage Attack Against Concatenation Combiner

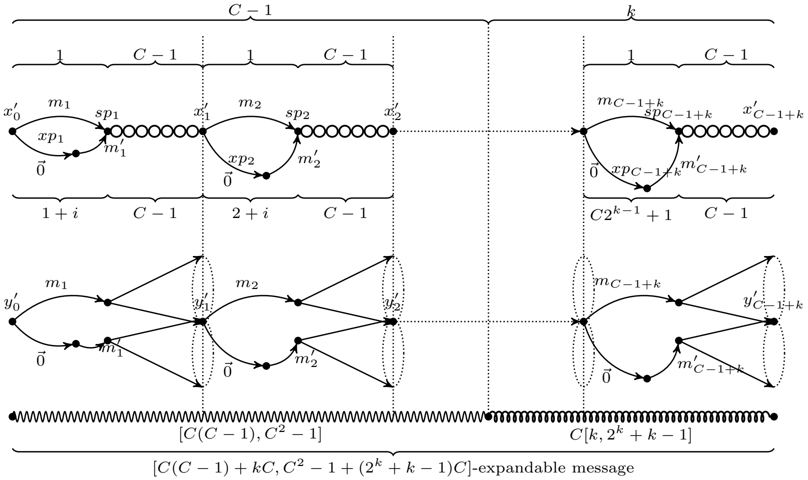
Goal:





Simultaneous Expandable Message (Parallel) (SEM [Din16])

$$T : n \cdot 2^k + n^2 \cdot 2^{\frac{n}{2}}, M : n^2 + k \cdot n, D : 2^{\frac{n}{2}}(n + k)$$



Functional Graph

The Functional Graph (FG) of Random Mapping:
Let $f \in \mathcal{F}_N$, $x \to f(x)$, FG of f is a directed graph, nodes are $[0 \ldots N-1]$ and edges are $\langle x, f(x) \rangle$

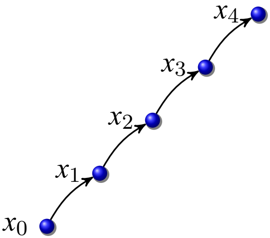
Functional Graph

The Functional Graph (FG) of Random Mapping:
Let $f \in \mathcal{F}_N$, $x \to f(x)$, FG of f is a directed graph, nodes are $[0 \ldots N-1]$ and edges are $\langle x, f(x) \rangle$

- Starting from a random point x_0

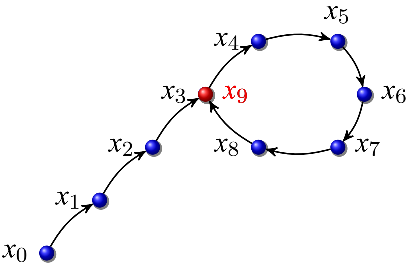
Functional Graph

The Functional Graph (FG) of Random Mapping:
Let $f \in \mathcal{F}_N$, $x \to f(x)$, FG of f is a directed graph, nodes are $[0 \ldots N-1]$ and edges are $\langle x, f(x) \rangle$



- Starting from a random point x_0
- Iterate: $x_1 = f(x_0)$, $x_2 = f(x_1), \ldots$

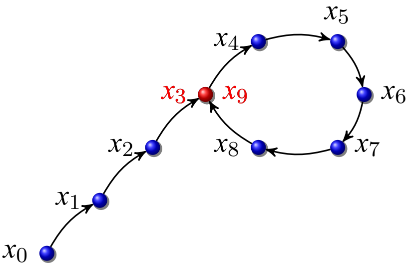
The Functional Graph (FG) of Random Mapping:
Let $f \in \mathcal{F}_N, x \to f(x)$, FG of f is a directed graph, nodes are $[0 \ldots N-1]$ and edges are $\langle x, f(x) \rangle$



- Starting from a random point x_0
- Iterate: $x_1 = f(x_0),\ x_2 = f(x_1), \ldots$
- Before N and $\approx \sqrt{N}$ iterations, we will find a value x_j equal to one of $x_0, x_1, \ldots, x_{j-1}$.

Functional Graph

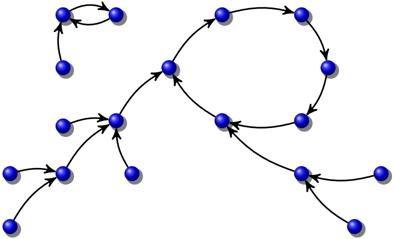
The Functional Graph (FG) of Random Mapping:
Let $f \in \mathcal{F}_N$, $x \to f(x)$, FG of f is a directed graph, nodes are $[0 \ldots N-1]$ and edges are $\langle x, f(x) \rangle$



- Starting from a random point x_0
- Iterate: $x_1 = f(x_0),\ x_2 = f(x_1), \ldots$
- Before N and $\approx \sqrt{N}$ iterations, we will find a value x_j equal to one of $x_0, x_1, \ldots, x_{j-1}$.
- We say collision x_j is an α-node and the path $x_0 \to x_1 \to \cdots \to x_{j-1} \to x_j$ connects to a cycle.

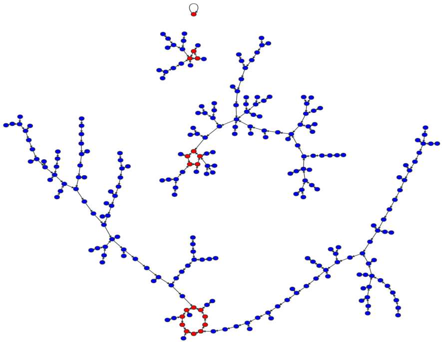
Functional Graph

The Functional Graph (FG) of Random Mapping:
Let $f \in \mathcal{F}_N$, $x \to f(x)$, FG of f is a directed graph, nodes are $[0 \ldots N-1]$ and edges are $\langle x, f(x) \rangle$



- Starting from a random point x_0
- Iterate: $x_1 = f(x_0),\ x_2 = f(x_1), \ldots$
- Before N and $\approx \sqrt{N}$ iterations, we will find a value x_j equal to one of $x_0, x_1, \ldots, x_{j-1}$.
- We say collision x_j is an α-node and the path $x_0 \to x_1 \to \cdots \to x_{j-1} \to x_j$ connects to a cycle.
- Starting from all possible points, paths confluence and form into trees; trees grafted on cycles form components; components forms a functional graph.

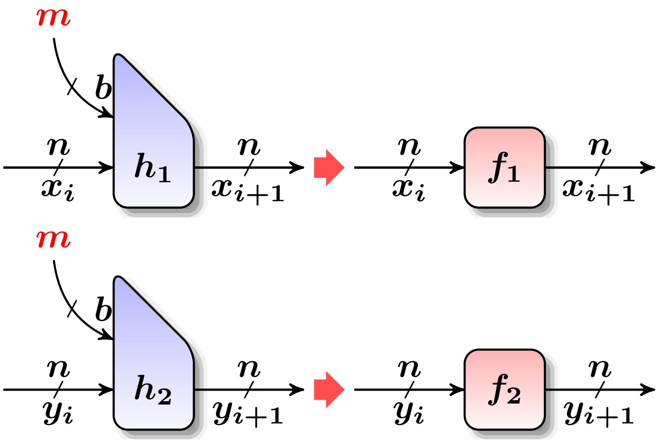
Properties of Functional Graph [FO90]



[PSW12; LPW13; PW14; Guo+14; DL14]

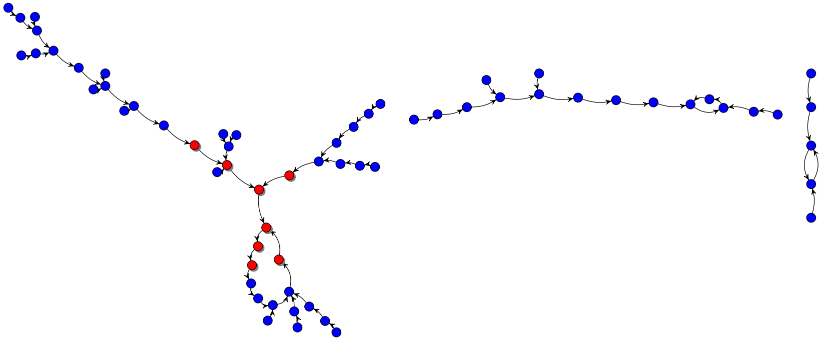
1. # Components: $\frac{1}{2}\log N = 0.5 \cdot n$
2. # Cyclic nodes: $\sqrt{\pi N/2} = 1.2 \cdot 2^{n/2}$
3. # Terminal nodes: $e^{-1}N = 0.37 \cdot 2^n$
4. # Image points: $(1 - e^{-1})N = 0.62 \cdot 2^n$
5. # k-th iterate image points: $(1 - \tau_k)N$, where the τ_k satisfy the recurrence $\tau_0 = 0$, $\tau_{k+1} = e^{-1+\tau_k}$.
6. Maxinum cycle length: $0.78 \cdot 2^{n/2}$.
7. Maxinum tail length: $1.74 \cdot 2^{n/2}$.
8. Maxinum rho length: $2.41 \cdot 2^{n/2}$.
9. Largest tree size: $0.48 \cdot 2^n$.
10. Largest component size: $0.76 \cdot 2^n$.

Functional Graph Corresponding to Underlying Compression Functions

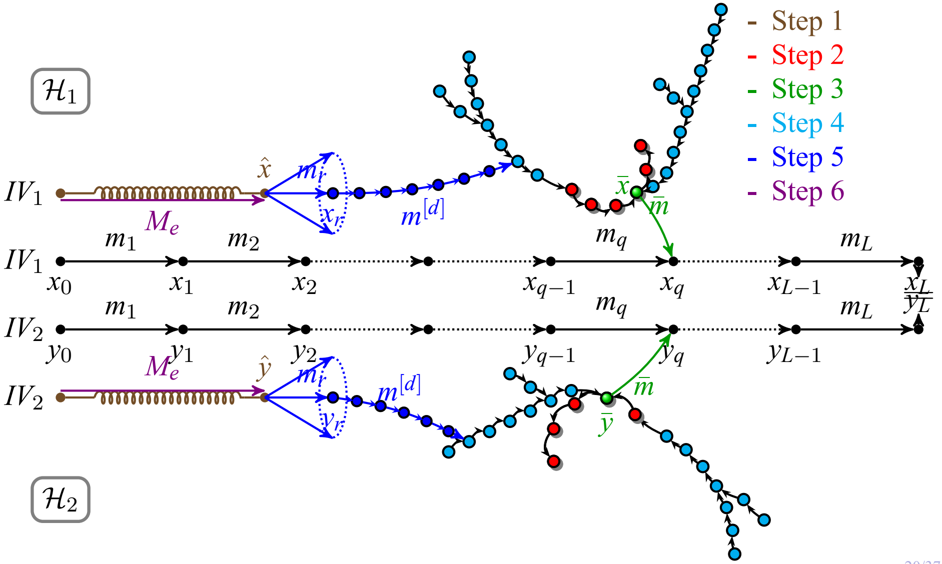


Deep Iterates in Functional Graph (FGDI [Din16])

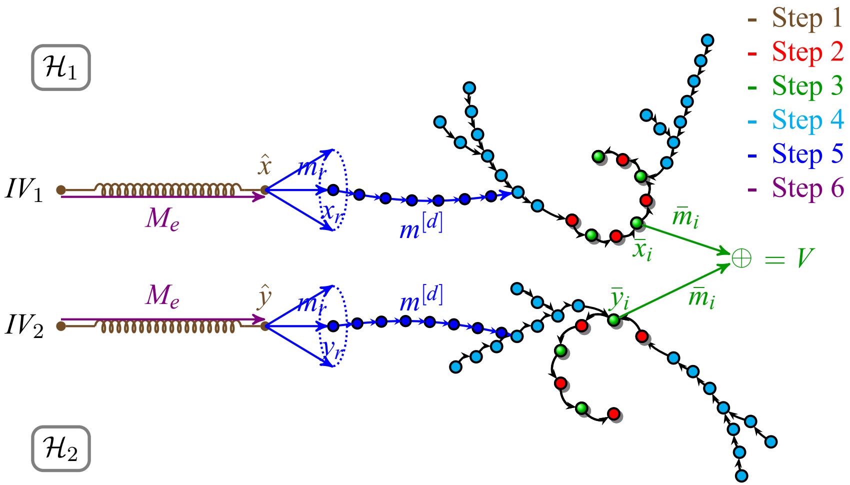
- It is easy to get a large set of deep iterates: $T : 2^k, M : 2^k, D : 2^k$
- A deep iterate has a relatively high probability to be reached from a randomly selected starting node.



Second Preimage Attacks on Concatenation Combiner Using Deep Iterates in FG [Din16]



Preimage Attacks on XOR Combiner Using Deep Iterates in FG [Din16]



(Second) Preimage Attack on Concatenation and XOR Combiner [Din16]

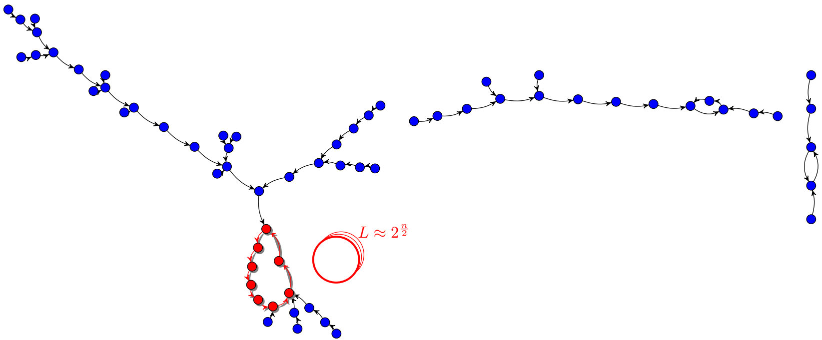
Simultaneous Expandable Message and Deep Iterates in FG (SEM+FGDI [Din16])

	Collision Resistance	Preimage Resistance	Second Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	$\cancel{2}^n$ $2^n/L$
Ideal $\mathcal{H}_1 \| \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD $\mathcal{H}_1 \| \mathcal{H}_2$	$\cancel{2}^n$ $\approx 2^{n/2}$	$\cancel{2}^{2n}$ $\approx 2^n$	$\cancel{2}^{2n}$ $\approx 2^{3n/4}$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	$\cancel{2}^n$ $\approx 2^{2n/3}$	$\cancel{2}^n$ $\approx 2^{2n/3}$

Functional Graph Multi-cycles (FGMC [Our's])

Cyclic Node and Multi-cycles in Functional Graph:

- It is easy to locate the largest cycle: Repeat the cycle search algorithm a few times $T : 2^{\frac{n}{2}}, M : 1, D : 2^{\frac{n}{2}}$
- It is effortless to loop around the cycles to correct differences between the distances to the target nodes.



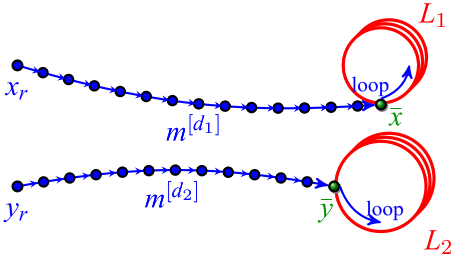
Functional Graph Multi-cycles (FGMC [Our's])

$$f_1^{d_1}(x_r) = \bar{x},\ f_1^{L_1}(\bar{x}) = \bar{x} \quad \Rightarrow \quad f_1^{d_1+i\cdot L_1}(x_r) = \bar{x} \text{ for } \forall\, i$$

$$f_2^{d_2}(y_r) = \bar{y},\ f_2^{L_2}(\bar{y}) = \bar{y} \quad \Rightarrow \quad f_2^{d_2+j\cdot L_2}(y_r) = \bar{y} \text{ for } \forall\, j$$

$$\Downarrow$$

$$\exists\,(i, j) \text{ s.t. } d_1 - d_2 = j\cdot L_2 - i\cdot L_1 \quad \Rightarrow \quad \exists\, d \text{ s.t. } f_1^{d}(x_r) = \bar{x},\, f_2^{d}(y_r) = \bar{y}$$



Functional Graph Multi-cycles (FGMC [Our's])

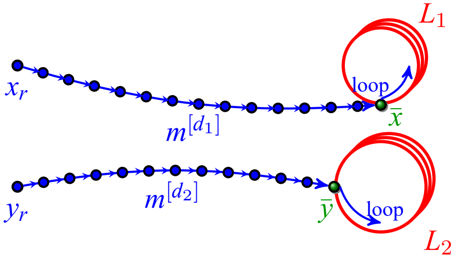
$$f_1^{d_1}(x_r) = \bar{x},\ f_1^{L_1}(\bar{x}) = \bar{x} \quad \Rightarrow \quad f_1^{d_1+i\cdot L_1}(x_r) = \bar{x} \text{ for } \forall\, i$$

$$f_2^{d_2}(y_r) = \bar{y},\ f_2^{L_2}(\bar{y}) = \bar{y} \quad \Rightarrow \quad f_2^{d_2+j\cdot L_2}(y_r) = \bar{y} \text{ for } \forall\, j$$

$$\Downarrow$$

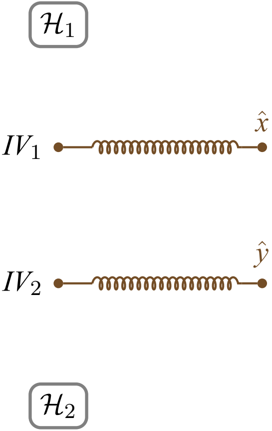
$$\exists\,(i,j) \text{ s.t. } d_1 - d_2 = j\cdot L_2 - i\cdot L_1 \quad \Rightarrow \quad \exists\, d \text{ s.t. } f_1^{d}(x_r) = \bar{x},\ f_2^{d}(y_r) = \bar{y}$$

correctable distance bias

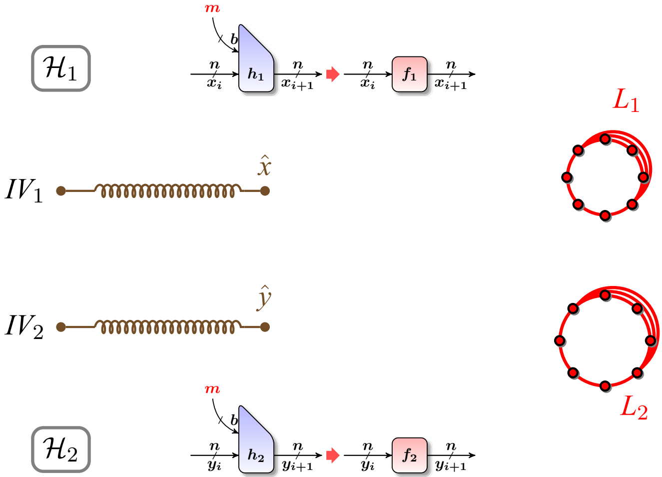


Preimage Attacks on XOR Combiner Using Multiple Cycles in FG

- Step 1

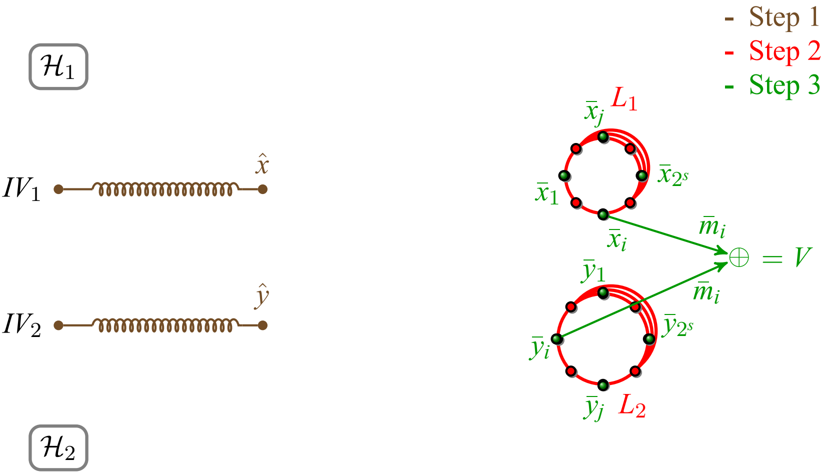


Preimage Attacks on XOR Combiner Using Multiple Cycles in FG

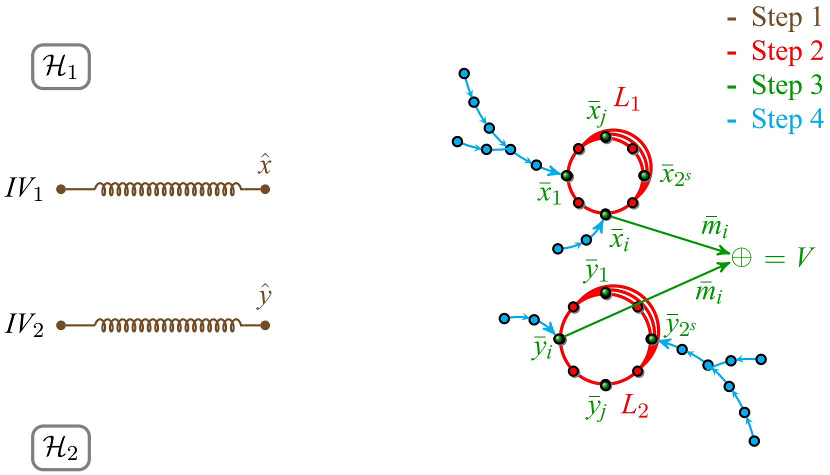


- Step 1
- Step 2

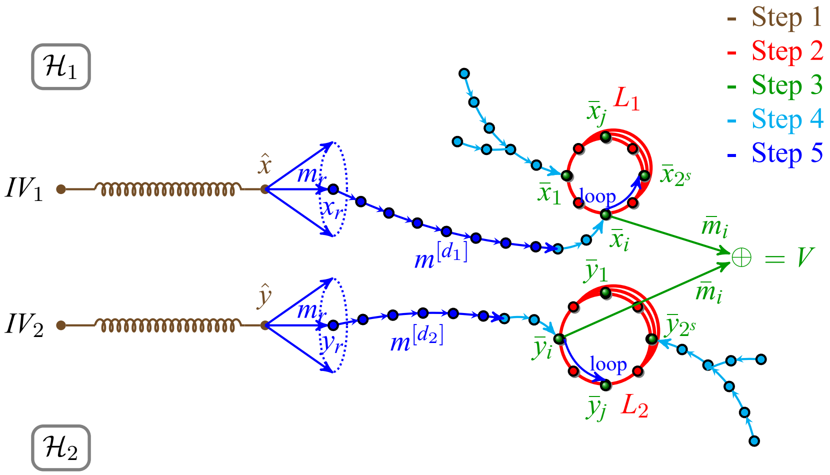
Preimage Attacks on XOR Combiner Using Multiple Cycles in FG



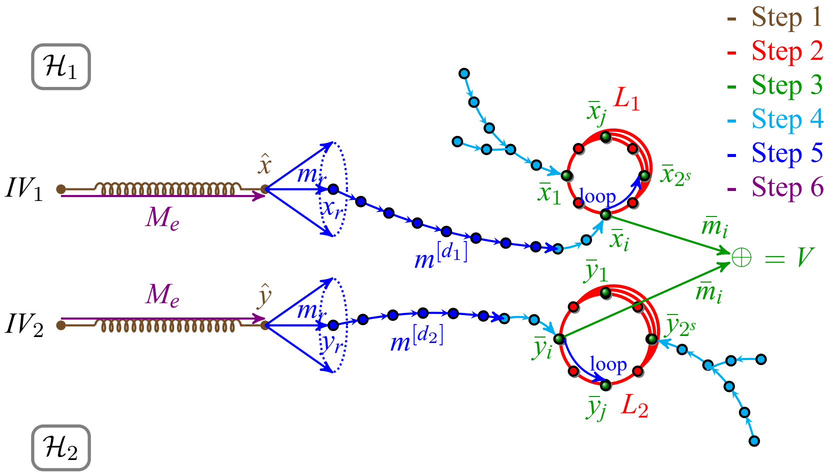
Preimage Attacks on XOR Combiner Using Multiple Cycles in FG



Preimage Attacks on XOR Combiner Using Multiple Cycles in FG

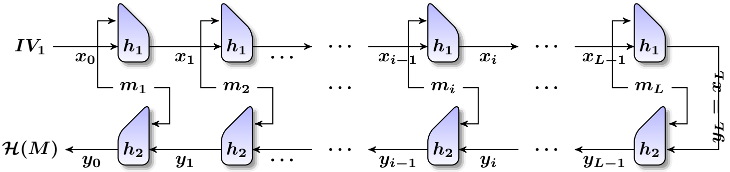


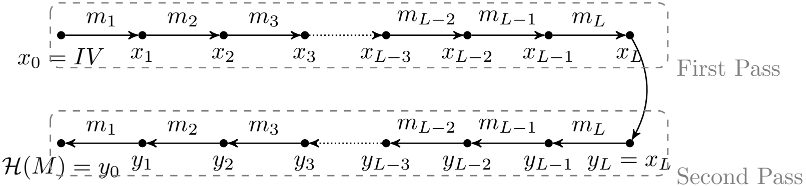
Preimage Attacks on XOR Combiner Using Multiple Cycles in FG



Hash Combiners - Cascade

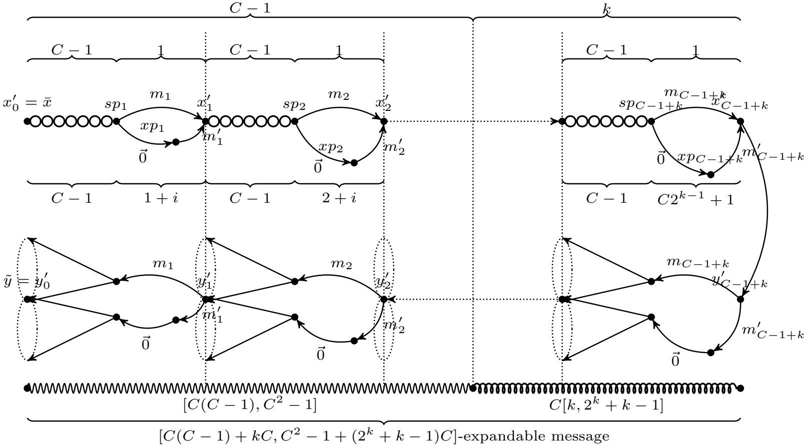
- Zipper Hash [Lis07]: $\mathcal{H}(M) = \mathcal{H}_2(\mathcal{H}_1(IV, M), \overleftarrow{M})$





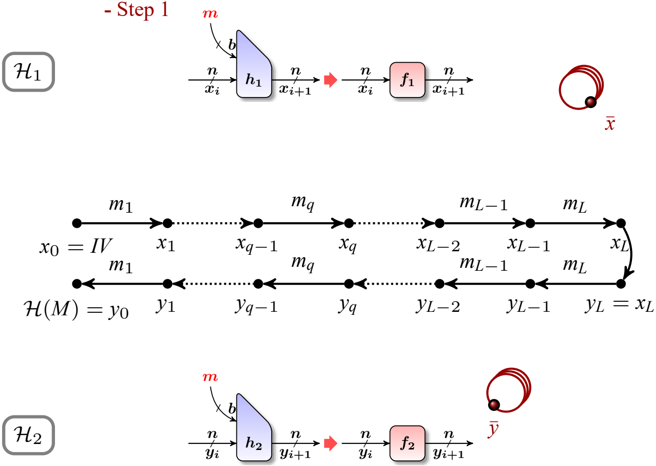
Simultaneous Expandable Message (Cascade)

$$T: n \cdot 2^k + n^2 \cdot 2^{\frac{n}{2}}, M: n^2 + k \cdot n, D: 2^{\frac{n}{2}}(n+k)$$



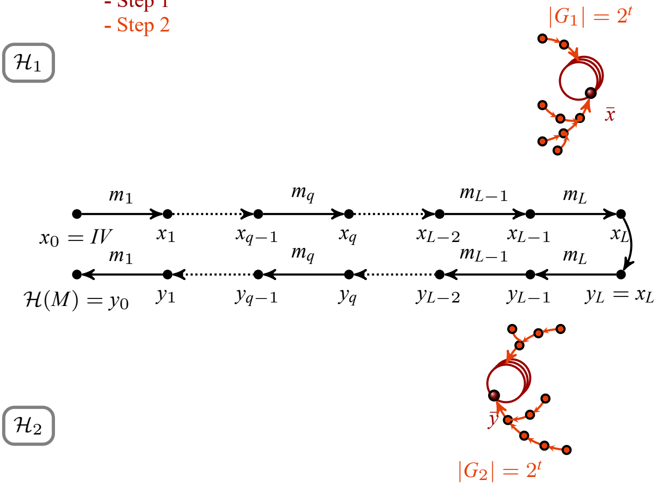
Second Preimage Attacks on Zipper Hash

- Step 1

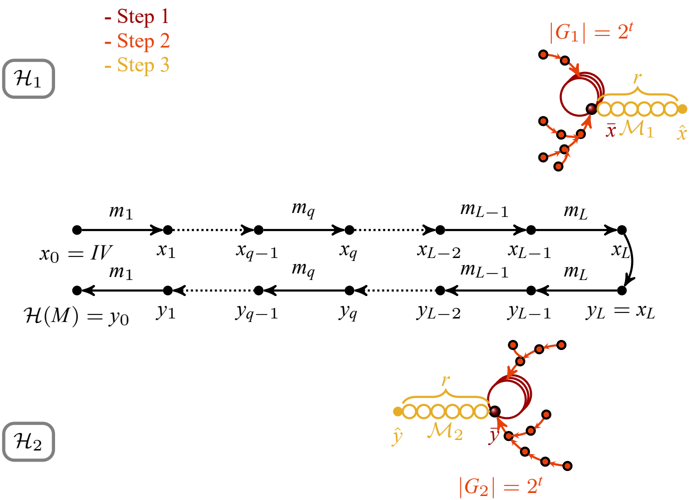


Second Preimage Attacks on Zipper Hash

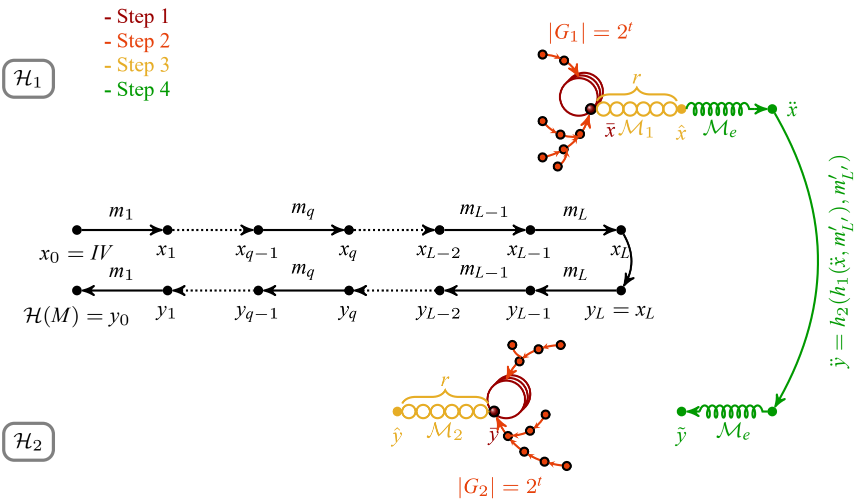
- Step 1
- Step 2



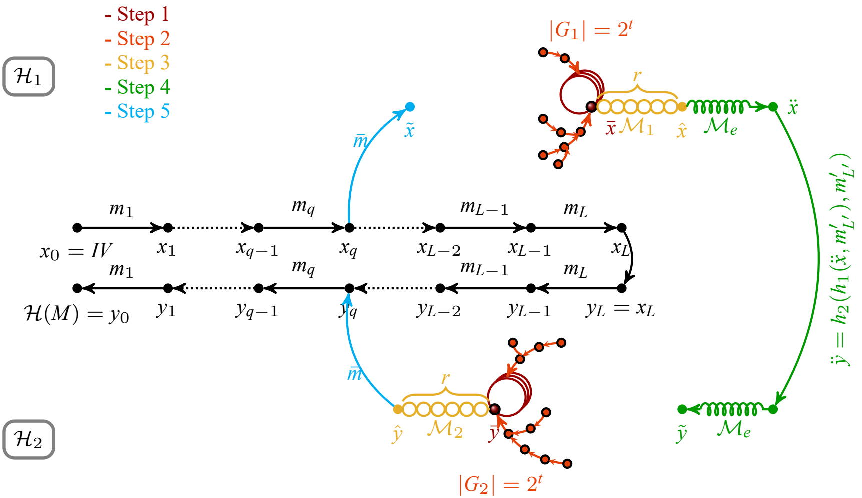
Second Preimage Attacks on Zipper Hash



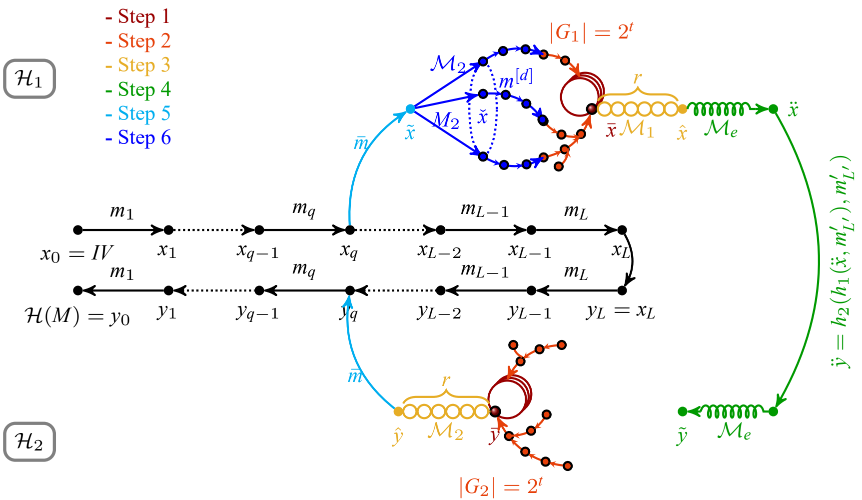
Second Preimage Attacks on Zipper Hash



Second Preimage Attacks on Zipper Hash

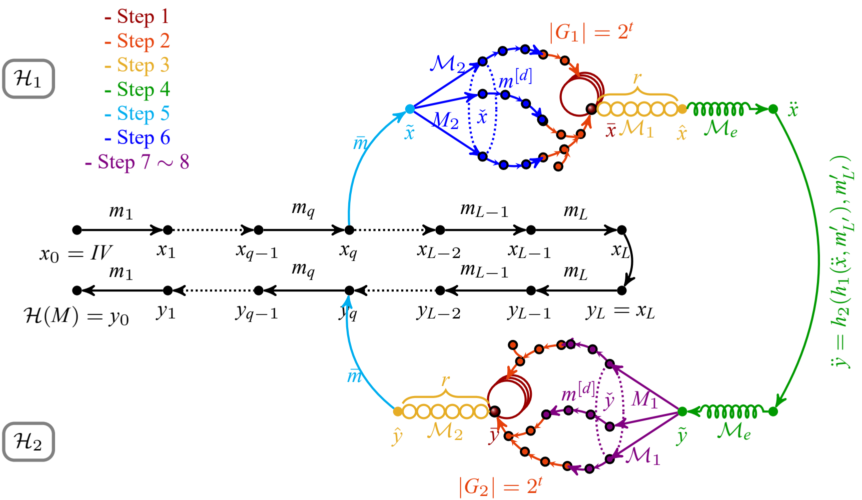


Second Preimage Attacks on Zipper Hash

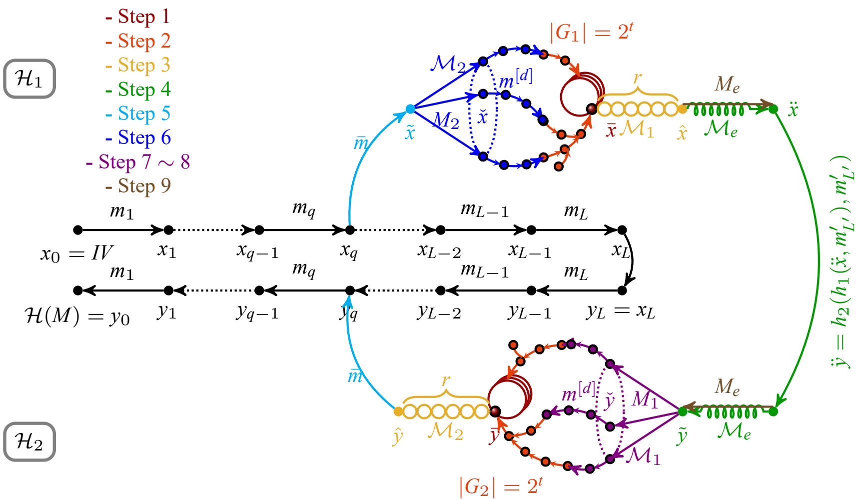


28/37

Second Preimage Attacks on Zipper Hash



Second Preimage Attacks on Zipper Hash



Upper Bounds vs Lower Bounds (Ignoring the factor n)

$\mathcal{H}_1 \Vert \mathcal{H}_2$	Collision Resistance	Preimage Resistance	2nd Preimage Resistance
Ideal	2^n	2^{2n}	2^{2n}
MD $\top$	([Jou04] JM) $2^{n/2}$	([Jou04] JM) 2^n	([Din16] SEM+FGDI) $2^{3n/4}$
MD $\perp$	$2^{n/2}$ [HS08]	$2^{n/2}$ [HS08]	$2^{n/2}$ [HS08]
HAIFA $\top$	([Jou04] JM) $2^{n/2}$	([Jou04] JM) 2^n	([Jou04] JM) 2^n
HAIFA $\perp$	$2^{n/2}$ [HS08]	$2^{n/2}$ [HS08]	$2^{n/2}$ [HS08]

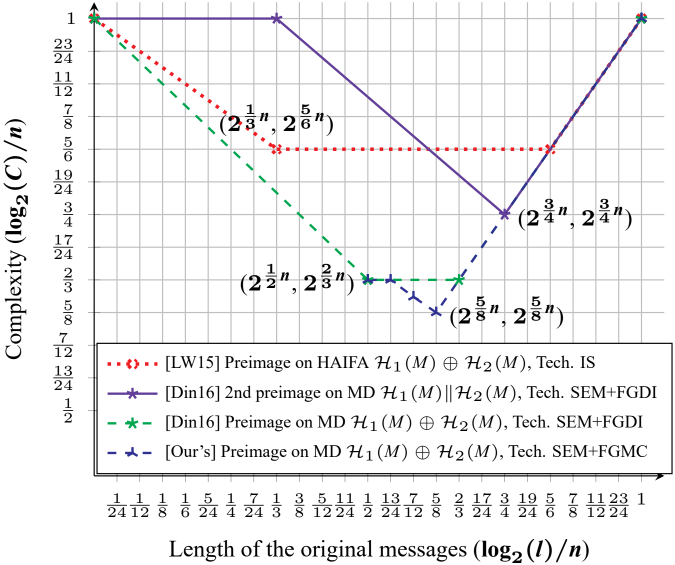
$\mathcal{H}_1 \oplus \mathcal{H}_2$	Collision Resistance	Preimage Resistance	2nd Preimage Resistance
Ideal	$2^{n/2}$	2^n	2^n
MD $\top$	Birthday $2^{n/2}$	([Din16] SEM+FGDI) $2^{2n/3}$ ([Our's] SEM+FGMC) $2^{5n/8}$	([Din16] SEM+FGDI) $2^{2n/3}$ ([Our's] SEM+FGMC) $2^{5n/8}$
MD $\perp$	$2^{n/2}$ [HS08]	$2^{n/2}$ [HS08]	$2^{n/2}$ [HS08]
HAIFA $\top$	Birthday $2^{n/2}$	([LW15] IS) $2^{5n/6}$	([LW15] IS) $2^{5n/6}$
HAIFA $\perp$	$2^{n/2}$ [HS08]	$2^{n/2}$ [HS08]	$2^{n/2}$ [HS08]

Upper Bounds vs Lower Bounds (Ignoring the factor n)

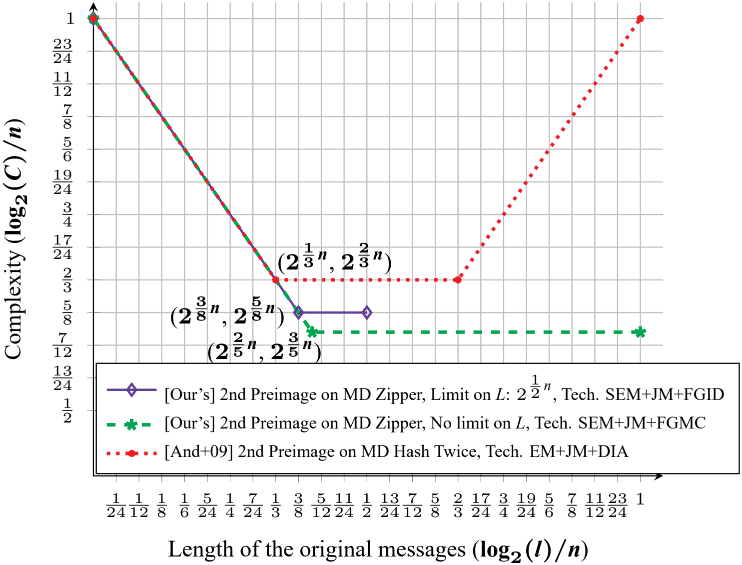
Hash Twice	Collision Resistance	Preimage Resistance	2nd Preimage Resistance
Ideal $\top$	$2^{n/2}$	2^n	2^n
MD $\top$	$2^{n/2}$	2^n	([And+09] EM+JM+DIA) $2^{2n/3}$
MD $\perp$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
HAIFA $\top$	$2^{n/2}$	2^n	2^n
HAIFA $\perp$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$

Zipper Hash	Collision Resistance	Preimage Resistance	2nd Preimage Resistance
Ideal $\top$	$2^{n/2}$	2^n	2^n
MD $\top$	$2^{n/2}$	2^n	([Our's] SEM+JM+FGMC) $2^{3n/5}$
MD $\perp$	$2^{\min(m,n)}$	$2^{\min(m,n)}$ [Lis07]	$2^{\min(m,n)}$ [Lis07]
HAIFA $\top$	$2^{n/2}$	2^n	2^n
HAIFA $\perp$	$2^{\min(m,n)}$	$2^{\min(m,n)}$ [Lis07]	$2^{\min(m,n)}$ [Lis07]

Trade-offs Between the Message Length and the Attack Complexity



Trade-offs Between the Message Length and the Attack Complexity



Thanks for your attention!

References I

[Mer90] Ralph C. Merkle. "One Way Hash Functions and DES". In: *Advances in Cryptology — CRYPTO' 89 Proceedings*. Ed. by Gilles Brassard. Vol. 435. Lecture Notes in Computer Science. New York, NY: Springer New York, 1990, pp. 428–446. ISBN: 978-0-387-34805-6. DOI: 10.1007/0-387-34805-0_40. URL: http://dx.doi.org/10.1007/0-387-34805-0_40.

[Dam90] Ivan Bjerre Damgård. "A Design Principle for Hash Functions". In: *Advances in Cryptology — CRYPTO' 89 Proceedings*. Ed. by Gilles Brassard. Vol. 435. Lecture Notes in Computer Science. New York, NY: Springer New York, 1990, pp. 416–427. ISBN: 978-0-387-34805-6. DOI: 10.1007/0-387-34805-0_39. URL: http://dx.doi.org/10.1007/0-387-34805-0_39.

[Lis07] Moses Liskov. "Constructing an Ideal Hash Function from Weak Ideal Compression Functions". In: *Selected Areas in Cryptography: 13th International Workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 Revised Selected Papers*. Ed. by Eli Biham and Amr M. Youssef. Vol. 4356. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 358–375. ISBN: 978-3-540-74462-7. DOI: 10.1007/978-3-540-74462-7_25. URL: http://dx.doi.org/10.1007/978-3-540-74462-7_25.

[Jou04] Antoine Joux. "Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions". In: *Advances in Cryptology – CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004. Proceedings*. Ed. by Matt Franklin. Vol. 3152. Lecture Notes in Computer Science (LNCS). Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 306–316. ISBN: 978-3-540-28628-8. DOI: 10.1007/978-3-540-28628-8_19. URL: http://dx.doi.org/10.1007/978-3-540-28628-8_19.

[KS05] John Kelsey and Bruce Schneier. "Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work". In: *Advances in Cryptology – EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings*. Ed. by Ronald Cramer. Vol. 3494. Lecture Notes in Computer Science (LNCS). Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 474–490. ISBN: 978-3-540-32055-5. DOI: 10.1007/11426639_28. URL: http://dx.doi.org/10.1007/11426639_28.

[Din16] Itai Dinur. "New Attacks on the Concatenation and XOR Hash Combiners". In: *Advances in Cryptology – EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9665. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 484–508. ISBN: 978-3-662-49890-3. DOI: 10.1007/978-3-662-49890-3_19. URL: http://dx.doi.org/10.1007/978-3-662-49890-3_19.

[PSW12] Thomas Peyrin, Yu Sasaki, and Lei Wang. "Generic Related-Key Attacks for HMAC". In: *Advances in Cryptology – ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*. Ed. by Xiaoyun Wang and Kazue Sako. Vol. 7658. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 580–597. ISBN: 978-3-642-34961-4. DOI: 10.1007/978-3-642-34961-4_35. URL: http://dx.doi.org/10.1007/978-3-642-34961-4_35.

[LPW13] Gaëtan Leurent, Thomas Peyrin, and Lei Wang. "New Generic Attacks against Hash-Based MACs". In: *Advances in Cryptology - ASIACRYPT 2013: 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II*. Ed. by Kazue Sako and Palash Sarkar. Vol. 8270. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–20. ISBN: 978-3-642-42045-0. DOI: 10.1007/978-3-642-42045-0_1. URL: http://dx.doi.org/10.1007/978-3-642-42045-0_1.

[PW14] Thomas Peyrin and Lei Wang. "Generic Universal Forgery Attack on Iterative Hash-Based MACs". In: *Advances in Cryptology – EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*. Ed. by Phong Q. Nguyen and Elisabeth Oswald. Vol. 8441. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 147–164. ISBN: 978-3-642-55220-5. DOI: 10.1007/978-3-642-55220-5_9. URL: http://dx.doi.org/10.1007/978-3-642-55220-5_9.

References III

[Guo+14] Jian Guo et al. "Updates on Generic Attacks against HMAC and NMAC". In: *Advances in Cryptology – CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*. Ed. by Juan A. Garay and Rosario Gennaro. Vol. 8616. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 131–148. ISBN: 978-3-662-44371-2. DOI: 10.1007/978-3-662-44371-2_8. URL: http://dx.doi.org/10.1007/978-3-662-44371-2_8.

[DL14] Itai Dinur and Gaëtan Leurent. "Improved Generic Attacks against Hash-Based MACs and HAIFA". In: *Advances in Cryptology – CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*. Ed. by Juan A. Garay and Rosario Gennaro. Vol. 8616. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 149–168. ISBN: 978-3-662-44371-2. DOI: 10.1007/978-3-662-44371-2_9. URL: http://dx.doi.org/10.1007/978-3-662-44371-2_9.

[FO90] Philippe Flajolet and Andrew M. Odlyzko. "Random Mapping Statistics". In: *Advances in Cryptology — EUROCRYPT '89: Workshop on the Theory and Application of Cryptographic Techniques Houthalen, Belgium, April 10–13, 1989 Proceedings*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Vol. 434. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1990, pp. 329–354. ISBN: 978-3-540-46885-1. DOI: 10.1007/3-540-46885-4_34. URL: http://dx.doi.org/10.1007/3-540-46885-4_34.

[HS08] Jonathan J. Hoch and Adi Shamir. "On the Strength of the Concatenated Hash Combiner When All the Hash Functions Are Weak". In: *Automata, Languages and Programming: 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II*. Ed. by Luca Aceto et al. Vol. 5126. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 616–630. ISBN: 978-3-540-70583-3. DOI: 10.1007/978-3-540-70583-3_50. URL: http://dx.doi.org/10.1007/978-3-540-70583-3_50.

References IV

[LW15] Gaëtan Leurent and Lei Wang. "The Sum Can Be Weaker Than Each Part". In: *Advances in Cryptology – EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9056. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 345–367. ISBN: 978-3-662-46800-5. DOI: `10.1007/978-3-662-46800-5_14`. URL: `http://dx.doi.org/10.1007/978-3-662-46800-5_14`.

[And+09] Elena Andreeva et al. "Herding, Second Preimage and Trojan Message Attacks beyond Merkle-Damgård". In: *Selected Areas in Cryptography: 16th Annual International Workshop, SAC 2009, Calgary, Alberta, Canada, August 13-14, 2009, Revised Selected Papers*. Ed. by Michael J. Jacobson, Vincent Rijmen, and Reihaneh Safavi-Naini. Vol. 5867. Lecture Notes in Computer Science (LNCS). Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 393–414. ISBN: 978-3-642-05445-7. DOI: `10.1007/978-3-642-05445-7_25`. URL: `http://dx.doi.org/10.1007/978-3-642-05445-7_25`.