Attacks on Beyond-Birthday-Bound MACs in the Quantum Setting

Tingting Guo, Peng Wang, Lei Hu, and Dingfeng Ye

2021/7/20

Message Authentication Code

- **Message authentication code (MAC)** is a fundamental symmetric-key primitive to provide the integrity and authenticity of message between two parties.

- MAC is a core element of real-word security protocols such as TLS,SSH or IPSEC.

Message Authentication Code

Key: K

Message M, Tag T

Key: K

Sender

Message: M

Tag : $T = MAC_K(M)$

Receiver

Receive M', T

Compute $T' = MAC_K(M')$

Verify $T = T'$?

Message Authentication Code

Query: Message M_0

Retuen:Tag T_0

Query: Message M_1

Return: Tag T_1

⋮

Key: K

Sender

Message: M_i

Tag : $T_i = MAC_K(M_i)$

No Key

Malicious Adversary

Forge a vailid message-tag pair (M^*, T^*).

Security of MAC :

The number of queries of adversary

$$M^* \notin \{M_i\}$$
$$T^* = MAC_K(M^*)$$

Birthday Bound MACs

- Commen block-cipher-based MACs: CBC-MAC, OMAC, PMAC,GMAC …
- They all suffer from **birthday bound attacks**, i.e. when the number of queries of the adversary is $2^{n/2}$, with n the block size, the MACs break.
- A lightweight cipher has a short block size, e.g., $n = 64$. Then the security of MACs based on such cipher is 2^{32}, which means it is vulnerable to practical attacks.

It is of great importance to introduce MACs with beyond birthday bound security!

Beyond-Birthday Bound MACs

- **Beyond-Birthday-Bound (BBB) MACs** are secure of above $2^{n/2}$ queries.
  SUM-ECBC-like MACs: SUM-ECBC, 2K-ECBC_Plus, PloyMAC, the authentication part of GCM-SIV2.
  PMAC_Plus-like MACs: PMAC_Plus, 1k-PMAC_Plus, 2K-PMAC_Plus, 3kf9, PMAC_TBC3k…
- They are all proved $O(2^{2n/3})$ or $O(2^{3n/4})$ security.
- Best classical attacks: Leurent et al. 2018[1] $O(2^{3n/4})$

[1] Leurent, G., Nandi, M., Sibleyras, F.: Generic attacks against beyond-birthday bound MACs. In: Advances in Cryptology - CRYPTO 2018, Proceedings, Part I. pp. 306-336 (2018)

Beyond-Birthday Bound MACs

- **Optimal secure MACs** are secure of 2^n queries, which are the best MACs of BBB MACs.

  mPMAC_Plus-like MACs: mPMAC+-f, mPMAC+-p1, mPMAC+-p2.

As we have seen, studies of the MACs in the classic setting have yielded many results. How about in quantum setting?

Quantum Attack on MACs

Key: K

Sender

$\vdots$

Superposition query: $\sum_{i,j} \alpha_{i,j} |M_i\rangle |Y_j\rangle$

$\longleftarrow$

Return: $\sum_{i,j} \alpha_{i,j} |M_i\rangle |Y_j \oplus MAC_K(M_i)\rangle$

$\longrightarrow$

$\vdots$

Query q times

No Key

Malicious Adversary

Forge $q+1$ vailid message-tag pairs (M_i^*, T_i^*).

Security of MAC :

The number of queries of adversary

Quantum Security of MACs

- Birthday-bound MACs: CBC-MAC, OMAC, PMAC,GMAC …

  They are broken by applying Simon’s algorithm in polynomial time.

- However, there hasn’t been any research on quantum security of BBB MACs.

- **Motivations of our work: What about the security of BBB MACs in quantum setting?**

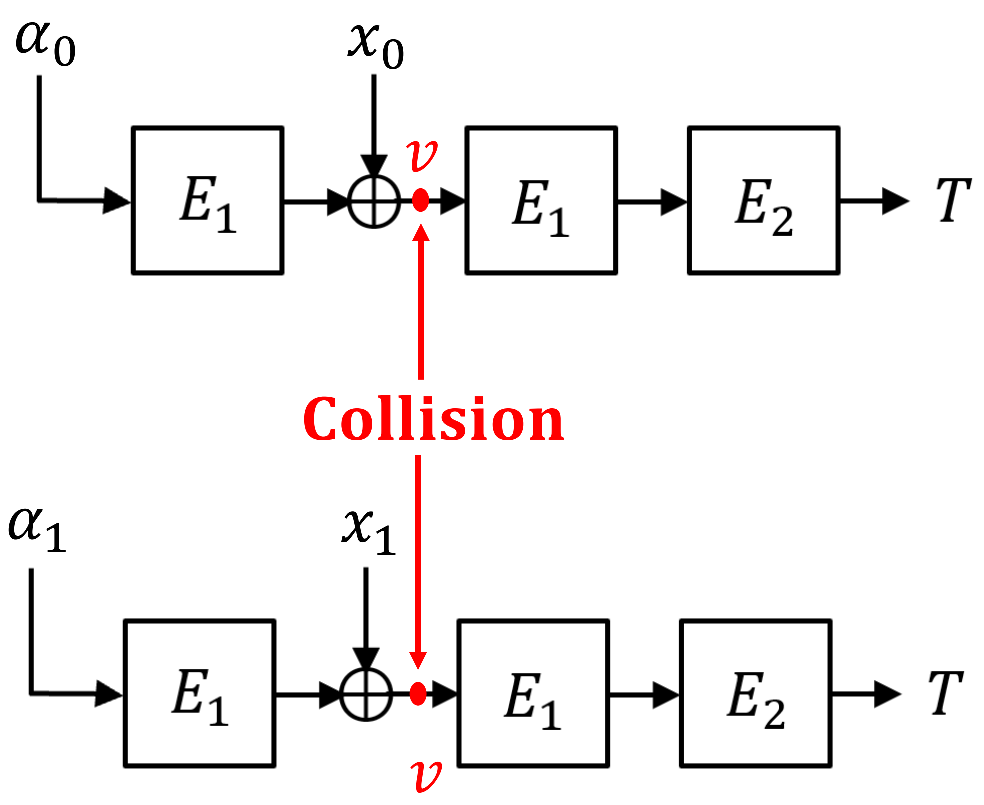
Our Works

Attacks on BBB MACs by secret state recovery and key recovery attacks in quantum setting.

Our First Work

- **Attacks on BBB MACs by secret state recovery in quantum setting.**

Classical Attack on ECBC MAC



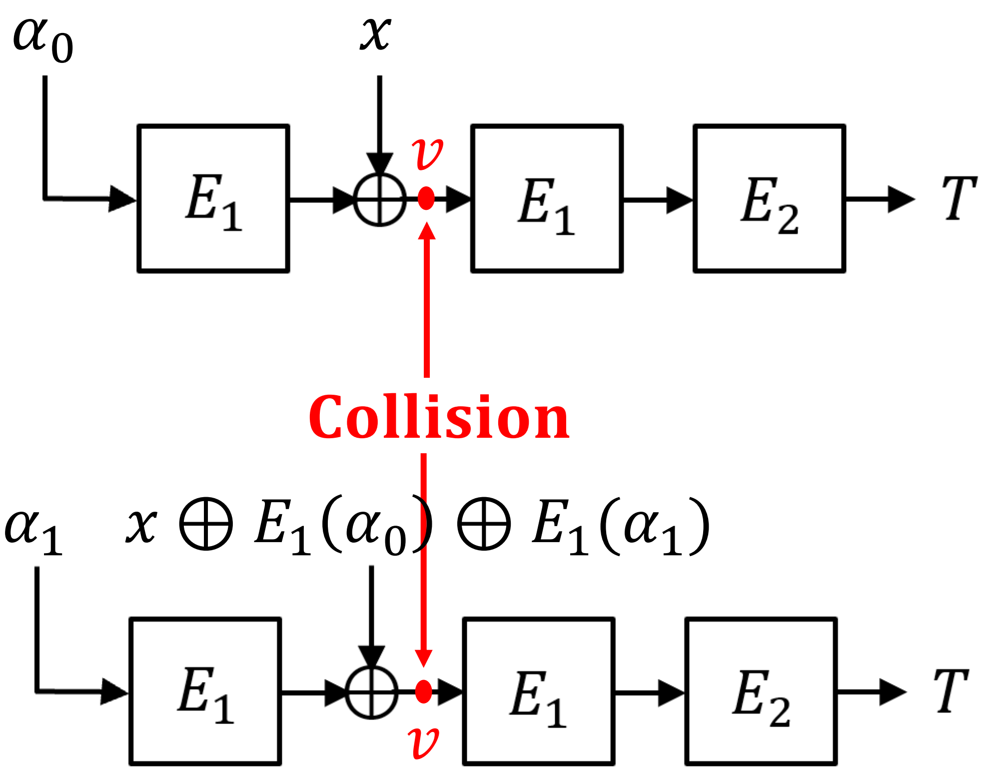
Step 1. Find two different messages $(\alpha_0, x_0) \neq (\alpha_1, x_1)$, which collide over point v when input them to the MAC.

Step 2. Query $(\alpha_0, x_0 \oplus \Delta)$ and get T.

Step 3. Forge message $(\alpha_1, x_1 \oplus \Delta)$ and its tag T.

$$O(2^{n/2})$$

Quantum Attack on ECBC MAC



$g(b, x) = MAC_K(\alpha_b, x)$,
where $b \in \{0,1\}. x \in \{0,1\}^n$

period $s = 1||E_1(\alpha_0) \oplus E_1(\alpha_1)$

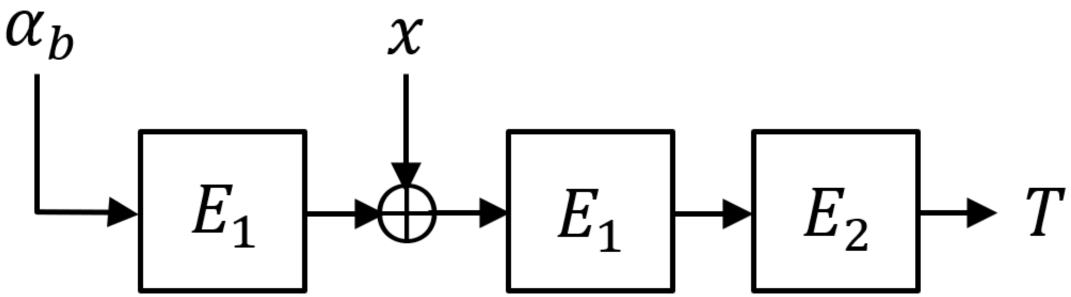
Quantum Attack on ECBC MAC

- Simon algorithm:
  Boolean function $f(x)$ where $x \in \{0,1\}^n$ has a period s.

$$f(x) = f(x \oplus s), \forall x$$

  Simon algorithm : recover the period s with $O(n)$ quantum queries to f.

Quantum Attack on ECBC MAC [1]



Step 1. Construct periodic function $g(b, x) = MAC_K(\alpha_b, x), b \in \{0,1\}$.
period $s = 1||E_1(\alpha_0) \oplus E_1(\alpha_1)$

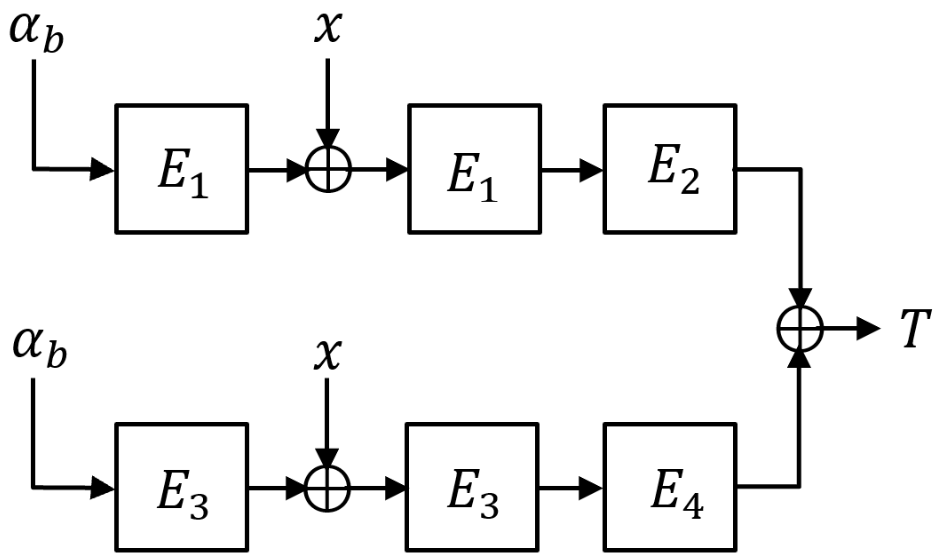
Step 2. Apply Simon's algorithm to recover the period s.

Step 3. Make forgery.

[1] Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Advances in Cryptology -CRYPTO 2016, Proceedings, Part II. pp. 207{237 (2016)

Quantum Attack on BBB MAC

SUM-ECBC:



$g(b,x) = E_2(E_1(x \oplus E_1(\alpha_b))$
period $1||s_1 = 1||E_1(\alpha_0) \oplus E_1(\alpha_1)$

$h(b,x) = E_4(E_3(x \oplus E_3(\alpha_b))$
period $1||s_2 = 1||E_3(\alpha_0) \oplus E_3(\alpha_1)$

Try: $f(b,x) = g(b,x) \oplus h(b,x)$ is not a period function.

Simon's algorithm is invalid.

Direct Quantum Acceleration

Classical attack[1] :

Look for a quadruple of messages (x, y, z, t), which leads to successful forgeries.

$$f^{MAC}(x) \oplus f^{MAC}(y) \oplus f^{MAC}(z) \oplus f^{MAC}(t) = 0^{3n}$$

Direct quantum acceleration:

$O\left(2^{\frac{3n}{5}}\right)$ quantum queries by quantum walk algorithm[2].

Is there any better quantum attack?

[1] Leurent, G., Nandi, M., Sibleyras, F.: Generic attacks against beyond-birthday bound MACs. In: Advances in Cryptology - CRYPTO 2018, Proceedings, Part I. pp. 306-336 (2018)

[2] Belovs, A., Spalek, R.: Adversary lower bound for the k-sum problem. In: Proceedings of the 4th Conference on Innovations in Theoretical Computer Science, pp. 323–328 (2013)

Grover-meet-Simon Algorithm

Boolean function $f(u,x)$, where $u \in \{0,1\}^m, x \in \{0,1\}^n$, satisfies

$$\begin{cases} f(u,\cdot) \text{ is periodic with period } s_u, & \text{if } u \in \mathcal{U} \\ f(u,\cdot) \text{ is not periodic,} & \text{if } u \notin \mathcal{U} \end{cases}$$

Grover-meet-Simon algorithm [1] : get a pair (u, s_u) where $u \in \mathcal{U}$ $\quad O(2^{m/2}n)$

$f(u,\cdot)$

Grover : $u \in \mathcal{U}$

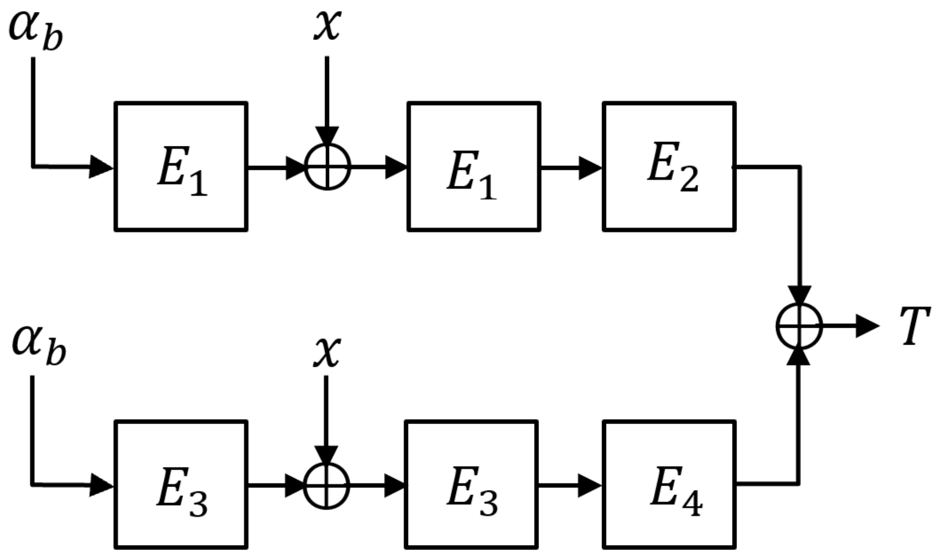
$O(2^{m/2})$

$$\mathrm{B}(u) = \begin{cases} 1, & \text{Simon}\big(f(u,x)\big) \text{ finds } s_u \\ 0, & \text{Simon}\big(f(u,x)\big) \text{ ouputs random number} \end{cases}$$

$O(n)$

[1] Leander, G., May, A.: Grover meets simon - quantumly attacking the FXconstruction. In: Advances in Cryptology - ASIACRYPT 2017, Proceedings, Part II. pp. 161{178 (2017)

Quantum Secret State Recovery Attack on BBB MAC (Our Work)



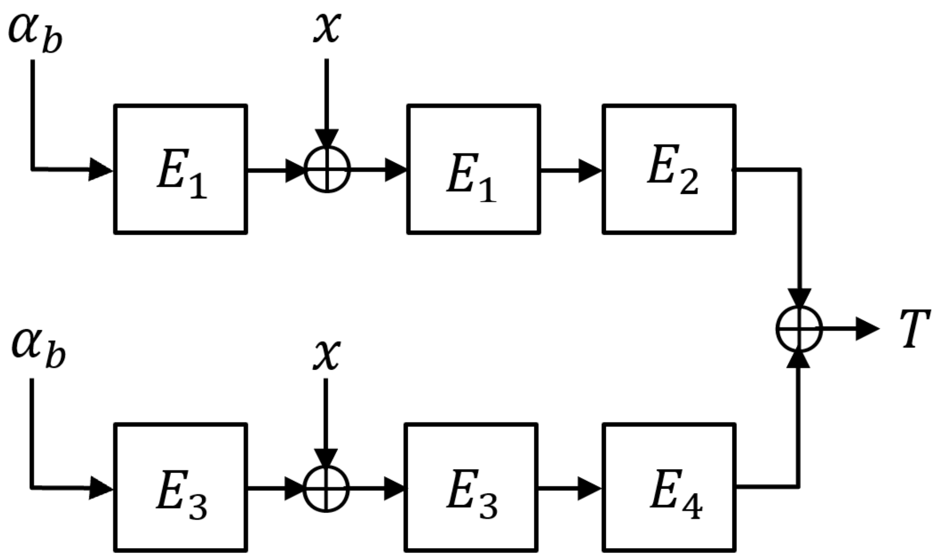
Step 1. Construct a function $f(u,x)$ based on SUM-ECBC MAC.

$$\begin{cases} f(u,\cdot) \text{ is periodic with period } s_u, & \text{if } u \in \mathcal{U} \\ f(u,\cdot) \text{ is not periodic,} & \text{if } u \notin \mathcal{U} \end{cases}$$

Step 2: Apply Grover-meet-Simon algorithm to get a pair (u, s_u) where $u \in \mathcal{U}$.

Step 3: Make forgery.

Quantum Secret State Recovery Attack on BBB MAC (Our Work)



$g(b,x) = E_2(E_1(x \oplus E_1(\alpha_b))$

period $1||s_1 = 1||E_1(\alpha_0) \oplus E_1(\alpha_1)$

$h(b,x) = E_4(E_3(x \oplus E_3(\alpha_b))$

period $1||s_2 = 1||E_3(\alpha_0) \oplus E_3(\alpha_1)$

Step 1. How to c onstruct a function $f(u,x)$ based on SUM-ECBC MAC?

$$f(u,x) = MAC(\alpha_0, x) \oplus MAC(\alpha_1, x \oplus u)$$

$$= g(0,x) \oplus g(1, x \oplus u) \oplus h(0,x) \oplus h(1, x \oplus u)$$

(when $u = s_1$) $= h(0,x) \oplus h(1, x \oplus s_1)$

(when $u = s_2$) $= g(0,x) \oplus g(1, x \oplus s_2)$ period $s_1 \oplus s_2$

Quantum Secret State Recovery Attack on BBB MAC (Our Work)

Step 2. Apply Grover-meet-Simon algorithm to recover s_1, s_2.

$O\left(2^{\frac{n}{2}}n\right)$ quantum queries

Quantum Secret State Recovery Attack on BBB MAC (Our Work)

Our Contribution 1

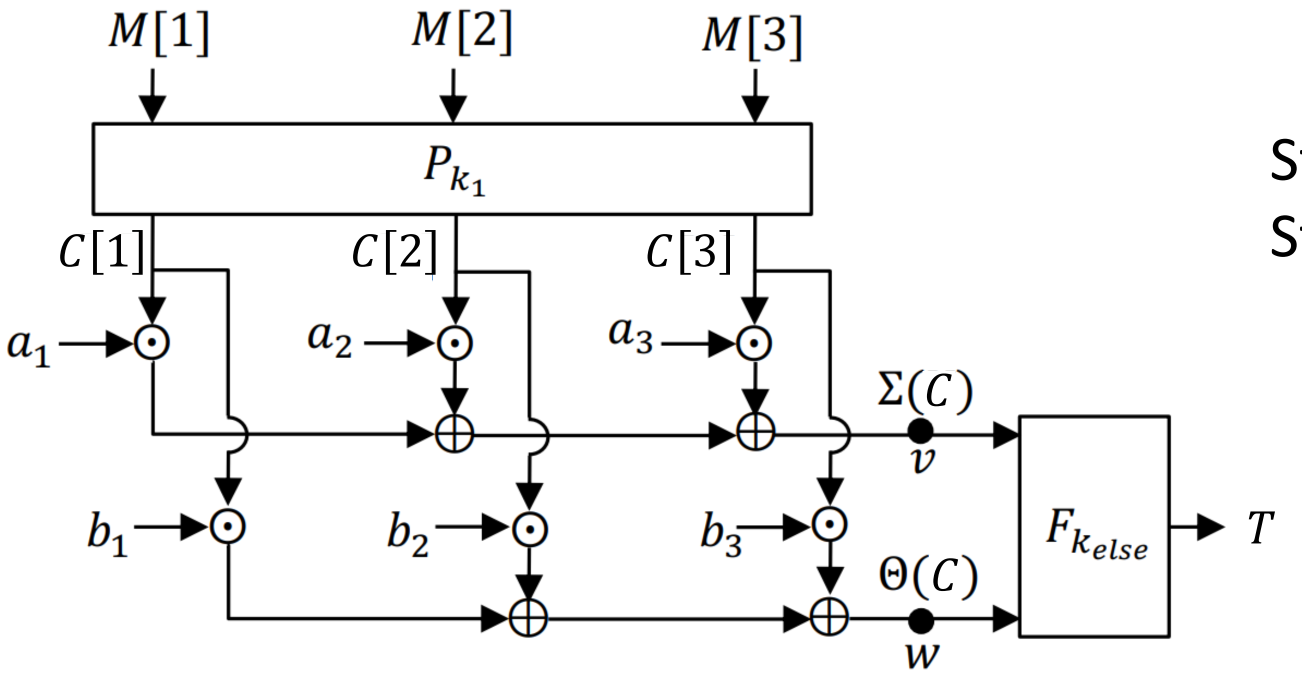
Scheme	Key space	Provable classical security query bound	Query complexity of classical attack	Query complexity of the quantum acceleration of classical attack	Quantum secret state recovery attack (our work)		Quantum key recovery attack (our work)	
					Queries	Qubits	Queries	Qubits
SUM-ECBC [32]	2^{4m}	$\Omega(2^{3n/4})$ [20]	$\mathcal{O}(2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^m n)$	$\mathcal{O}(m+n^2)$
2K-ECBC_Plus [7]	2^{3m}	$\Omega(2^{2n/3})$ [7]	$\mathcal{O}(2^{3n/4})$	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^m n)$	$\mathcal{O}(m+n^2)$
PolyMAC [20]	2^{2m+2n}	$\Omega(2^{3n/4})$ [20]	$\mathcal{O}(2^{3n/4})$	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{(n+m)/2}n)$	$\mathcal{O}(m+n^2)$
GCM-SIV2 [16]	2^{4m+2n}	$\Omega(2^{2n/3})$ [16]	$\mathcal{O}(2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{(n+m)/2}n)$	$\mathcal{O}(m+n^2)$
PMAC_Plus [33]	2^{3m}	$\Omega(2^{3n/4})$ [20]	$\mathcal{O}(2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
1k-PMAC_Plus [9]	2^m	$\Omega(2^{2n/3})$ [9]	$\mathcal{O}(2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
2K-PMAC_Plus [7]	2^{2m}	$\Omega(2^{2n/3})$ [7]	$\mathcal{O}(2^{3n/4})$	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
3kf9 [34]	2^{3m}	$\Omega(2^{3n/4})$ [20]	$\mathcal{O}(\sqrt[4]{n}2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2})$	$\mathcal{O}(n)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
mPMAC+-f [6]	2^{5m}	$\Omega(2^n)$ [6]	-	-	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
mPMAC+-p1 [6]	2^{5m}	$\Omega(2^n)$ [6]	-	-	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
mPMAC+-p2 [6]	2^{5m}	$\Omega(2^n)$ [6]	-	-	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
PMAC_TBC3k [25]	2^{3m}	$\Omega(2^n)$ [25]	-	-	-	-	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$

Our Second Work

- **Attacks on BBB MACs by key recovery attack in quantum setting.**

Quantum Key Recovery Attack on BBB MACs (Our Work)

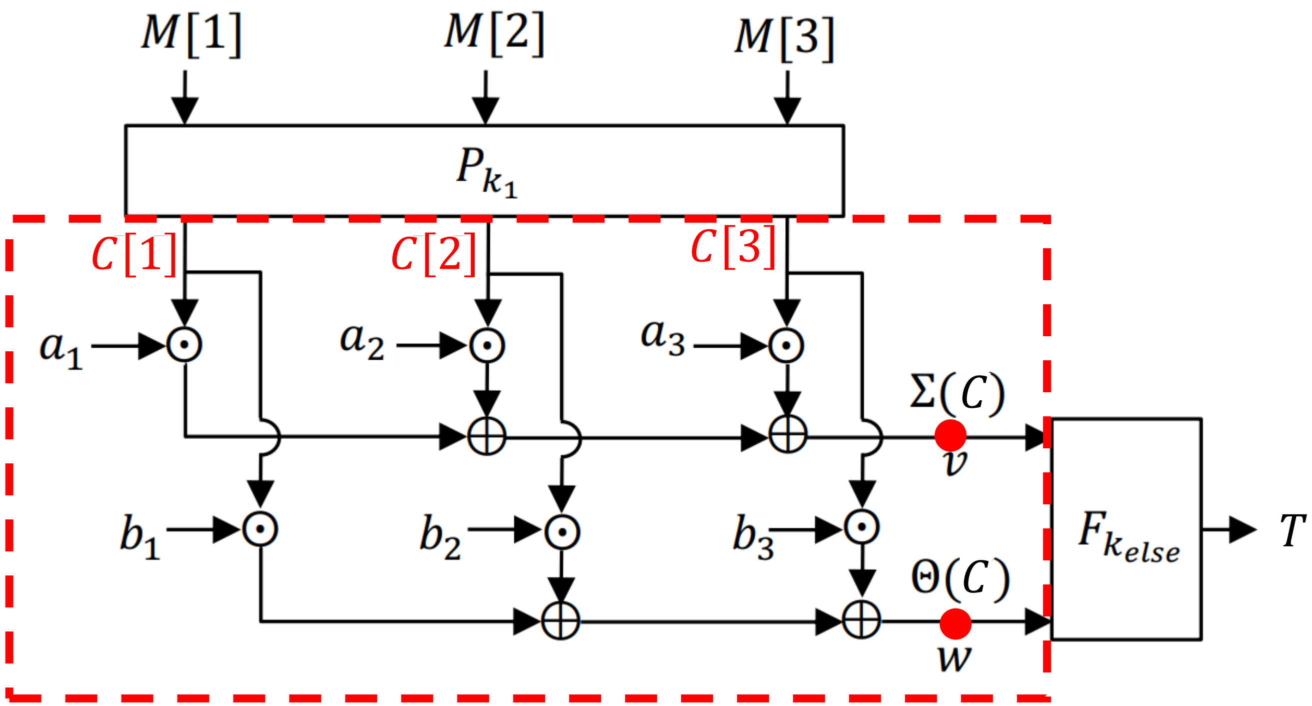
PMAC_Plus-like MACs with three message blocks:



Step 1. Recover k_1 by Grover's search.
Step 2. Make forgeries.

Quantum Key Recovery Attack on BBB MACs (Our Work)

Step 1. How to recover k_1 by Grover's search?



Key point:

Let $C = (C[1], C[2], C[3])$

linear combination process:

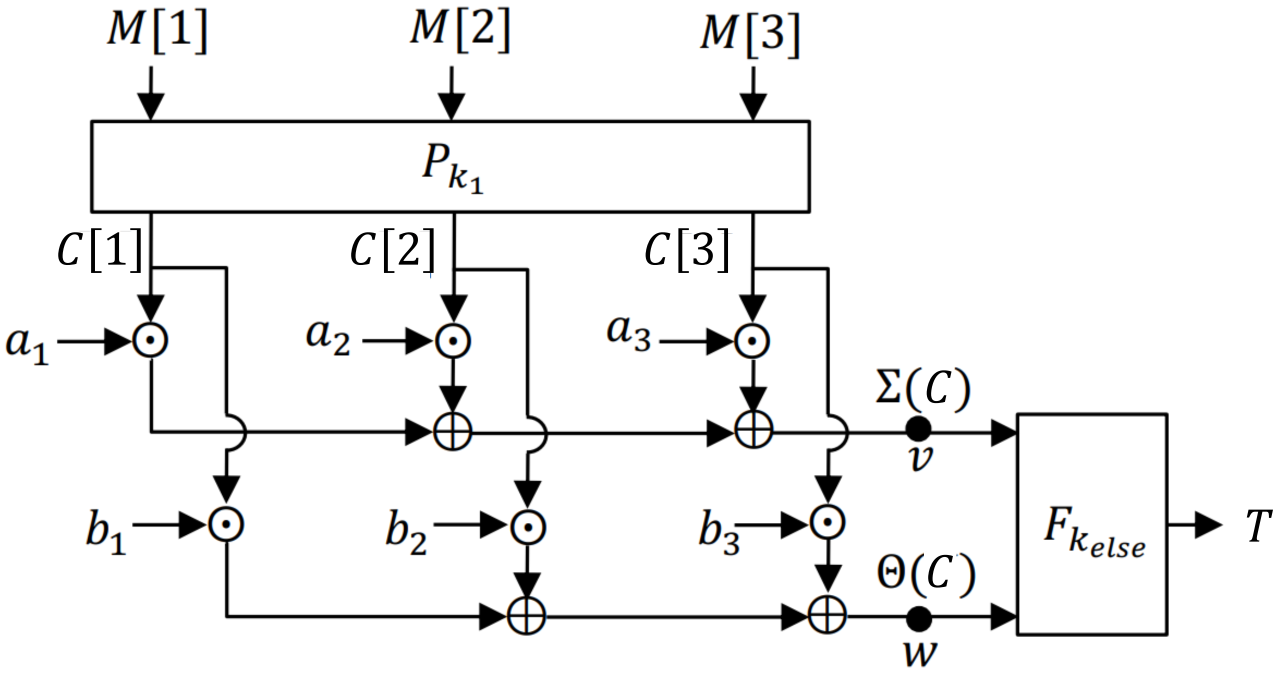
$$\begin{cases} a_1C[1] \oplus a_2C[2] \oplus a_3C[3] = v \\ a_1C[1] \oplus a_2C[2] \oplus a_3C[3] = w \end{cases}$$

Solutions: $C = C_0, C_1, C_2, \ldots$

more than one solution

Quantum Key Recovery Attack on BBB MACs (Our Work)

Step 1. How to recover k_1 by Grover's search?



Step 1.1. Fix arbitrary values at points $\Sigma(C)$ and $\Theta(C)$.

Step 1.2. Reverse the linear combination process to get two arbitrary different solutions $C_0, C_1 \in \{0,1\}^{3n}$.

Step 1.3. Guess k_1' and reverse $P_{k_1'}$ to get two messages M_0, M_1.

Step 1.4. Input the two messages into $MAC_{k_1,k_{else}}(\cdot)$ to get two tags T_0, T_1.

If $k_1' = k_1$ ➡ $T_0 = T_1$

Grover search k_1 $O(2^{m/2})$

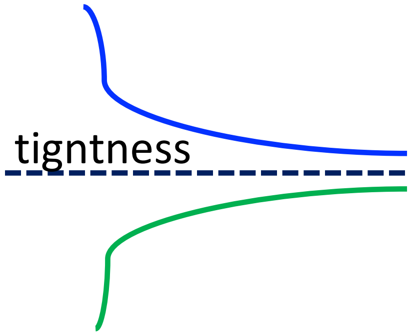
Quantum Key Recovery Attack on BBB MACs (Our Work)

Scheme	Key space	Provable classical security query bound	Query complexity of classical attack	Query complexity of the quantum acceleration of classical attack	Quantum secret state recovery attack (our work)		Quantum key recovery attack (our work)	
					Queries	Qubits	Queries	Qubits
SUM-ECBC [32]	2^{4m}	$\Omega(2^{3n/4})$ [20]	$\mathcal{O}(2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m}n)$	$\mathcal{O}(m+n^2)$
2K-ECBC_Plus [7]	2^{3m}	$\Omega(2^{2n/3})$ [7]	$\mathcal{O}(2^{3n/4})$	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m}n)$	$\mathcal{O}(m+n^2)$
PolyMAC [20]	2^{2m+2n}	$\Omega(2^{3n/4})$ [20]	$\mathcal{O}(2^{3n/4})$	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{(n+m)/2}n)$	$\mathcal{O}(m+n^2)$
GCM-SIV2 [16]	2^{4m+2n}	$\Omega(2^{2n/3})$ [16]	$\mathcal{O}(2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{(n+m)/2}n)$	$\mathcal{O}(m+n^2)$
PMAC_Plus [33]	2^{3m}	$\Omega(2^{3n/4})$ [20]	$\mathcal{O}(2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
1k-PMAC_Plus [9]	2^{m}	$\Omega(2^{2n/3})$ [9]	$\mathcal{O}(2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
2K-PMAC_Plus [7]	2^{2m}	$\Omega(2^{2n/3})$ [7]	$\mathcal{O}(2^{3n/4})$	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
3kf9 [34]	2^{3m}	$\Omega(2^{3n/4})$ [20]	$\mathcal{O}(\sqrt[4]{n}2^{3n/4})$ [23]	$\mathcal{O}(2^{3n/5})$	$\mathcal{O}(2^{n/2})$	$\mathcal{O}(n)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
mPMAC+-f [6]	2^{5m}	$\Omega(2^{n})$ [6]	-	-	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
mPMAC+-p1 [6]	2^{5m}	$\Omega(2^{n})$ [6]	-	-	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
mPMAC+-p2 [6]	2^{5m}	$\Omega(2^{n})$ [6]	-	-	$\mathcal{O}(2^{n/2}n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$
PMAC_TBC3k [25]	2^{3m}	$\Omega(2^{n})$ [25]	-	-	-	-	$\mathcal{O}(2^{m/2})$	$\mathcal{O}(m+n)$

Our Contribution 2

Open Problem

BBB MACs	Classic	Quantum
Attacks	$O(2^{3n/4})$ [1]	$O(2^{\frac{n}{2}}n)$ or $O(2^{\frac{m}{2}})$
Proofs	$O(2^{2n/3})$ [2] $O(2^{3n/4})$ [3] $O(2^{n})$ [4]	**?**



[1] Gaëtan Leurent and Mridul Nandi and Ferdinand Sibleyras. Generic Attacks against Beyond-Birthday-Bound MACs. IACR-CRYPTO-2018

[2] Nilanjan Datta and Avijit Dutta and Mridul Nandi and Goutam Paul. Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. IACR-FSE-2019

[3] Seongkwang Kim, Byeonghak Lee, Jooyoung Lee. Tight Security Bounds for Double-block Hash-then-Sum MACs. Eurocrypt 2020.

[4] Cogliati, B., Jha, A., Nandi, M.: How to build optimally secure PRFs using block ciphers. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020. Part I. LNCS, vol.12491, pp. 754–784. Springer, Cham (2020).

Thanks！