

Quantum Cryptanalysis of OTR and OPP: Attacks on Confidentiality, and Key- Recovery

Authors: Melanie Jauch and Varun Maram

Presented by Andrea Basso

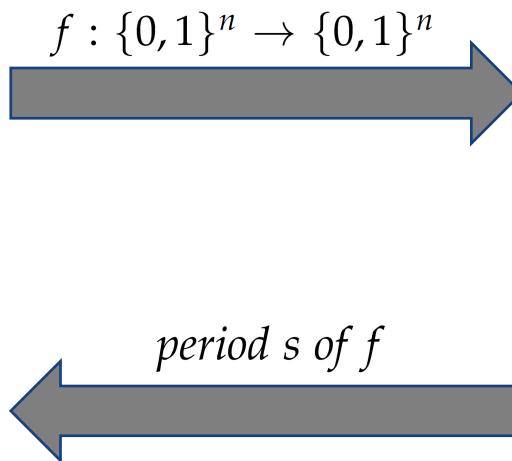
SAC'23, August 2023

Introduction

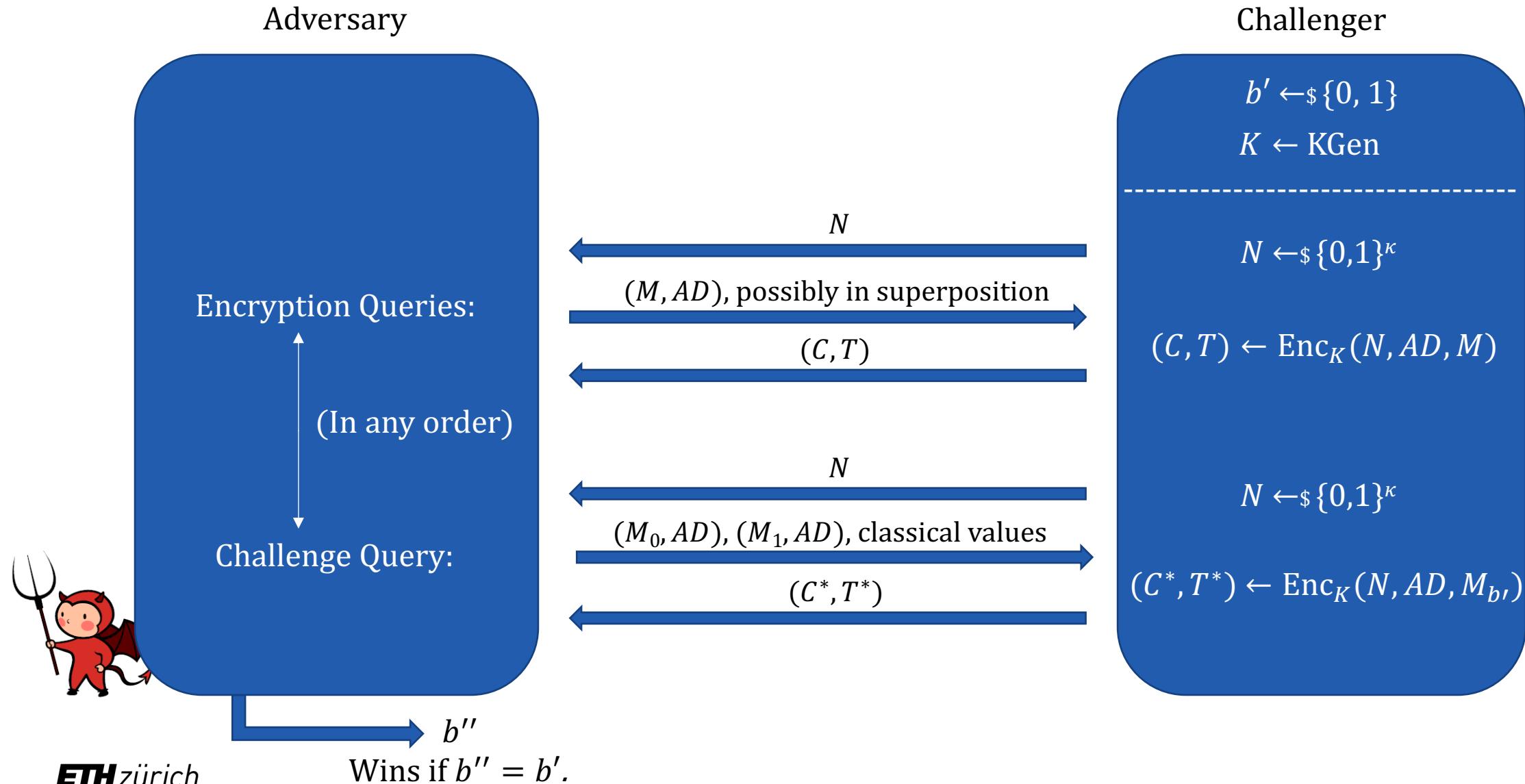
- **Quantum** security: adversary has quantum access to secret-keyed encryption or decryption oracles.
 - In contrast to **post-quantum** security: adversary has quantum access to public oracles (e.g., hash functions).
- In our setting, adversary can make encryption queries on a quantum superposition of messages.
- Prior work: quantum superposition attacks by Kaplan *et al.* (Crypto 2016) on **CBC-MAC**, **PMAC**, **GMAC**, **GCM**, **OCB**, etc. breaking unforgeability (EUF-qCMA).
- More recently: confidentiality (IND-qCPA) analysis of **OCB** modes by Maram *et al.* (ToSC 2022).
- In this work, we focus on related authenticated encryption (AE) modes **OPP** and **AES-OTR**.

Simon's Algorithm

- Given **quantum access** to a Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ for which it holds:
 $\exists s \in \{0,1\}^n : \forall x, y \in \{0,1\}^n$
$$f(x) = f(y) \Leftrightarrow y \in \{x, x \oplus s\}$$
- Can recover s in $\mathcal{O}(n)$ quantum queries (in a classical setting $\Theta(2^{n/2})$ needed).
- In each iteration, an independent vector orthogonal to the period s is recovered with high probability.



IND-qCPA Security Game



Breaking AES-OTR's IND-qCPA Security

Specifications of AES-OTR

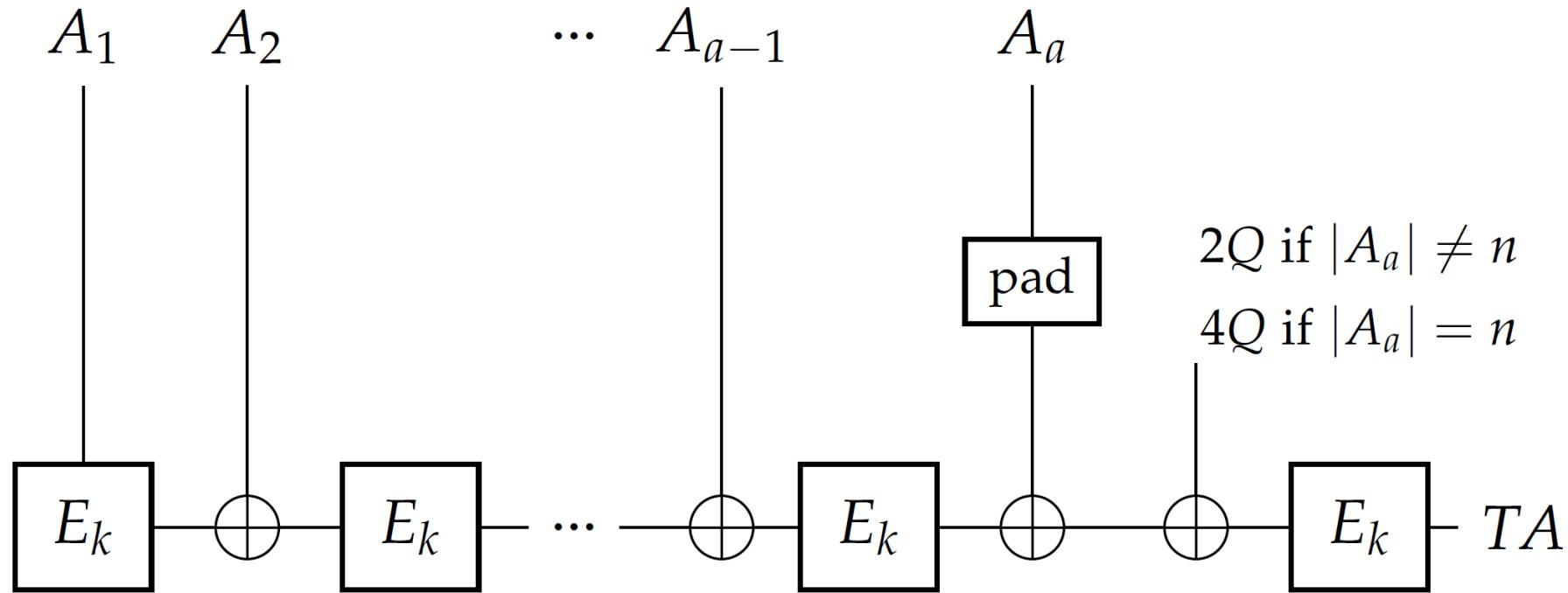
Algorithm OTR- $\mathcal{E}_{K,s}(N, A, M)$

- 1: **if** $A \neq \varepsilon$ **then**
 - 2: $TA \leftarrow \text{AF-S}_K(A)$ 
 - 3: **else** $TA \leftarrow 0^n$
 - 4: $(C, TE) \leftarrow \text{EF-S}_{K,\tau}(N, M, TA)$
 - 5: $T \leftarrow \text{msb}_\tau(TE)$
 - 6: **return** (C, T)
-

AD Processing

Specifications of AES-OTR: Authentication Core $\mathbf{AF}\text{-}\mathbf{S}_K(A)$

- Associated Data $A = A_1 \parallel \dots \parallel A_a$ processed in serial
- $Q = E_K(0^n)$



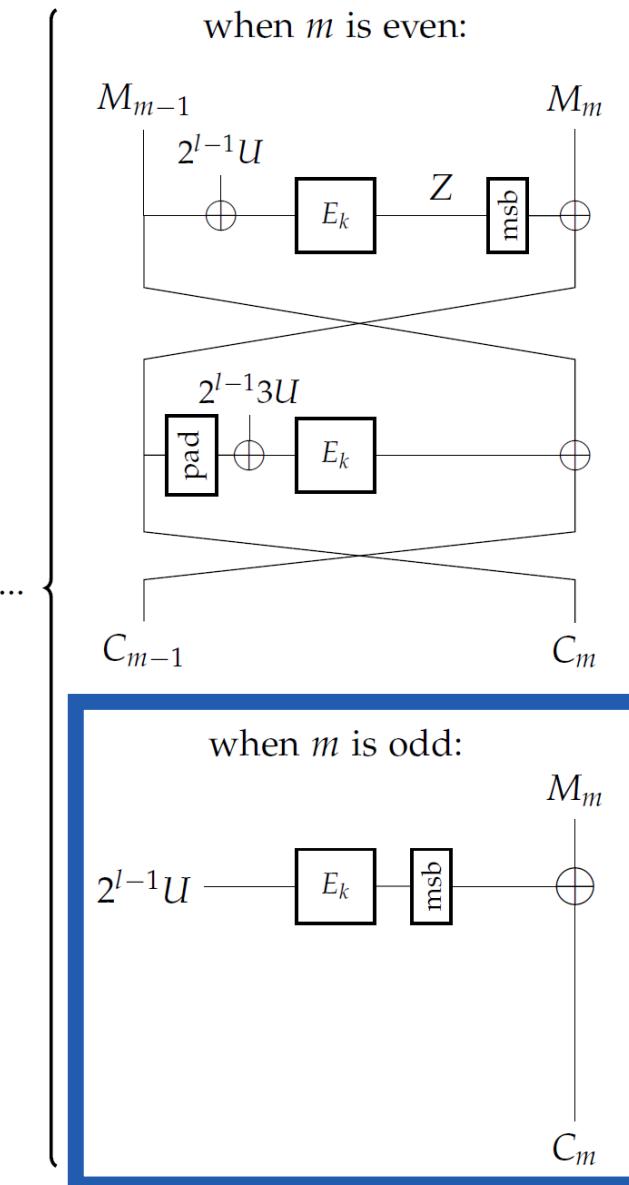
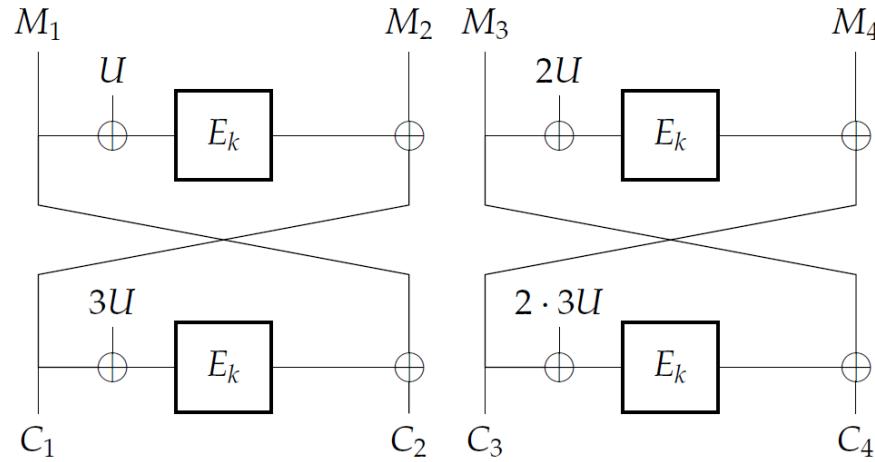
Specifications of AES-OTR

Algorithm OTR- $\mathcal{E}_{K,s}(N, A, M)$

- 1: **if** $A \neq \varepsilon$ **then**
 - 2: $TA \leftarrow \text{AF-S}_K(A)$ 
 AD Processing
 - 3: **else** $TA \leftarrow 0^n$
 - 4: $(C, TE) \leftarrow \text{EF-S}_{K,\tau}(N, M, TA)$ 
 Encryption Core
 - 5: $T \leftarrow \text{msb}_\tau(TE)$
 - 6: **return** (C, T)
-

Specifications of AES-OTR: Encryption Core $\mathbf{EF-S}_{K,\tau}(N, M)$

- Nonce N and key K
- Plaintext $M = M_1 \parallel \dots \parallel M_m$, $l = \lceil m/2 \rceil$
- $U = 2(E_K(\text{Format}(\tau, N)) \oplus TA)$
- $\text{Format}(\tau, N) = \text{bin}(\tau \bmod n, 7) \parallel 0^{n-8-\kappa} \parallel 1 \parallel N$



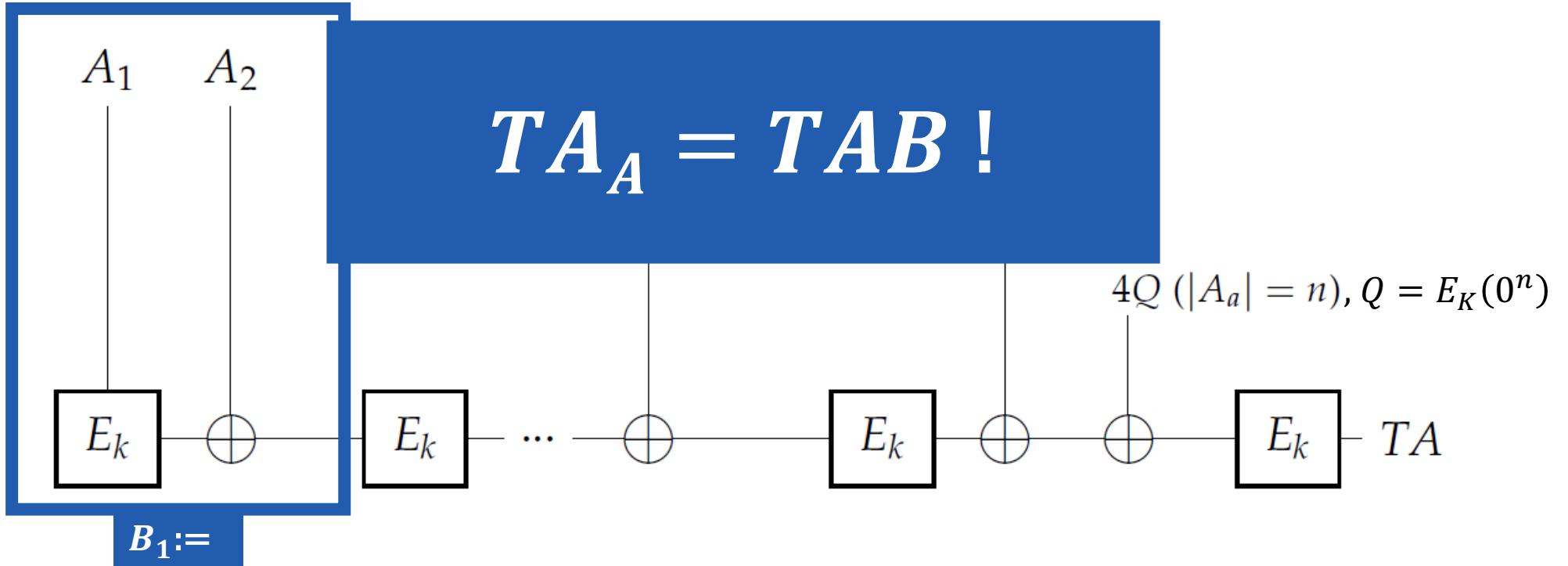
Specifications of AES-OTR

Algorithm 2 $\text{OTR-}\mathcal{E}_{K,s}(N, A, M)$

```
1: if  $A \neq \varepsilon$  then
2:    $TA \leftarrow \text{AF-S}_K(A)$  ← AD Processing
3: else  $TA \leftarrow 0^n$ 
4:  $(C, TE) \leftarrow \text{EF-S}_{K,\tau}(N, M, TA)$  ← Encryption Function
5:  $T \leftarrow \text{msb}_\tau(TE)$  ← Tag Computation
6: return  $(C, T)$ 
```

Finding Collisions in Serial AD Processing

- High-level attack on unforgeability first described by Kaplan *et al.* (Crypto 2016).
 - Detailed attack followed by Chang *et al.* (Symmetry 2022).
- AD $A = A_1 \parallel \dots \parallel A_a$ with $A_i \in \{0,1\}^n$
- Define AD $B = B_1 \parallel \dots \parallel B_{a-1}$ with $B_1 = A_2 \oplus E_K(A_1), B_i = A_{i+1}$



IND-qCPA Attack on AES-OTR with Serial AD Processing

- **Raw block cipher access:** Let $B \in \{0,1\}^n$. Define function $f_2 : \{0,1\}^{n+1} \rightarrow \{0,1\}^\tau$

$$f_2(b||A) = \begin{cases} \text{OTR-}\mathcal{E}_{K,s}(N, B||A, \varepsilon) & \text{if } b = 0 \\ \text{OTR-}\mathcal{E}_{K,s}(N, A, \varepsilon) & \text{if } b = 1 \end{cases}$$

with $b \in \{0,1\}$ and $A \in \{0,1\}^n$.

- Where

$$\text{OTR-}\mathcal{E}_{K,s}(N, D, \varepsilon) = \text{msb}_\tau \left(E_K \left(3^3 2 \left(TA_D \oplus E_K(\text{Format}(\tau, N)) \right) \right) \right)$$

 depends on AD

Period of f_2 only depends on TA_D !

IND-qCPA Attack on AES-OTR with Serial AD Processing

- Define new function $g : \{0, 1\}^{n+1} \rightarrow \{0, 1\}^n$, (inner function of f_2)

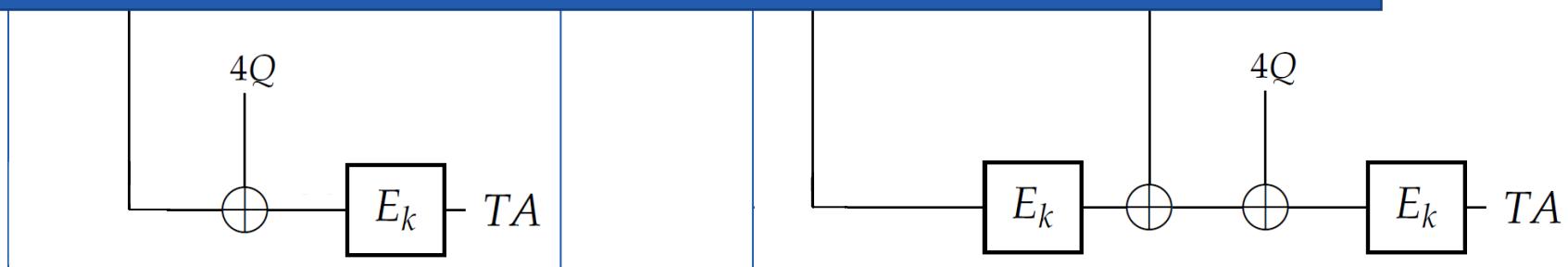
$$\begin{cases} \text{AE-S}_\nu(B \parallel A) & \text{if } h = 0 \\ \dots & \dots \end{cases}$$

- Claim: g (and the

$$g(0 \parallel A \oplus$$

We can recover $E_k(B)$
for any $B \in \{0, 1\}^n$!

$$= g(0 \parallel A)$$



IND-qCPA Attack on AES-OTR with Serial AD Processing

Sketch of IND-qCPA attack:

1. Pick single block messages M_0 and M_1 and empty AD as input for the challenger.
Record response (C^*, T^*) and the nonce N .
2. Compute

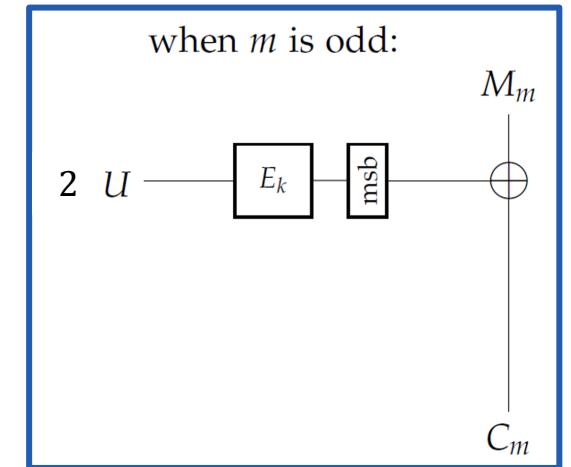
$$V = E_K \left(2 \cdot E_K \left(\text{Format}(\tau, N) \right) \right)$$

in $2\mathcal{O}(n)$ quantum encryption queries

3. Output the bit $b'' = b'$ if $M_{b'} = C^* \oplus V$

Why does this work?

→ For empty AD and single block message:

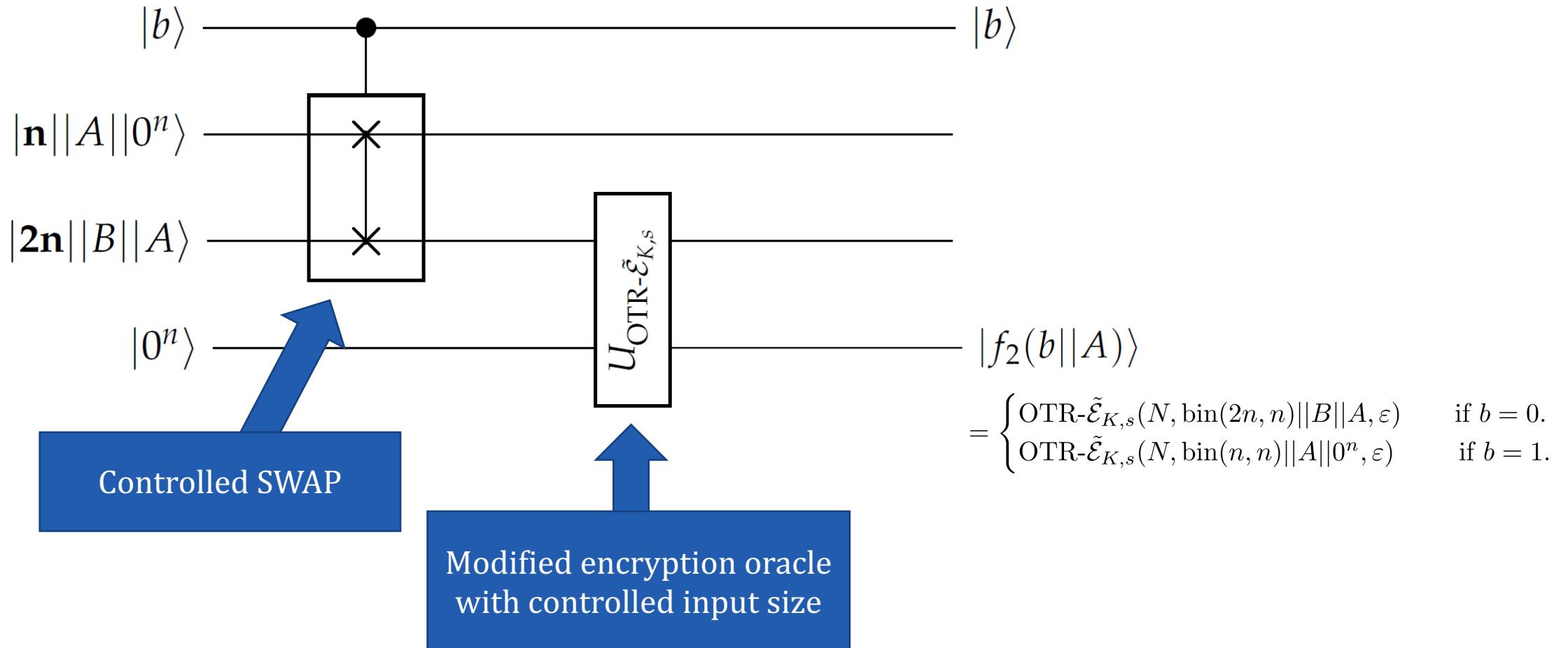


$$U = 2(E_K(\text{Format}(\tau, N)) \oplus TA)$$

$$\text{OTR-}\mathcal{E}_{K,s}(N, \varepsilon, M) \Big|_C = E_K \left(2 \cdot E_K \left(\text{Format}(\tau, N) \right) \right) \oplus M$$

Superposition Over Unequal-Length Data

- We need to have quantum access to f_2 with a single query to the encryption oracle!

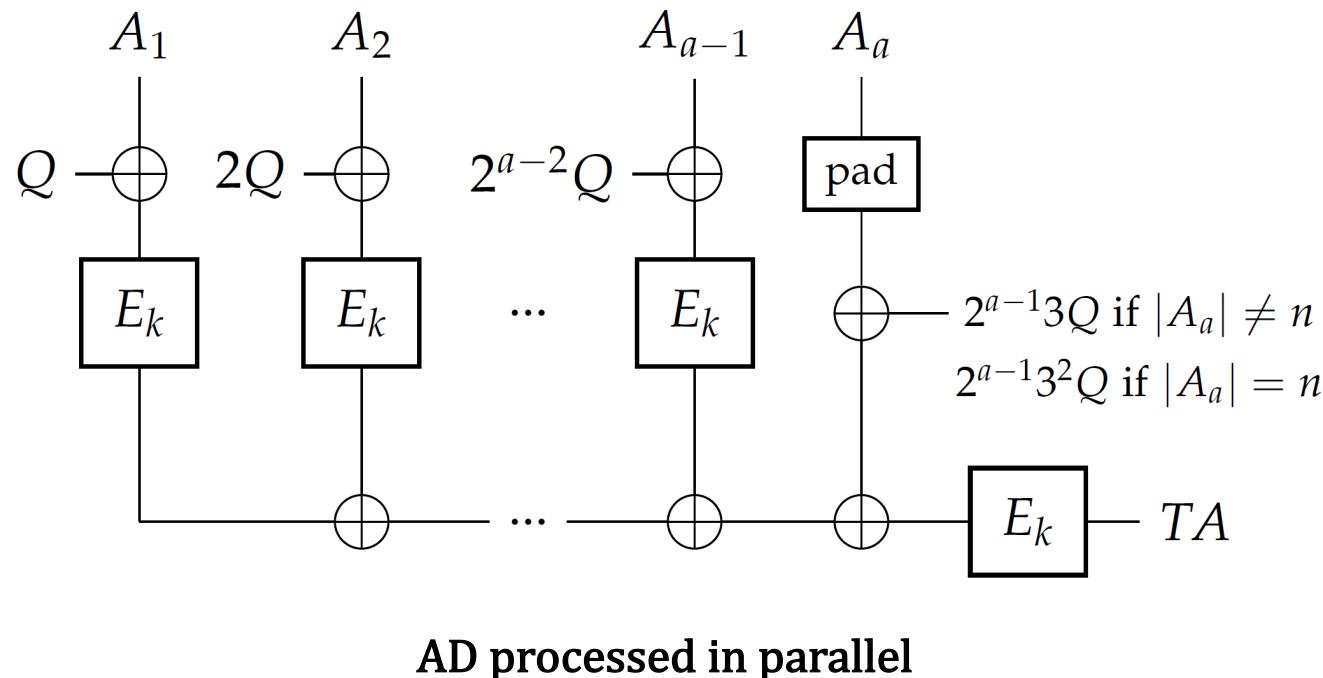


Superposition Over Unequal-Length Data

- Laws of quantum physics define a superposition only over states with the same number of qubits.
- We can overcome this restriction in the IND-qCPA setting with this modified quantum encryption oracle!
- Allows for **stronger** quantum attacks: e.g., we gain raw block cipher access directly via Simon's algorithm.
 - This contrasts with the IND-qCPA attacks against OCB by Maram *et al.* (ToSC 2022) which also requires Deutsch's algorithm, along with Simon's algorithm.
- This model can also be extended to cryptanalysis in the more realistic **post-quantum** setting – e.g., attacking (public) hash functions.

Further Attacks on AES-OTR

- IND-qCPA attack when AD is processed in parallel.
- IND-qCPA attack when AD is always empty.



Quantum Key-Recovery Attack on OPP

Specifications of OPP (simplified)

- Offset Public Permutation Mode

Algorithm $\text{OPP-}\mathcal{E}(K, N, AD, M)$

- 1: $X \leftarrow \text{pad}_{n-\kappa-k}^0(N)$ 
 - 2: $C, S \leftarrow \text{OPPEnc}(K, X, M)$ 
 - 3: $T \leftarrow \text{OPPAbs}(K, X, AD, S)$ 
 - 4: **return** C, T
-

Zero padding

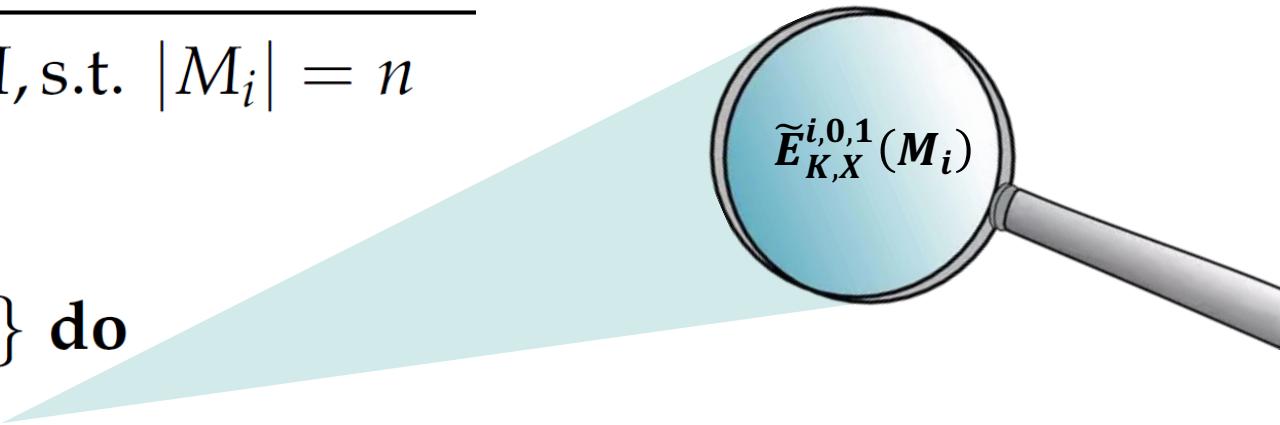
Encryption Core

Authentication Core
(not relevant for the
attack)

Specifications of OPP: Encryption Core $\mathbf{OPP}\mathbf{Enc}(K, X, M)$

Algorithm $\mathbf{OPP}\mathbf{Enc}(K, X, M)$

```
1:  $M_0||\dots||M_{m-1} \leftarrow M$ , s.t.  $|M_i| = n$ 
2:  $C \leftarrow \varepsilon$ 
3:  $S \leftarrow 0^n$ 
4: for  $i \in \{0, \dots, m-1\}$  do
5:    $C_i \leftarrow \tilde{E}_{K,X}^{i,0,1}(M_i)$ 
6:    $C \leftarrow C||C_i$ 
7:    $S \leftarrow S \oplus M_i$ 
8: return  $C, \tilde{E}_{K,X}^{m-1,2,1}(S)$ 
```



Checksum: Xor of all plaintext blocks

What is $\tilde{E}_{K,X}^{i,0,1}(M_i)$?

$$X = \text{pad}_{n-\kappa-k}^0(N)$$

$$\bar{i} = (i_0, i_1, i_2) \in \mathbb{N}^3$$

Key

$$\tilde{E}(K, X, \bar{i}, M) = P\left(\delta(K, X, \bar{i}) \oplus M\right) \oplus \delta(K, X, \bar{i})$$

$$\gamma^{i_2} \circ \beta^{i_1} \circ \alpha^{i_0}(P(X \parallel K))$$

$$\gamma(x) = \varphi^2(x) \oplus \varphi(x) \oplus x$$

$$\beta(x) = \varphi(x) \oplus x$$

$$\alpha(x) = \varphi(x)$$

$$\varphi(x) = Mx, M \text{ a matrix}$$

$$\delta(K, X, (i, 0, 1)) = \varphi^{i+2}(\Omega) \oplus \varphi^{i+1}(\Omega) \oplus \varphi^i(\Omega) \quad \Omega = P(X||K)$$

Quantum Key-Recovery Attack on OPP: Preparation

- Ciphertext block as a function of its corresponding plaintext block: $f_i : \{0,1\}^n \rightarrow \{0,1\}^n$

What if we can recover

$$\Omega = P(X||K)?$$

Quantum Key-Recovery Attack on OPP

- **Idea:** (By Bhaumik *et al.* (Asiacrypt 2021)) Create periodic function that contains n copies of the earlier periodic function in the linear function $g : \{0,1\}^{(2n+1)n+\tau} \rightarrow \{0,1\}^{(n+1)n}$

$$g(C_0, C_1, \dots, C_{2n}, t) = (C_0, C_1 \oplus C_2, \dots, C_{2n-1} \oplus C_{2n})$$

- Using g , define $\tilde{f}_N : \{0,1\}^{n^2} \rightarrow \{0,1\}^{(n+1)n}$ such that

$$\tilde{f}_N(M_1, \dots, M_n) = g \circ \text{OPP-}\mathcal{E}(K, N, \varepsilon, 0^n || M_1 || M_1 || M_2 || \dots || M_n || M_n)$$

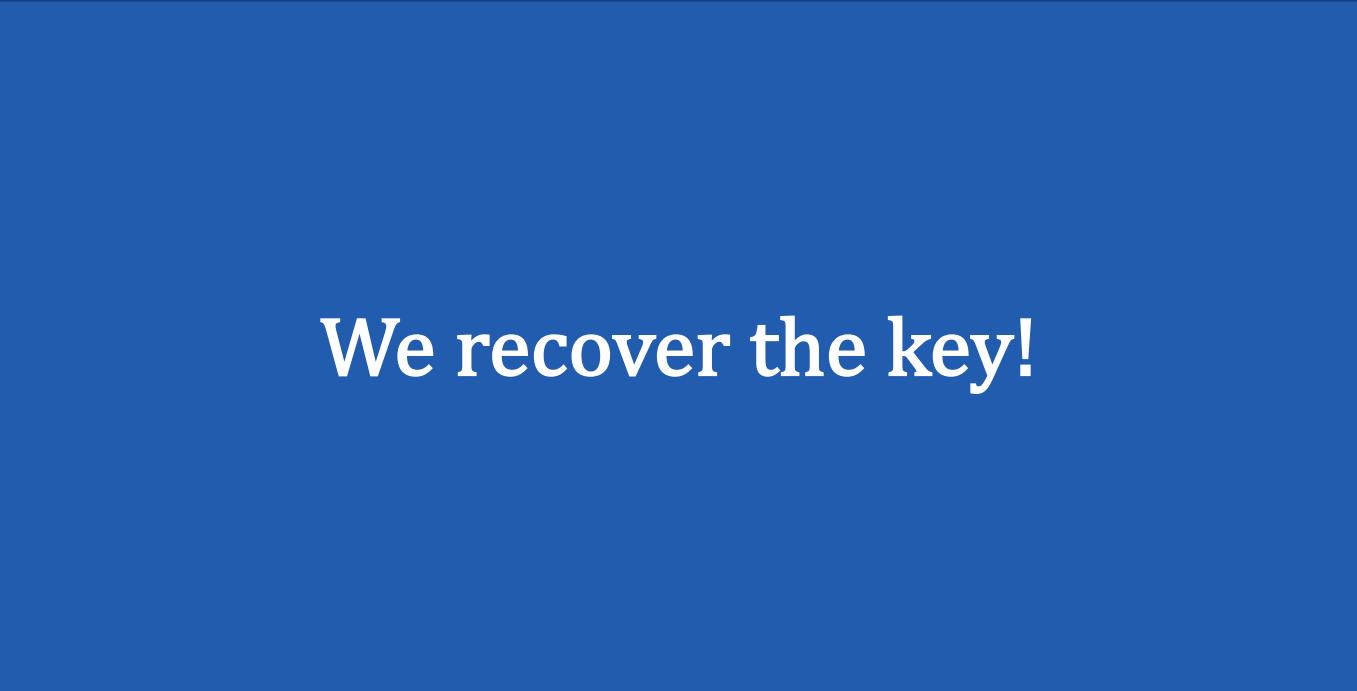
- \tilde{f}_N has n linearly independent periods $\langle s_i \rangle_{i \in [n]}$

$$s_i = \left((0^n)^{i-1} || \varphi^{2i+2}(\Omega) \oplus \varphi^{2i-1}(\Omega) || (0^n)^{n-i} \right)$$

$$\Omega = P(X || K)$$

Quantum Key-Recovery Attack on OPP

- Apply Simon's algorithm and recover $y = (y_1, \dots, y_n) \in \{0, 1\}^{n^2}$ orthogonal to **each** of the periods with a single quantum query
- We get n linear equ



We recover the key!

which we are able to

- P is a public, efficient



For questions, please reach out to the authors:

Melanie Jauch - mjauch@student.ethz.ch

Varun Maram - vmaram@inf.ethz.ch

Extra Slide

- Periodicity of f_2 :

$$\begin{aligned} g(1||A \oplus 1||E_K(B)) &= g(0||A \oplus E_K(B)) = \text{AF-}S_K(B||A \oplus E_K(B)) \\ &= E_K(4Q \oplus A \oplus E_K(B) \oplus E_K(B)) = E_K(4Q \oplus A) \\ &= \text{AF-}S_K(A) = g(1||A) \end{aligned} \tag{3.4.2}$$

- f_2 is not periodic when computed with two quantum encryption queries:

$$\begin{aligned} f_2(0||A \oplus 1||E_K(B)) &= f_2(1||A \oplus E_K(B)) \stackrel{\text{def}}{=} \text{OTR-}E_{K,s}(N_2, A \oplus E_K(B), \varepsilon) \\ &\neq \text{OTR-}E_{K,s}(N_1, B||A, \varepsilon) \stackrel{\text{def}}{=} f_2(0||A) \end{aligned}$$