SoK: Functional Graphs and Their Applications in Generic Attacks on Iterated Hash Constructions

Zhenzhen Bao Jian Guo Lei Wang

NANYANG TECHNOLOGICAL UNIVERSITY

SHANGHAI JIAO TONG UNIVERSITY

FSE 2018 March 5–7
Bruges, Belgium

Outline

Functional Graph

Preliminaries

Attacks on Hash-based MAC Based on FG

Attacks on Hash Combiners Based on FG

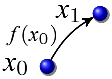
Summary and Open Problems

The Functional Graph of Random Mappings (FG)

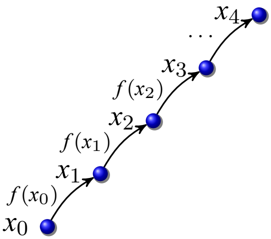
Let $f \xleftarrow{\$} \mathcal{F}_N$. $\mathcal{FG}_f$ is a directed graph, whose nodes are $0 \dots N-1$ and edges are $\langle x, f(x) \rangle$

The Functional Graph of Random Mappings (FG)

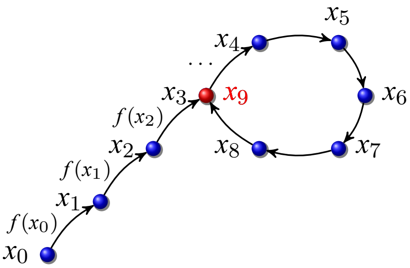
The Functional Graph of Random Mappings (FG)



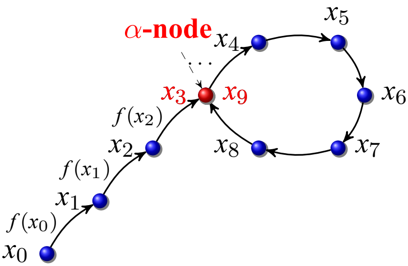
The Functional Graph of Random Mappings (FG)



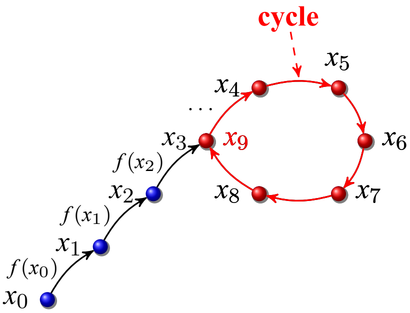
The Functional Graph of Random Mappings (FG)



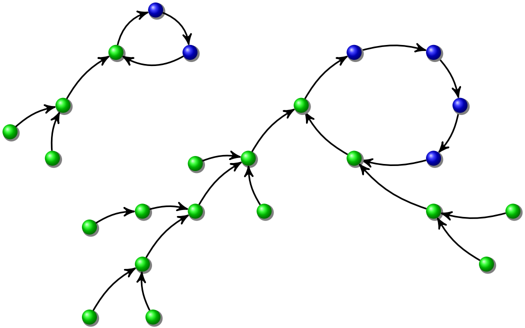
The Functional Graph of Random Mappings (FG)



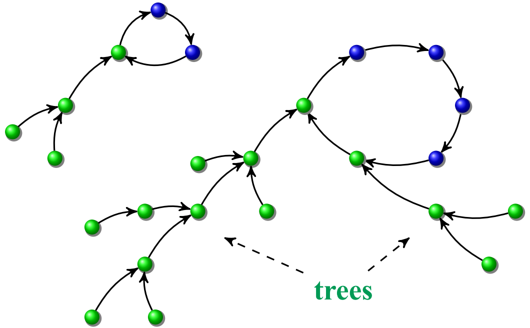
The Functional Graph of Random Mappings (FG)



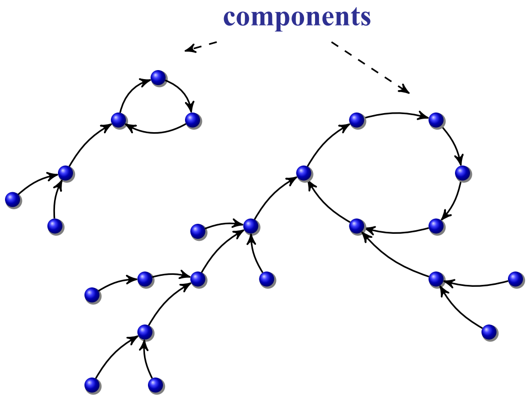
The Functional Graph of Random Mappings (FG)



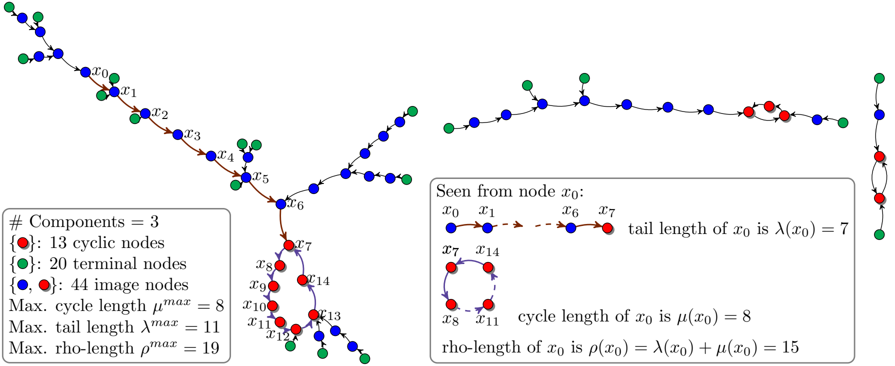
The Functional Graph of Random Mappings (FG)



The Functional Graph of Random Mappings (FG)

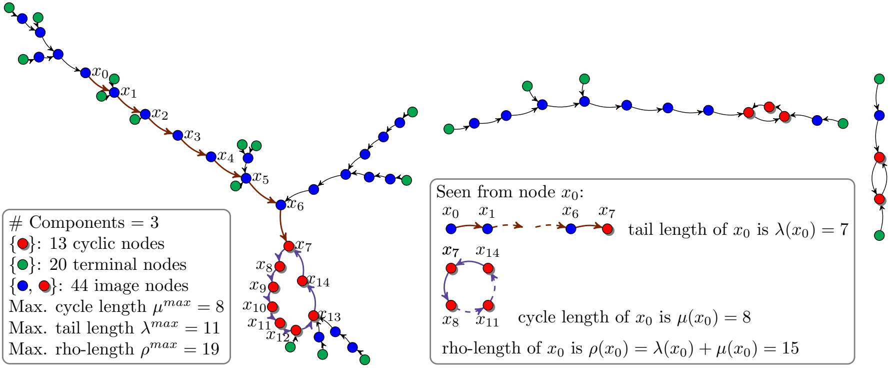


Statistical Properties of Functional Graph [FO89]



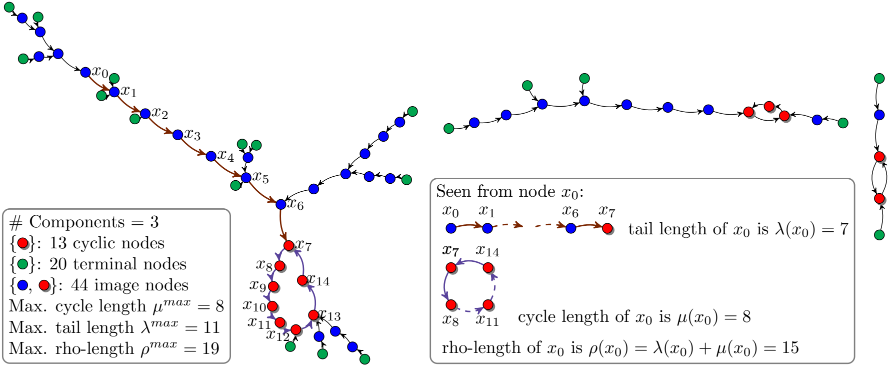
- # Components: $0.5 \cdot n$
- # Cyclic nodes: $1.2 \cdot 2^{n/2}$
- # Terminal nodes: $0.37 \cdot 2^n$
- # Image notes: $0.62 \cdot 2^n$
- # k-th iterate image notes: $(1 - \tau_k)N$ where the τ_k satisfies the recurrence $\tau_0 = 0, \tau_{k+1} = e^{-1+\tau_k}$.

Statistical Properties of Functional Graph [FO89]



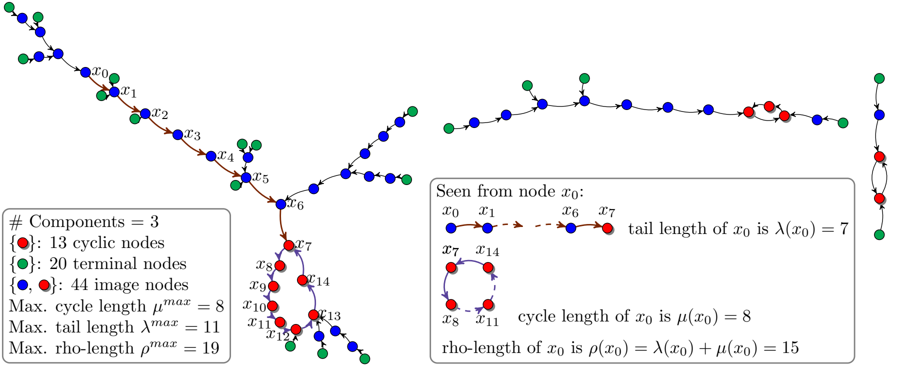
- Tail length (λ): $0.62 \cdot 2^{n/2}$
- Cycle length (μ): $0.62 \cdot 2^{n/2}$
- Rho-length (ρ): $1.2 \cdot 2^{n/2}$
- Tree size: $0.34 \cdot 2^n$
- Component size: $0.67 \cdot 2^n$
- Predecessors size: $0.62 \cdot 2^{n/2}$

Statistical Properties of Functional Graph [FO89]



- r-nodes: $N \cdot e^{-1}/r!$
- r-predecessor trees: $N \cdot t_r e^{-1}/r!$
- r-cycle trees: $\sqrt{\pi N/2} \cdot t_r e^{-1}/r!$
- r-cycles: $1/r$
- r-components: $c_r e^{-r}/r!$

Statistical Properties of Functional Graph [FO89]



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

Outline

Functional Graph

Preliminaries

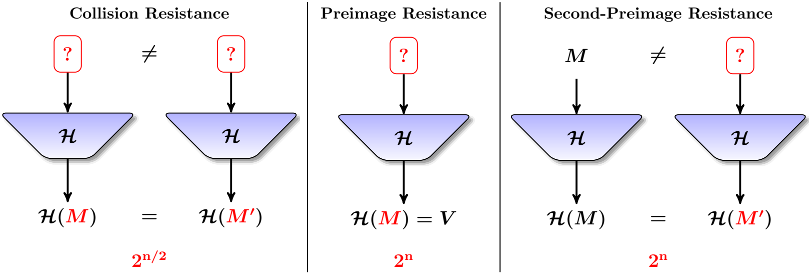
Attacks on Hash-based MAC Based on FG

Attacks on Hash Combiners Based on FG

Summary and Open Problems

Cryptographic Hash Functions

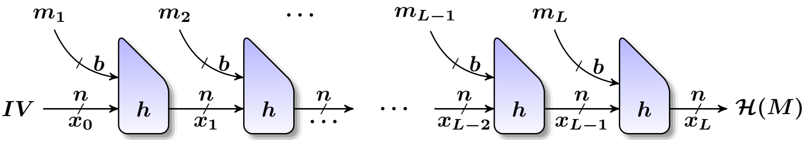
- A hash function $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^n$ maps a message of arbitrary length to a digest of fixed length n-bit.



Credit: *Bart Preneel*

Underlying Construction - Iterative Hash Functions

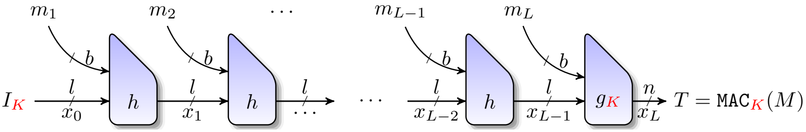
- The Merkle-Damgård construction (MD) [Mer89; Dam89]: Padding and dividing $M = m_1 \| m_2 \| \dots \| m_L$, m_L is encoded with $|M|$ (length padding or Merkle-Damgård strengthening):



Outline

Hash-based MACs

- Message Authentication Codes (MACs): symmetric method to provide authenticity
- One approach: Use hash functions with key K



Credit: *[LPW13]*

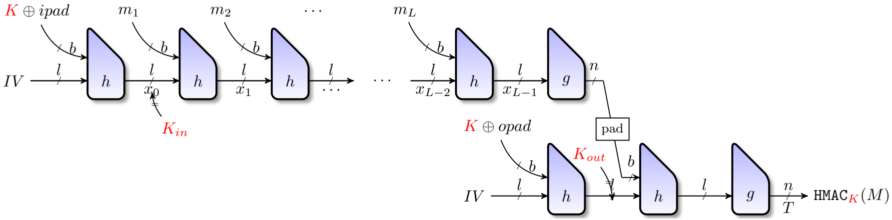
Hash-based MACs - Two Classical Designs

- NMAC:

$$\texttt{NMAC}(K_{out}, K_{in}, M) = \mathcal{H}_{K_{out}}(\mathcal{H}_{K_{in}}(M)).$$

- HMAC:

$$\texttt{HMAC}(K, M) = \mathcal{H}(K \oplus opad \| \mathcal{H}(K \oplus ipad \| M)).$$



HMAC with a Merkle-Damgård hash function

Credit: *[Guo+14]*

Security Requirement for Hash-based MACs

- Key recovery resistance: recover the key $\geq 2^k$
- State recovery resistance: recover the state $\geq \min(2^k, 2^l)$
- Forgery resistance: forge a valid tag of $M \geq \min(2^k, 2^n)$
  - Existential forgery: M is chosen by the adversary
  - Selective forgery: M is committed on by the adversary
  - Universal forgery: M is given to the adversary as a challenge

Security Requirement for Hash-based MACs

- Distinguishing-R:
  e.g. distinguish HMAC from a PRF
- Distinguishing-H:
  e.g. distinguish HMAC-SHA1 from HMAC-PRF

Distinguishing-H (recall)

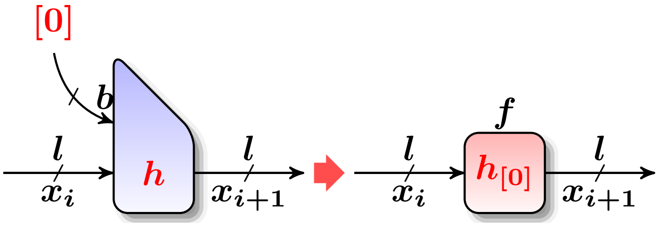
- Distinguishing-H:
  e.g. distinguish `HMAC-SHA1` from `HMAC-PRF`

$$Adv(\mathcal{A}) = \left|\Pr\left[\mathcal{A}(\texttt{MAC}_K^h) = 1\right] - \Pr\left[\mathcal{A}(\texttt{MAC}_K^r) = 1\right]\right|.$$

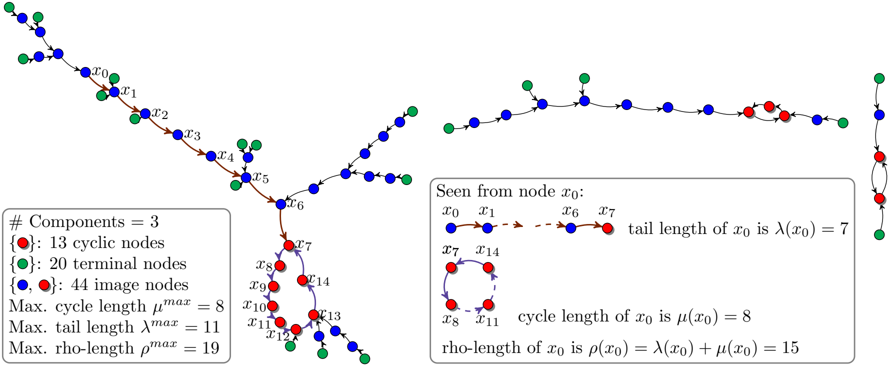
Distinguishing-H (recall)

- Distinguishing-H:
  e.g. distinguish HMAC-SHA1 from HMAC-PRF

$$Adv(\mathcal{A}) = \left| \Pr\left[\mathcal{A}(\texttt{MAC}_K^h) = 1\right] - \Pr\left[\mathcal{A}(\texttt{MAC}_K^r) = 1\right] \right|.$$

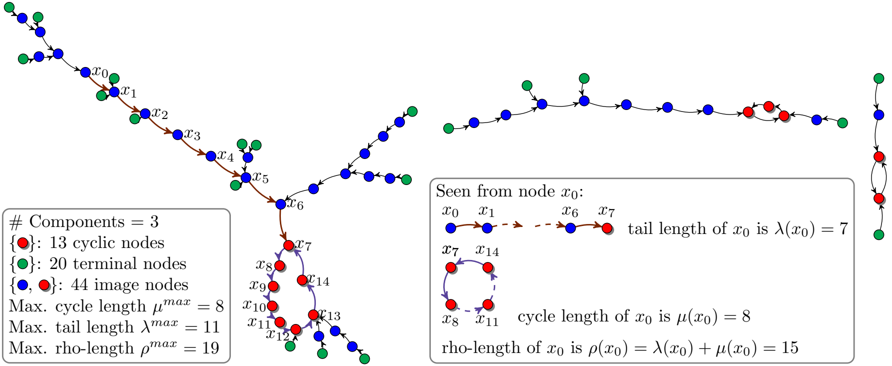


Statistical Properties of Functional Graph [FO89] (recall)



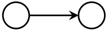
- Tail length (λ): $0.62 \cdot 2^{n/2}$
- Cycle length (μ): $0.62 \cdot 2^{n/2}$
- Rho-length (ρ): $1.2 \cdot 2^{n/2}$
- $\mathbf{E}\{\mu^{max} \mid \mathcal{F}_N\} = 0.78 \cdot 2^{n/2}$
- $\mathbf{E}\{\text{tree}^{largest} \mid \mathcal{F}_N\} = 0.48 \cdot 2^{n}$
- $\mathbf{E}\{\text{component}^{largest} \mid \mathcal{F}_N\} = 0.76 \cdot 2^{n}$

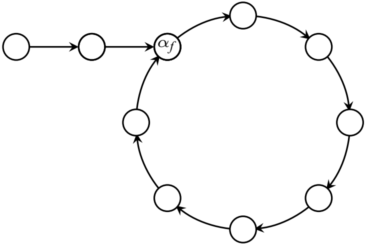
Statistical Properties of Functional Graph [FO89] (recall)



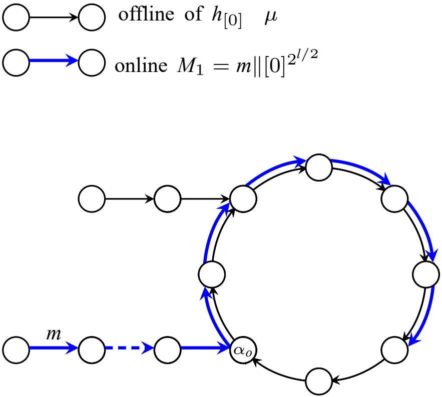
- Tail length (λ): $0.62 \cdot 2^{n/2}$
- Cycle length (μ): $0.62 \cdot 2^{n/2}$
- Rho-length (ρ): $1.2 \cdot 2^{n/2}$
- $\mathbf{E}\{\mu^{max} \mid \mathcal{F}_N\} = 0.78 \cdot 2^{n/2}$
- $\mathbf{E}\{\text{tree}^{largest} \mid \mathcal{F}_N\} = 0.48 \cdot 2^{n}$
- $\mathbf{E}\{\text{component}^{largest} \mid \mathcal{F}_N\} = 0.76 \cdot 2^{n}$

Cycle-based Distinguishing-H Attack [LPW13]

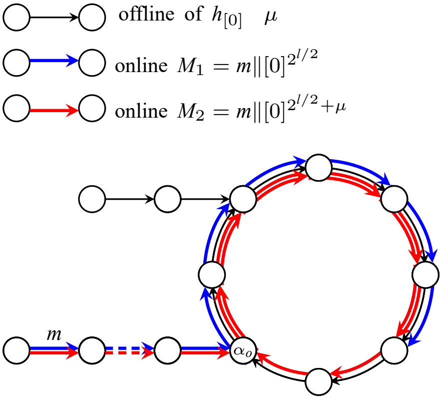
 offline of $h_{[0]}$ μ



Cycle-based Distinguishing-H Attack [LPW13]



Cycle-based Distinguishing-H Attack [LPW13]

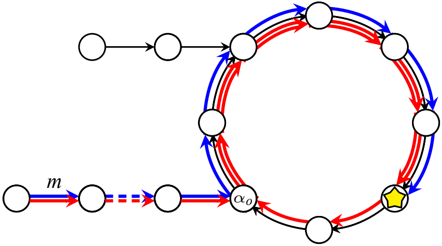


Cycle-based Distinguishing-H Attack [LPW13]

offline of $h_{[0]}$ μ

online $M_1 = m\|[0]^{2^{l/2}}$

online $M_2 = m\|[0]^{2^{l/2}+\mu}$



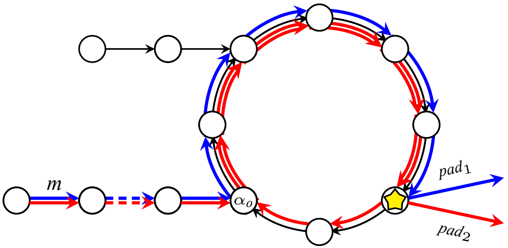
$\mathbf{0.76 \times 1/2}$

Cycle-based Distinguishing-H Attack [LPW13]

offline of $h_{[0]}$ μ

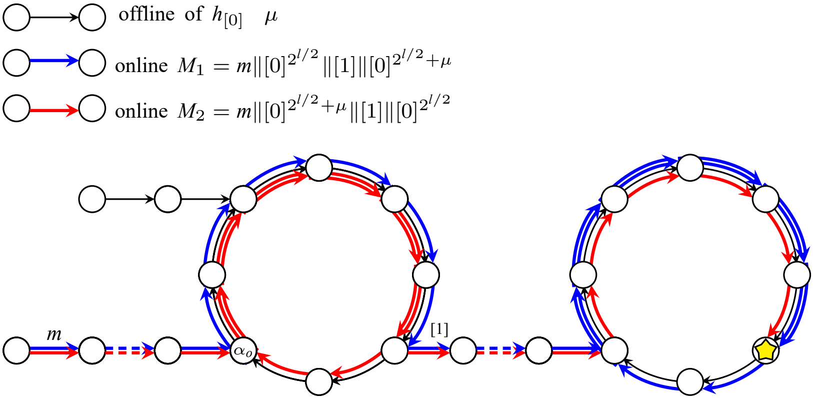
online $M_1 = m\|[0]^{2^{l/2}}$

online $M_2 = m\|[0]^{2^{l/2}+\mu}$



$\mathbf{0.76 \times 1/2}$

Cycle-based Distinguishing-H Attack [LPW13]



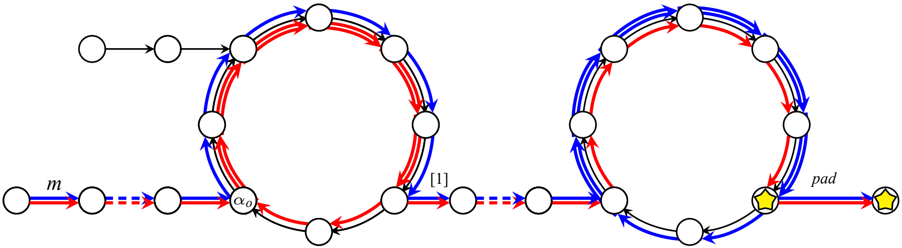
$\mathbf{0.76 \times 1/2}$ $\mathbf{\times 0.76 \times 1/2 \approx 0.14}$

Cycle-based Distinguishing-H Attack [LPW13]

offline of $h_{[0]}$ μ

online $M_1 = m\|[0]^{2^{l/2}}\|[1]\|[0]^{2^{l/2}+\mu}$

online $M_2 = m\|[0]^{2^{l/2}+\mu}\|[1]\|[0]^{2^{l/2}}$



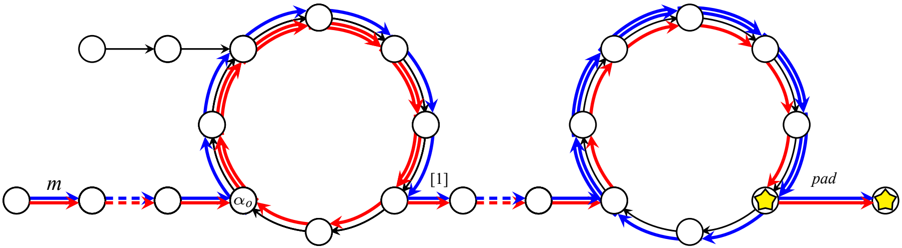
$\mathbf{0.76 \times 1/2}$ $\quad$ $\mathbf{\times 0.76 \times 1/2 \approx 0.14}$

Cycle-based Distinguishing-H Attack [LPW13]

offline of $h_{[0]}$ μ

online $M_1 = m\|[0]^{2^{l/2}}\|[1]\|[0]^{2^{l/2}+\mu}$

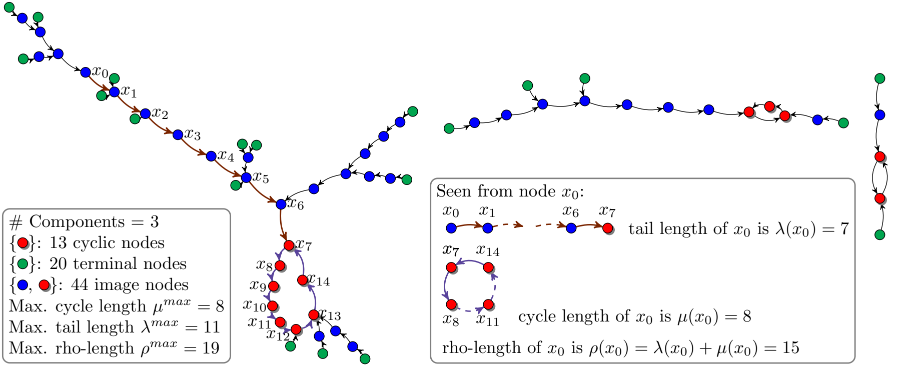
online $M_2 = m\|[0]^{2^{l/2}+\mu}\|[1]\|[0]^{2^{l/2}}$



0.76 × 1/2 **×0.76 × 1/2 ≈ 0.14**

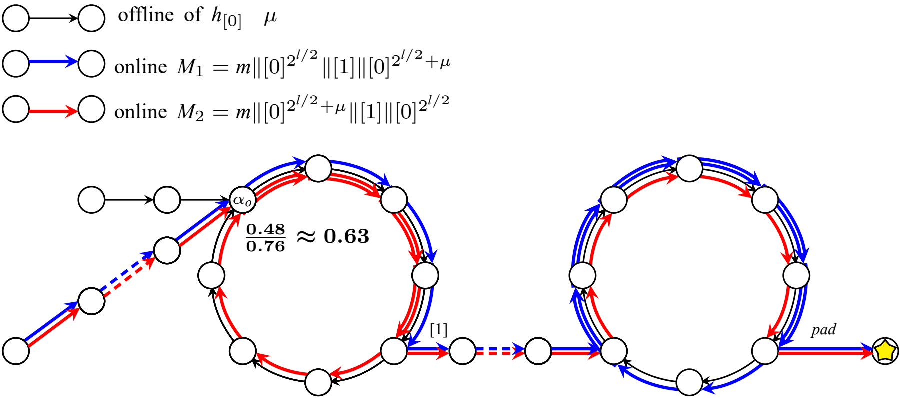
$$Adv(\mathcal{A}) = |0.14 - 2^{-l/2}| \approx 0.14$$

Statistical Properties of Functional Graph [FO89] (recall)



- Tail length (λ): $0.62 \cdot 2^{n/2}$
- Cycle length (μ): $0.62 \cdot 2^{n/2}$
- Rho-length (ρ): $1.2 \cdot 2^{n/2}$
- $\mathbf{E}\{\mu^{max} \mid \mathcal{F}_N\} = 0.78 \cdot 2^{n/2}$
- $\mathbf{E}\{\text{tree}^{largest} \mid \mathcal{F}_N\} = 0.48 \cdot 2^{n}$
- $\mathbf{E}\{\text{component}^{largest} \mid \mathcal{F}_N\} = 0.76 \cdot 2^{n}$

Cycle-based State Recovery Attack [LPW13]



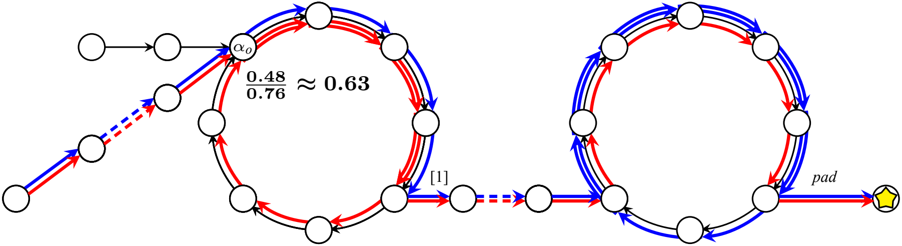
Cycle-based State Recovery Attack [LPW13]

offline of $h_{[0]}$ μ

online $M_1 = m\|[0]^{X'}\|[i]\|[0]^{2^{l/2}+\mu}$

online $M_2 = m\|[0]^{X'+\mu}\|[i]\|[0]^{2^{l/2}}$

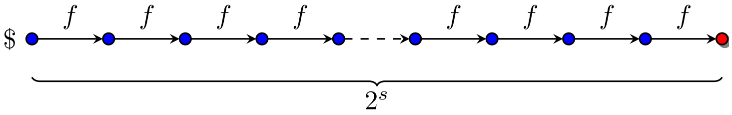
Binary Search:
1. $X_1 \leftarrow 0$, $X_2 \leftarrow 2^{l/2}$
2. $X' \leftarrow (X_1 + X_2)/2$, query with M_1 and M_2
3. $X_2 \leftarrow X'$ if collide, $X_1 \leftarrow X'$ other, go to 2.



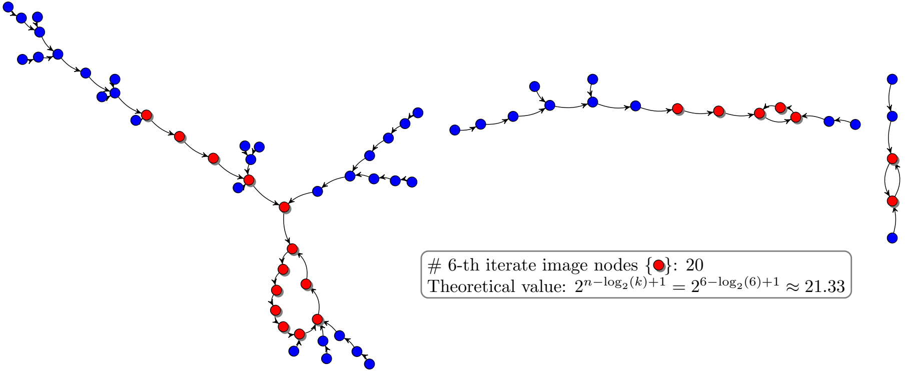
Entropy Loss of Chain Evaluation

Lemma 1 ([DL17], Lemma 1)

Let $s \leq l/2$ be a non-negative integer. Let f be a random function over the set of 2^l elements. Then, the images of two arbitrary inputs to f^{2^s} collide with probability of about 2^{s-l}, i.e.,
$\Pr_{x,y}[f^{2^s}(x) = f^{2^s}(y)] = \Theta(2^{s-l})$.



Statistical Properties of Functional Graph [FO89] (recall)



A k-th iterate image node in the functional graph of a random mapping $f \in \mathcal{F}_N$ is an image of the k-th iterate f^k of f.

k-th iterate image nodes $(1-\tau_k)N$, where the τ_k satisfies the recurrence $\tau_0 = 0, \tau_{k+1} = e^{-1+\tau_k}$.

The Expected Number of k-th Iterate Image Nodes in FG

Lemma 2

Let f be a random mapping in $\mathcal{F}_N$. Denote $N = 2^n$. For $k \leq 2^{n/2}$, the expectation of number of k-th iterate image nodes in the functional graph of f is

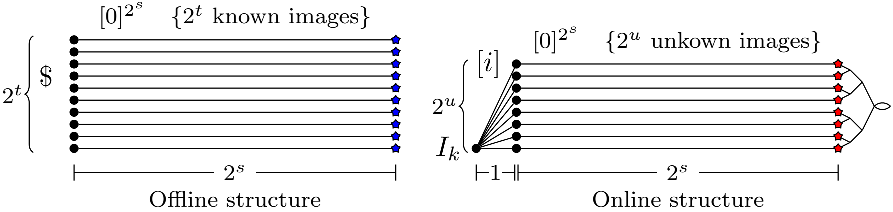
$$(1 - \tau_k) \cdot N \approx (\frac{2}{k} - \frac{2}{3}\frac{\log k}{k^2} - \frac{c}{k^2} - \cdots) \cdot N.$$

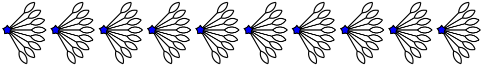
It suggests that $\lim_{k\to\infty} k \cdot (1 - \tau_k) = 2$. *Thus,*

$$\lim_{N\to\infty, k\to\infty, k\leq\sqrt{N}} (1 - \tau_k) \cdot N \approx 2^{n - \log_2(k) + 1},$$

where τ_k satisfies the recurrence $\tau_0 = 0$, $\tau_{k+1} = e^{-1+\tau_k}$, and c is a certain constant.

State Recovery Attack Based on Reduction of Image-set Size [DL17]



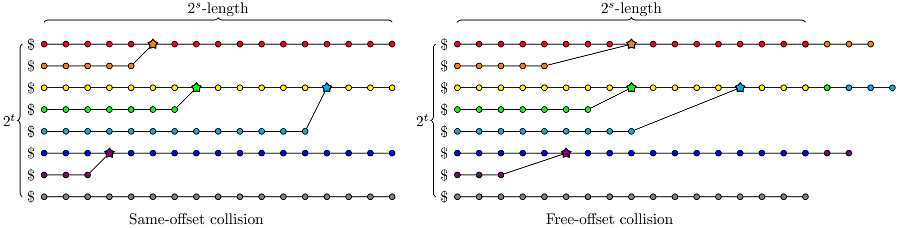


$t + u = l - s$

We detect (off-line) a match between 2^t off-line known states (blue star) with 2^u on-line unknown states (red star) using the diamond filter built on-line.

Step 1: $2^{t+s} = 2^{l-u}$ **Step 2:** $2^{u+s} + u \cdot 2^{s+u/2+l/2}$
Step 3: $2^{t+u} \cdot u = 2^{l-s} \cdot u$ Total complexity: $\tilde{O}(2^{l-s})$ for $s \leq l/5$;
Optimal complexity $4l/5$ when $s = l/5$.

Entropy Loss of Collision Search [LPW13; DL17]

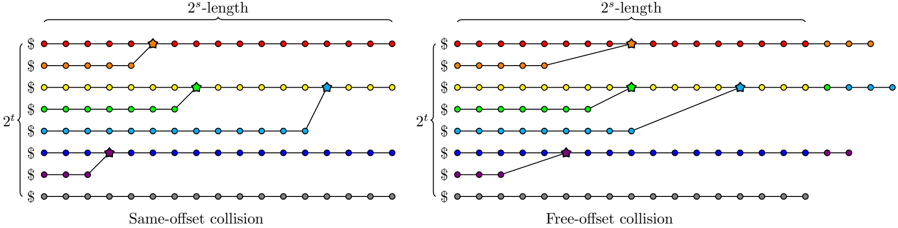


Suppose the iteration functions are all identical, and $2^{t+2s} \leq 2^l$

- For same-offset collisions:
- Expected number: 2^{2t+s-l}
- Complexity to get 2^c: $2^{l/2+s/2+c/2}$

- For free-offset collisions:
- Expected number: $2^{2(t+s)-l}$
- Complexity to get 2^c: $2^{l/2+c/2}$

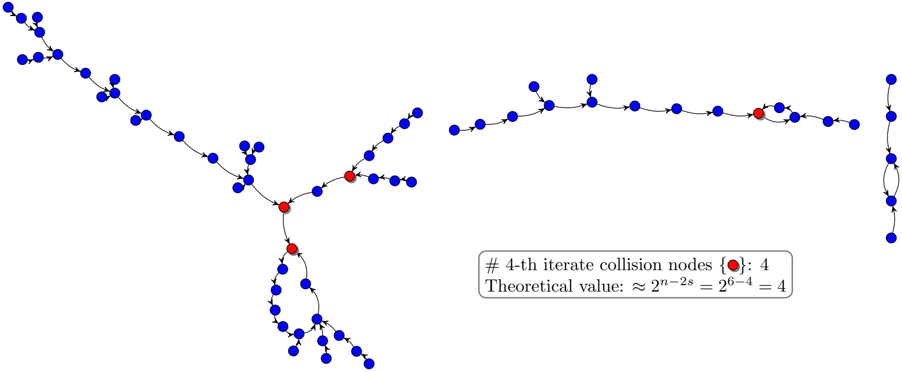
Entropy Loss of Collision Search [LPW13; DL17]



Lemma 3 ([DL17], Lemma 3)

Let $\hat{x}$ and $\hat{y}$ be two random collisions found by a collision search algorithm using 2^t chains of length 2^s, with a fixed l-bit random function f such that $2s + t \leq l$. Then $\Pr[\hat{x} = \hat{y}] = \Theta(2^{2s-l})$.

The Expected Number of k-th Iterate Collision Nodes



Definition 4 (k-th iterate collision node)

A k-th iterate collision node in the functional graph of a random mapping $f \in \mathcal{F}_N$, is an r-node (a node of in-degree r), where $r \geq 2$ and at least two of its pre-images are k-th iterate image nodes.

The Expected Number of k-th Iterate Collision Nodes

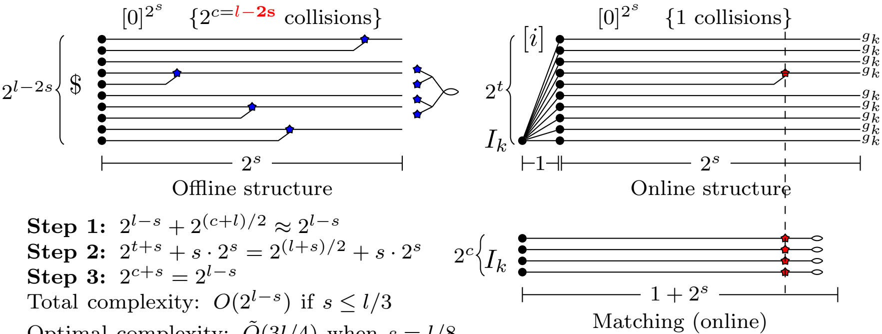
Theorem 5 ([FO89])

The expected number of r-nodes (a node of in-degree r) is $N \cdot e^{-1}/r!$. *The expected total number of collision nodes (*0*-th iterate collision nodes) in the functional graph of a random mapping* $f \in \mathcal{F}_N$ *is* $(1 - 2 \cdot e^{-1}) \cdot N = 0.2642 \cdot N$.

Lemma 6

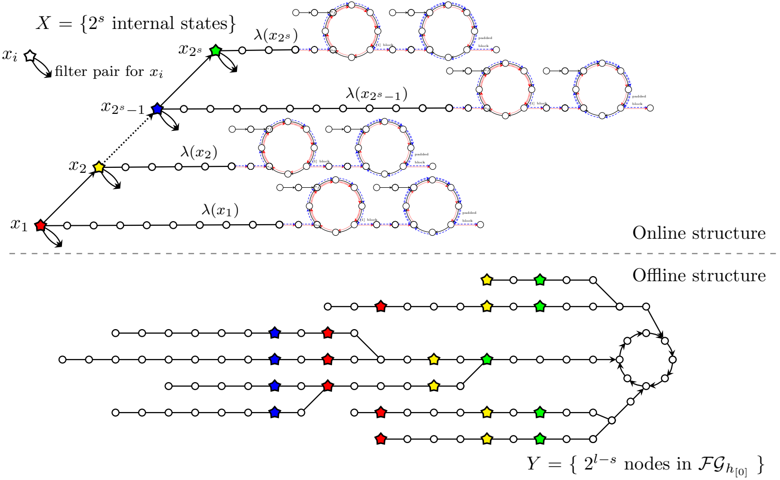
Denote $N = 2^n$. *For* $N \to \infty,\ k \to \infty$ *and* $k \leq 2^{n/2}$, *the expected number of k-th iterate collision nodes in the functional graph of a random mapping* $f \in \mathcal{F}_N$ *is* $\Theta(k^{-2} \cdot N)$.

State Recovery Attack Based on Collisions [DL17]



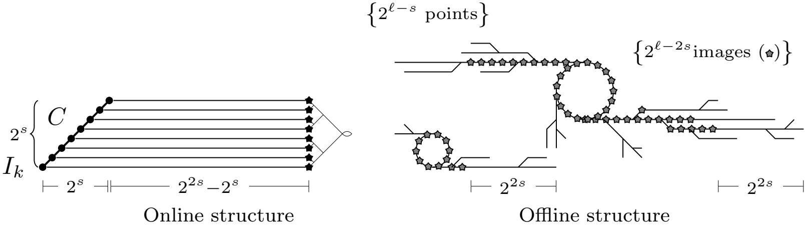
Step 1: $2^{l-s} + 2^{(c+l)/2} \approx 2^{l-s}$
Step 2: $2^{t+s} + s \cdot 2^s = 2^{(l+s)/2} + s \cdot 2^s$
Step 3: $2^{c+s} = 2^{l-s}$
Total complexity: $O(2^{l-s})$ if $s \leq l/3$
Optimal complexity: $\tilde{O}(3l/4)$ when $s = l/8$.

Universal Forgery Attacks Based on Cycles and Height [PW14; Guo+14]



Only match elements in X and elements in Y at same height (same color impling same height).

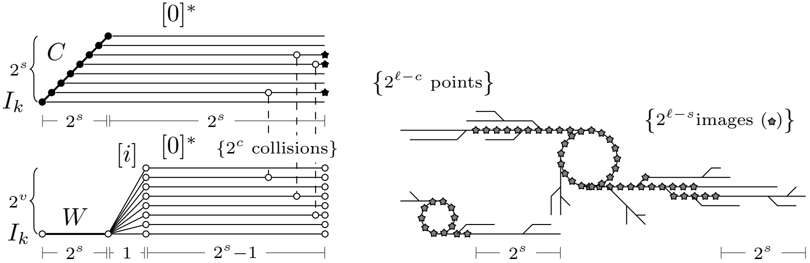
Universal Forgery Attacks Based on Chain and Collisions [DL14; DL17]



We efficiently detect a match between the challenge points (•) and the offline structure, by first matching X (★) and Y (☆).

Total complexity: $\tilde{O}(2^{l-s})$ for any $s \leq l/7$.
Optimal complexity: $2^{6l/7}$, obtained when $s = l/7$.

Universal Forgery Attacks Based on Chain and Collisions [DL14; DL17]



Online structure | Offline structure

We match the known points in X (⬟) and Y (⬠) in order to detect a match between the challenge points (•) and the offline structure.

Total complexity: $\tilde{O}(2^{l-s/2})$ for any $s \leq 2l/5$.
Optimal complexity: $2^{4l/5}$, when $s = 2l/5$.

Outline

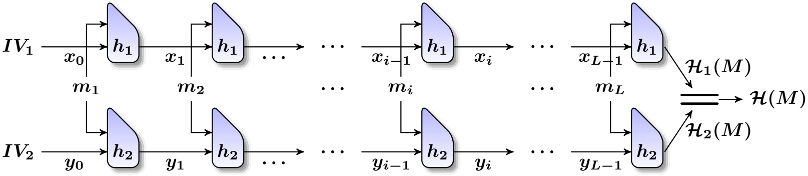
Hash Combiners

An approach to construct a secure hash function

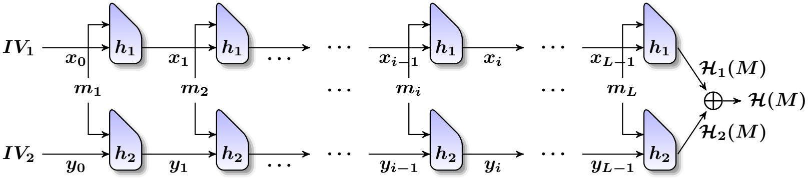
- Security amplification
  the combiner is more secure than its underlying hash functions;
- Security robustness
  the combiner is secure as long as any one of its underlying hash functions is secure

Hash Combiners - Parallel

- Concatenation combiner:



- XOR combiner:



Expected Security of Hash Combiners Before 2004

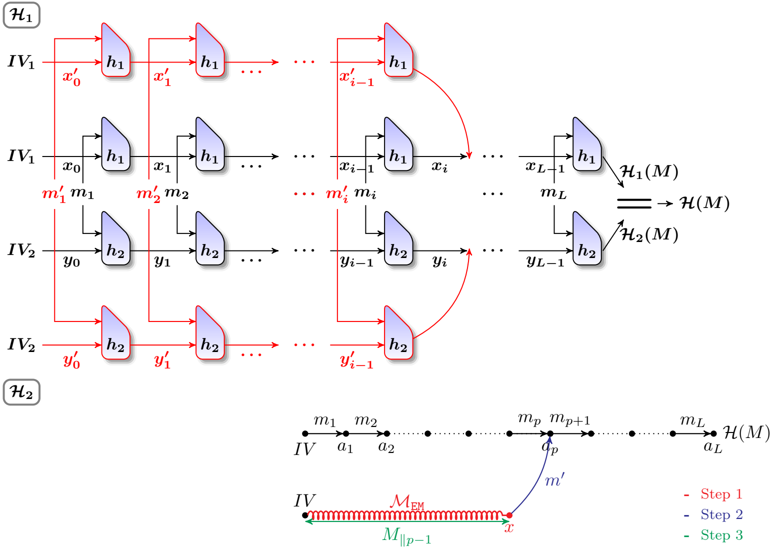
	Digest Size	Collision Resistance	Preimage Resistance	Second Preimage Resistance
Ideal $\mathcal{H}$	n	$2^{n/2}$	2^n	2^n
Ideal $\mathcal{H}_1 \| \mathcal{H}_2$	$2n$	2^n	2^{2n}	2^{2n}
Ideal $\mathcal{H}_1 \oplus \mathcal{H}_2$	n	$2^{n/2}$	2^n	2^n

⇑ birthday bound half of digest size (Collision Resistance)

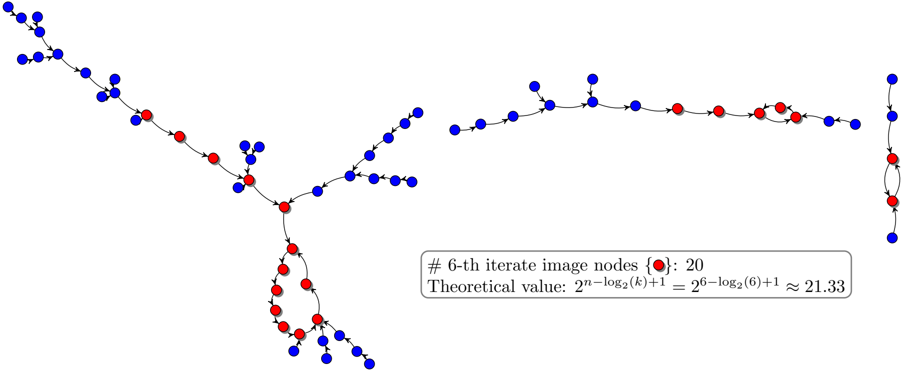
⇑ full digest size (Preimage Resistance and Second Preimage Resistance)

Second-Preimage Attack on Concatenation Combiner

Goal:



The k-th Iterate Image Nodes (deep iterates) in FG (recall)

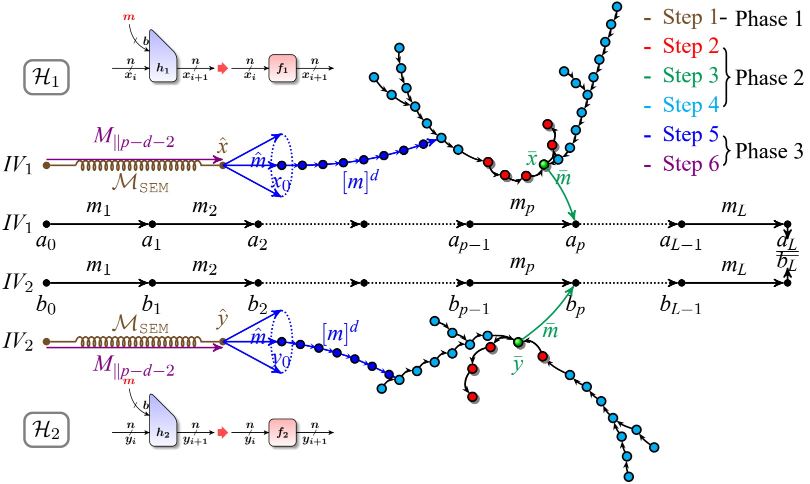


The expectation of number of k-th iterate image nodes is $\approx 2^{n-\log_2(k)+1}$

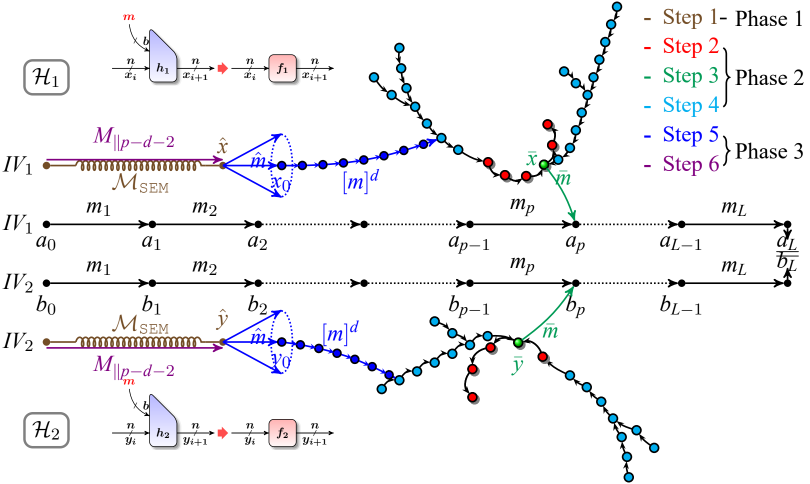
Lemma 7

Let f be an n-bit random mapping, and x'_0 an arbitrary point. Let $D \leq 2^{n/2}$ and define the chain $x'_i = f(x'_{i-1})$ for $i \in \{1, \ldots, D\}$. Let x_0 be a randomly chosen point, and define $x_d = f(x_{d-1})$. Then, for any $d \in \{1, \ldots, D\}$, $Pr[x_d = x'_D] = \Theta(d \cdot 2^{-n})$.

Second-Preimage Attack Based on Deep Iterates [Din16]



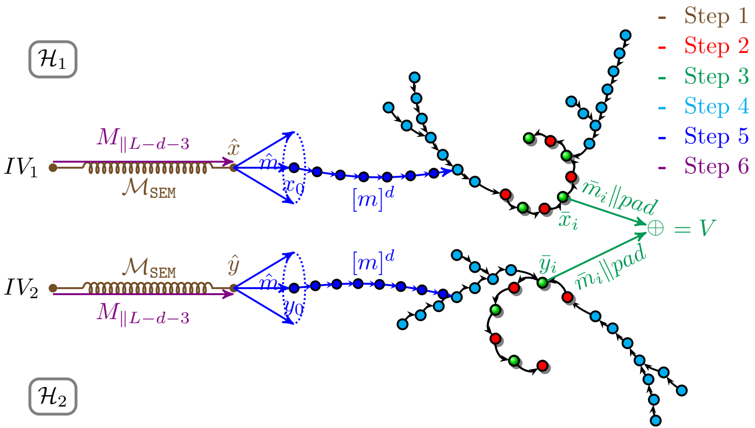
Second-Preimage Attack Based on Deep Iterates [Din16]



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

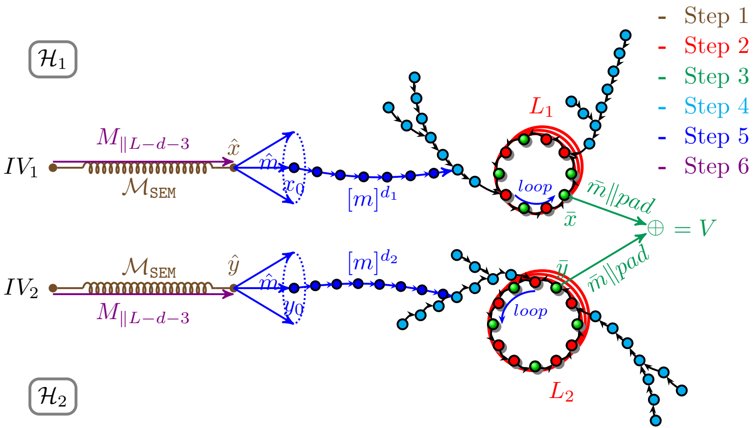
(use 2^g-deep iterates, set $g = n/5 + 2l/5$. Total: $2^{6n/5-3l/5}$ if $l < 3n/4$)

Preimage Attack on XOR Combiner Based on Deep Iterates [Din16]



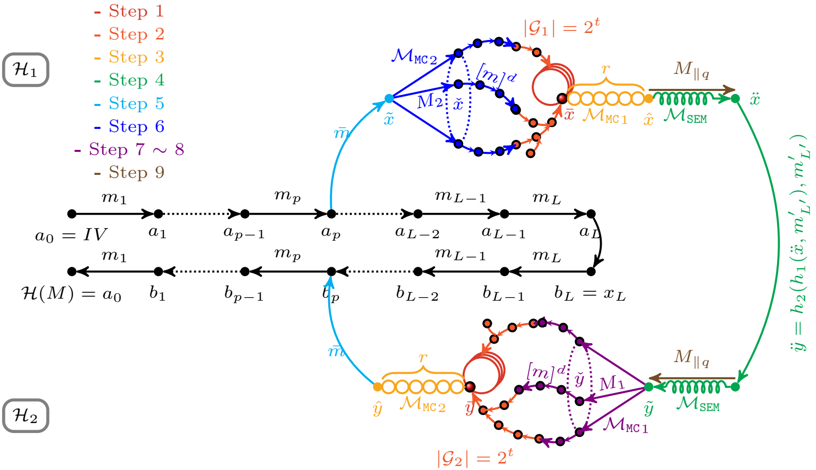
Optimal complexity: $2^{2n/3}$, obtained when $l = n/2$.

Preimage Attack on XOR Combiner Based on Multi-Cycles [Bao+17]



Optimal complexity: $2^{5n/8}$, obtained when $l = 5n/8$.

Second-Preimage Attack on Zipper Hash Based on Multi-Cycles [Bao+17]



Optimal complexity: $2^{3n/5}$, obtained when $l \geq 2n/5$ and $l' = 3n/5$.

Outline

Functional Graph

Preliminaries

Attacks on Hash-based MAC Based on FG

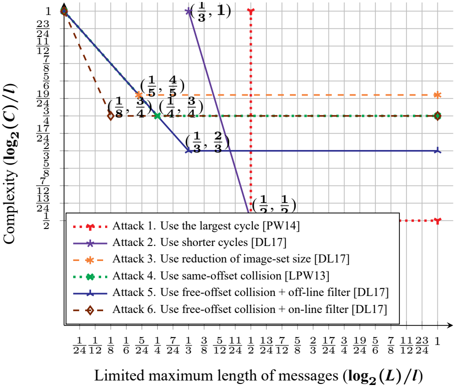
Attacks on Hash Combiners Based on FG

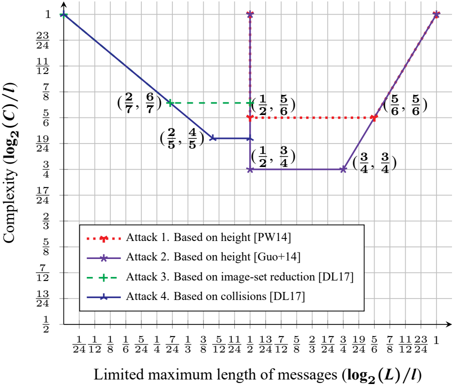
Summary and Open Problems

Relations Between Properties Utilized in Various Attacks and Properties of Functional Graphs

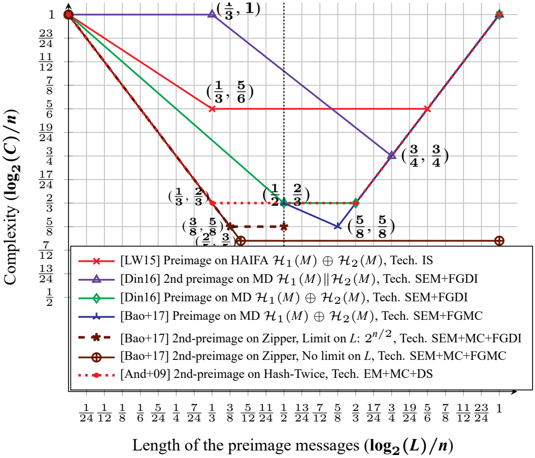
- Cycle search algorithm
  - output the cycle length and cyclic nodes
  - two outputs collide with constant probability
  - entropy loss is about l bits
- Chain evaluation algorithm
  - output deep (2^s) iterate nodes
  - two outputs collide with probability 2^{s-l}
  - entropy loss is about s bits
- Collision search algorithm
  - output deep (2^s) collision nodes
  - two outputs collide with probability 2^{2s-l}
  - entropy loss is about $2s$ bits

Summary on Generic Attacks against Hash-based MACs





Summary on Generic Attacks against Hash Combiners



Remarks on Approaches from Analytic Combinatorics

- Approaches from analytic combinatorics – the symbolic method, generating functions, and asymptotic analysis
- Is it possible to use analytic combinatorics to directly get asymptotic formulas for more special parameters (e.g., the expected number of k-th iterate collision nodes)?
- Is it possible to build combinatorial models for other concerned objects in cryptanalysis (e.g., the partial functional graph restored by some probabilistic algorithm)?

Thanks for your attention!

References I

[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.

[Mut88] Ljuben R Mutafchiev. "The limit distribution of the number of nodes in low strata of a random mapping". In: *Statistics & Probability Letters* 7.3 (1988), pp. 247 –251. ISSN: 0167-7152. DOI: http://dx.doi.org/10.1016/0167-7152(88)90058-2. URL: http://www.sciencedirect.com/science/article/pii/0167715288900582.

[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. LNCS. 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.

[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. LNCS. 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.

[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. LNCS. Springer, 2013, pp. 1–20. ISBN: 978-3-642-42044-3. DOI: 10.1007/978-3-642-42045-0_1. URL: https://doi.org/10.1007/978-3-642-42045-0_1.

References II

[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. LNCS. Springer, 2014, pp. 131–148. ISBN: 978-3-662-44370-5. DOI: 10.1007/978-3-662-44371-2_8. URL: https://doi.org/10.1007/978-3-662-44371-2_8.

[DL17] Itai Dinur and Gaëtan Leurent. "Improved Generic Attacks Against Hash-Based MACs and HAIFA". In: *Algorithmica* 79.4 (2017), pp. 1161–1195. DOI: 10.1007/s00453-016-0236-6. URL: https://doi.org/10.1007/s00453-016-0236-6.

[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. LNCS. Springer, 2014, pp. 147–164. ISBN: 978-3-642-55219-9. DOI: 10.1007/978-3-642-55220-5_9. URL: https://doi.org/10.1007/978-3-642-55220-5_9.

[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. LNCS. Springer, 2014, pp. 149–168. ISBN: 978-3-662-44370-5. DOI: 10.1007/978-3-662-44371-2_9. URL: https://doi.org/10.1007/978-3-662-44371-2_9.

[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.

References III

[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.

[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.

[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.

[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.

[GG14] Juan A. Garay and Rosario Gennaro, eds. *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*. Vol. 8616. LNCS. Springer, 2014. ISBN: 978-3-662-44370-5. DOI: 10.1007/978-3-662-44371-2. URL: https://doi.org/10.1007/978-3-662-44371-2.

References IV

[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. LNCS. Springer, 1990. ISBN: 3-540-97317-6. DOI: 10.1007/0-387-34805-0. URL: https://doi.org/10.1007/0-387-34805-0.