Quantum Attacks on Hash Constructions with Low Quantum Random Access Memory

Xiaoyang Dong[1,2,6,7] Shun Li[3] Phuong Pham[3] Guoyan Zhang[4,5,7]

[1]Institute for Advanced Study, BNRist, Tsinghua University, Beijing, China

[2]State Key Laboratory of Cryptology, P.O.Box 5159, Beijing, 100878, China

[3]School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore,

[4]School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China,

[5]Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China

[6]Zhongguancun Laboratory, Beijing, China

[7]Shandong Institute of Blockchain, Jinan, China

ASIACRYPT 2023, Dec 6

Security Level of Cryptographic Hash Functions I

For a hash function $\mathcal{H} : \{0,1\}^\star \to \{0,1\}^n$,

Pre-image resistance

Given a hash value y, it is difficult to find a message x such that $\mathcal{H}(x) = y$.

Security Level of Cryptographic Hash Functions I

For a hash function $\mathcal{H} : \{0,1\}^\star \to \{0,1\}^n$,

Pre-image resistance

Given a hash value y, it is difficult to find a message x such that $\mathcal{H}(x) = y$.

Second pre-image resistance

Given a hash value $\mathcal{H}(x')$, it is difficult to find a message x ($x \neq x'$) such that $\mathcal{H}(x) = \mathcal{H}(x')$.

Security Level of Cryptographic Hash Functions I

For a hash function $\mathcal{H} : \{0,1\}^\star \rightarrow \{0,1\}^n$,

Pre-image resistance

Given a hash value y, it is difficult to find a message x such that $\mathcal{H}(x) = y$.

Second pre-image resistance

Given a hash value $\mathcal{H}(x')$, it is difficult to find a message x ($x \neq x'$) such that $\mathcal{H}(x) = \mathcal{H}(x')$.

Collision resistance

It is difficult to find two messages x and x' such that $\mathcal{H}(x) = \mathcal{H}(x')$.

Security Level of Cryptographic Hash Functions I

For a hash function $\mathcal{H} : \{0,1\}^\star \to \{0,1\}^n$, the generic time complexity is:

Pre-image resistance

Given a hash value y, it requires $O(2^n)$ to find a message x such that $\mathcal{H}(x) = y$.

Second pre-image resistance

Given a hash value $\mathcal{H}(x')$, it requires $O(2^n)$ to find a message x ($x \neq x'$) such that $\mathcal{H}(x) = \mathcal{H}(x')$.

Collision resistance

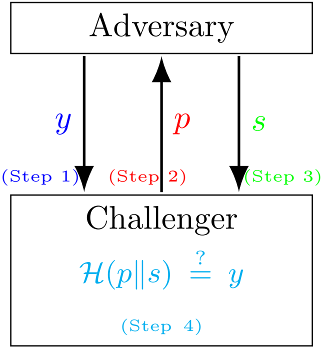
It requires $O(2^{n/2})$ to find two messages x and x' such that $\mathcal{H}(x) = \mathcal{H}(x')$.

Security Level of Cryptographic Hash Functions II

For a hash function $\mathcal{H} : \{0,1\}^\star \to \{0,1\}^n$,

Chosen Target Forced Prefix preimage resistance[KK06]

The adversary has the liberty to choose any hash value y, and in response, the challenger selects a message prefix p. It is difficult for the adversary to find a suitable message suffix s such that $\mathcal{H}(p\|s) = y$.



For **iterated** hash functions, [KK06] proposed a generic algorithm requiring time complexity of $O(2^{2n/3})$, known as **Herding Attack**.

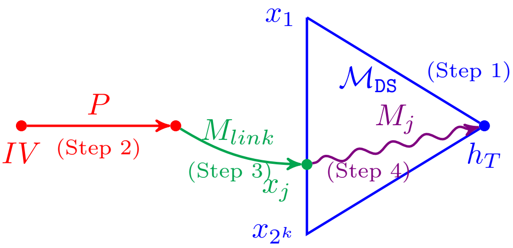
[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

Quantum Speedup

Summary of our results. QRACM: quantum accessible classical memory, QRAQM: quantum accessible quantum memory, cRAM: classical random access memory

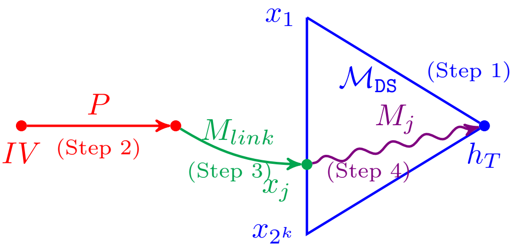
Target	Attacks	Settings	Time	Qubits	QRACM	QRAQM	cRAM	Generic	Ref.
$\mathcal{H}$	Herding	Classical	$2^{0.67n}$	-	-	-	$2^{0.67n}$	-	[KK06]
		Quantum	$2^{0.43n}$	$\mathcal{O}(n)$	$2^{0.43n}$	-	-	-	[BFH22]
		Quantum	$2^{0.46n}$	$\mathcal{O}(n)$	-	-	$2^{0.23n}$	-	**Ours**
$\mathcal{H}_1 \oplus \mathcal{H}_2$	Preimage	Classical	$2^{0.83n}$	-	-	-	$2^{0.33n}$	2^{n}	[LW15]
		Classical	$2^{0.67n}$	-	-	-	-	2^{n}	[Din16]
		Classical	$2^{0.612n}$	-	-	-	$2^{0.61n}$	2^{n}	[BDG+20]
		Quantum	$2^{0.476n}$	$\mathcal{O}(n)$	-	$2^{0.333n}$	-	$2^{0.5n}$	[BGLP22]
		Quantum	$2^{0.495n}$	$2^{0.143n}$	$2^{0.033n}$	-	$2^{0.2n}$	$2^{0.5n}$	[BGLP22]
		Quantum	$2^{0.493n}$	$2^{0.013n}$	$2^{0.047n}$	-	$2^{0.2n}$	$2^{0.5n}$	**Ours**
		Quantum	$2^{0.485n}$	$\mathcal{O}(n)$	$2^{0.057n}$	$2^{0.0285n}$	$2^{0.2n}$	$2^{0.5n}$	**Ours**
		Quantum	$2^{0.485n}$	$\mathcal{O}(n)$	$2^{0.043n}$	$2^{0.0285n}$	$2^{0.2n}$	$2^{0.5n}$	**Ours**
$\mathcal{H}_1 \Vert \mathcal{H}_2$	Collision	Classical	$2^{0.5n}$	-	-	-	-	2^{n}	[J04]
		Quantum	$2^{0.333n}$	$\mathcal{O}(n)$	-	$2^{0.333n}$	-	$2^{0.67n}$	[BGLP22]
		Quantum	$2^{0.43n}$	$2^{0.143n}$	-	-	$2^{0.2n}$	$2^{0.67n}$	[BGLP22]
		Quantum	$2^{0.4n}$	$\mathcal{O}(n)$	-	-	$2^{0.2n}$	$2^{0.67n}$	**Ours**
	Herding	Classical	$2^{0.67n}$	-	-	-	$2^{0.33n}$	-	[ABDK09]
		Quantum	$2^{0.444n}$	$\mathcal{O}(n)$	-	$2^{0.333n}$	-	-	[BGLP22]
		Quantum	$2^{0.49n}$	$2^{0.143n}$	-	-	$2^{0.2n}$	-	[BGLP22]
		Quantum	$2^{0.467n}$	$\mathcal{O}(n)$	-	-	$2^{0.2n}$	-	**Ours**
Hash-Twice	Herding	Classical	$2^{0.667n}$	-	-	-	$2^{0.33n}$	-	[ABDK09]
		Quantum	$2^{0.467n}$	$\mathcal{O}(n)$	-	-	$2^{0.2n}$	-	**Ours**
Zipper	Herding	Classical	$2^{0.667n}$	-	-	-	$2^{0.33n}$	-	[ABDK09]
		Quantum	$2^{0.467n}$	$\mathcal{O}(n)$	-	-	$2^{0.2n}$	-	**Ours**

Quantum Herding Attack on $\mathcal{H}$ without qRAM



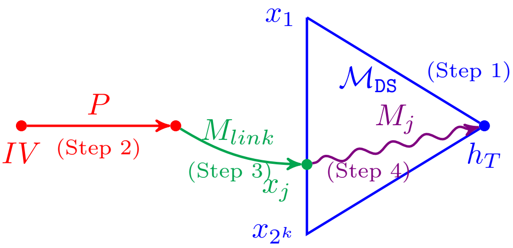
- Step 1: build a 2^k-diamond structure. The r most significant bits (MSB) of x_i are zeros. Store the diamond in D with classical memory.

Quantum Herding Attack on $\mathcal{H}$ without qRAM



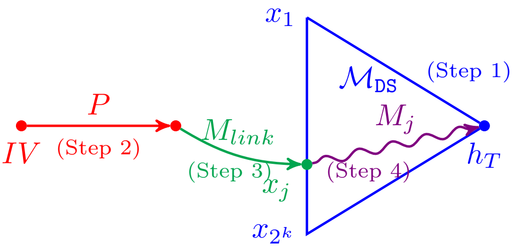
- Step 1: build a 2^k-diamond structure. The r most significant bits (MSB) of x_i are zeros. Store the diamond in D with classical memory.
- Step 2: calculate the chaining hash value x from given prefix.

Quantum Herding Attack on $\mathcal{H}$ without qRAM



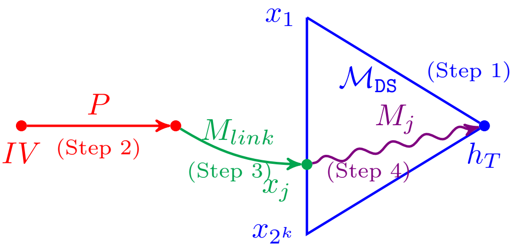
- Step 1: build a 2^k-diamond structure. The r most significant bits (MSB) of x_i are zeros. Store the diamond in D with classical memory.
- Step 2: calculate the chaining hash value x from given prefix.
- Step 3: find a single block message M_{link} to connect x with some value $x_j \in D$.

Quantum Herding Attack on $\mathcal{H}$ without qRAM



- Step 1: build a 2^k-diamond structure. The r most significant bits (MSB) of x_i are zeros. Store the diamond in D with classical memory.
- Step 2: calculate the chaining hash value x from given prefix.
- Step 3: find a single block message M_{link} to connect x with some value $x_j \in D$.
- Step 4: check D for the message blocks M_j linking x_j to h_T and output the message $M = P \| M_{link} \| M_j$.

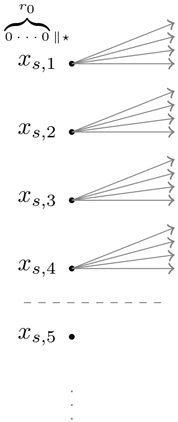
Quantum Herding Attack on $\mathcal{H}$ without qRAM



Step 1 and Step 3 have been adaptively modified in compared to [BFH22], incorporating quantum algorithms as outlined in [CNS17].

- Step 1: build a 2^k-diamond structure. The r most significant bits (MSB) of x_i are zeros. Store the diamond in D with classical memory.
- Step 2: calculate the chaining hash value x from given prefix.
- Step 3: find a single block message M_{link} to connect x with some value $x_j \in D$.
- Step 4: check D for the message blocks M_j linking x_j to h_T and output the message $M = P \| M_{link} \| M_j$.

Adaptive Modification to Step 1

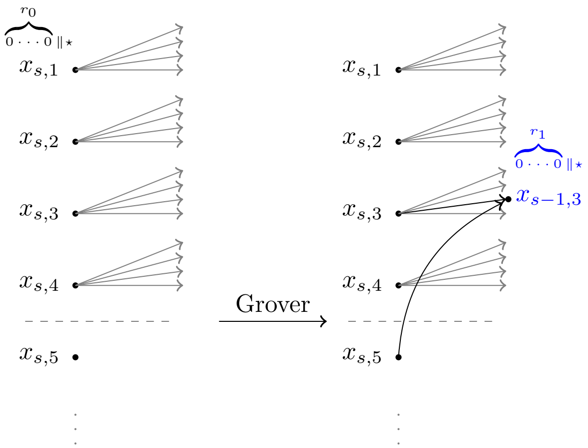


1. Choose first layer with restriction on r_0 MSB

Start with 2^s leave nodes whose r_0-bit suffix are zeros.

Leaf nodes with r_0 0s suffix are not relevant to this diamond building algorithm. After a diamond is built whose leaves are suffixed with r_0 0s, we can apply the CNS algorithm to find a linking message whose digest collides to one of those leaves.

Adaptive Modification to Step 1

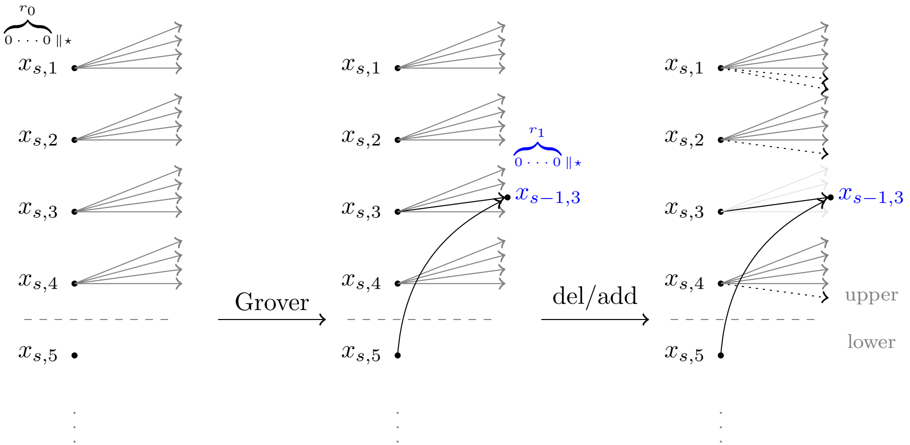


2. Compute the hash values of upper half with restriction on r_1 MSB

i For each node $x_{s,i}$ in the upper half, run Grover's algorithm to find m_j so that the r_1 MSBs of $h(m_j, x_{s,i})$ are zeros.

ii Repeat above step $\frac{2^l}{2^{s-1}}$ times to obtain a list Y of 2^l hash values $h(m_j, x_{s,i})$ whose r_1 MSBs are zeros.

Adaptive Modification to Step 1



3. Repeat the procedure

Adaptive Modification to Step 3

/* Finding the linking message M_{link} by applying variant of CNS collision-finding algorithm: */

Store $D = \{x_1, x_2, \cdots, x_{2^k}\}$ in a classical memory L.

Define $S_r^h := \{(m, h(\bar{x}, m)) : \exists z \in \{0,1\}^{n-r}, h(\bar{x}, m) = \underbrace{0 \cdots 0}_{r \ \ times} \| z, z \in \{0,1\}^{n-r}\}$,

where h is the compression function with n-bit chaining value $\bar{x}$. Let $f_L^h(m) := 1$ if $\exists x' \in L$, $h(\bar{x}, m) = x'$, and $f_L^h(m) := 0$ otherwise.

Apply quantum amplification algorithm:

begin

The setup $\mathcal{A}$ is the construction of $|\phi\rangle := \frac{1}{\sqrt{|S_r^h|}} \sum_{m \in S_r^h} |m, h(\bar{x}, m)\rangle$.

The projector is a quantum oracle query to $O_{f_L^h}$ meaning that

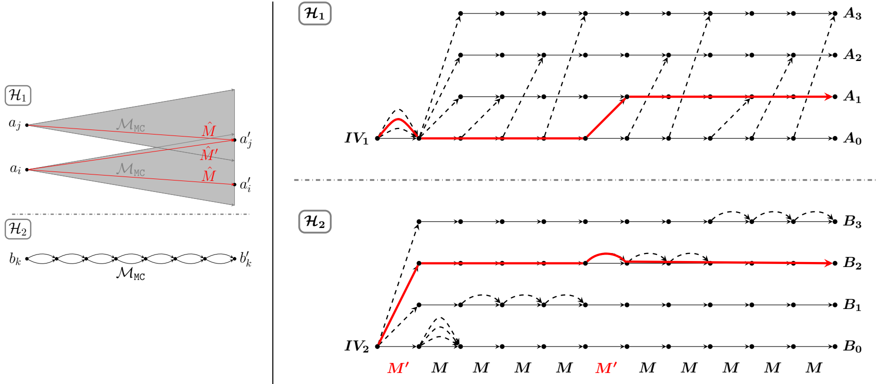
$$O_{f_L^h}(|m, h(\bar{x}, m)\rangle|b\rangle) = |m, h(\bar{x}, m)\rangle|b \oplus O_{f_L^h}(m)\rangle.$$

end

Let $M_{link} = m$

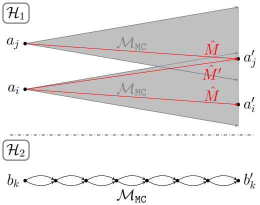
Preimage Attack on XOR Combiners

Given XOR Combiner $\mathcal{H}_1 \oplus \mathcal{H}_2 : \{0,1\}^\star \to \{0,1\}^n$ and the target value of V, Leurent and Wang [LW15] invented the **Interchange Structure (IS)** to implement a classical attack with time complexity of $2^{0.83n}$ combining with the Meet-in-the-Middle approach.



(a) Building a switch **(b)** Interchange structure

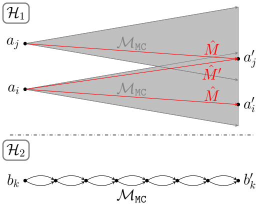
Quantum Adaption



Step 1: Build a switch from (a_i, b_k) to (a_j, b_k) such that $\mathcal{H}_1(a_j, \hat{M}) = \mathcal{H}_1(a_i, \hat{M}')$ and $\mathcal{H}_2(b_k, \hat{M}) = \mathcal{H}_2(b_k, \hat{M}')$;

(i) Apply CNS algorithm to search for 2^t-$\mathcal{M}_{MC}$, requiring time $t \cdot 2^{2n/5}$, cRAM $2^{n/5}$, QRACM $O(t \cdot n)$;

Quantum Adaption

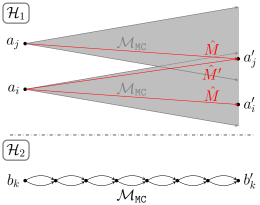


Step 1: Build a switch from (a_i, b_k) to (a_j, b_k) such that $\mathcal{H}_1(a_j, \hat{M}) = \mathcal{H}_1(a_i, \hat{M}')$ and $\mathcal{H}_2(b_k, \hat{M}) = \mathcal{H}_2(b_k, \hat{M}')$;

(i) Apply CNS algorithm to search for 2^t-$\mathcal{M}_{\text{MC}}$, requiring time $t \cdot 2^{2n/5}$, cRAM $2^{n/5}$, QRACM $O(t \cdot n)$;

(ii) Apply Grover algorithm to find 2^x messages M_i from $\mathcal{M}_{\text{MC}}$ such that r MSBs of $\mathcal{H}_1(a_j, M_i)$ are zero, requiring time $2^x \cdot 2^{r/2} = 2^{x+r/2}$, cRAM 2^x;

Quantum Adaption



Step 1: Build a switch from (a_i, b_k) to (a_j, b_k) such that $\mathcal{H}_1(a_j, \hat{M}) = \mathcal{H}_1(a_i, \hat{M}')$ and $\mathcal{H}_2(b_k, \hat{M}) = \mathcal{H}_2(b_k, \hat{M}')$;

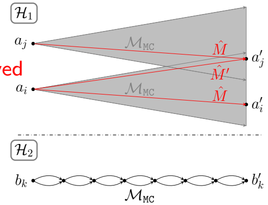
(i) Apply CNS algorithm to search for 2^t-$\mathcal{M}_{\text{MC}}$, requiring time $t \cdot 2^{2n/5}$, cRAM $2^{n/5}$, QRACM $O(t \cdot n)$;

(ii) Apply Grover algorithm to find 2^x messages M_i from $\mathcal{M}_{\text{MC}}$ such that r MSBs of $\mathcal{H}_1(a_j, M_i)$ are zero, requiring time $2^x \cdot 2^{r/2} = 2^{x+r/2}$, cRAM 2^x;

(iii) Apply CNS algorithm to find $\hat{M}'$ whose hash value at a_i collides with one of 2^x hash values above, requiring time $2^{\frac{n-r-x}{2}} \cdot (2^{r/2} + 2^x)$.

Quantum Adaption

Optimum time complexity $O(\frac{4n}{5} \cdot 2^{2n/5})$ is achieved

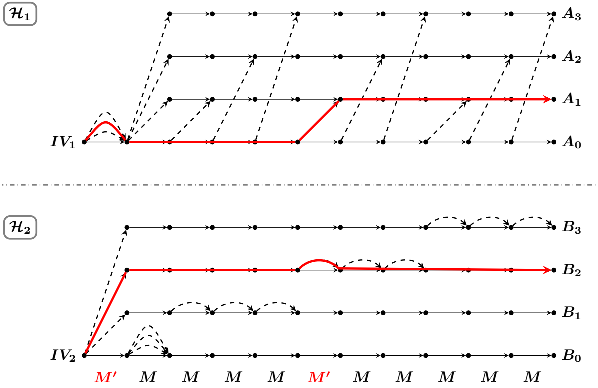


when $x = \frac{r}{2} = \frac{n}{5}, t = \frac{4n}{5}$

Step 1: Build a switch from (a_i, b_k) to (a_j, b_k) such that $\mathcal{H}_1(a_j, \hat{M}) = \mathcal{H}_1(a_i, \hat{M}')$ and $\mathcal{H}_2(b_k, \hat{M}) = \mathcal{H}_2(b_k, \hat{M}')$;

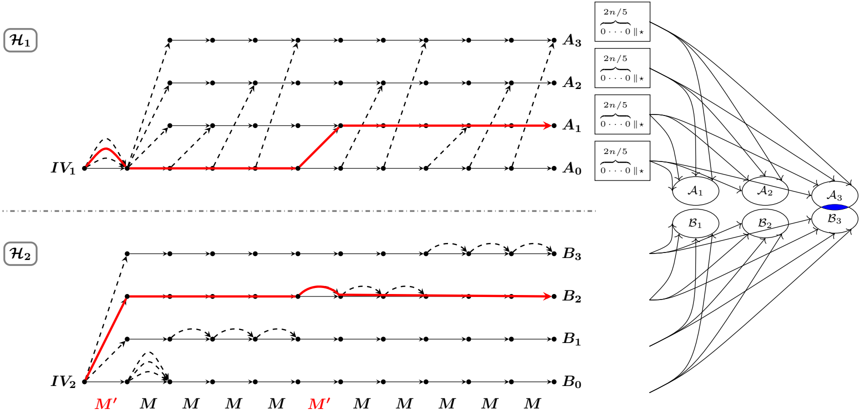
(i) Apply CNS algorithm to search for 2^t-$\mathcal{M}_{\text{MC}}$, requiring time $t \cdot 2^{2n/5}$, cRAM $2^{n/5}$, QRACM $O(t \cdot n)$;
(ii) Apply Grover algorithm to find 2^x messages M_i from $\mathcal{M}_{\text{MC}}$ such that r MSBs of $\mathcal{H}_1(a_j, M_i)$ are zero, requiring time $2^x \cdot 2^{r/2} = 2^{x+r/2}$, cRAM 2^x;
(iii) Apply CNS algorithm to find $\hat{M}'$ whose hash value at a_i collides with one of 2^x hash values above, requiring time $2^{\frac{n-r-x}{2}} \cdot (2^{r/2} + 2^x)$.

Quantum Adaption



Step 2: Cascade $2^{3k} - 1$ quantum single switches to build $(2^{2k}, 2^k)$-interchange structure, requiring time $O(\frac{4n}{5} \cdot 2^{3k+2n/5})$, cRAM $2^{n/5}$;

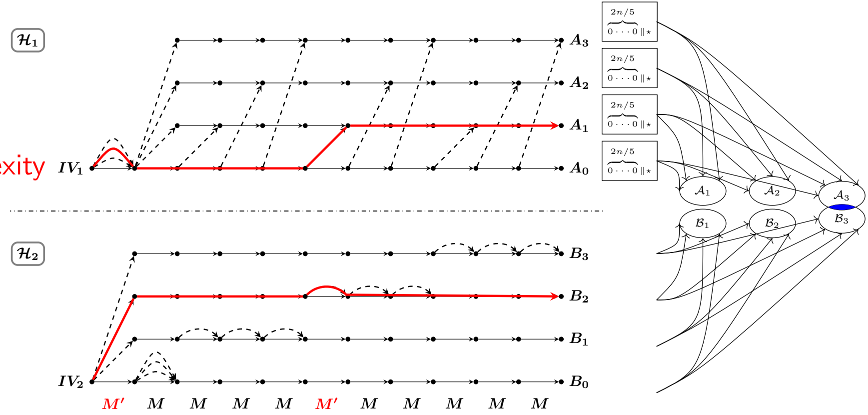
Quantum Adaption



Step 3: Launch a MitM procedure between the two sets $A_0, \ldots, A_{2^{2k}-1}$ and $B_0, \ldots, B_{2^k-1}$ to find a message block m such that $\mathcal{H}_1(A_j, m) = V \oplus \mathcal{H}_2(B_i, m)$, requiring time $2^{\frac{n-3k}{2}} \cdot 2^k = 2^{\frac{n-k}{2}}$. The overall complexity is $O(2^{3k+\frac{2n}{5}} + 2^{\frac{n-k}{2}})$.

Quantum Adaption

Optimum time complexity is $O(2^{17n/35})$ when $k = n/35$



Step 3: Launch a MitM procedure between the two sets $A_0, \ldots, A_{2^{2k}-1}$ and $B_0, \ldots, B_{2^k-1}$ to find a message block m such that $\mathcal{H}_1(A_j, m) = V \oplus \mathcal{H}_2(B_i, m)$, requiring time $2^{\frac{n-3k}{2}} \cdot 2^k = 2^{\frac{n-k}{2}}$. The overall complexity is $O(2^{3k+\frac{2n}{5}} + 2^{\frac{n-k}{2}})$.

Variant II with Low qRAM

II Attack based on Ambainis' element distinctness algorithm

- Prepare a $(2^k, 2^k)$-interchange structure and store it with 2^k QRACM, time complexity is $2^{2k} \cdot 2^{2n/5}$.
- Utilize Grover's algorithm, incorporating Ambainis' algorithm, to assess whether a given message m results in a collision. This determination necessitates a time complexity of $2^{(n-2k)/2} \cdot 2^{2(k+1)/3} = 2^{n/2-k/3}$, along with $2^{2(k+1)/3}$ QRAQM, 2^k QRACM, and 2^k cRAM.
- The overall optimum time complexity for both step 1 and step 2, $O(2^{17n/35})$, is achieved when $k = 3n/70$.

Variant III without QRAQM

III Attack based on Jaques-Schrottenloher's golden collision finding algorithm

- Create a $(2^k, 2^k)$-interchange structure and allocate it using 2^k QRACM, necessitating a time complexity of $2^{2k} \cdot 2^{2n/5}$.
- Utilize Grover's algorithm, coupled with Jaques-Schrottenloher's algorithm integration, to identify a colliding message within the lists L_1 and L_2. This variant costs a time complexity of $2^{(n-2k)/2} \cdot 2^{6(k+1)/7} = 2^{n/2-k/7}$, with corresponding 2^k QRACM and $2^{n/5}$ classical memory.
- The overall optimum time complexity for both step 1 and step 2, $O(2^{37n/75})$, is achieved when $k = 7n/150$.

Thanks

References I

Elena Andreeva, Charles Bouillaguet, Orr Dunkelman, and John Kelsey. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography, 16th Annual International Workshop, SAC 2009, Calgary, Alberta, Canada, August 13-14, 2009, Revised Selected Papers*, volume 5867 of *Lecture Notes in Computer Science*, pages 393–414. Springer, 2009.

Zhenzhen Bao, Itai Dinur, Jian Guo, Gaëtan Leurent, and Lei Wang. *J. Cryptol.*, 33(3):742–823, 2020.

Barbara Jiabao Benedikt, Marc Fischlin, and Moritz Huppert. In Shweta Agrawal and Dongdai Lin, editors, *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*, volume 13793 of *Lecture Notes in Computer Science*, pages 583–613. Springer, 2022.

References II

Zhenzhen Bao, Jian Guo, Shun Li, and Phuong Pham. In Xingliang Yuan, Guangdong Bai, Cristina Alcaraz, and Suryadipta Majumdar, editors, *Network and System Security - 16th International Conference, NSS 2022, Denarau Island, Fiji, December 9-12, 2022, Proceedings*, volume 13787 of *Lecture Notes in Computer Science*, pages 687–711. Springer, 2022.

Itai Dinur. In Marc Fischlin and Jean-Sébastien Coron, editors, *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*, volume 9665 of *Lecture Notes in Computer Science*, pages 484–508. Springer, 2016.

References III

John Kelsey and Tadayoshi Kohno. In Serge Vaudenay, editor, *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*, volume 4004 of *Lecture Notes in Computer Science*, pages 183–200. Springer, 2006.

Gaëtan Leurent and Lei Wang. In Elisabeth Oswald and Marc Fischlin, editors, *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*, volume 9056 of *Lecture Notes in Computer Science*, pages 345–367. Springer, 2015.