Generic Attacks on Hash Combiners

Zhenzhen Bao Itai Dinur Jian Guo Gaëtan Leurent Lei Wang

ASK 2019, December 13–15
Kobe, Japan

Acknowledgments

The works are reported in Zhenzhen Bao, Itai Dinur, Jian Guo, Gaëtan Leurent, and Lei Wang. "Generic Attacks on Hash Combiners". In: *Journal of Cryptology* (2019)

This is a combination and extension of three conference papers

- 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. LNCS. Springer, 2015
- 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. LNCS. Springer, 2016
- Zhenzhen Bao, Lei Wang, Jian Guo, and Dawu Gu. "Functional Graph Revisited: Updates on (Second) Preimage Attacks on Hash Combiners". In: *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*. ed. by Jonathan Katz and Hovav Shacham. Vol. 10402. LNCS. Springer, 2017

Outline

Cryptographic Hash Combiners

Motivation of design of hash combiners
(share the common motivation with other cryptographic combiners, e.g., encryption combiners):

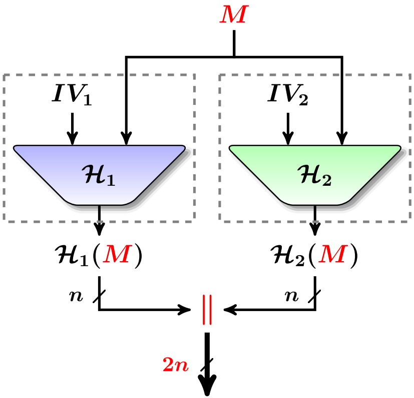
- Security robustness
  the combiner is *secure as long as any one* of its underlying hash functions is secure
- Security amplification
  the combiner is *more secure* than its underlying hash functions

Besides, regarding implementations

- Backward-compatible
  the combiner is compatible with existing infrastructure

Constructions of Hash Combiners – Parallel

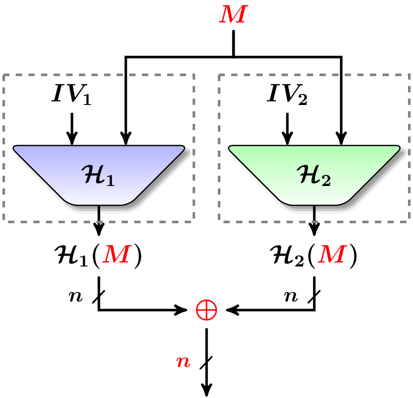
Concatenation Combiner



$$\mathcal{C}^{\mathcal{H}_1,\mathcal{H}_2}(M) = \mathcal{H}_1(M) \| \mathcal{H}_2(M)$$

(collision $\mathbf{2^n}$, 2nd-preimage $\mathbf{2^{2n}}$, preimage $\mathbf{2^{2n}}$)

XOR Combiner



$$\mathcal{C}^{\mathcal{H}_1,\mathcal{H}_2}(M) = \mathcal{H}_1(M) \oplus \mathcal{H}_2(M)$$

(collision $\mathbf{2^{n/2}}$, 2nd-preimage $\mathbf{2^n}$, preimage $\mathbf{2^n}$)

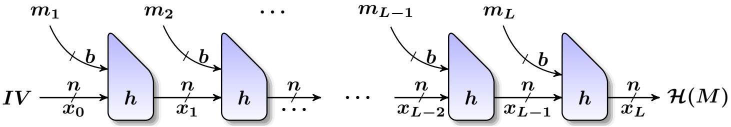
Theoretical Research on Hash Combiners

Security of classical hash combiners

- Security proofs: lower bound; [Her05; Can+07; FL07; FL08; FLP08; Her09; Leh10; FLP14; BB06; Pie07; Pie08; Rja09]
- Generic attacks: upper bound; the main focus of this work
  The underlying compression functions are ideal (random)

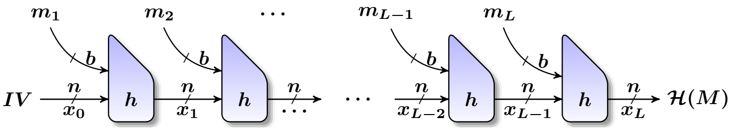
Underlying Construction - Iterative Hash Functions

- The Merkle-Damgård construction (MD) [Dam89; Mer89]:
  Padding and dividing $M = m_1 \parallel m_2 \parallel \cdots \parallel m_L$, where m_L is encoded with the length the message $|M|$: $x_0 = IV \quad x_i = h(x_{i-1}, m_i) \quad \mathcal{H}(M) = h(x_{L-1}, m_L)$

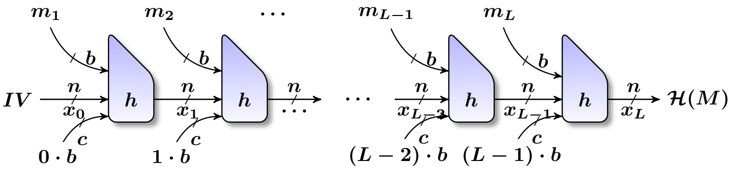


Underlying Construction - Iterative Hash Functions

- The Merkle-Damgård construction (MD) [Dam89; Mer89]:
  Padding and dividing $M = m_1 \| m_2 \| \cdots \| m_L$, where m_L is encoded with the length the message $|M|$: $x_0 = IV \quad x_i = h(x_{i-1}, m_i) \quad \mathcal{H}(M) = h(x_{L-1}, m_L)$

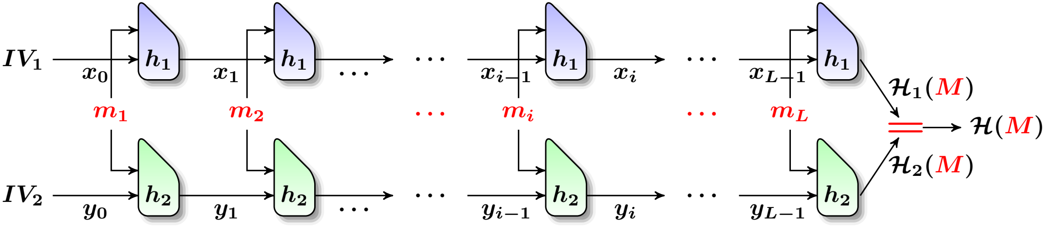


- The HAIFA construction [BD07]:
  $x_0 = IV_m \quad x_{i+1} = h_i(x_i, m_i, \#bits, salt) \quad \mathcal{H}(M) = g(x_{l+1}, |M|')$

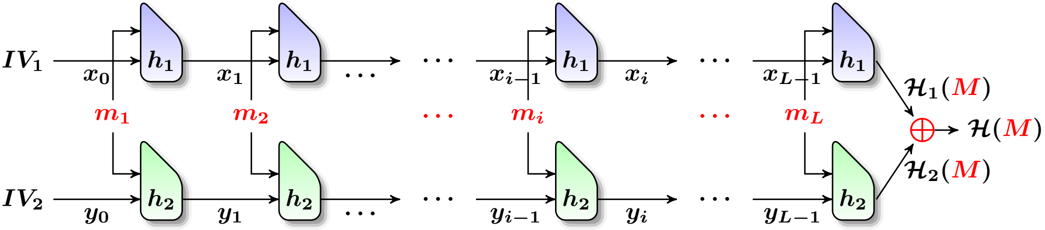


Our Focus: Combiners of Iterative Hash Functions – Parallel

- Concatenation combiner: $\mathcal{C}^{\mathcal{H}_1,\mathcal{H}_1}(M) = \mathcal{H}_1(M) \parallel \mathcal{H}_2(M)$



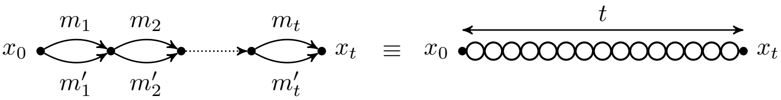
- XOR combiner: $\mathcal{C}^{\mathcal{H}_1,\mathcal{H}_1}(M) = \mathcal{H}_1(M) \oplus \mathcal{H}_2(M)$



Outline

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

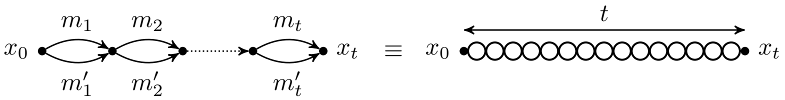
- Get 2^t-multi-collision by successively applying birthday attack t times. Cplx $t \cdot 2^{n/2}$.



denoted by $\mathcal{M}_{\mathtt{MC}}$

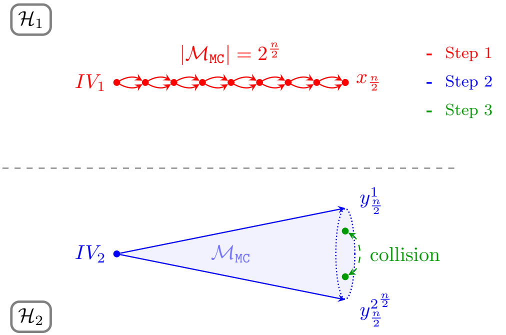
Joux's Multi-collisions (JM [Jou04])

- Get 2^t-multi-collision by successively applying birthday attack t times. Cplx $t \cdot 2^{n/2}$.

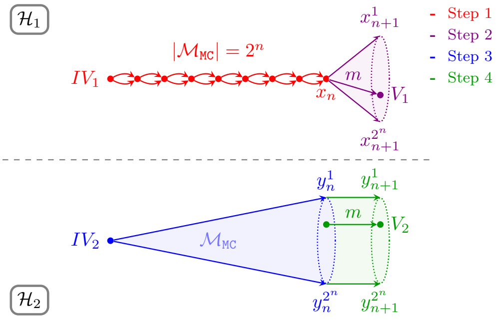


denoted by $\mathcal{M}_{\text{MC}}$

- Attacks on concatenation combiner using Joux's Multi-collisions



(a) Collision attack. Cplx: $n \cdot 2^{n/2}$



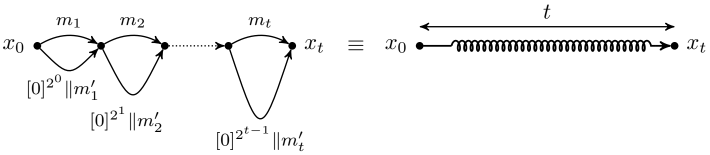
(b) Preimage attack. Cplx: $n \cdot 2^n$

Attacks on Concatenation Combiner (JM [Jou04])

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	2^n
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD / HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^{2n}~~ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
MD / HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n

Expandable Message (EM [DA99; KS05])

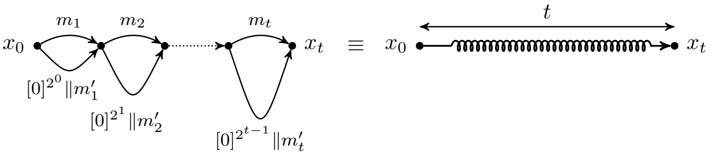
- Get 2^t colliding messages whose lengths cover the whole range of $t + [0, 2^t - 1]$ by iteratively generating t collisions with message fragments of carefully chosen length.
  Cplx $2^t + t \cdot 2^{n/2}$



denoted by $\mathcal{M}_{\mathtt{EM}}$

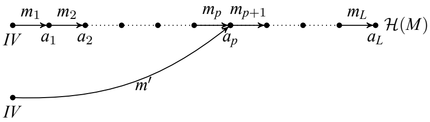
Expandable Message (EM [DA99; KS05])

- Get 2^t colliding messages whose lengths cover the whole range of $t + [0, 2^t - 1]$ by iteratively generating t collisions with message fragments of carefully chosen length.
  Cplx $2^t + t \cdot 2^{n/2}$

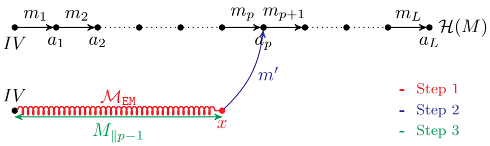


denoted by $\mathcal{M}_{\mathtt{EM}}$

- The long message 2nd-preimage attack on MD Hash using expandable message.
  Cplx: $\max(2^n/L, 2^t + t \cdot 2^{n/2})$.



(a) Foiled by MD message length padding



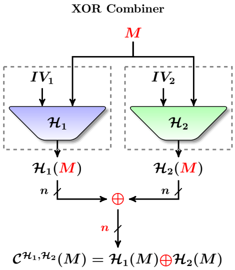
(b) Using Kelsey and Schneier's EM [KS05]

Second Preimage Attack on Single MD Hash Using Expandable Message [DA99; KS05]

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD / HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^{2n}~~ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
MD / HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n

Outline

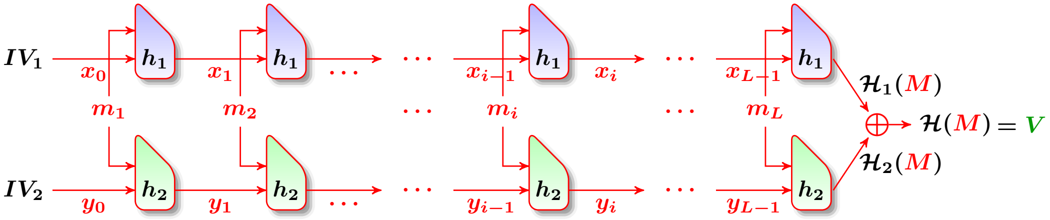
Preimage Attacks on XOR Combiners



(collision $2^{n/2}$, 2nd-preimage 2^n, preimage 2^n)

Goal of the attack

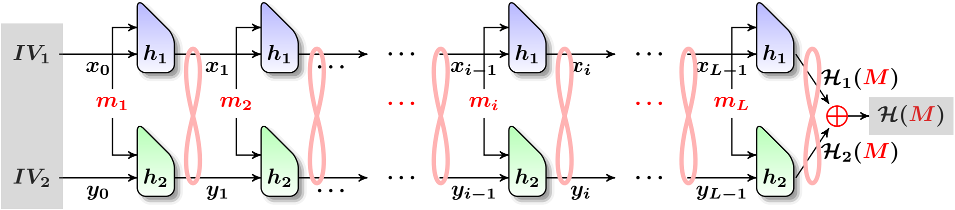
Given an n-bit target V, find the message M, s.t., $\mathcal{H}_1(M) \oplus \mathcal{H}_2(M) = V$, with Cplx $\ll 2^n$



Preimage Attacks on XOR Combiners

Goal of the attack

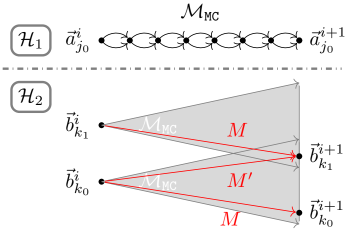
Given an n-bit target V, find the message $\boldsymbol{M}$, s.t., $\mathcal{H}_1(\boldsymbol{M}) \oplus \mathcal{H}_2(\boldsymbol{M}) = V$, with Cplx $\ll 2^n$



Interchange Structure

- Breaking the pairwise relation between internal states of hash computations which share the same input message by a sequences of switches - an interchange structure

Build Switches for Interchange Structure



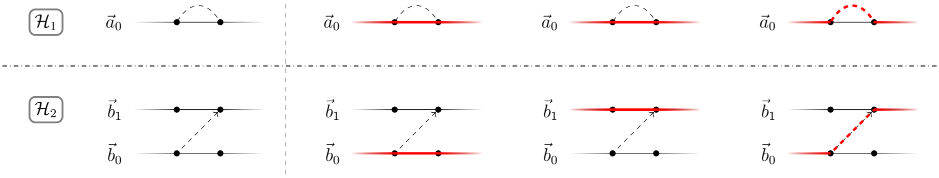
$$\vec{a}^{i+1}_{j_0} = h_1^*(\vec{a}^{i}_{j_0}, M_i) = h_1^*(\vec{a}^{i}_{j_0}, M'_i)$$

$$\vec{b}^{i+1}_{k_1} = h_2^*(\vec{b}^{i}_{k_1}, M_i) = h_2^*(\vec{b}^{i}_{k_0}, M'_i)$$

$$\vec{b}^{i+1}_{k_0} = h_2^*(\vec{b}^{i}_{k_0}, M_i) \neq \vec{b}^{i+1}_{k_1}$$

Building a single switch Cplx: $n \cdot 2^{\frac{n}{2}}$

First, M and M' are selected from $\mathcal{M}_{\mathtt{MC}}$ to generate a collision (defining the new $\vec{b}_{k_1}$), then $\vec{b}_{k_0}$ is evaluated using M.



A single swich:

$(\vec{a}_0, \vec{b}_0) \overset{M}{\rightsquigarrow} (\vec{a}_0, \vec{b}_0)$ normal transition

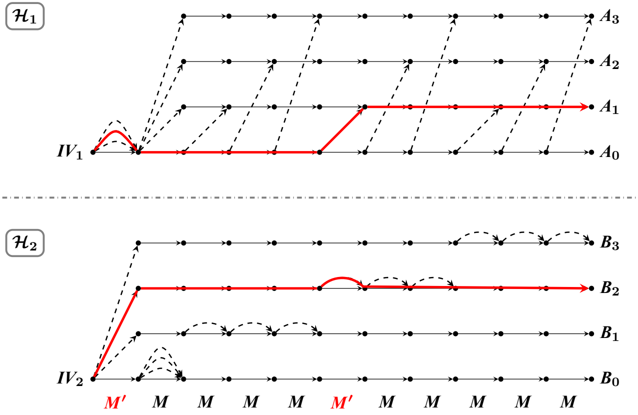
$(\vec{a}_0, \vec{b}_1) \overset{M}{\rightsquigarrow} (\vec{a}_0, \vec{b}_1)$ normal transition

$(\vec{a}_0, \vec{b}_0) \overset{M'}{\rightsquigarrow} (\vec{a}_0, \vec{b}_1)$ jump transition

Jump from $(\vec{a}_0, \vec{b}_0)$ to $(\vec{a}_0, \vec{b}_1)$ by using M' (dashed lines) instead of M (solid lines).

Interchange Structure (IS)

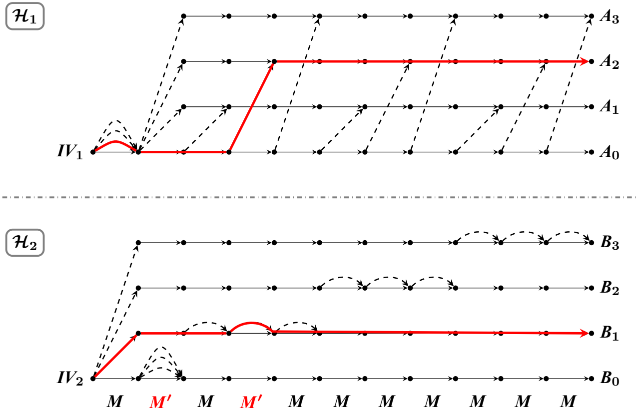
- The interchange structure has starting points IV_1 and IV_2, and ending points $\{A_j \mid j = 0 \ldots 2^t - 1\}$ and $\{B_k \mid k = 0 \ldots 2^t - 1\}$, s.t., for any state pair (A_j, B_k), one can easily select a message mapping (IV_1, IV_2) to it.



(A_1, B_2)

Interchange Structure (IS)

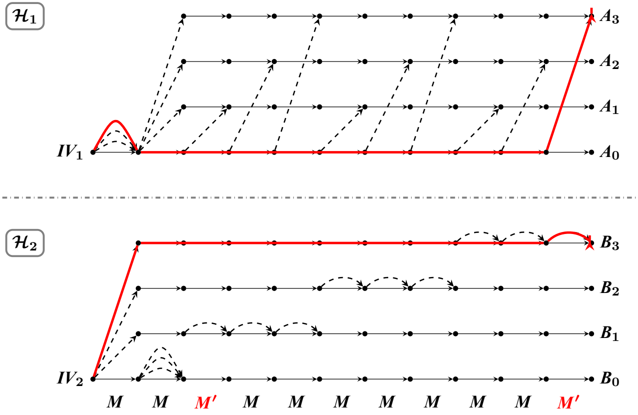
- The interchange structure has starting points IV_1 and IV_2, and ending points $\{A_j \mid j = 0 \ldots 2^t - 1\}$ and $\{B_k \mid k = 0 \ldots 2^t - 1\}$, s.t., for any state pair (A_j, B_k), one can easily select a message mapping (IV_1, IV_2) to it.



(A_2, B_1)

Interchange Structure (IS)

- The interchange structure has starting points IV_1 and IV_2, and ending points $\{A_j \mid j = 0 \ldots 2^t - 1\}$ and $\{B_k \mid k = 0 \ldots 2^t - 1\}$, s.t., for any state pair (A_j, B_k), one can easily select a message mapping (IV_1, IV_2) to it.

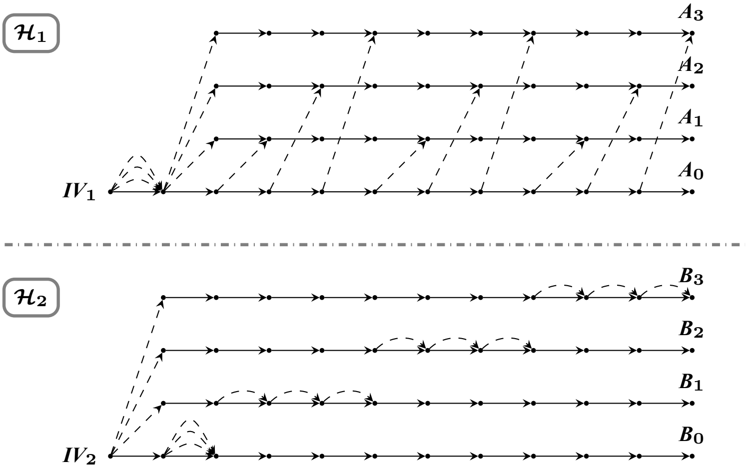


Can be applied to any state pair (A_j, B_k) for $j = 0 \cdots 2^t - 1$ and $k = 0 \cdots 2^t - 1$

A 2^t-interchange structure based on switches will need $\Theta(2^{2t})$ switches

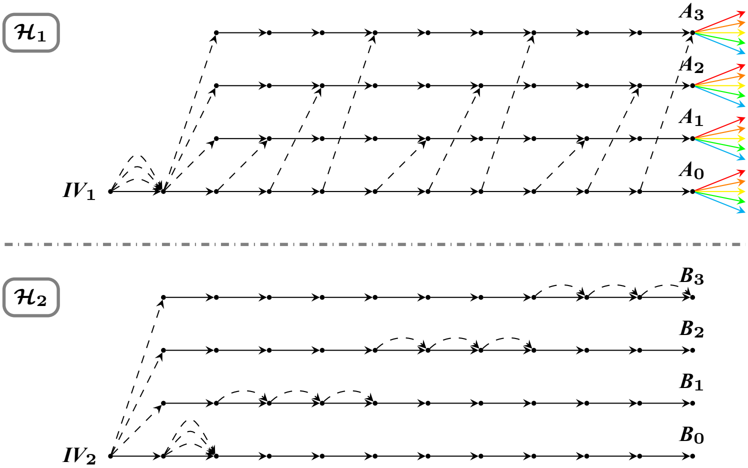
Cplx: $\Theta(2^{2t+n/2})$

Preimage Attacks on XOR Combiner Using Interchange Structure



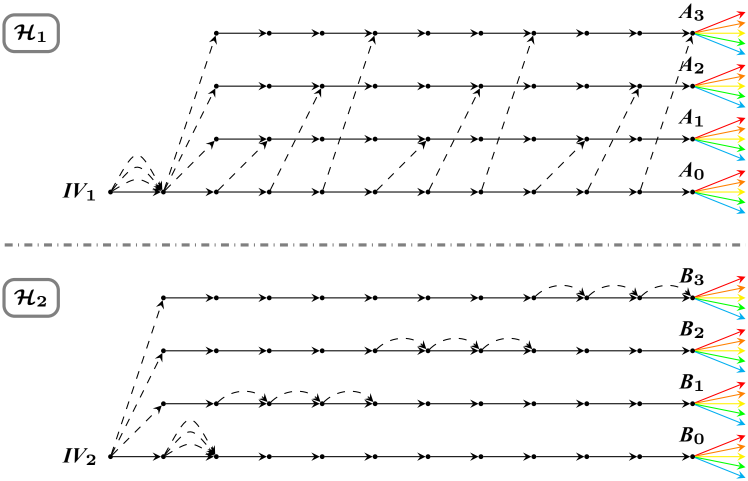
Step 1: $n \cdot 2^{2t+\frac{n}{2}}$

Preimage Attacks on XOR Combiner Using Interchange Structure



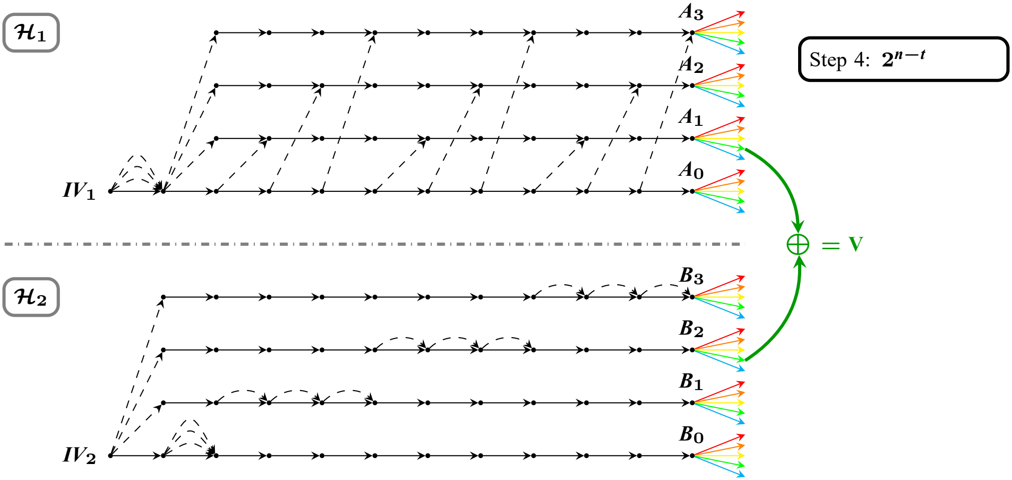
Step 2: $\mathbf{2^t \cdot 2^{n-2t}}$

Preimage Attacks on XOR Combiner Using Interchange Structure

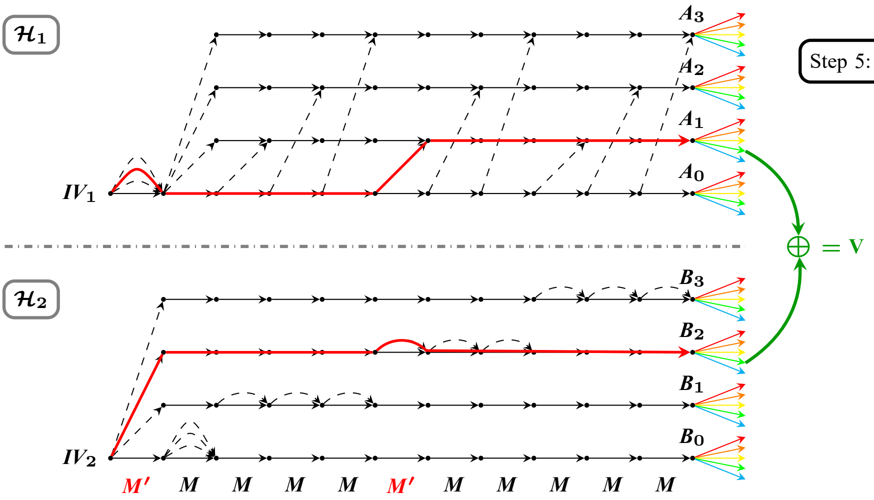


Step 3: $2^t \cdot 2^{n-2t}$

Preimage Attacks on XOR Combiner Using Interchange Structure

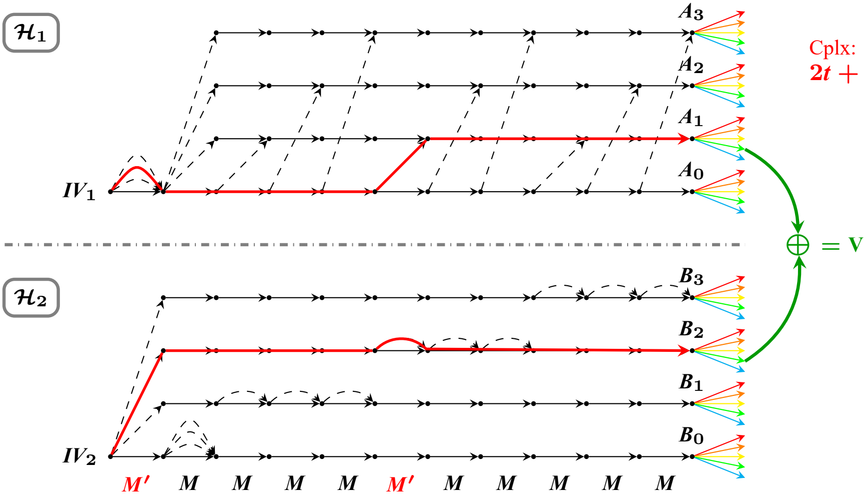


Preimage Attacks on XOR Combiner Using Interchange Structure



Step 5: $n \cdot 2^{2t}$

Preimage Attacks on XOR Combiner Using Interchange Structure



Cplx: $\tilde{O}(2^{\frac{5n}{6}})$

$2t + \frac{n}{2} = n - t$

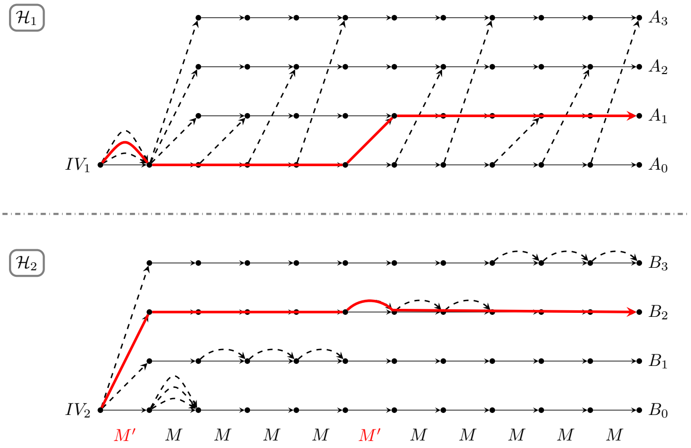
Preimage Attack on XOR Combiner Using Interchange Structure

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD / HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^{2n}~~ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
MD / HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~2^n~~ $\approx 2^{5n/6}$	~~2^n~~ $\approx 2^{5n/6}$

Outline

Interchange Structure (recap)

- The interchange structure has starting points IV_1 and IV_2, and ending points $\{A_j \mid j = 0 \dots 2^t - 1\}$ and $\{B_k \mid k = 0 \dots 2^t - 1\}$, s.t., for any state pair (A_j, B_k), one can easily select a message M mapping (IV_1, IV_2) to it.



Cplx: $\Theta(2^{2t+n/2})$

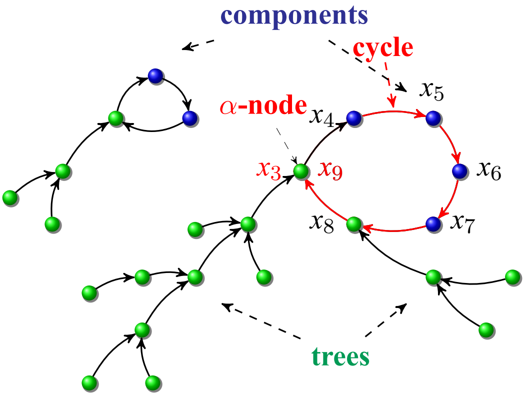
A 2^t-interchange structure based on switches will need $\Theta(2^{2t})$ switches

Total Cplx: $\tilde{O}(2^{5n/6})$

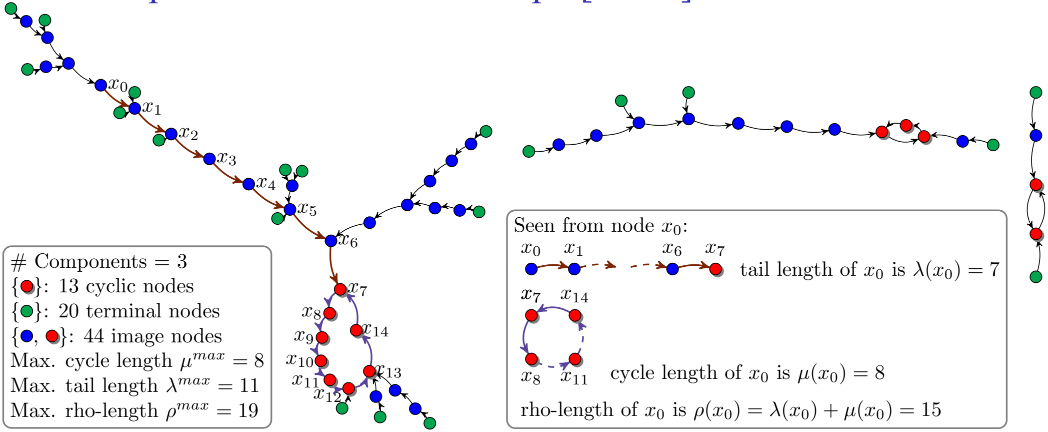
Trade-off: $2^{2t+n/2}$ vs. 2^{n-t}

The Functional Graph of Random Mappings (FG)

- Let $f \xleftarrow{\$} \mathcal{F}_N$, where $\mathcal{F}_N$ is the set of mappings from N-set to N-set ($N = 2^n$).
- The functional graph of f, denoted by $\mathcal{FG}_f$, is a directed graph, whose nodes are $0 \ldots N-1$ and edges are $\langle x, f(x) \rangle$

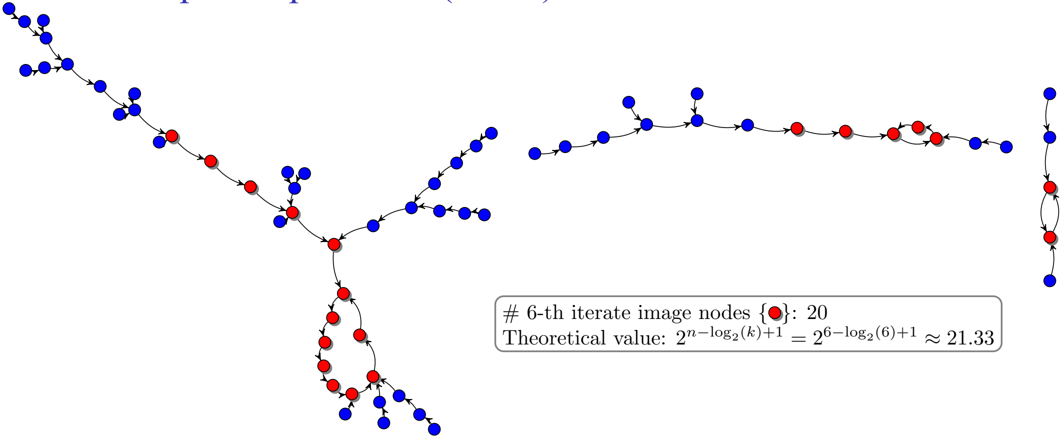


Statistical Properties of Functional Graph [FO89]



- # Components: $0.5 \cdot n$
- # Cyclic nodes: $1.2 \cdot 2^{n/2}$
- # Terminal nodes: $0.37 \cdot 2^n$
- # Image notes: $0.62 \cdot 2^n$
- # k-th iterate image notes: $(1 - \tau_k)N$
  where the τ_k satisfies the recurrence $\tau_0 = 0, \tau_{k+1} = e^{-1+\tau_k}$.

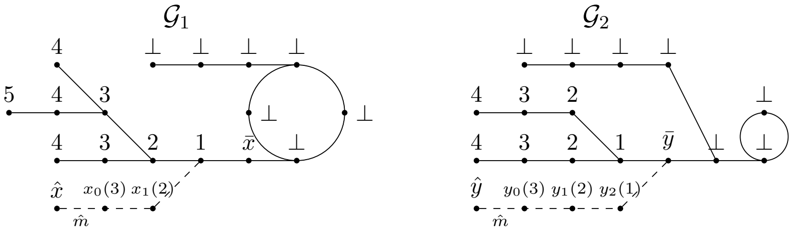
Functional Graph Deep Iterates (FGDI)



- Observation 1: It is easy to get a large set of deep iterates: $T : 2^t$, $M : 2^t$, $D : 2^t$
- Observation 2: A deep iterate has a relatively high probability to be reached from a randomly selected starting node.

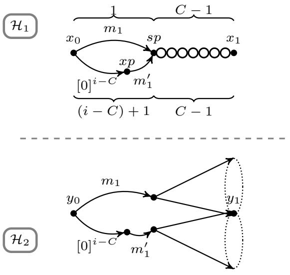
Functional Graph Deep Iterates (FGDI)

- The probability that a deep iterate $\bar{x}$ (resp. $\bar{y}$) will be encountered at distance d from randomly chosen node x_0 (resp. y_0) is $\Pr[f_1^d(x_0) = \bar{x}] \approx d \cdot 2^{-n}$ (resp. $\Pr[f_2^d(y_0) = \bar{y}] \approx d \cdot 2^{-n}$).
  Thus, $\Pr[f_1^d(x_0) = \bar{x} \bigwedge f_2^d(y_0) = \bar{y}] \approx (d \cdot 2^{-n})^2$ due to the independence of f_1 and f_2.
- The probability that a pair of 2^g-th iterates $\bar{x}$ and $\bar{y}$ will be encountered at the same distance is approximately $(2^g)^3 \cdot 2^{-2n} = 2^{3g-2n}$ $(g \leq n/2)$.
  One need to compute $\approx 2^{2n-3g}$ chains from different starting points to find one pair of starting points reaching the pair of 2^g-th iterates $(\bar{x}, \bar{y})$ at the same distance.

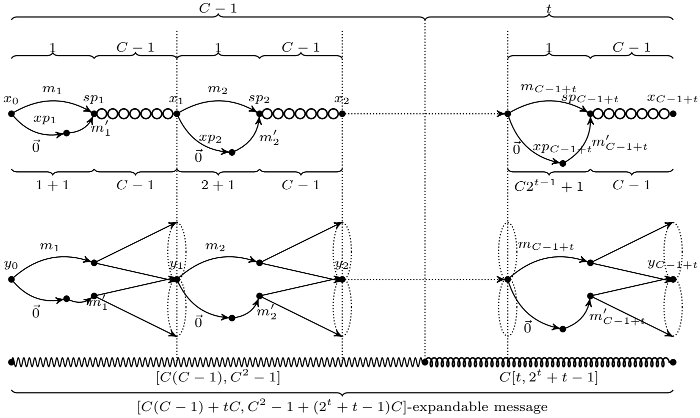


Simultaneous Expandable Message (SEM)

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



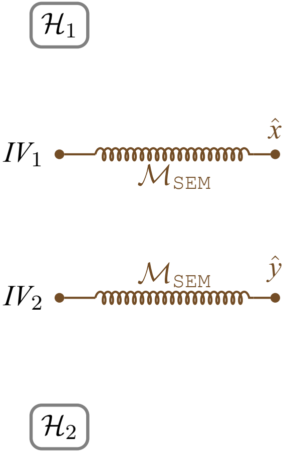
(a) A building module



(b) The full construction

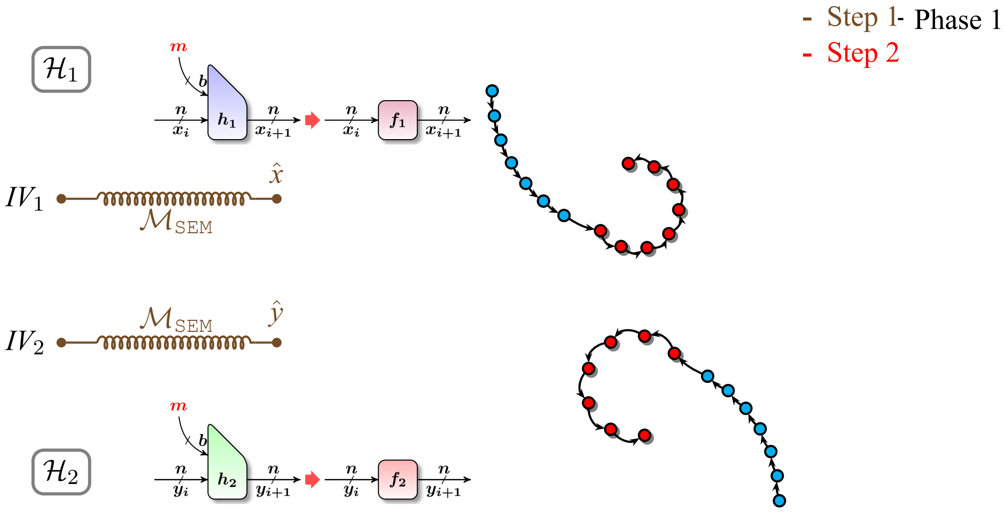
Improved Preimage Attack on XOR Combiners Based on FGDI

- Step 1- Phase 1



Phase 1: $2^\ell + n^2 \cdot 2^{n/2}$

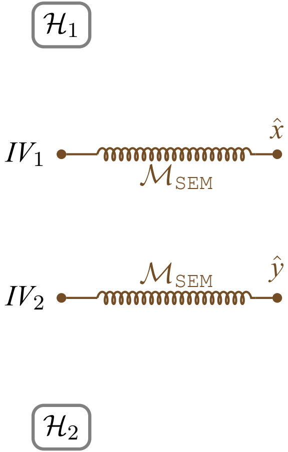
Improved Preimage Attack on XOR Combiners Based on FGDI

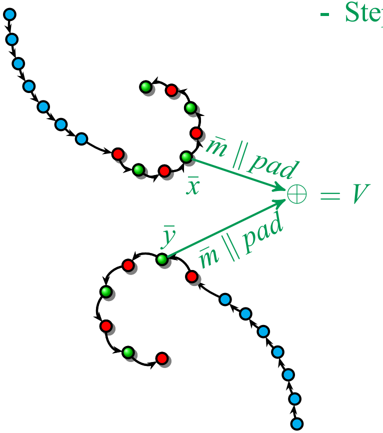


Phase 1: $2^\ell + n^2 \cdot 2^{n/2}$

Improved Preimage Attack on XOR Combiners Based on FGDI

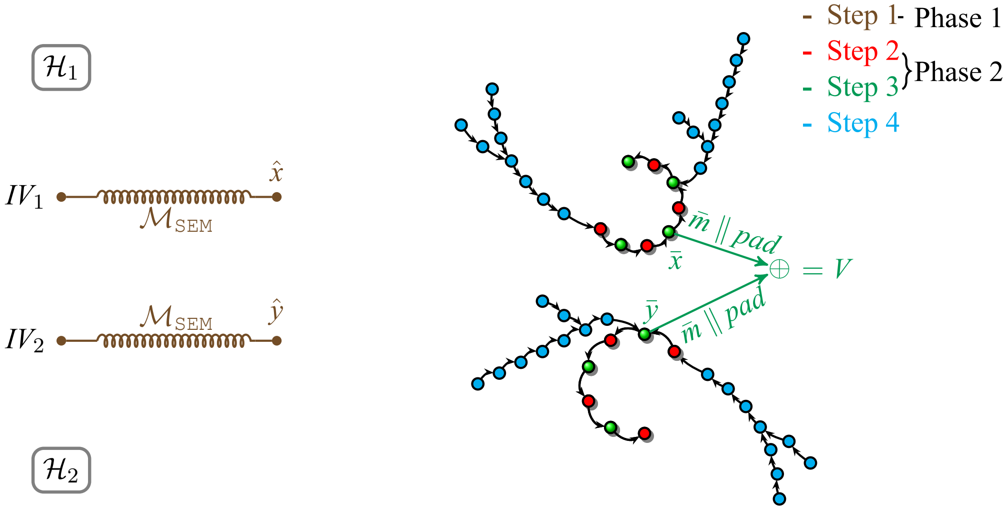
- Step 1- Phase 1
- Step 2 } Phase 2
- Step 3





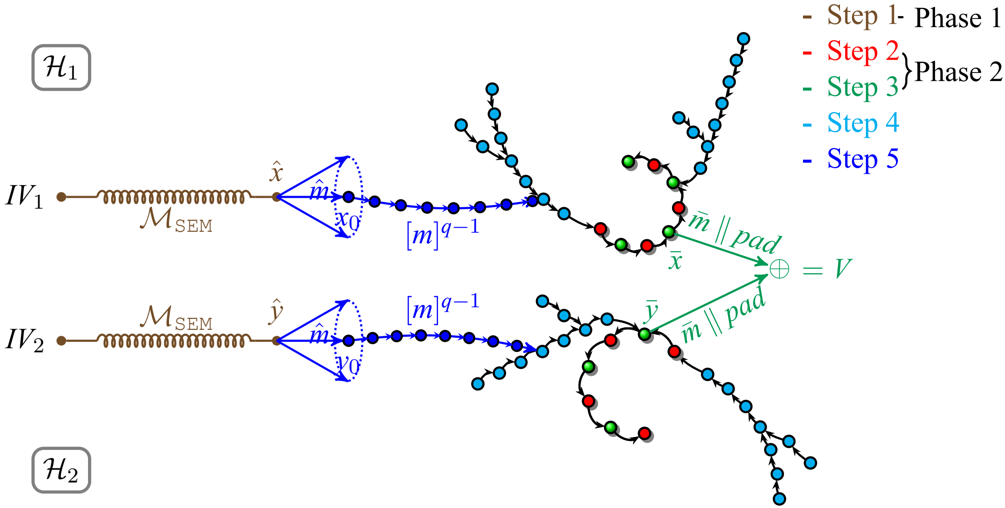
Phase 1: $2^{\ell} + n^2 \cdot 2^{n/2}$ **Phase 2:** 2^{g+s}

Improved Preimage Attack on XOR Combiners Based on FGDI



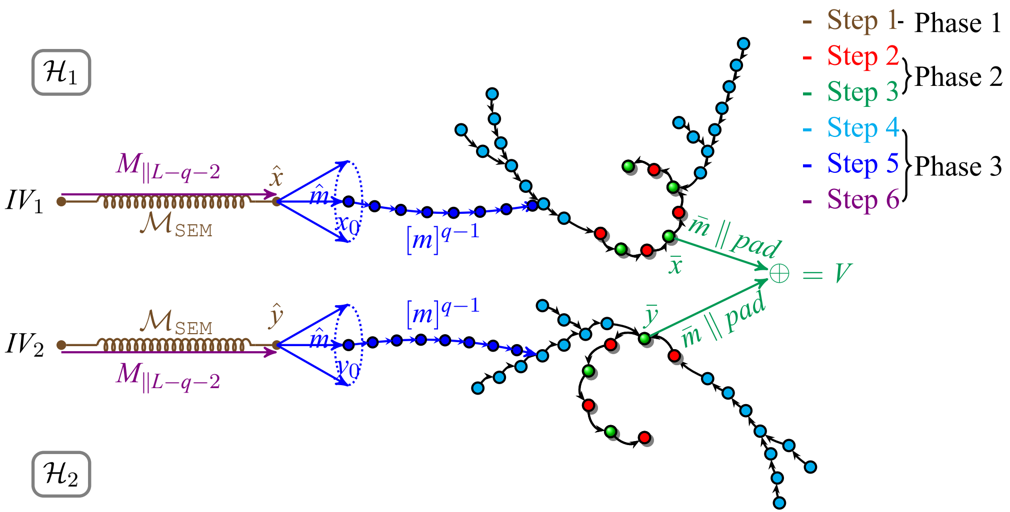
Phase 1: $2^\ell + n^2 \cdot 2^{n/2}$ **Phase 2:** 2^{g+s}

Improved Preimage Attack on XOR Combiners Based on FGDI



Phase 1: $2^{\ell} + n^2 \cdot 2^{n/2}$ **Phase 2:** 2^{g+s}

Improved Preimage Attack on XOR Combiners Based on FGDI

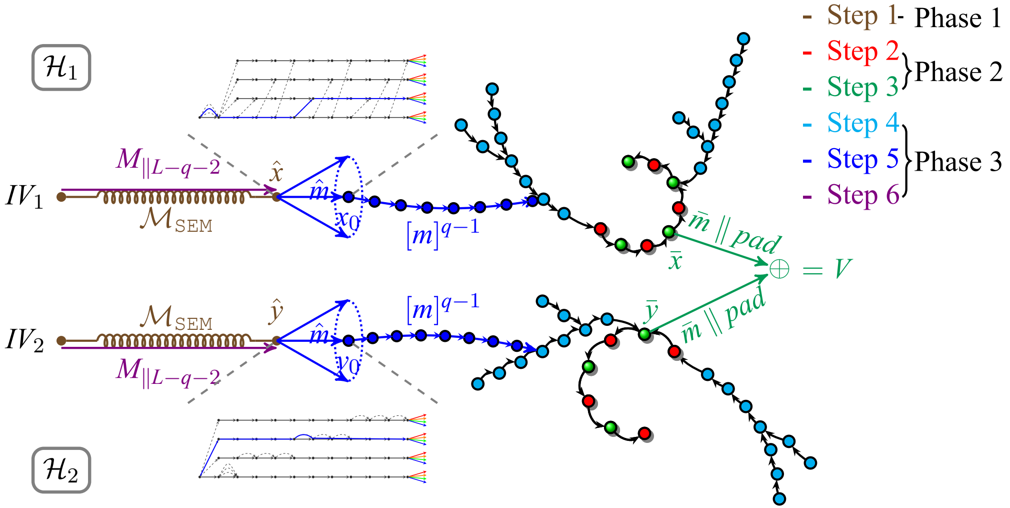


Phase 1: $2^{\ell} + n^2 \cdot 2^{n/2}$ **Phase 2:** 2^{g+s} **Phase 3:** $2^{3n/2-3g/2-s/2} + 2^{5n/2-9g/2-3s/2+\ell} + 2^{n-2g+\ell}$

Improved Preimage Attack on XOR Combiners Based on FGDI

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD / HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^{2n}~~ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~2^n~~ $\approx 2^{5n/6}$	~~2^n~~ $\approx 2^{5n/6}$
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~$2^{5n/6}$~~ $\approx 2^{2n/3}$	~~$2^{5n/6}$~~ $\approx 2^{2n/3}$

Improved Preimage Attack on XOR Combiners Based on FGDI



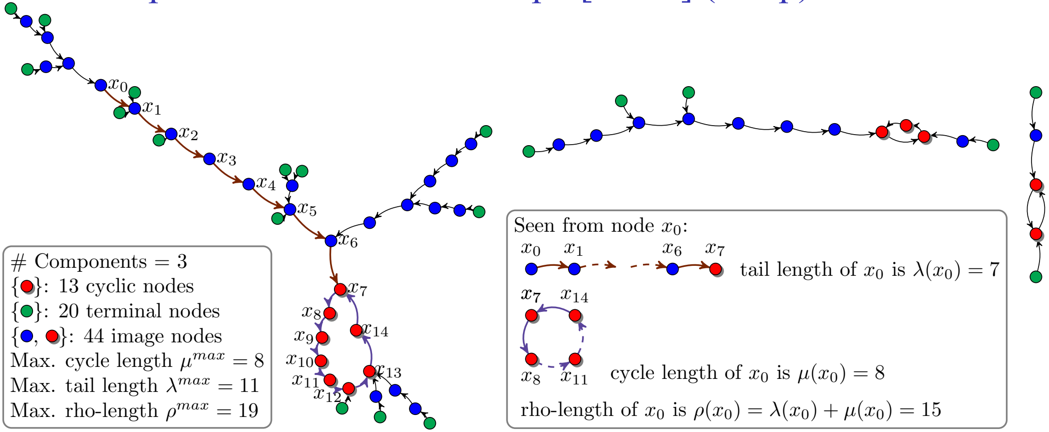
Phase 1: $2^{\ell} + n^2 \cdot 2^{n/2}$ **Phase 2:** 2^{g+s} **Phase 3:** $2^{3n/2-3g/2-s/2} + 2^{5n/2-9g/2-3s/2+\ell} + 2^{n-2g+\ell}$

Improved Preimage Attack on XOR Combiners Based on FGDI

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	$\not{2}^n$ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD / HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	$\not{2}^n$ $\approx 2^{n/2}$	$\not{2}^{2n}$ $\approx 2^n$	$\not{2}^{2n}$ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	$\not{2}^n$ $\approx 2^{5n/6}$	$\not{2}^n$ $\approx 2^{5n/6}$
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	$\not{2}^{5n/6}$ $\approx 2^{2n/3} \Rightarrow 2^{9n/14}$	$\not{2}^{5n/6}$ $\approx 2^{2n/3} \Rightarrow 2^{9n/14}$

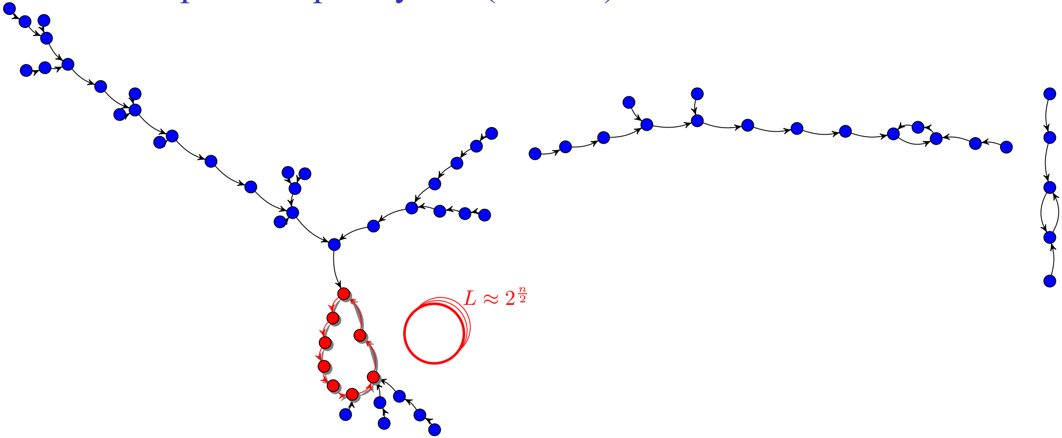
Outline

Statistical Properties of Functional Graph [FO89] (recap)



- $\mathbf{E}\{\mu^{max} \mid \mathcal{F}_N\} = 0.78 \cdot 2^{n/2}$
- $\mathbf{E}\{\lambda^{max} \mid \mathcal{F}_N\} = 1.74 \cdot 2^{n/2}$
- $\mathbf{E}\{\rho^{max} \mid \mathcal{F}_N\} = 2.41 \cdot 2^{n/2}$
- $\mathbf{E}\{\text{tree}^{largest} \mid \mathcal{F}_N\} = 0.48 \cdot 2^{n}$
- $\mathbf{E}\{\text{component}^{largest} \mid \mathcal{F}_N\} = 0.76 \cdot 2^{n}$

Functional Graph Multiple Cycles (FGMC)



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

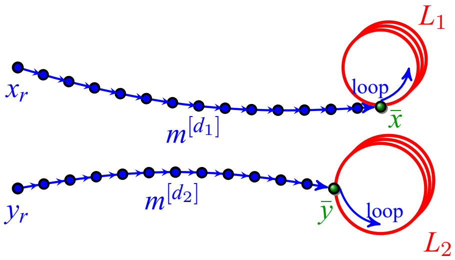
Functional Graph Multi-cycles (FGMC)

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

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

$$\Downarrow$$

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



Functional Graph Multi-cycles (FGMC)

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

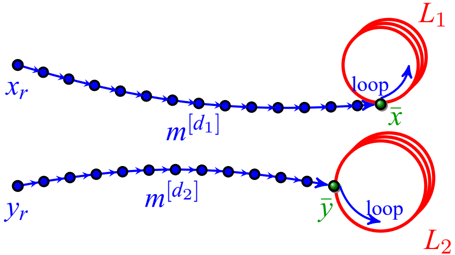
$$f_2^{d_2}(y_r) = \bar{y},\ f_2^{L_2}(\bar{y}) = \bar{y} \quad \Rightarrow \quad f_2^{d_2+j\cdot L_2}(y_r) = \bar{y} \text{ for } \forall\, j$$

$$\Downarrow$$

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

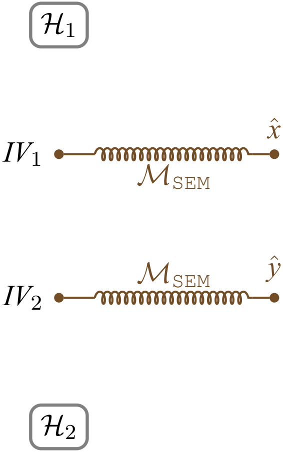
correctable distance bias

the probability of reaching $(\bar{x}, \bar{y})$ from a random pair at a common distance is amplified by roughly t times, where t is the number of cycles to the maximum.



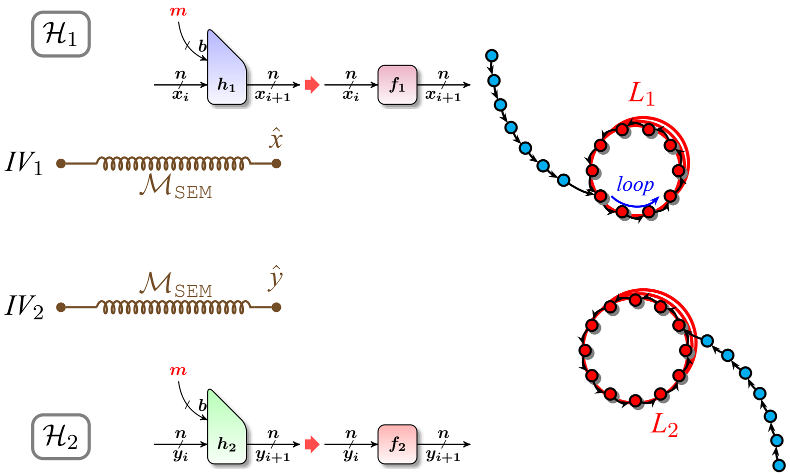
Improved Preimage Attack on XOR Combiners Based on FGMC

- Step 1 - $L + n^2 \cdot 2^{n/2}$



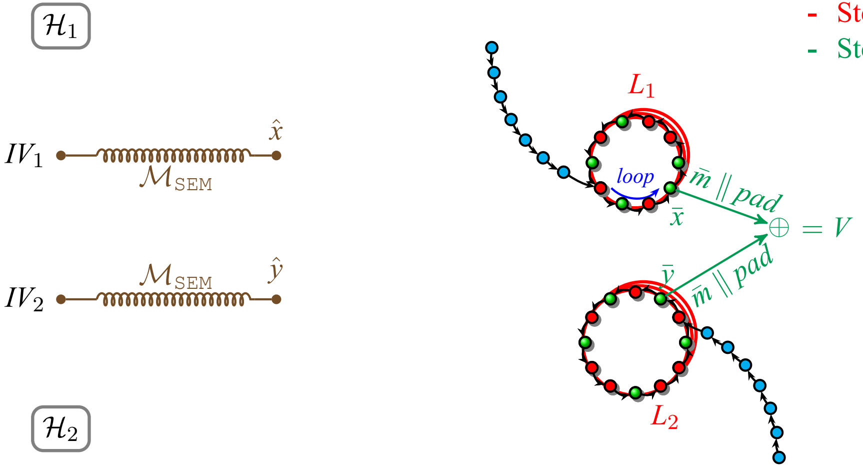
Improved Preimage Attack on XOR Combiners Based on FGMC

- Step 1 - $L + n^2 \cdot 2^{n/2}$
- Step 2 - $2^{n/2}$



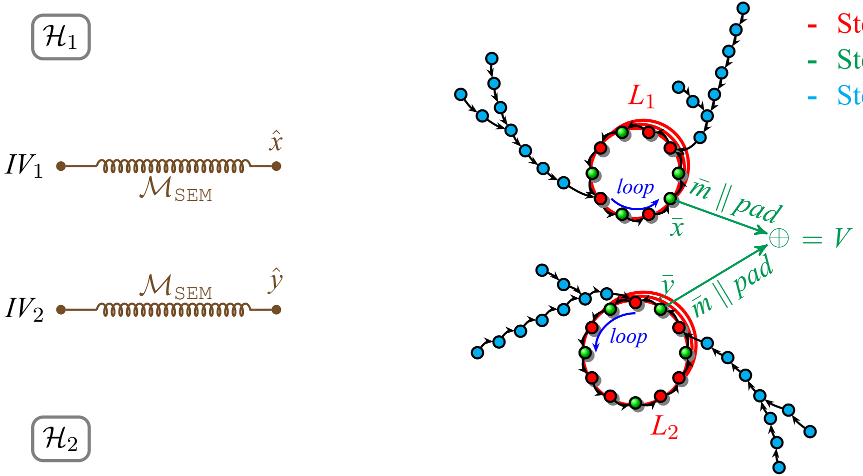
Improved Preimage Attack on XOR Combiners Based on FGMC

- Step 1 - $L + n^2 \cdot 2^{n/2}$
- Step 2 - $2^{n/2}$
- Step 3 - $2^{s+n/2}$



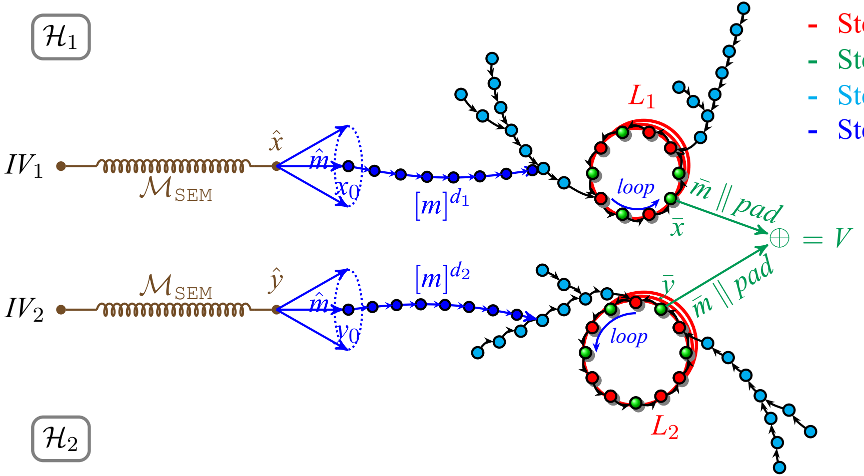
Improved Preimage Attack on XOR Combiners Based on FGMC

- Step 1 - $L + n^2 \cdot 2^{n/2}$
- Step 2 - $2^{n/2}$
- Step 3 - $2^{s+n/2}$
- Step 4 - $2^t + 2^{n/2}$



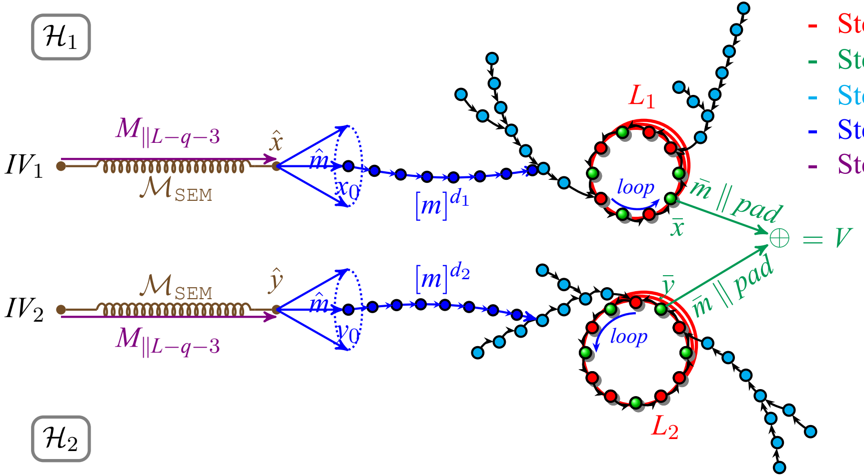
Improved Preimage Attack on XOR Combiners Based on FGMC

- Step 1 - $L + n^2 \cdot 2^{n/2}$
- Step 2 - $2^{n/2}$
- Step 3 - $2^{s+n/2}$
- Step 4 - $2^t + 2^{n/2}$
- Step 5 - $2^{2n-t-s}/L$

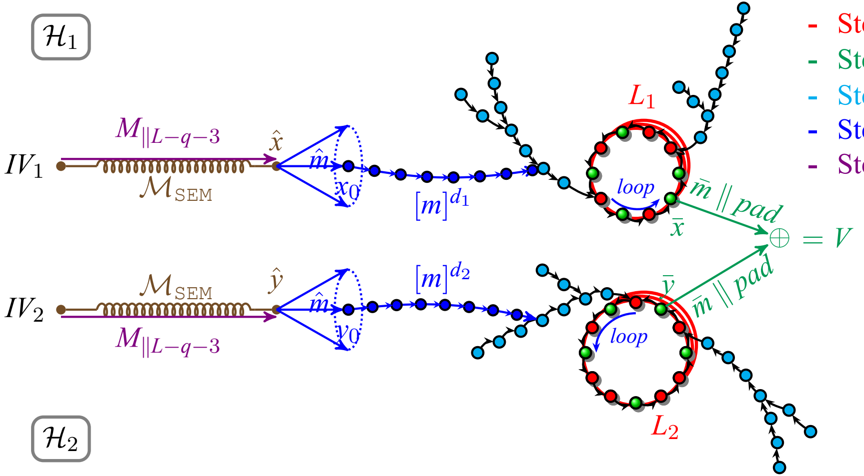


Improved Preimage Attack on XOR Combiners Based on FGMC

- Step 1 - $L + n^2 \cdot 2^{n/2}$
- Step 2 - $2^{n/2}$
- Step 3 - $2^{s+n/2}$
- Step 4 - $2^t + 2^{n/2}$
- Step 5 - $2^{2n-t-s}/L$
- Step 6 - $\mathcal{O}(L)$



Improved Preimage Attack on XOR Combiners Based on FGMC



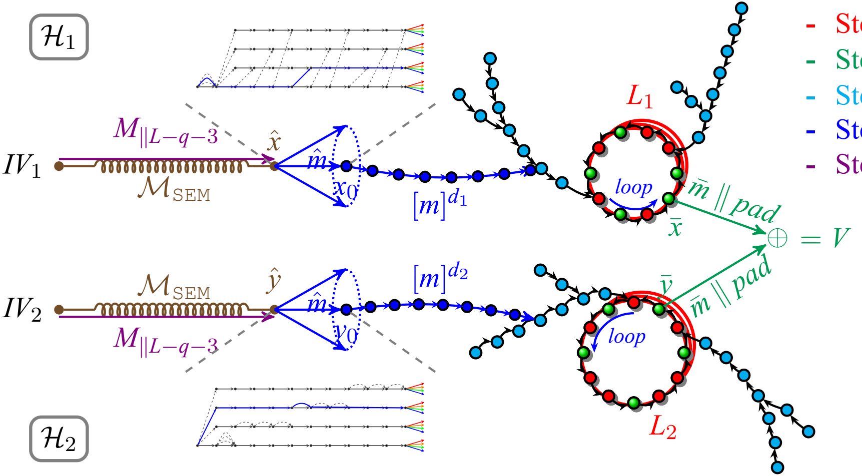
- Step 1 - $L + n^2 \cdot 2^{n/2}$
- Step 2 - $2^{n/2}$
- Step 3 - $2^{s+n/2}$
- Step 4 - $2^t + 2^{n/2}$
- Step 5 - $2^{2n-t-s}/L$
- Step 6 - $\mathcal{O}(L)$

- The overall Cplx: $2^\ell + 2^{s+n/2} + 2^t + 2^t + 2^{n/2} + 2^{2n-t-s-\ell}$
- Search for t and s that give the lowest Cplx, the total Cplx: $2^\ell + 2^{5n/6-\ell/3}$

Improved Preimage Attack on XOR Combiners Based on FGMC

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD / HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^{2n}~~ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~2^n~~ $\approx 2^{5n/6}$	~~2^n~~ $\approx 2^{5n/6}$
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~$2^{2n/3}$~~ $\approx 2^{5n/8}$	~~$2^{2n/3}$~~ $\approx 2^{5n/8}$

Improved Preimage Attack on XOR Combiners Based on FGMC



- Step 1 - $L + n^2 \cdot 2^{n/2}$
- Step 2 - $2^{n/2}$
- Step 3 - $2^{s+n/2}$
- Step 4 - $2^t + 2^{n/2}$
- Step 5 - $2^{2n-t-s}/L$
- Step 6 - $\mathcal{O}(L)$

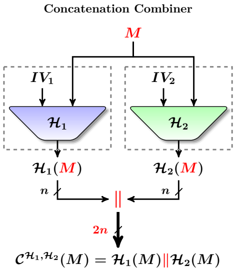
- The overall Cplx: $2^\ell + 2^{s+n/2} + 2^t + 2^t + 2^{n/2} + 2^{2n-t-s-\ell}$
- Search for t and s that give the lowest Cplx, the total Cplx: $2^\ell + 2^{5n/6-\ell/3}$

Improved Preimage Attack on XOR Combiners Based on FGMC

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
MD / HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^{2n}~~ $\approx 2^n$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~2^n~~ $\approx 2^{5n/6}$	~~2^n~~ $\approx 2^{5n/6}$
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~$2^{2n/3}$~~ $\approx 2^{5n/8} \Rightarrow 2^{11n/18}$	~~$2^{2n/3}$~~ $\approx 2^{5n/8} \Rightarrow 2^{11n/18}$

Outline

Second-Preimage Attack on Concatenation Combiner

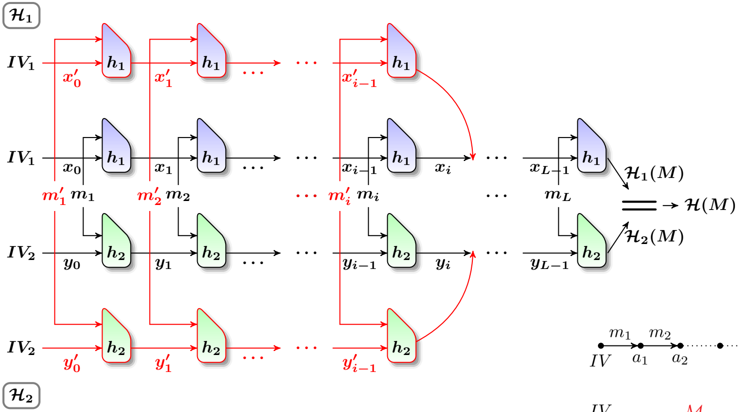


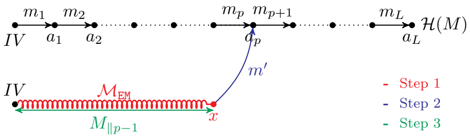
(collision 2^n, 2nd-preimage 2^{2n}, preimage 2^{2n})

Goal of the attack

Given a challenge message $\boldsymbol{M}$, find another message $\boldsymbol{M'}$, s.t.

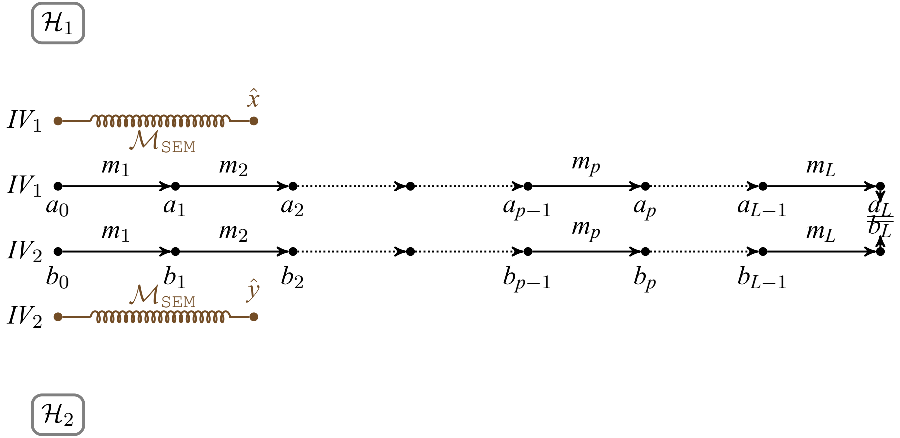
$\mathcal{H}_1(\boldsymbol{M'}) \parallel \mathcal{H}_2(\boldsymbol{M'}) = \mathcal{H}_1(\boldsymbol{M}) \parallel \mathcal{H}_2(\boldsymbol{M})$ with Cplx $\ll 2^n$





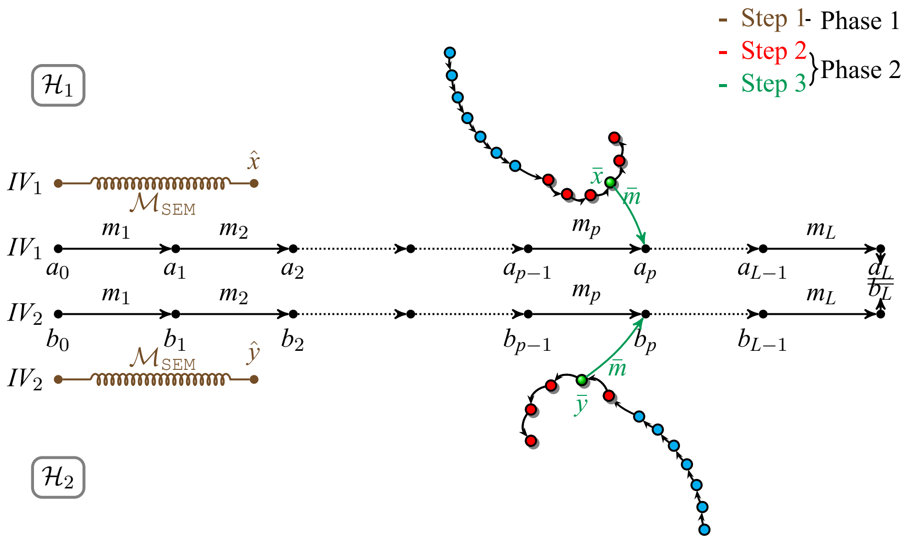
Second-Preimage Attack on Concatenation Combiner Based on FGDI

- Step 1- Phase 1



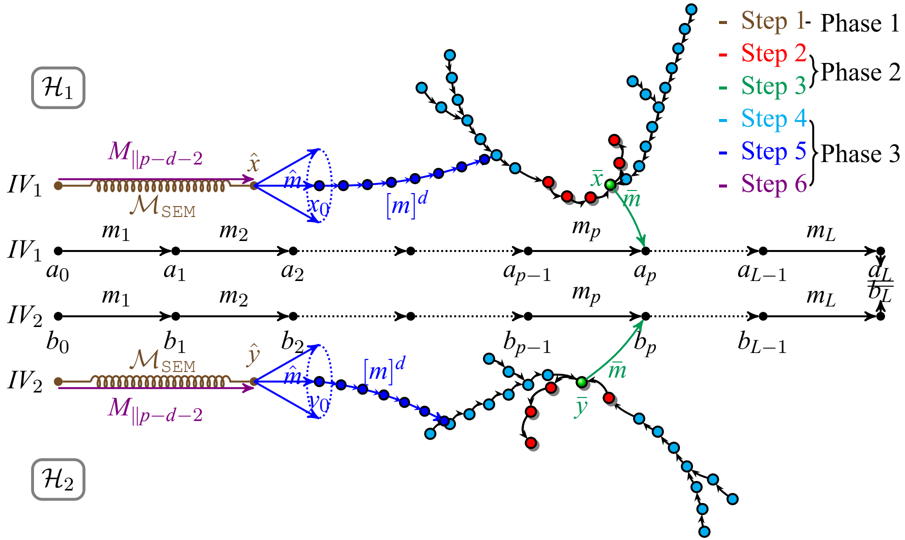
Phase 1: $2^{\ell} + n^2 \cdot 2^{n/2}$

Second-Preimage Attack on Concatenation Combiner Based on FGDI



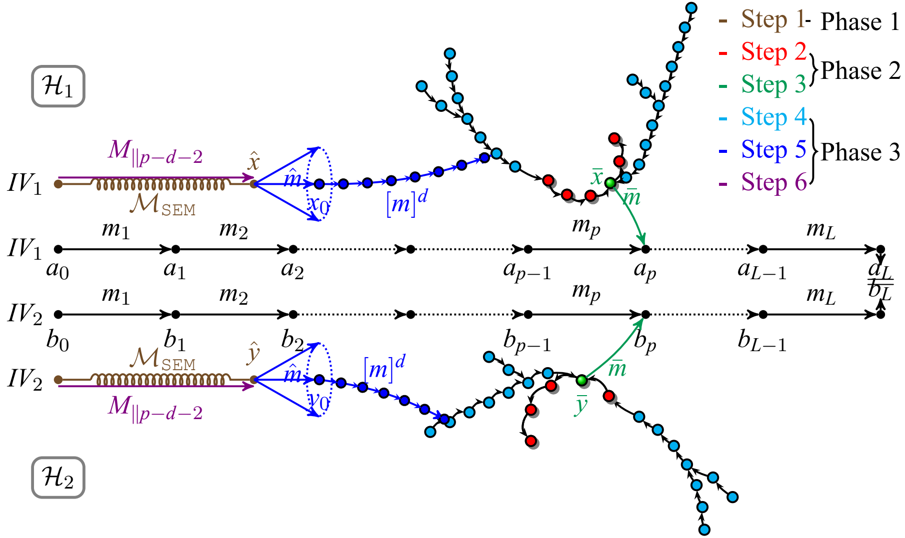
Phase 1: $2^{\ell} + n^2 \cdot 2^{n/2}$ **Phase 2:** $2^{n+g-\ell}$

Second-Preimage Attack on Concatenation Combiner Based on FGDI



Phase 1: $2^{\ell} + n^2 \cdot 2^{n/2}$ **Phase 2:** $2^{n+g-\ell}$ **Phase 3:** $2^{3n/2-3g/2}$

Second-Preimage Attack on Concatenation Combiner Based on FGDI

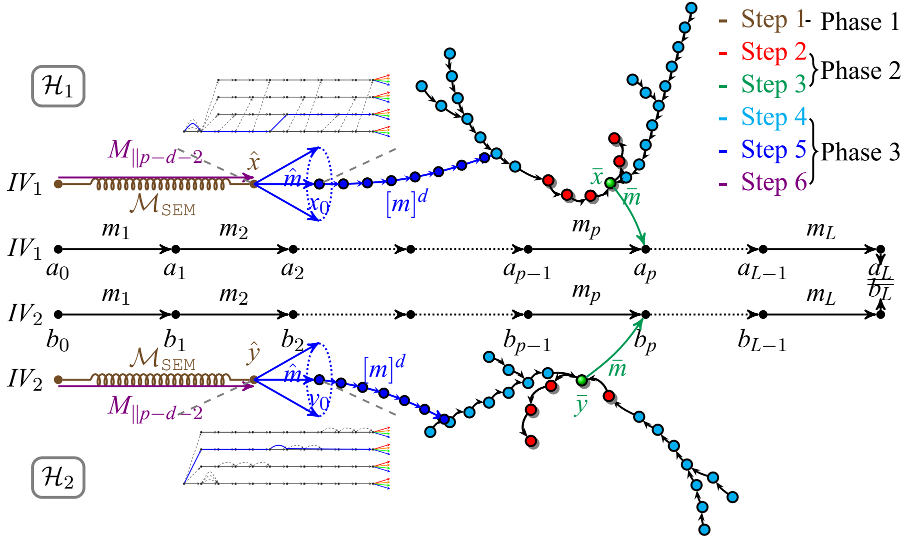


Phase 1: $2^\ell + n^2 \cdot 2^{n/2}$ **Phase 2:** $2^{n+g-\ell}$ **Phase 3:** $2^{3n/2-3g/2}$ Cplx: $2^{6n/5-3\ell/5}$ for $l < 3n/4$

Second-Preimage Attack on Concatenation Combiner Based on FGDI

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^{2n}~~ $\approx 2^n$
MD $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^n~~ $\approx 2^{3n/4}$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~2^n~~ $\approx 2^{5n/6}$	~~2^n~~ $\approx 2^{5n/6}$
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~2^n~~ $\approx 2^{5n/8}$	~~2^n~~ $\approx 2^{5n/8}$

Second-Preimage Attack on Concatenation Combiner Based on FGDI



Phase 1: $2^{\ell} + n^2 \cdot 2^{n/2}$ **Phase 2:** $2^{n+g-\ell}$ **Phase 3:** $2^{3n/2-3g/2}$ Cplx: $2^{6n/5-3\ell/5}$ for $l < 3n/4$

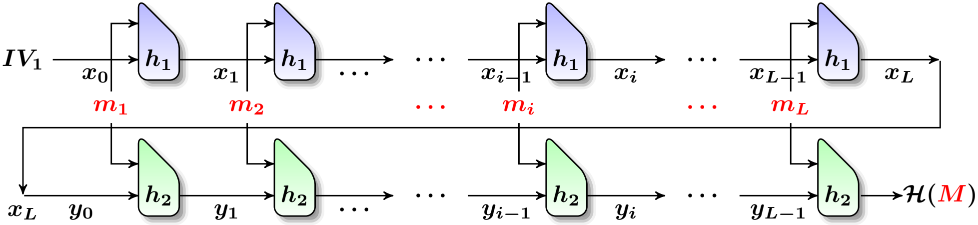
Second-Preimage Attack on Concatenation Combiner Based on FGDI

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \parallel \mathcal{H}_2$	2^n	2^{2n}	2^{2n}
HAIFA $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^{2n}~~ $\approx 2^n$
MD $\mathcal{H}_1 \parallel \mathcal{H}_2$	~~2^n~~ $\approx 2^{n/2}$	~~2^{2n}~~ $\approx 2^n$	~~2^n~~ $\approx 2^{3n/4} \Rightarrow 2^{25n/34}$
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	2^n	2^n
HAIFA $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~2^n~~ $\approx 2^{5n/6}$	~~2^n~~ $\approx 2^{5n/6}$
MD $\mathcal{H}_1 \oplus \mathcal{H}_2$	$2^{n/2}$	~~2^n~~ $\approx 2^{5n/8}$	~~2^n~~ $\approx 2^{5n/8}$

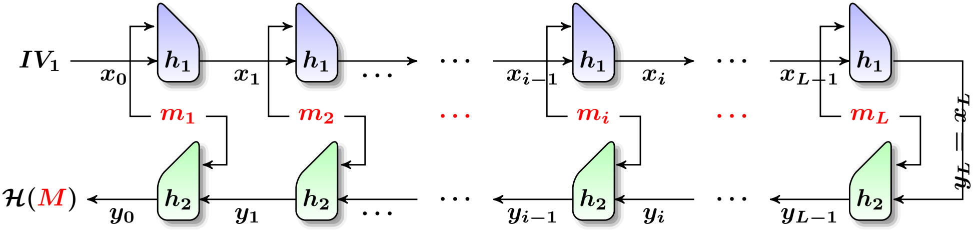
Outline

Combiners of Iterative Hash Functions - Cascade

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



- Zipper Hash: $\mathcal{C}^{\mathcal{H}_1,\mathcal{H}_1}(M) = \mathcal{H}_2(\mathcal{H}_1(IV, M), \overleftarrow{M})$

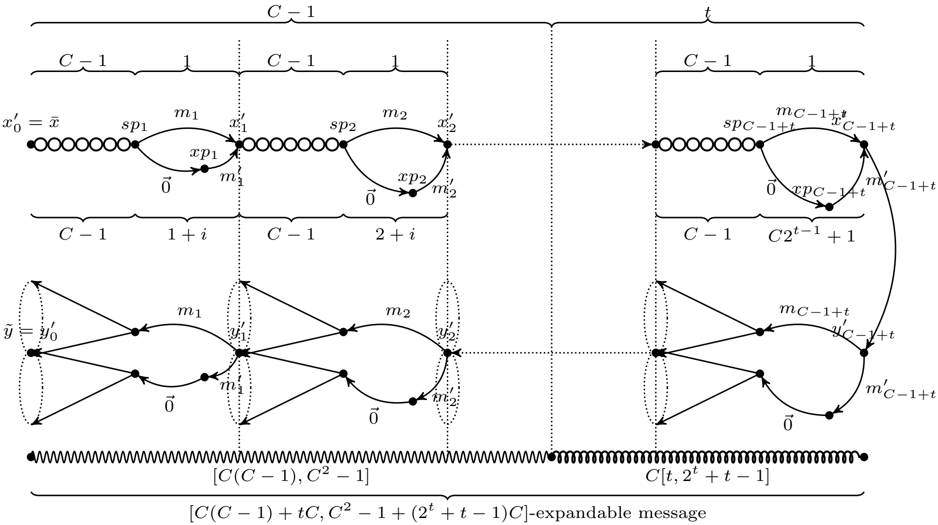


Second-Preimage Attack on the Zipper Hash

There are two main differences between the attack on the Zipper hash and the 2nd-preimage attack on concatenation combiners and the preimage attacks on XOR combiners.

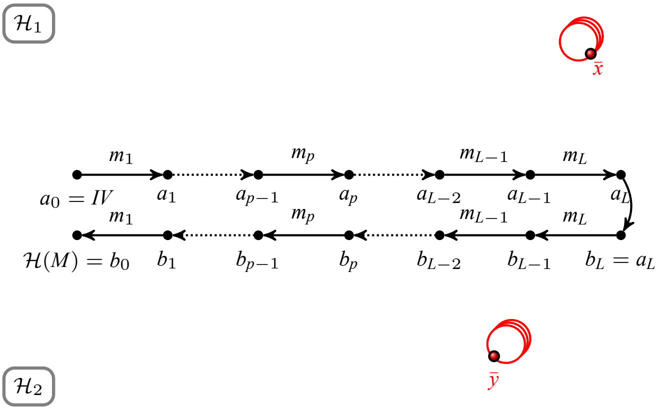
- One is that linking random starting node $\tilde{x}$ to targeted deep-iterate $\bar{x}$ and random starting node $\tilde{y}$ to targeted deep-iterate $\bar{y}$ can be carried out independently, resulting in a meet-in-the-middle-like effect.
- The other is that the message length is embedded inside the expandable message $\mathcal{M}_{\texttt{SEM}}$, which enables to choose the length of second preimage to optimize the complexity.

Simultaneous Expandable Message – Cascade



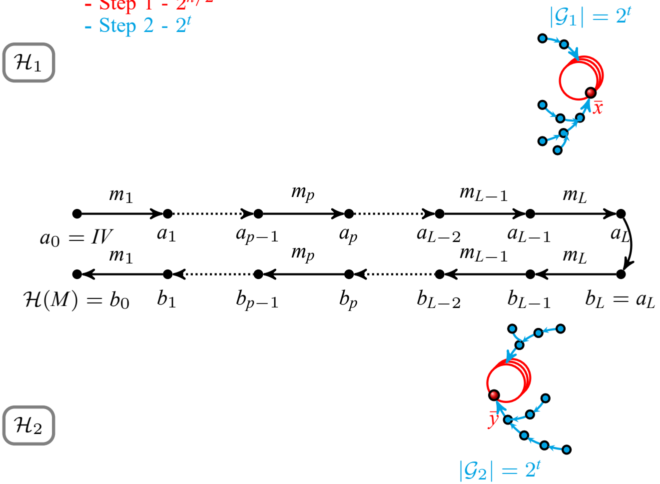
Second-Preimage Attack on the Zipper Hash

- Step 1 - $2^{n/2}$



Second-Preimage Attack on the Zipper Hash

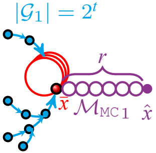
- Step 1 - $2^{n/2}$
- Step 2 - 2^t

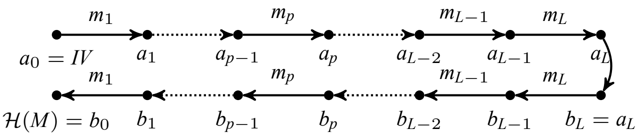


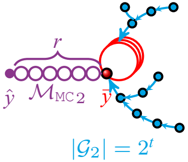
Second-Preimage Attack on the Zipper Hash

- Step 1 - $2^{n/2}$
- Step 2 - 2^{t}
- Step 3 - $2^{n/2}$

$\mathcal{H}_1$



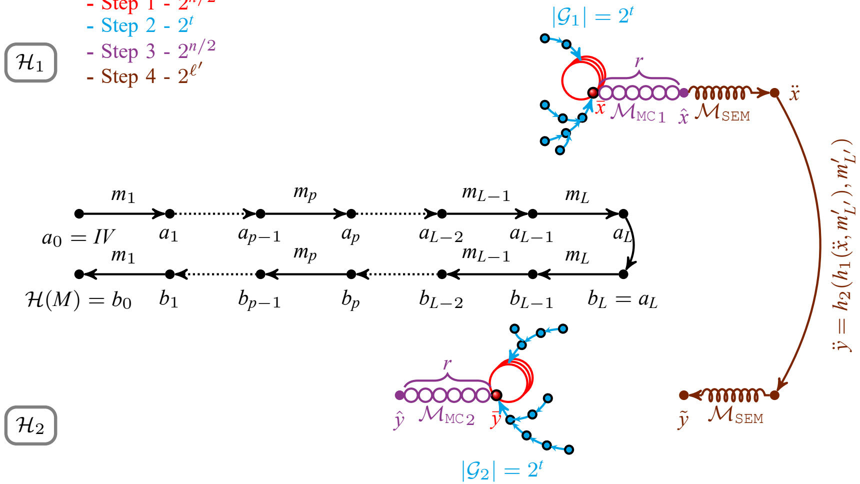




$\mathcal{H}_2$

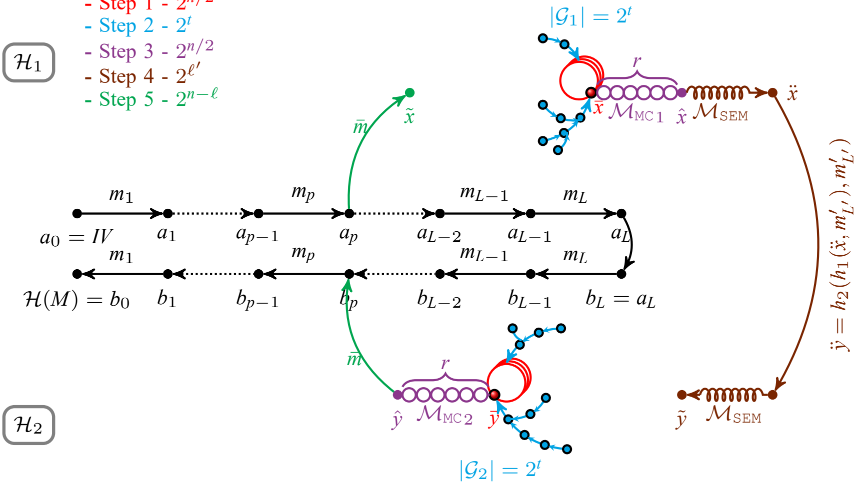
Second-Preimage Attack on the Zipper Hash

- Step 1 - $2^{n/2}$
- Step 2 - 2^{t}
- Step 3 - $2^{n/2}$
- Step 4 - $2^{\ell'}$



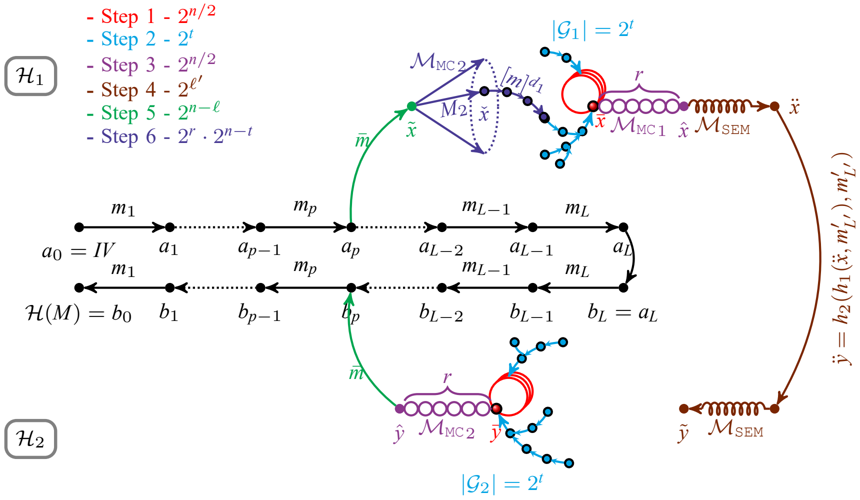
Second-Preimage Attack on the Zipper Hash

- Step 1 - $2^{n/2}$
- Step 2 - 2^{t}
- Step 3 - $2^{n/2}$
- Step 4 - $2^{\ell'}$
- Step 5 - $2^{n-\ell}$



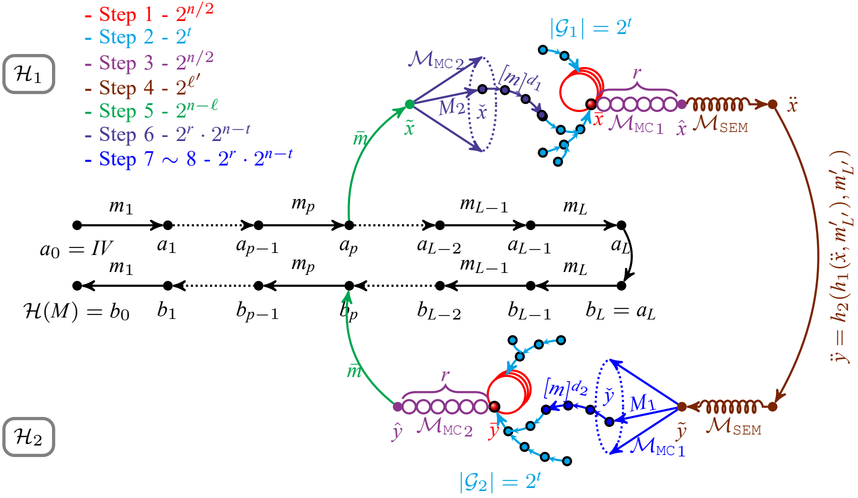
Second-Preimage Attack on the Zipper Hash

- Step 1 - $2^{n/2}$
- Step 2 - 2^{t}
- Step 3 - $2^{n/2}$
- Step 4 - $2^{\ell'}$
- Step 5 - $2^{n-\ell}$
- Step 6 - $2^{r} \cdot 2^{n-t}$



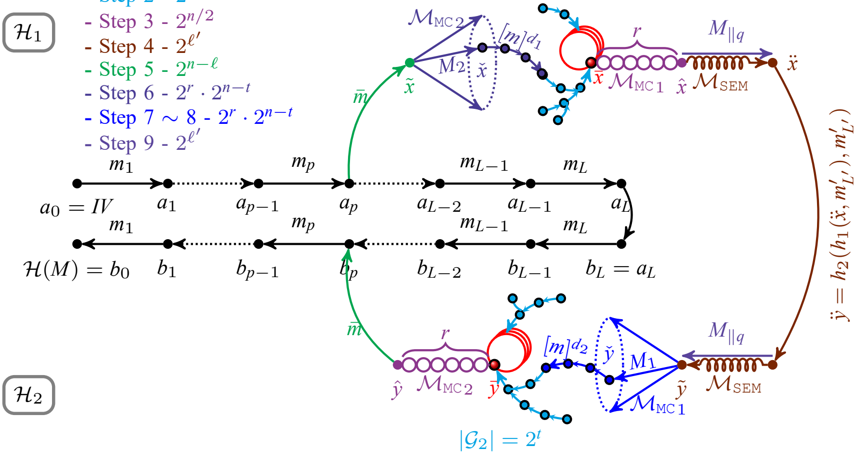
Second-Preimage Attack on the Zipper Hash

- Step 1 - $2^{n/2}$
- Step 2 - 2^{t}
- Step 3 - $2^{n/2}$
- Step 4 - $2^{\ell'}$
- Step 5 - $2^{n-\ell}$
- Step 6 - $2^{r} \cdot 2^{n-t}$
- Step 7 ∼ 8 - $2^{r} \cdot 2^{n-t}$



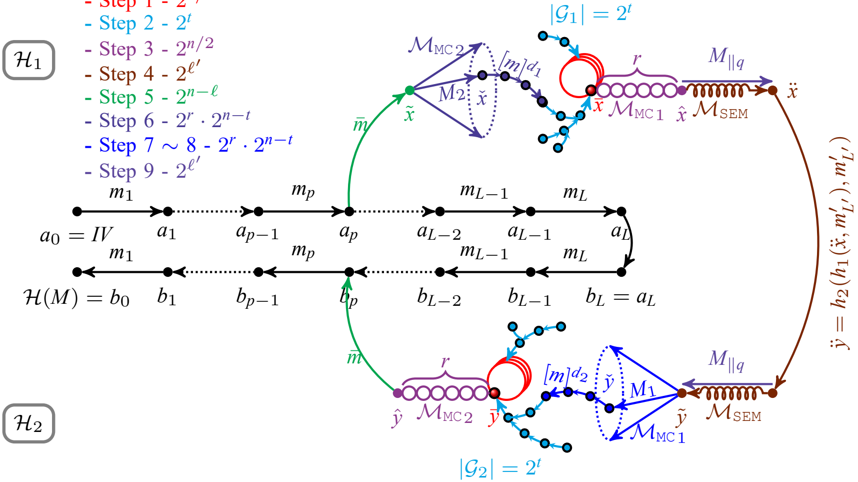
Second-Preimage Attack on the Zipper Hash

- Step 1 - $2^{n/2}$
- Step 2 - 2^{t}
- Step 3 - $2^{n/2}$
- Step 4 - $2^{\ell'}$
- Step 5 - $2^{n-\ell}$
- Step 6 - $2^{r} \cdot 2^{n-t}$
- Step 7 $\sim$ 8 - $2^{r} \cdot 2^{n-t}$
- Step 9 - $2^{\ell'}$



Second-Preimage Attack on the Zipper Hash

- Step 1 - $2^{n/2}$
- Step 2 - 2^{t}
- Step 3 - $2^{n/2}$
- Step 4 - $2^{\ell'}$
- Step 5 - $2^{n-\ell}$
- Step 6 - $2^{r} \cdot 2^{n-t}$
- Step 7 $\sim$ 8 - $2^{r} \cdot 2^{n-t}$
- Step 9 - $2^{\ell'}$



- The overall Cplx: $2^t + 2^{\ell'} + 2^{n-\ell} + 2^r \cdot 2^{n-t}$
- Search for t and r that give the lowest Cplx, the total Cplx: $2^{n/2+r/2} + 2^{\ell'} + 2^{n-\ell}$

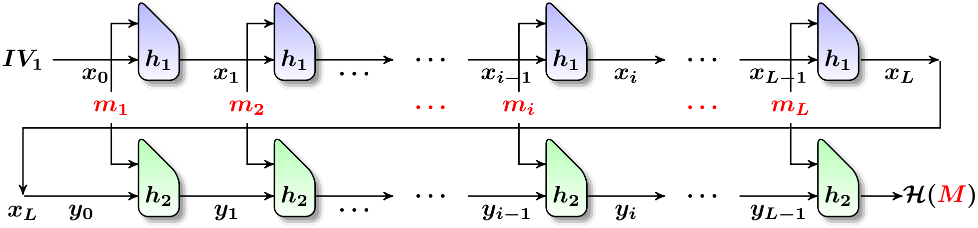
Second-Preimage Attack on the Zipper Hash

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal Zipper	$2^{n/2}$	2^n	2^n
HAIFA Zipper	$2^{n/2}$	2^n	2^n
MD Zipper	$2^{n/2}$	2^n	~~2^n~~ $\approx 2^{5n/8}$, $L \leq 2^{n/2}$ $\approx 2^{3n/5}$, No limit L
Ideal Hash-Twice	$2^{n/2}$	2^n	2^n
HAIFA Hash-Twice	$2^{n/2}$	2^n	2^n
MD Hash-Twice	$2^{n/2}$	2^n	~~2^n~~ $\approx 2^{2n/3}$

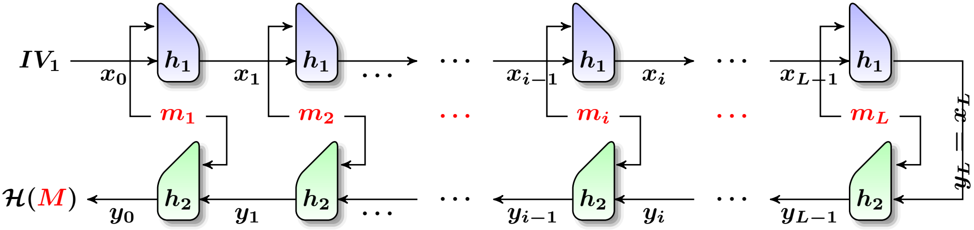
Outline

Combiners of Iterative Hash Functions - Cascade

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

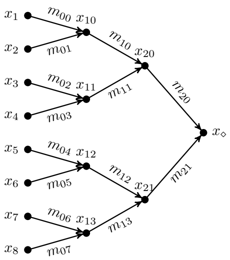


- Zipper Hash: $\mathcal{C}^{\mathcal{H}_1,\mathcal{H}_1}(M) = \mathcal{H}_2(\mathcal{H}_1(IV, M), \overleftarrow{M})$

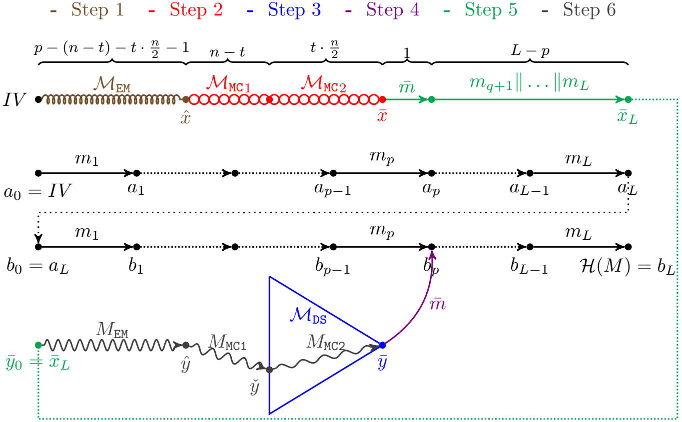


Diamond Structure (DS [KK06]) and the 2nd-Preimage Attack on Hash-Twice [And+08; And+09]

- A 2^t-diamond maps 2^t starting states to a common final state. Cplx: $n \cdot \sqrt{t} \cdot 2^{\frac{(n+t)}{2}}$
- The 2nd-preimage attack Cplx: $2^{(n+t)/2} + 2^{n-\ell} + 2^{n-t}$, 2^ℓ is the message len.



(a) A 2^3-diamond

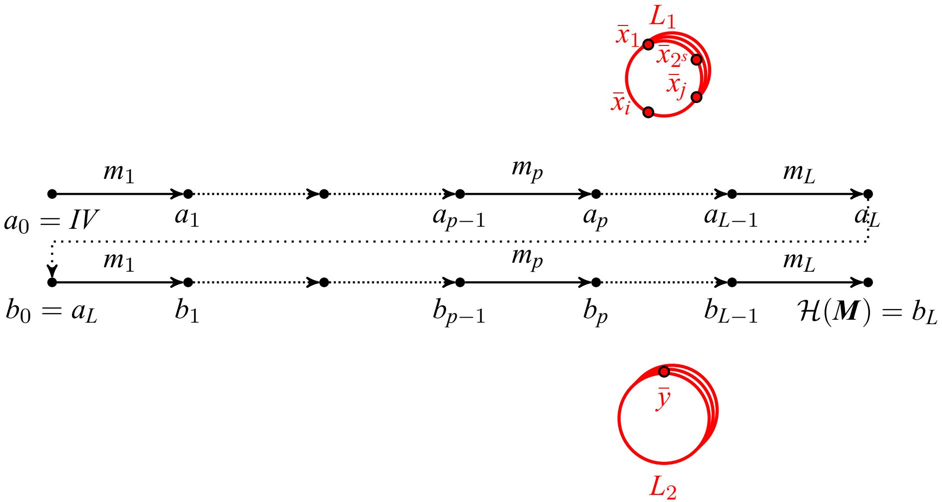


(b) Second-preimage attack on Hash-Twice using DS

Second-Preimage Attack on Hash-Twice

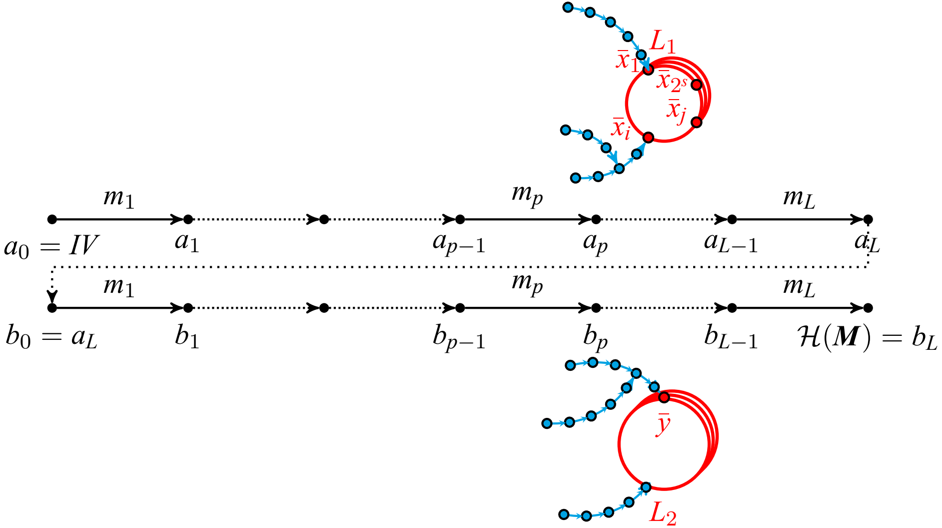
- Step 1

$2^{n/2}$



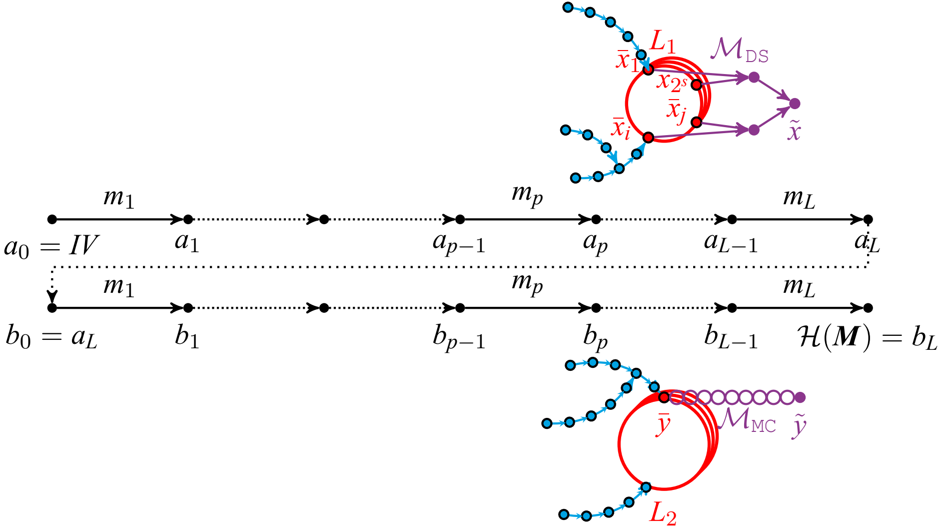
Second-Preimage Attack on Hash-Twice

- Step 1 $2^{n/2}$
- Step 2 2^t



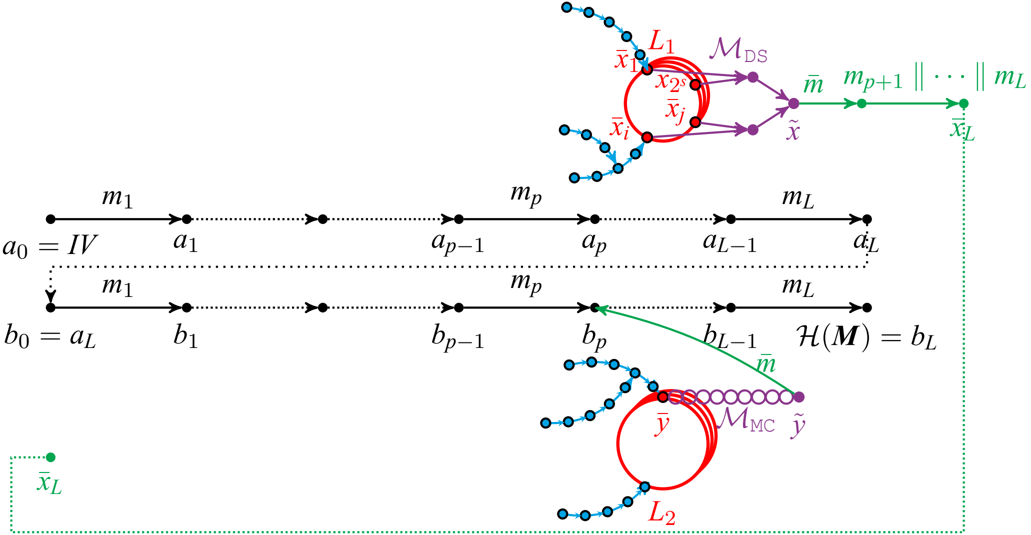
Second-Preimage Attack on Hash-Twice

- Step 1 $2^{n/2}$
- Step 2 2^t
- Step 3 $n\sqrt{s} \cdot 2^{(n+s)/2}$

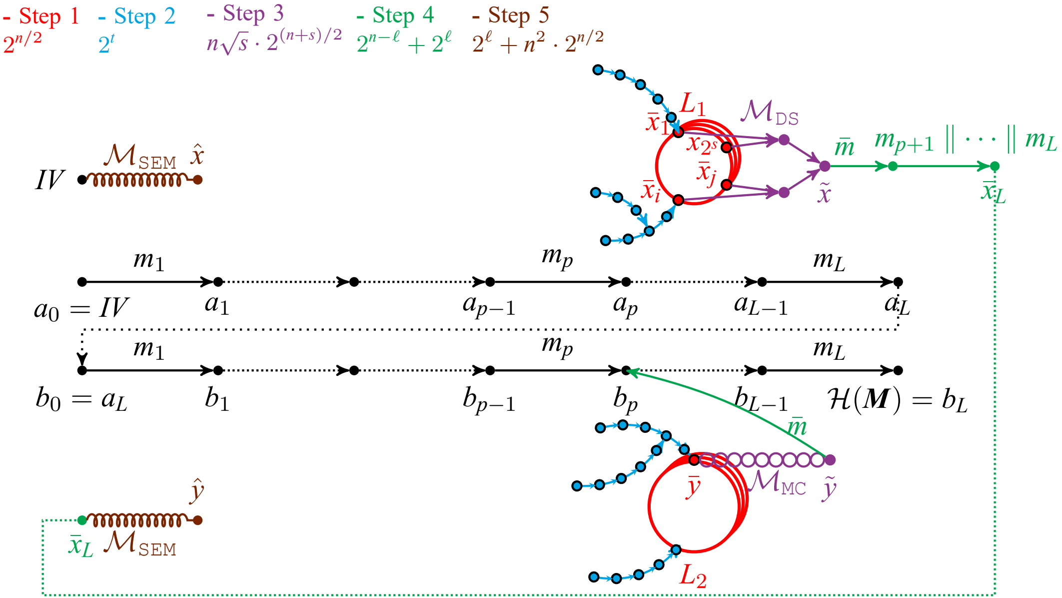


Second-Preimage Attack on Hash-Twice

- Step 1: $2^{n/2}$
- Step 2: 2^{t}
- Step 3: $n\sqrt{s} \cdot 2^{(n+s)/2}$
- Step 4: $2^{n-\ell} + 2^{\ell}$

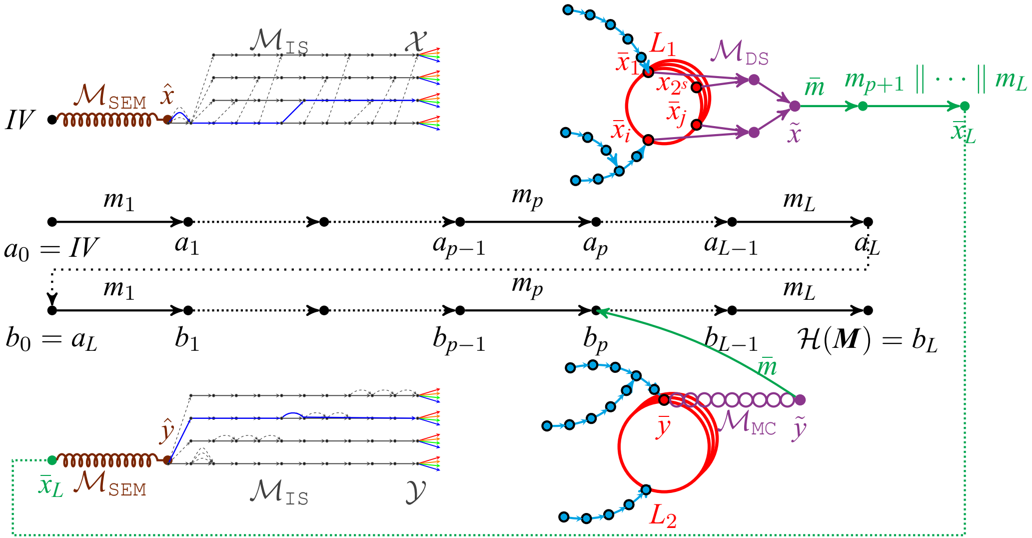


Second-Preimage Attack on Hash-Twice



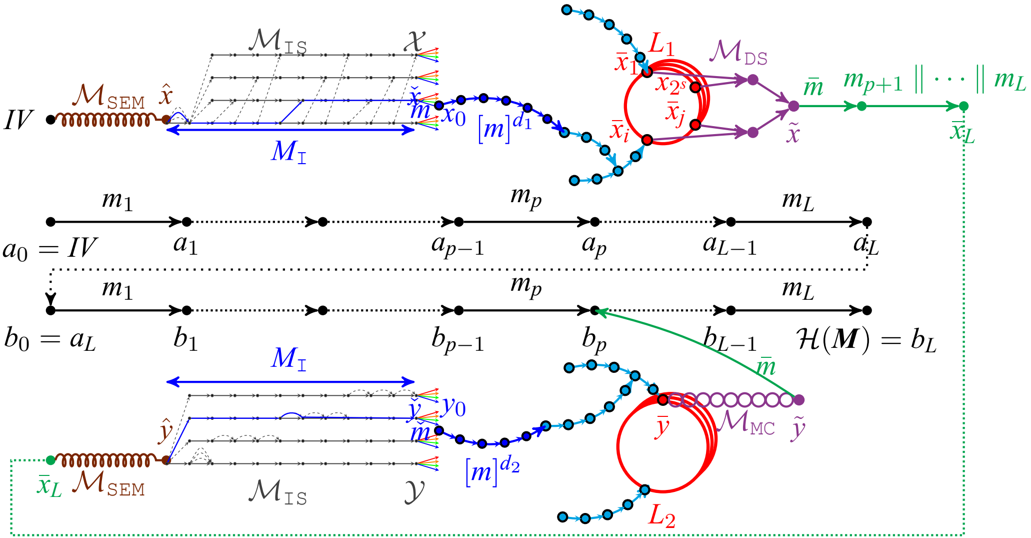
Second-Preimage Attack on Hash-Twice

- Step 1: $2^{n/2}$
- Step 2: 2^{t}
- Step 3: $n\sqrt{s} \cdot 2^{(n+s)/2}$
- Step 4: $2^{n-\ell} + 2^{\ell}$
- Step 5: $2^{\ell} + n^2 \cdot 2^{n/2}$
- Step 6: $2^{n/2+2r}$



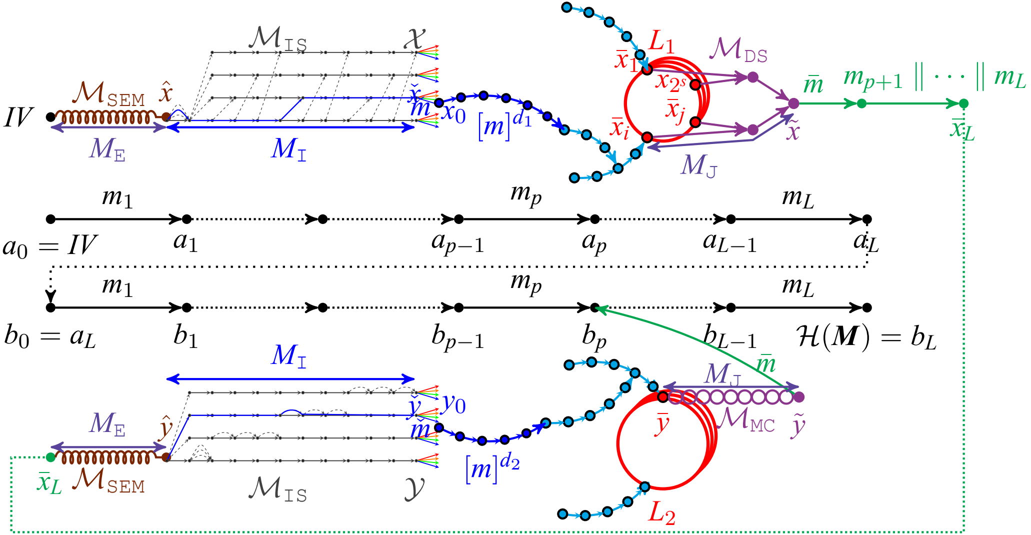
Second-Preimage Attack on Hash-Twice

- Step 1 $2^{n/2}$
- Step 2 2^{t}
- Step 3 $n\sqrt{s} \cdot 2^{(n+s)/2}$
- Step 4 $2^{n-\ell} + 2^{\ell}$
- Step 5 $2^{\ell} + n^2 \cdot 2^{n/2}$
- Step 6 $2^{n/2+2r}$
- Step 7 $2^{r} \cdot 2^{n-t} \cdot 2^{n-2r-s-\ell}$



Second-Preimage Attack on Hash-Twice

- Step 1: $2^{n/2}$
- Step 2: 2^{t}
- Step 3: $n\sqrt{s} \cdot 2^{(n+s)/2}$
- Step 4: $2^{n-\ell} + 2^{\ell}$
- Step 5: $2^{\ell} + n^2 \cdot 2^{n/2}$
- Step 6: $2^{n/2+2r}$
- Step 7: $2^{r} \cdot 2^{n-t} \cdot 2^{n-2r-s-\ell}$
- Step 8: 2^{ℓ}



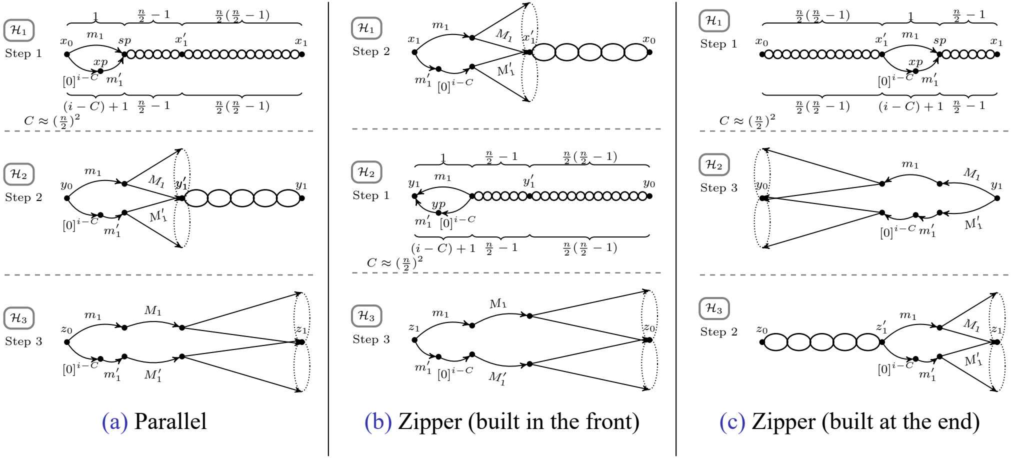
Second-preimage attack on Hash-Twice

	Collision Resistance	Preimage Resistance	2nd-Preimage Resistance
Ideal $\mathcal{H}$	$2^{n/2}$	2^n	2^n
MD $\mathcal{H}$	$2^{n/2}$	2^n	~~2^n~~ $2^n/L$
HAIFA $\mathcal{H}$	$2^{n/2}$	2^n	2^n
Ideal Zipper	$2^{n/2}$	2^n	2^n
HAIFA Zipper	$2^{n/2}$	2^n	2^n
MD Zipper	$2^{n/2}$	2^n	~~2^n~~ $\approx 2^{5n/8}, L \leq 2^{n/2}$ $\approx 2^{3n/5}$, No limit L
Ideal Hash-Twice	$2^{n/2}$	2^n	2^n
HAIFA Hash-Twice	$2^{n/2}$	2^n	2^n
MD Hash-Twice	$2^{n/2}$	2^n	~~$2^{2n/3}$~~ $\approx 2^{11n/18}, L \leq 2^{n/2}$ $\approx 2^{13n/22}, L > 2^{n/2}$

Outline

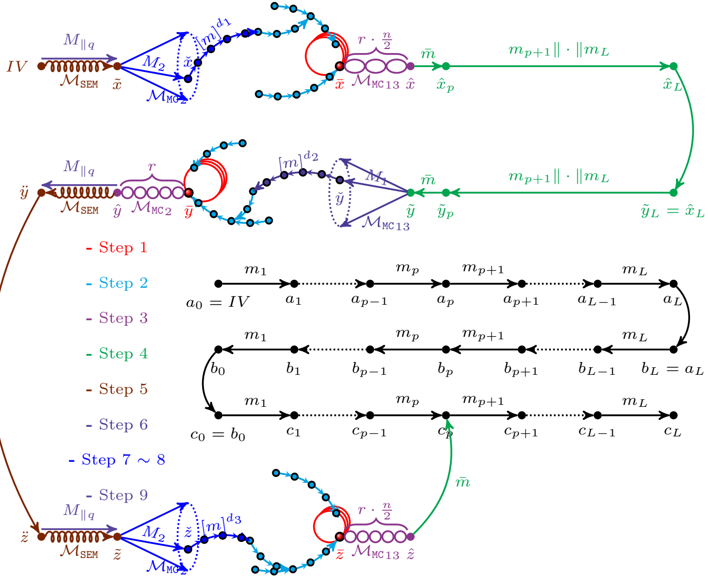
Extensions to the Combination of Three or More Hash Functions

Construct a building block for a 3-pass simultaneous expandable message:



(a) Parallel (b) Zipper (built in the front) (c) Zipper (built at the end)

Second-Preimage Attacks on 3-pass Zipper

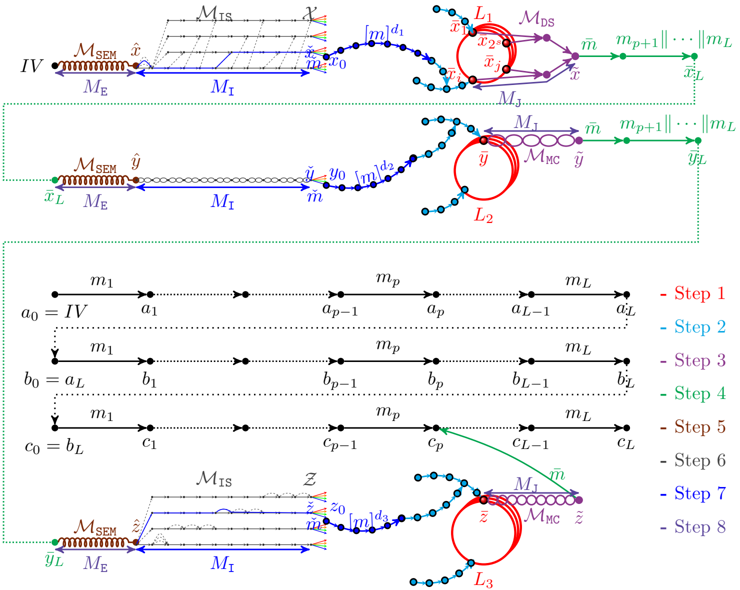


Let k be the # of passes

Cplx $< 2^n$ for $k < 6$

$$\begin{cases} 2^{7n/10} & \text{for } k = 3 \\ 2^{4n/5} & \text{for } k = 4 \\ 2^{9n/10} & \text{for } k = 5 \end{cases}$$

Second-Preimage Attacks on 3-pass Hash-Twice



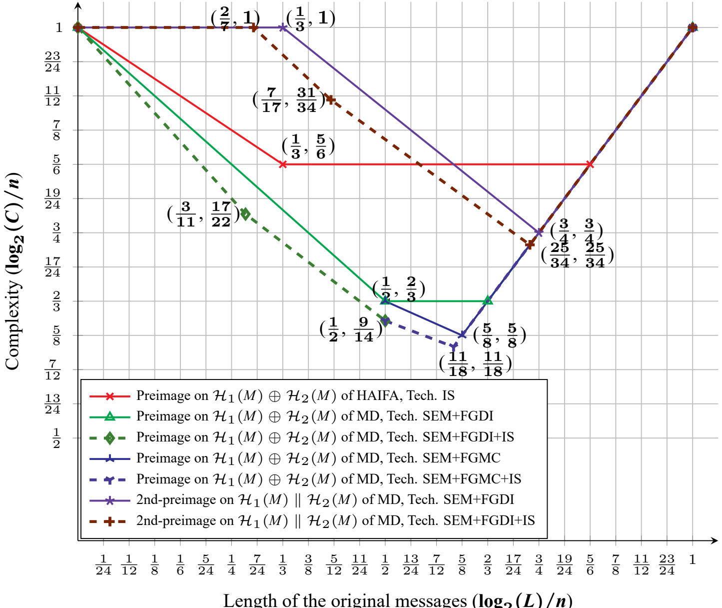
Let k be the # of passes

Cplx $< 2^n$ for $k < 7$

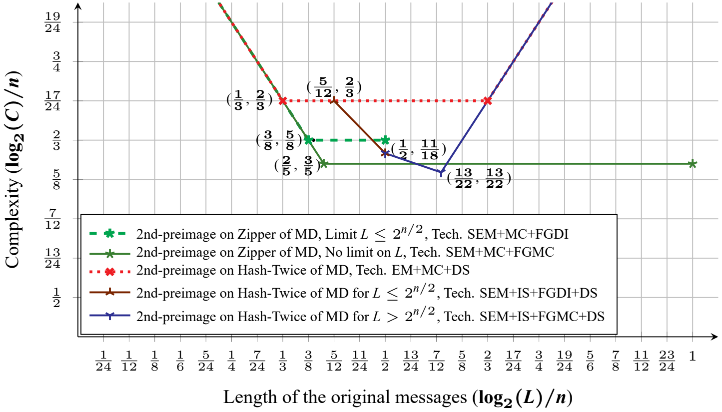
$$\begin{cases} 2^{15n/22} & \text{for } k = 3 \\ 2^{17n/22} & \text{for } k = 4 \\ 2^{19n/22} & \text{for } k = 5 \\ 2^{21n/22} & \text{for } k = 6 \end{cases}$$

Outline

Trade-offs curves on the complexity of attacks on parallel hash combiners



Trade-offs curves on the complexity of attacks on cascade hash combiners



Summary and Open Problems

- For combiners with underlying hash functions using MD, the gaps between the security upper bounds and the security lower bounds provided by security proof are quite narrow. However, that is true only for very long messages.
- For short messages, the gap remains large. That mainly results from the limitation of the key techniques used in the attacks, which highly exploit the iterated property of the underlying hash functions.
- Thus, one open problem is how to extend the attacks to apply to short messages.
- Another open problem is how to improve the attacks to combiners with at least one underlying hash function following the HAIFA framework.

Thanks for your attention!

References I

[Bao+19] Zhenzhen Bao et al. "Generic Attacks on Hash Combiners". In: *Journal of Cryptology* (2019). ISSN: 1432-1378. DOI: 10.1007/s00145-019-09328-w. URL: https://doi.org/10.1007/s00145-019-09328-w.

[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. LNCS. Springer, 2015, pp. 345–367. ISBN: 978-3-662-46799-2. DOI: 10.1007/978-3-662-46800-5_14. URL: https://doi.org/10.1007/978-3-662-46800-5_14.

[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. LNCS. Springer, 2016, pp. 484–508. ISBN: 978-3-662-49889-7. DOI: 10.1007/978-3-662-49890-3_19. URL: https://doi.org/10.1007/978-3-662-49890-3_19.

[Bao+17] Zhenzhen Bao et al. "Functional Graph Revisited: Updates on (Second) Preimage Attacks on Hash Combiners". In: *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10402. LNCS. Springer, 2017, pp. 404–427. ISBN: 978-3-319-63714-3. DOI: 10.1007/978-3-319-63715-0_14. URL: https://doi.org/10.1007/978-3-319-63715-0_14.

[Her05] Amir Herzberg. "On Tolerant Cryptographic Constructions". In: *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*. Ed. by Alfred Menezes. Vol. 3376. Lecture Notes in Computer Science. Springer, 2005, pp. 172–190. ISBN: 3-540-24399-2. DOI: 10.1007/978-3-540-30574-3_13. URL: https://doi.org/10.1007/978-3-540-30574-3_13.

[Can+07] Ran Canetti et al. "Amplifying Collision Resistance: A Complexity-Theoretic Treatment". In: *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*. Ed. by Alfred Menezes. Vol. 4622. Lecture Notes in Computer Science. Springer, 2007, pp. 264–283. ISBN: 978-3-540-74142-8. DOI: 10.1007/978-3-540-74143-5_15. URL: https://doi.org/10.1007/978-3-540-74143-5_15.

[FL07] Marc Fischlin and Anja Lehmann. "Security-Amplifying Combiners for Collision-Resistant Hash Functions". In: *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*. Ed. by Alfred Menezes. Vol. 4622. Lecture Notes in Computer Science. Springer, 2007, pp. 224–243. ISBN: 978-3-540-74142-8. DOI: 10.1007/978-3-540-74143-5_13. URL: https://doi.org/10.1007/978-3-540-74143-5_13.

References II

[FL08] Marc Fischlin and Anja Lehmann. "Multi-property Preserving Combiners for Hash Functions". In: *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008*. Ed. by Ran Canetti. Vol. 4948. Lecture Notes in Computer Science. Springer, 2008, pp. 375–392. ISBN: 978-3-540-78523-1. DOI: 10.1007/978-3-540-78524-8_21. URL: https://doi.org/10.1007/978-3-540-78524-8_21.

[FLP08] Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. "Robust Multi-property Combiners for Hash Functions Revisited". In: *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II - Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations*. Ed. by Luca Aceto et al. Vol. 5126. Lecture Notes in Computer Science. Springer, 2008, pp. 655–666. ISBN: 978-3-540-70582-6. DOI: 10.1007/978-3-540-70583-3_53. URL: https://doi.org/10.1007/978-3-540-70583-3_53.

[Her09] Amir Herzberg. "Folklore, practice and theory of robust combiners". In: *Journal of Computer Security* 17.2 (2009), pp. 159–189. DOI: 10.3233/JCS-2009-0336. URL: https://doi.org/10.3233/JCS-2009-0336.

[Leh10] Anja Lehmann. "On the security of hash function combiners". PhD thesis. Darmstadt University of Technology, 2010. URL: http://tuprints.ulb.tu-darmstadt.de/2094/.

[FLP14] Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. "Robust Multi-Property Combiners for Hash Functions". In: *J. Cryptology* 27.3 (2014), pp. 397–428. DOI: 10.1007/s00145-013-9148-7. URL: https://doi.org/10.1007/s00145-013-9148-7.

[BB06] Dan Boneh and Xavier Boyen. "On the Impossibility of Efficiently Combining Collision Resistant Hash Functions". In: *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*. Ed. by Cynthia Dwork. Vol. 4117. Lecture Notes in Computer Science. Springer, 2006, pp. 570–583. ISBN: 3-540-37432-9. DOI: 10.1007/11818175_34. URL: https://doi.org/10.1007/11818175_34.

[Pie07] Krzysztof Pietrzak. "Non-trivial Black-Box Combiners for Collision-Resistant Hash-Functions Don't Exist". In: *Advances in Cryptology - EUROCRYPT 2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings*. Ed. by Moni Naor. Vol. 4515. Lecture Notes in Computer Science. Springer, 2007, pp. 23–33. ISBN: 978-3-540-72539-8. DOI: 10.1007/978-3-540-72540-4_2. URL: https://doi.org/10.1007/978-3-540-72540-4_2.

References III

[Pie08] Krzysztof Pietrzak. “Compression from Collisions, or Why CRHF Combiners Have a Long Output”. In: *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*. Ed. by David A. Wagner. Vol. 5157. Lecture Notes in Computer Science. Springer, 2008, pp. 413–432. ISBN: 978-3-540-85173-8. DOI: 10.1007/978-3-540-85174-5_23. URL: https://doi.org/10.1007/978-3-540-85174-5_23.

[Rja09] Michal Rjasko. “On Existence of Robust Combiners for Cryptographic Hash Functions”. In: *Proceedings of the Conference on Theory and Practice of Information Technologies, ITAT 2009, Horský hotel Kralova studna, Slovakia, September 25-29, 2009*. Ed. by Peter Vojtás. Vol. 584. CEUR Workshop Proceedings. CEUR-WS.org, 2009, pp. 71–76. URL: http://ceur-ws.org/Vol-584/paper10.pdf.

[Dam89] Ivan Damgård. “A Design Principle for Hash Functions”. In: *Advances in Cryptology - CRYPTO ’89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*. Ed. by Gilles Brassard. Vol. 435. Lecture Notes in Computer Science. Springer, 1989, pp. 416–427. ISBN: 3-540-97317-6. DOI: 10.1007/0-387-34805-0_39. URL: https://doi.org/10.1007/0-387-34805-0_39.

[Mer89] Ralph C. Merkle. “One Way Hash Functions and DES”. In: *Advances in Cryptology - CRYPTO ’89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*. Ed. by Gilles Brassard. Vol. 435. Lecture Notes in Computer Science. Springer, 1989, pp. 428–446. ISBN: 3-540-97317-6. DOI: 10.1007/0-387-34805-0_40. URL: https://doi.org/10.1007/0-387-34805-0_40.

[BD07] Eli Biham and Orr Dunkelman. “A Framework for Iterative Hash Functions - HAIFA”. In: *IACR Cryptology ePrint Archive* 2007 (2007), p. 278. URL: http://eprint.iacr.org/2007/278.

[Jou04] Antoine Joux. “Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions”. In: *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*. Ed. by Matthew K. Franklin. Vol. 3152. LNCS. Springer, 2004, pp. 306–316. ISBN: 3-540-22668-0. DOI: 10.1007/978-3-540-28628-8_19. URL: https://doi.org/10.1007/978-3-540-28628-8_19.

[DA99] Richard Drews Dean and Andrew Appel. *Formal Aspects of Mobile Code Security*. PhD thesis, Princeton University Princeton, 1999.

[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. LNCS. Springer, 2005, pp. 474–490. ISBN: 3-540-25910-4. DOI: 10.1007/11426639_28. URL: https://doi.org/10.1007/11426639_28.

References IV

[FO89] Philippe Flajolet and Andrew M. Odlyzko. "Random Mapping Statistics". In: *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Vol. 434. LNCS. Springer, 1989, pp. 329–354. ISBN: 3-540-53433-4. DOI: 10.1007/3-540-46885-4_34. URL: https://doi.org/10.1007/3-540-46885-4_34.

[KK06] John Kelsey and Tadayoshi Kohno. "Herding Hash Functions and the Nostradamus Attack". In: *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*. Ed. by Serge Vaudenay. Vol. 4004. LNCS. Springer, 2006, pp. 183–200. ISBN: 3-540-34546-9. DOI: 10.1007/11761679_12. URL: https://doi.org/10.1007/11761679_12.

[And+08] Elena Andreeva et al. "Second Preimage Attacks on Dithered Hash Functions". In: *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*. Ed. by Nigel P. Smart. Vol. 4965. LNCS. Springer, 2008, pp. 270–288. ISBN: 978-3-540-78966-6. DOI: 10.1007/978-3-540-78967-3_16. URL: https://doi.org/10.1007/978-3-540-78967-3_16.

[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 Jr., Vincent Rijmen, and Reihaneh Safavi-Naini. Vol. 5867. LNCS. Springer, 2009, pp. 393–414. ISBN: 978-3-642-05443-3. DOI: 10.1007/978-3-642-05445-7_25. URL: https://doi.org/10.1007/978-3-642-05445-7_25.

[Men07] Alfred Menezes, ed. *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*. Vol. 4622. Lecture Notes in Computer Science. Springer, 2007. ISBN: 978-3-540-74142-8. DOI: 10.1007/978-3-540-74143-5. URL: https://doi.org/10.1007/978-3-540-74143-5.

[Bra90] Gilles Brassard, ed. *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*. Vol. 435. Lecture Notes in Computer Science. Springer, 1990. ISBN: 3-540-97317-6. DOI: 10.1007/0-387-34805-0. URL: https://doi.org/10.1007/0-387-34805-0.