Classical and Quantum Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing

Zhiyu Zhang [1,3]   Siwei Sun* [2]   Caibing Wang [1,3,4]   Lei Hu [1,3]

[1]Institute of Information Engineering, CAS

[2]School of Cryptology, University of Chinese Academy of Sciences

[3]School of Cyber Security, University of Chinese Academy of Sciences

[4]Beijing Electronic Science and Technology Institute

FSE 2024, March 29, 2024

University of Chinese Academy of Sciences

Outline

Outline

University of Chinese Academy of Sciences

Background

Mr. Nostradamus and his friends passed by a lottery shop in Leuven several days ago. He said to his friends:
“I can predict the lottery numbers of March 27th, I have written them down in my diary. I won’t show you my diary now, but I could tell you the hash value of it.”

University of Chinese Academy of Sciences

Background

Mr. Nostradamus and his friends passed by a lottery shop in Leuven several days ago. He said to his friends:
"I can predict the lottery numbers of March 27th, I have written them down in my diary. I won't show you my diary now, but I could tell you the hash value of it."

Mr. Nostradamus sent a hash value $\mathcal{T}$ to his friends.

Background

After the winning numbers were announced,
Mr. Nostradamus showed his diary $\mathcal{D}$ to his friend.

The first line of the diary is:
"The lottery numbers of March 27th are 2 3 19 40 42 43 4."
Which is exactly the same as the winning numbers.
Furthermore, it could be verified that $H(\mathcal{D}) = \mathcal{T}$.

Background

After the winning numbers were announced,
Mr. Nostradamus showed his diary $\mathcal{D}$ to his friend.

The first line of the diary is:
“The lottery numbers of March 27th are 2 3 19 40 42 43 4.”
Which is exactly the same as the winning numbers.
Furthermore, it could be verified that $H(\mathcal{D}) = \mathcal{T}$.

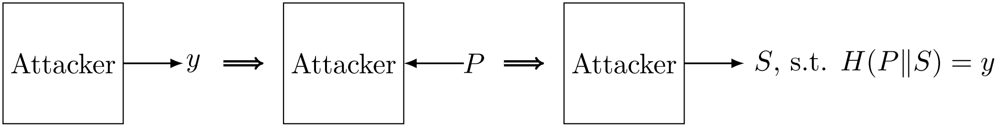
How did Mr. Nostradamus do that?

Outline

University of Chinese Academy of Sciences

The Herding Attack [KK06]

The chosen target forced prefix (CTFP) attack was first introduced by Kelsey and Kohno at EUROCRYPT 2006. They proposed the herding attack on iterated hash functions.

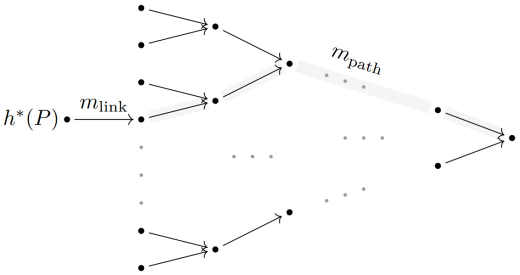


The "Nostradamus attack" is the use of herding to commit to the hash of a message that the attacker doesn't even know.

The Herding Attack [KK06]

The attack is divided into two phases:

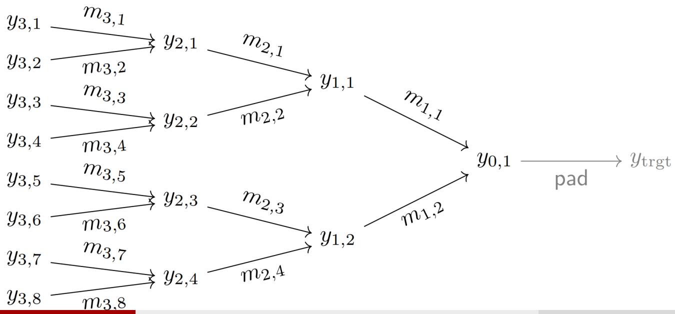
1. **Offline phase**: Construct a diamond structure.
2. **Online phase**: Search for the link message.



The Herding Attack [KK06]: Offline phase

Diamond structure: 2^k multi collisions

- Node $y_{i,j}$: the intermediate value of the Merkel-Damgård constructions.
- Edge $m_{i,j}$: the message block that links two intermediate value, $CF(y_{i,j}, m_{i,j}) = y_{i-1,\lceil j/2 \rceil}$
- Time complexity: $\mathcal{O}(2^{\frac{n+k}{2}})$. Memory complexity: $\mathcal{O}(2^k)$.

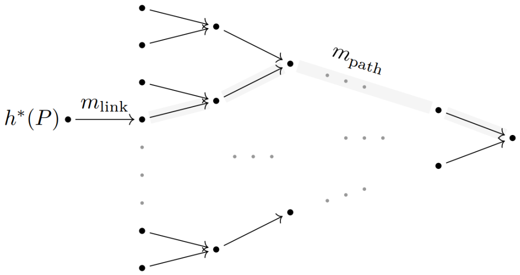


University of Chinese Academy of Sciences

The Herding Attack [KK06]: Online phase

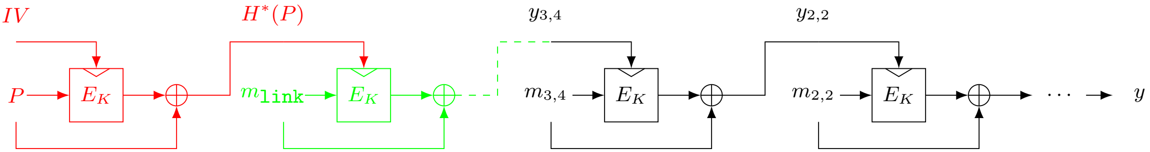
Once the prefix P is given, the attacker could exhaustive search for the link message, connecting the prefix with a leaf node.

Time complexity: $\mathcal{O}(2^{n-k})$. Memory complexity: $\mathcal{O}(2^k)$.



The Herding Attack [KK06]

To minimize the time complexity of both phases, the optimal choice of k is $\frac{n}{3}$.
Time complexity: $\mathcal{O}(\sqrt{n} \cdot 2^{2n/3})$. Memory complexity: $\mathcal{O}(2^{n/3})$.



Online Phase
Exhaustive Search

Offline Phase
Collision-based Method

The Quantum Nostradamus Attack

At ASIACRYPT 2022, Benedikt, Fischli, and Huppert [BFH22] followed the classical herding attack and use Grover-based quantum algorithms to accelerate both offline and online phases.

The Quantum Nostradamus Attack

At ASIACRYPT 2022, Benedikt, Fischli, and Huppert [BFH22] followed the classical herding attack and use Grover-based quantum algorithms to accelerate both offline and online phases.

At ASIACRYPT 2023, Dong et al. [Don+23] proposed a quantum Nostradamus attack with little quantum memory.

The Quantum Nostradamus Attack

At ASIACRYPT 2022, Benedikt, Fischli, and Huppert [BFH22] followed the classical herding attack and use Grover-based quantum algorithms to accelerate both offline and online phases.

At ASIACRYPT 2023, Dong et al. [Don+23] proposed a quantum Nostradamus attack with little quantum memory.

Table: The Generic Nostradamus Attacks

Ref.	Time	c-Memory	qRam	Setting
[KK06]	$2^{\frac{2n}{3}}$	$2^{\frac{2n}{3}}$	0	Classical
[BFH22]	$2^{\frac{3n}{7}}$	0	$2^{\frac{n}{7}}$	Quantum
[Don+23]	$2^{\frac{6n}{13}}$	$2^{\frac{3n}{13}}$	$\mathcal{O}(n)$	Quantum

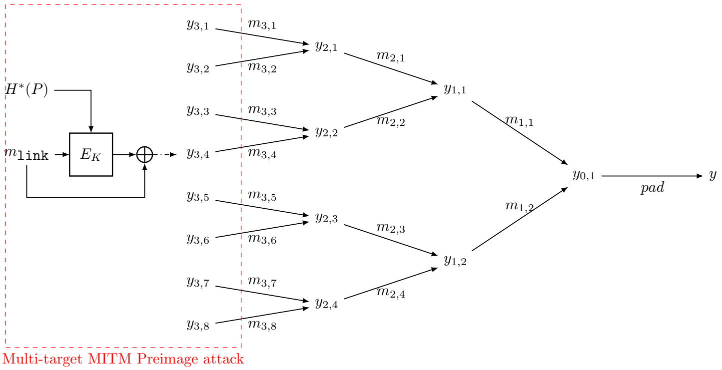
University of Chinese Academy of Sciences

Outline

University of Chinese Academy of Sciences

An insight on the herding attack

The online phase of a herding attack can be viewed as a multi-target preimage attack.



The Meet-in-the-Middle Attack

The meet-in-the-middle attack is one of the most effective methods for attacking hash functions.

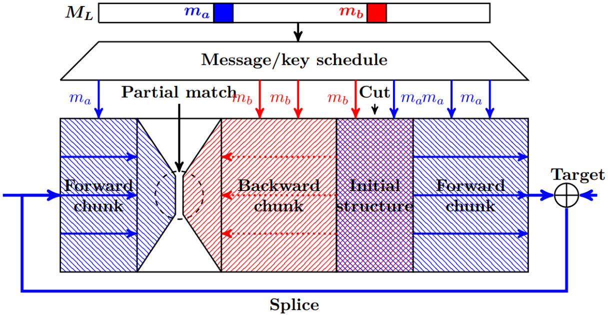


Figure: An overview of the meet-in-the-middle attack.

University of Chinese Academy of Sciences

The Meet-in-the-Middle Attack

The Meet-in-the-Middle Attack

MILP-based Methods

- First introduced by Bao et al. [Bao+21] at EUROCRYPT 2021.
- Further researches were conducted in [Don+21; SS22; Bao+22; Qin+23].

The Meet-in-the-Middle Attack

MILP-based Methods

- First introduced by Bao et al. [Bao+21] at EUROCRYPT 2021.
- Further researches were conducted in [Don+21; SS22; Bao+22; Qin+23].

The Quantum MITM Attack

- Proposed by Schrottenloher and Stevens [SS22] at CRYPTO 2022.
- Could be be quadratically accelerated when choosing the parameters properly.

The Meet-in-the-Middle Attack

MILP-based Methods

- First introduced by Bao et al. [Bao+21] at EUROCRYPT 2021.
- Further researches were conducted in [Don+21; SS22; Bao+22; Qin+23].

The Quantum MITM Attack

- Proposed by Schrottenloher and Stevens [SS22] at CRYPTO 2022.
- Could be be quadratically accelerated when choosing the parameters properly.

Attack Complexity (in log_2)

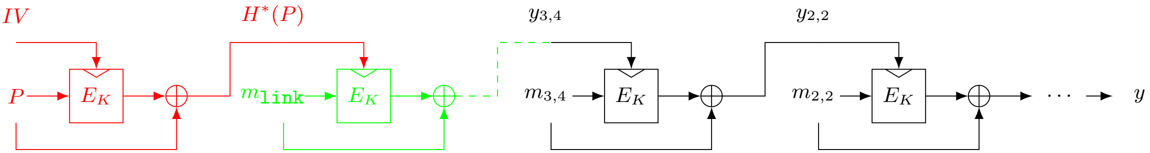
- Classical : $n - \min(d_{\mathcal{B}}, d_{\mathcal{R}}, d_{\mathcal{M}})$
- Quantum : $(n - \min(|d_{\mathcal{B}} - d_{\mathcal{R}}|, d_{\mathcal{B}}, d_{\mathcal{R}}, d_{\mathcal{M}}))/2$

University of Chinese Academy of Sciences

The MITM Nostradamus Attack

The Meet-in-the-Middle Nostradamus Attack

- **Offline phase**: Construct a diamond structure utilizing the previous methods [KK06; BFH22].
- **Online phase**: Mount a meet-in-the-middle attack on the compression function to find a linking message.



Online Phase
MITM Attack

Offline Phase
Collision-based Method

The MITM Nostradamus Attack

Complexities

- Time complexity:

$$\max\left(2^{n-\min(d_{\mathcal{B}},d_{\mathcal{R}},d_{\mathcal{M}})}, \sqrt{k}\cdot 2^{(n+k)/2}\right),$$

- Memory complexity:

$$\max\left(2^{k}, min(2^{d_{\mathcal{B}}}, 2^{d_{\mathcal{R}}})\right).$$

To perform a faster attack than the generic attack, we need (we omit the factor $\sqrt{k}$ here.)

$$k < \frac{n}{3} \text{ and } \min\left(d_{\mathcal{B}}, d_{\mathcal{R}}, d_{\mathcal{M}}\right) > \frac{n}{3}.$$

The Quantum MITM Nostradamus Attack

Complexities

- Time complexity:

$$\max(2^{\frac{1}{2}(n-\min(|d_{\mathcal{B}}-d_{\mathcal{R}}|,d_{\mathcal{B}},d_{\mathcal{R}},d_{\mathcal{M}}))}, \sqrt[3]{k}\cdot 2^{(n+2k)/3}),$$

- Memory complexity:

$$\max\left(2^k, min(2^{d_{\mathcal{B}}}, 2^{d_{\mathcal{R}}})\right).$$

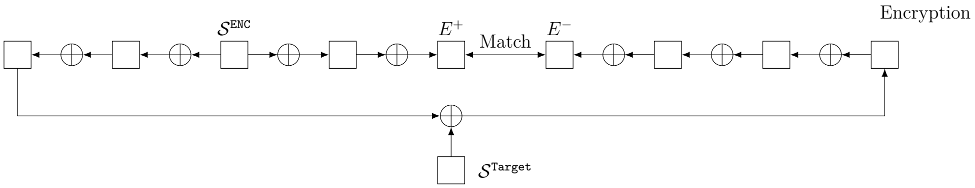
To perform a faster attack than the generic attack, we need (we omit the factor $\sqrt{k}$ here.)

$$k \leq \frac{n}{7}, \min\left(\left|d_{\mathcal{B}} - d_{\mathcal{R}}\right|, d_{\mathcal{B}}, d_{\mathcal{R}}, d_{\mathcal{M}}\right) \geq \frac{n}{7}.$$

University of Chinese Academy of Sciences

MILP-based search method for MITM Nostradamus Attacks

Based on the MILP model of the MITM preimage attack, we proposed an automated seach method for the MITM Nostradamus attacks on AES-like hashing. The notations and propagation rules are the same as previous works [Bao+21; Don+21; Bao+22].



University of Chinese Academy of Sciences

MILP-based search method for MITM Nostradamus Attacks

Additional Rules for MITM Nostradamus Attacks

$$\begin{cases} O_{\texttt{mitm}} & \leq & \mathrm{DoF}^{\mathcal{B}}, \\ O_{\texttt{mitm}} & \leq & \mathrm{DoF}^{\mathcal{R}}, \\ O_{\texttt{mitm}} & \leq & \mathrm{DoM}, \end{cases} \quad \begin{cases} O_{\texttt{total}} & \geq & \frac{n+k}{2}, \\ O_{\texttt{total}} & \geq & n - w \cdot O_{\texttt{mitm}}. \end{cases}$$

Additional Rules for Quantum MITM Nostradamus Attacks

$$\begin{cases} O_{\texttt{mitm}} & \leq & \frac{\mathrm{DoF}^{\mathcal{B}}}{2}, \\ O_{\texttt{mitm}} & \leq & \frac{\mathrm{DoF}^{\mathcal{R}}}{2}, \\ O_{\texttt{mitm}} & \leq & \frac{\max(\mathrm{DoF}^{\mathcal{B}} - \mathrm{DoF}^{\mathcal{R}}, \mathrm{DoF}^{\mathcal{R}} - \mathrm{DoF}^{\mathcal{B}})}{2}, \\ O_{\texttt{mitm}} & \leq & \frac{\mathrm{DoM}}{2}, \end{cases} \quad \begin{cases} O_{\texttt{total}} & \geq & \frac{n+2\cdot k}{3}, \\ O_{\texttt{total}} & \geq & \frac{n}{2} - w \cdot O_{\texttt{mitm}}, \end{cases}$$

University of Chinese Academy of Sciences

Outline

University of Chinese Academy of Sciences

Results

Table: Results of Nostradamus attacks.

Target	Rounds	Time	C-Mem	QRAM	Setting	Ref.
AES-MMO	6/10	$2^{82.7}$	2^{48}	-	Classic	This work
	7/10	2^{56}	-	2^{8}	Quantum	This work
	7/10	$2^{54.1}$	-	2^{14}	Quantum	This work
	any	$2^{88.8}$	$2^{42.6}$	-	Classic	[KK06]
	any	$2^{57.2}$	-	$2^{18.3}$	Quantum	[BFH22]
WHIRLPOOL	4/10	2^{320}	2^{192}	-	Classic	This work
	6/10	$2^{216.7}$	-	2^{64}	Quantum	This work
	any	$2^{351.8}$	$2^{170.6}$	-	Classic	[KK06]
	any	$2^{226.3}$	-	$2^{73.1}$	Quantum	[BFH22]

Conclusions and Future Works

- The first dedicated Nostradamus attack on AES-like hashing.
- Could be quadratically accelerated in quantum setting.

Conclusions and Future Works

- The first dedicated Nostradamus attack on AES-like hashing.
- Could be quadratically accelerated in quantum setting.

Future works

- Constructing diamond structures by dedicated methods.
- Improved the MITM attack: more techniques, more refined models, partial preimage attacks.

Conclusions and Future Works

- The first dedicated Nostradamus attack on AES-like hashing.
- Could be quadratically accelerated in quantum setting.

Future works

- Constructing diamond structures by dedicated methods.
- Improved the MITM attack: more techniques, more refined models, partial preimage attacks.

Thank you for listening!

Reference I

Some figures are from [Zha+23; KK06; BFH22].

[KK06] John Kelsey and Tadayoshi Kohno. "Herding hash functions and the Nostradamus attack". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2006, pp. 183–200.

[BFH22] Barbara Jiabao Benedikt, Marc Fischlin, and Moritz Huppert. "Nostradamus goes quantum". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2022, pp. 583–613.

[Don+23] Xiaoyang Dong et al. "Quantum Attacks on Hash Constructions with Low Quantum Random Access Memory". In: *Cryptology ePrint Archive* (2023).

Reference II

[Bao+21] Zhenzhen Bao et al. “Automatic search of meet-in-the-middle preimage attacks on AES-like hashing”. In: *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I 40*. Springer. 2021, pp. 771–804.

[Don+21] Xiaoyang Dong et al. “Meet-in-the-middle attacks revisited: key-recovery, collision, and preimage attacks”. In: *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part III 41*. Springer. 2021, pp. 278–308.

[SS22] André Schrottenloher and Marc Stevens. “Simplified MITM modeling for permutations: New (quantum) attacks”. In: *Annual International Cryptology Conference*. Springer. 2022, pp. 717–747.

Reference III

[Bao+22] Zhenzhen Bao et al. "Superposition meet-in-the-middle attacks: updates on fundamental security of AES-like hashing". In: *Annual International Cryptology Conference*. Springer. 2022, pp. 64–93.

[Qin+23] Lingyue Qin et al. "Meet-in-the-middle preimage attacks on sponge-based hashing". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 158–188.

[Zha+23] Zhiyu Zhang et al. "Classical and Quantum Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing". In: *IACR Transactions on Symmetric Cryptology* (2023), pp. 224–252.