Improved Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing

Xiaoyang Dong[1,3,5,6] Jian Guo[2] Shun Li[4,2(✉)] Phuong Pham[2] **Tianyu Zhang**[2]

[1]Tsinghua University, Beijing, China
[2]Nanyang Technological University, Singapore
[3]State Key Laboratory of Cryptology, Beijing, China
[4]University of Chinese Academy of Sciences, Beijing, China
[5]Zhongguancun Laboratory, Beijing, China
[6]Shandong Institute of Blockchain, Jinan, China

FSE 2024
Leuven, Belgium

Outline

Outline

Nostradamus: Origin and Evolution

Chosen Target Forced Prefix (CTFP) Preimage Resistance[1]

- CTFP resembles the setting of a commitment scheme.
- For a hash function H, it should be hard to find a hash value h_T, such that for any prefix P of a known length, the attacker can construct a suffix S that $H(P||S) = h_T$ efficiently.
- The generic CTFP preimage attack on Merkel-Damgård constructions is known as the Nostradamus attack.

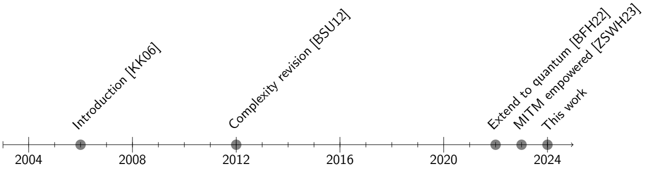
[1] John Kelsey and Tadayoshi Kohno. Herding Hash Functions and the Nostradamus Attack. EUROCRYPT 2006.

Nostradamus: Origin and Evolution

Chosen Target Forced Prefix (CTFP) Preimage Resistance[1]

- CTFP resembles the setting of a commitment scheme.
- For a hash function H, it should be hard to find a hash value h_T, such that for any prefix P of a known length, the attacker can construct a suffix S that $H(P||S) = h_T$ efficiently.
- The generic CTFP preimage attack on Merkel-Damgård constructions is known as the Nostradamus attack.

Evolution of Nostradamus Attacks



[1] John Kelsey and Tadayoshi Kohno. Herding Hash Functions and the Nostradamus Attack. EUROCRYPT 2006.

Offline Phase

Build a diamond structure with 2^k leaf nodes $\rightarrow$ multi-collisions

- Node x_i: hash values
- Edge $x_i x_j$: a message block m such that $CF(x_i, m) = x_j$

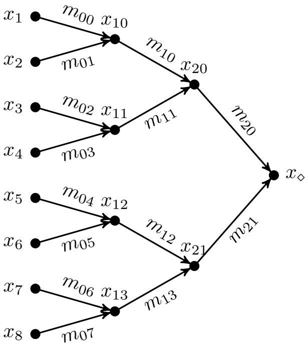


Figure: A diamond structure with 2^3 leaves

Offline Phase

Build a diamond structure with 2^k leaf nodes $\rightarrow$ multi-collisions

- Node x_i: hash values
- Edge $x_i x_j$: a message block m such that $CF(x_i, m) = x_j$

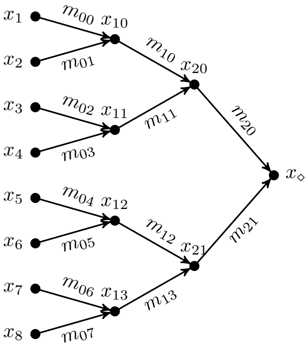


Figure: A diamond structure with 2^3 leaves

Constructing 2^k leaves

Fix $n - k$ bits as constants and enumerate the rest k bits

$n-k$ fixed bits	k free bits

Figure: A construction of the leaf nodes

Online Phase

Find a "link" to diamond structure $\rightarrow$ preimage

- Compute the initial hash value $x_0 = CF(IV, P)$.
- Find M_{link} that links x_0 to any leaf node x_j of the stored diamond structure.

$$CF(x_0, M_{link}) = x_j, \quad 1 \leq j \leq 2^k$$

- Look up the pathway from x_j to h_T as M_j, obtain the suffix $S = M_{link}||M_j$.

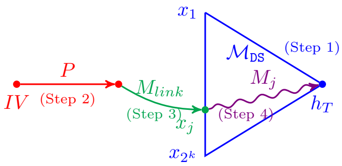


Figure: Nostradamus attack process [BGLP22]

Generic Bounds of Nostradamus

	Classic	Quantum
Offline	$\mathcal{O}(k^{1/2} \cdot 2^{(n+k)/2})$	$\mathcal{O}(k^{1/3} \cdot 2^{(n+2k)/3})$
Online	$\mathcal{O}(2^{n-k})$	$\mathcal{O}(2^{(n-k)/2})$
Balance cond.	$k = n/3$	$k = n/7$
Overall cplx.	$\mathcal{O}(n^{1/2} \cdot 2^{2n/3})$	$\mathcal{O}(n^{1/3} \cdot 2^{3n/7})$

[2] Zhiyu Zhang, Siwei Sun, Caibing Wang, and Lei Hu. Classical and Quantum Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing. ToSC 2023

Generic Bounds of Nostradamus

	Classic	Quantum
Offline	$\mathcal{O}(k^{1/2} \cdot 2^{(n+k)/2})$	$\mathcal{O}(k^{1/3} \cdot 2^{(n+2k)/3})$
Online	$\mathcal{O}(2^{n-k})$	$\mathcal{O}(2^{(n-k)/2})$
Balance cond.	$k = n/3$	$k = n/7$
Overall cplx.	$\mathcal{O}(n^{1/2} \cdot 2^{2n/3})$	$\mathcal{O}(n^{1/3} \cdot 2^{3n/7})$

Integration of Meet-In-The-Middle (MITM) Attack[2]

- Use MITM attack to accelerate the online phase
- Shift the optimum towards a more efficient overall time complexity

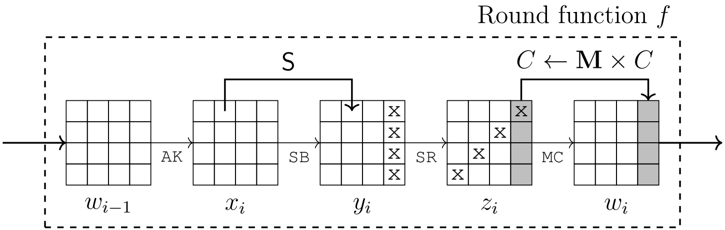
[2] Zhiyu Zhang, Siwei Sun, Caibing Wang, and Lei Hu. Classical and Quantum Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing. ToSC 2023

Outline

AES-like Round function

Operators

- SubBytes: byte-wise substitution
- ShiftRows: byte-wise permutation, visualized as a circular left shift
- MixColumns: column-wise left multiplication of a 4-by-4 (MDS) matrix
- AddRoundKey: bit-wise XOR of the round key



Overview of MITM Attacks

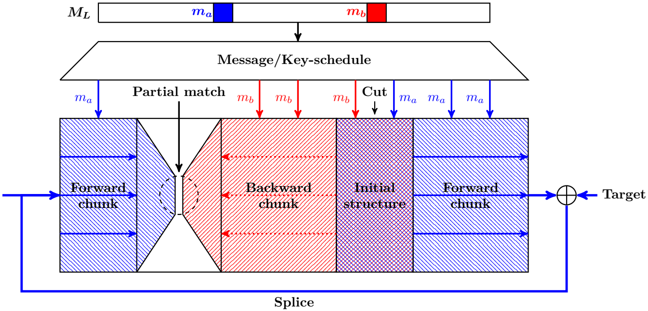


Figure: A high-level overview of MITM attacks by Sasaki

1. Partition the compression function into two independent chunks
2. Distribute DoF to both chunks and compute to the matching point
3. Obtain candidates that pass the partial match filter

Automatic search of MITM attacks

Automation by MILP

- Model propagation rules and objective in MILP
- Use optimizers to search for the optimal attack strategy

Conventional byte classification

- neutral byte: only known in the current chunk, its influence to the opposite chunk is constant (computational independence)
  - ■ (blue) denotes a neutral byte for forward chunk
  - ■ (red) denotes a neutral byte for backward chunk
- constant byte: predefined and known in both chunks, denote by ■ (gray)
- unknown byte: not known in either chunk, denote by □

Outline

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Complexity of MITM Nostradamus Attack in [ZSWH23]

	Classic	Quantum
Offline	$\mathcal{O}(k^{1/2} \cdot 2^{(n+k)/2})$	$\mathcal{O}(k^{1/3} \cdot 2^{(n+2k)/3})$
Online (generic)	$\mathcal{O}(2^{n-k})$	$\mathcal{O}(2^{n/2-k/2})$
Online (MITM)	$\mathcal{O}(2^{n-\tau^C})$	$\mathcal{O}(2^{n/2-\tau^Q})$
Attack cond.	$k < n/3$, $\tau^C > n/3$	$k < n/7$, $\tau^Q > n/7$

- τ^C/τ^Q: classic/quantum MITM attack advantage
- Distribute blue/red initial DoF in the target for a multi-target MITM attack
- Lower bound of the diamond structure size (in $\log 2$): $k \geq B^{\mathtt{TAG}} + R^{\mathtt{TAG}}$

Extend the Multi-target Setting

Recall the format of diamond leaves:

$n-k$ fixed bits	k free bits

Previous approach [ZSWH23]

- Allow only blue, red and gray bytes in target during search (preimage attack)
- Set the gray bytes as the fixed part
- Use the blue/red bytes to match the free part (multi-target)

Modification done in this work

- Search for a parital preimage attack instead of a preimage attack
- Introduce white bytes in target, and use all non-gray bytes to match the free part
- Modify the objective and expand the search space
- Lead to round breakthroughs on AES and Whirlpool

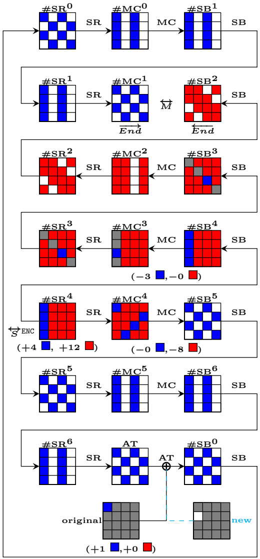
Refined Complexity Analysis

	Classic	Quantum
Offline	$\mathcal{O}(k^{1/2} \cdot 2^{(n+k)/2})$	$\mathcal{O}(k^{1/3} \cdot 2^{(n+2k)/3})$
Online (generic)	$\mathcal{O}(2^{n-k})$	$\mathcal{O}(2^{n/2-k/2})$
Online (prev)	$\mathcal{O}(2^{n-\tau^C_{prev}})$	$\mathcal{O}(2^{n/2-\tau^Q_{prev}})$
Online (new)	$\mathcal{O}(2^{n-k_w-\tau^C_{new}})$	$\mathcal{O}(2^{n/2-k_w/2-\tau^Q_{new}})$
Attack cond.	$k < n/3$, $k_w + \tau^C_{new} > n/3$	$k < n/7$, $k_w + \tau^C_{new} > n/7$

- τ^C/τ^Q: classic/quantum MITM attack advantage
- $k_w \leq W^{\mathtt{TAG}}$: length of bits that are not matched in a partial preimage attack
- Lower bound of the diamond structure size (in $\log 2$): $k \geq k_w + B^{\mathtt{TAG}} + R^{\mathtt{TAG}}$

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Effect of Our Modification

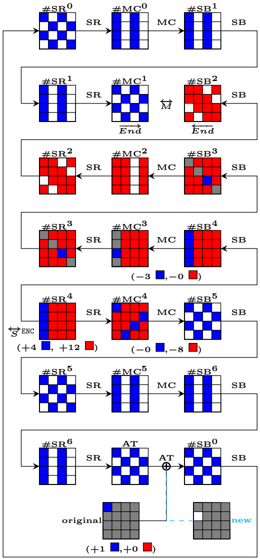


Offline	$\mathcal{O}(k^{1/2} \cdot 2^{(n+k)/2})$
Online (prev)	$\mathcal{O}(2^{n-\tau^C_{prev}})$
Online (new)	$\mathcal{O}(2^{n-k_w-\tau^C_{new}})$

Previous

- $k = B^{\mathtt{TAG}} = 8$ (1 byte)
- $Adv = \tau^C_{prev} = \min(d_B, d_R, m)$

Effect of Our Modification



Offline	$\mathcal{O}(k^{1/2} \cdot 2^{(n+k)/2})$
Online (prev)	$\mathcal{O}(2^{n-\tau^C_{prev}})$
Online (new)	$\mathcal{O}(2^{n-k_w-\tau^C_{new}})$

Previous

- $k = B^{\mathtt{TAG}} = 8$ (1 byte)
- $Adv = \tau^C_{prev} = \min(d_B, d_R, m)$

Modification $B^{\mathtt{TAG}} \rightarrow W^{\mathtt{TAG}}$

- $k = k_w = W^{\mathtt{TAG}} = 8$ (1 byte)
- $Adv = k_w + \tau^C_{new} = 8 + \min(d_B - 8, d_R, m)$
  $\geq \min(d_B, d_R, m) = \tau^C_{prev}$

Outline

Result Summary (Classical)

Target	Setting	#Rounds	Time	C-Mem	qRAM	Source
AES-MMO	Classical	6	$2^{82.7}$	$2^{82.2}$	-	[ZSWH23]
	Classical	6	2^{77}	2^{76}	-	This work
	Classical	7	2^{83}	2^{82}	-	This work
	Classical	any	$2^{88.1}$	$2^{87.8}$	-	[KK06; BFH22]
	Quantum	7	$2^{54.1}$	2^{14}	$2^{49.5}$ QRACM+2^{8} QRAQM	This work, [ZSWH23]
	Quantum	any	$2^{56.4}$	2^{17}	$2^{56.3}$ QRACM	[BFH22]
	Quantum	7	2^{58}	2^{30}	2^{8} QRAQM	This work
	Quantum	any	$2^{60.9}$	$2^{31.6}$	$O(n)$	[DLPZ23]
Whirlpool	Classical	4	2^{320}	2^{192}	-	[ZSWH23]
	Classical	6	2^{334}	2^{333}	-	This work
	Classical	any	$2^{344.7}$	$2^{344.2}$	-	[KK06; BFH22]
	Quantum	6	$2^{216.7}$	2^{64}	$2^{215.3}$ QRACM+2^{16} QRAQM	[ZSWH23]
	Quantum	6	2^{214}	2^{61}	$2^{207.4}$ QRACM+2^{24} QRAQM	This work
	Quantum	any	$2^{221.3}$	2^{71}	$2^{220.1}$ QRACM	[BFH22]
	Quantum	6	2^{230}	2^{117}	2^{24} QRAQM	This work
	Quantum	any	$2^{238.3}$	$2^{121.2}$	$O(n)$	[DLPZ23]

Result Summary (Quantum)

Target	Setting	#Rounds	Time	C-Mem	qRAM	Source
AES-MMO	Classical	6	$2^{82.7}$	$2^{82.2}$	-	[ZSWH23]
	Classical	6	2^{77}	2^{76}	-	This work
	Classical	7	2^{83}	2^{82}	-	This work
	Classical	any	$2^{88.1}$	$2^{87.8}$	-	[KK06; BFH22]
	Quantum	7	$2^{54.1}$	2^{14}	$2^{49.5}$ QRACM+2^{8} QRAQM	This work, [ZSWH23]
	Quantum	any	$2^{56.4}$	2^{17}	$2^{56.3}$ QRACM	[BFH22]
	Quantum	7	2^{58}	2^{30}	2^{8} QRAQM	This work
	Quantum	any	$2^{60.9}$	$2^{31.6}$	$O(n)$	[DLPZ23]
Whirlpool	Classical	4	2^{320}	2^{192}	-	[ZSWH23]
	Classical	6	2^{334}	2^{333}	-	This work
	Classical	any	$2^{344.7}$	$2^{344.2}$	-	[KK06; BFH22]
	Quantum	6	$2^{216.7}$	2^{64}	$2^{215.3}$ QRACM+2^{16} QRAQM	[ZSWH23]
	Quantum	6	2^{214}	2^{61}	$2^{207.4}$ QRACM+2^{24} QRAQM	This work
	Quantum	any	$2^{221.3}$	2^{71}	$2^{220.1}$ QRACM	[BFH22]
	Quantum	6	2^{230}	2^{117}	2^{24} QRAQM	This work
	Quantum	any	$2^{238.3}$	$2^{121.2}$	$O(n)$	[DLPZ23]

References

[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. Lecture Notes in Computer Science. Springer, 2006, pp. 183–200. DOI: 10.1007/11761679_12. URL: https://doi.org/10.1007/11761679%5C_12.

[BGLP22] Zhenzhen Bao, Jian Guo, Shun Li, and Phuong Pham. "Evaluating the Security of Merkle-Damgård Hash Functions and Combiners in Quantum Settings". In: *Network and System Security - 16th International Conference, NSS 2022, Denarau Island, Fiji, December 9-12, 2022, Proceedings*. Ed. by Xingliang Yuan, Guangdong Bai, Cristina Alcaraz, and Suryadipta Majumdar. Vol. 13787. Lecture Notes in Computer Science. Springer, 2022, pp. 687–711. DOI: 10.1007/978-3-031-23020-2_39. URL: https://doi.org/10.1007/978-3-031-23020-2%5C_39.

[BFH22] Barbara Jiabao Benedikt, Marc Fischlin, and Moritz Huppert. "Nostradamus Goes Quantum". In: *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III*. Ed. by Shweta Agrawal and Dongdai Lin. Vol. 13793. Lecture Notes in Computer Science. Springer, 2022, pp. 583–613. DOI: 10.1007/978-3-031-22969-5_20. URL: https://doi.org/10.1007/978-3-031-22969-5%5C_20.

[DLPZ23] Xiaoyang Dong, Shun Li, Phuong Pham, and Guoyan Zhang. "Quantum Attacks on Hash Constructions with Low Quantum Random Access Memory". In: *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part III*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14440. Lecture Notes in Computer Science. Springer, 2023, pp. 3–33. DOI: 10.1007/978-981-99-8727-6_1. URL: https://doi.org/10.1007/978-981-99-8727-6%5C_1.

[ZSWH23] Zhiyu Zhang, Siwei Sun, Caibing Wang, and Lei Hu. "Classical and Quantum Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing". In: *IACR Trans. Symmetric Cryptol.* 2023.2 (2023), pp. 224–252. DOI: 10.46586/TOSC.V2023.I2.224-252. URL: https://doi.org/10.46586/tosc.v2023.i2.224-252.

TYFL