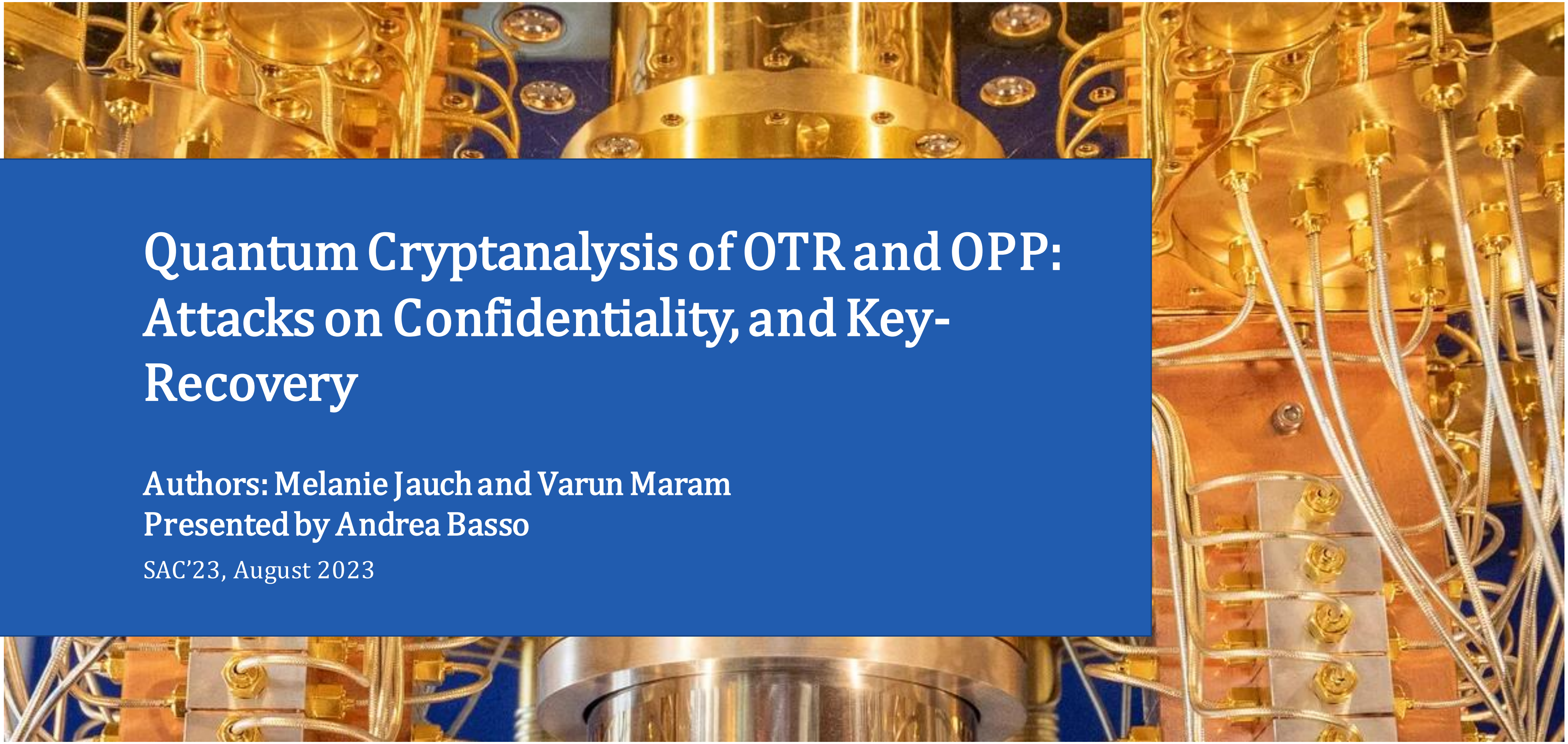
ETH zürich



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

Authors: Melanie Jauch and Varun Maram
Presented by Andrea Basso

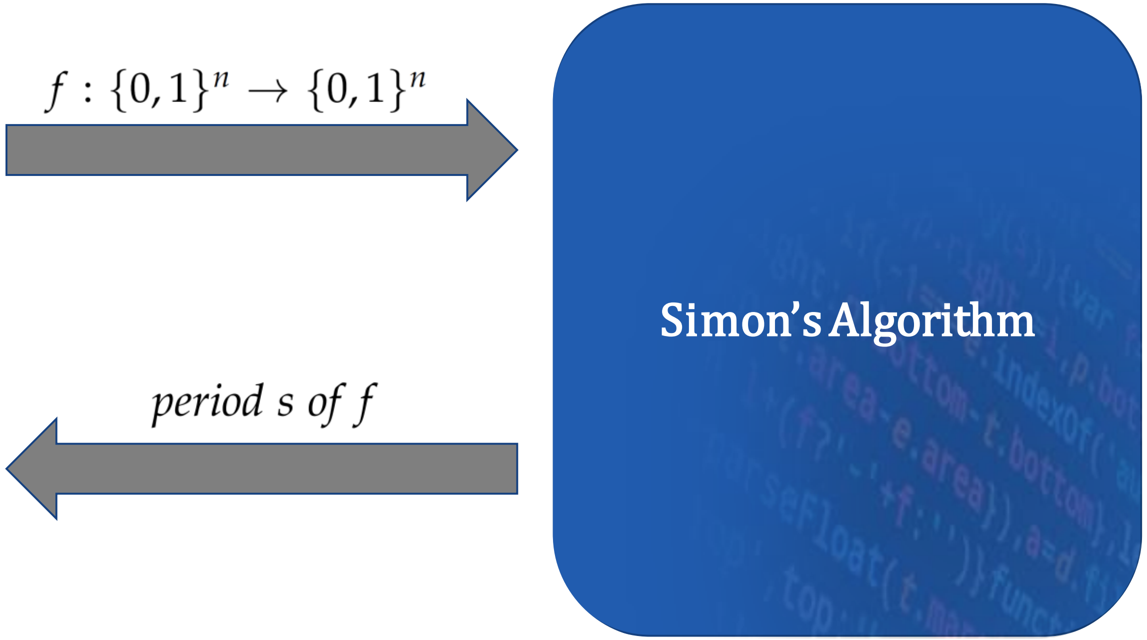
SAC'23, August 2023

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-**q**CMA).
- More recently: confidentiality (IND-**q**CPA) 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 $f\colon \{0,1\}^n \rightarrow \{0,1\}^n$ 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 <u>orthogonal</u> to the period s is recovered with high probability.



IND-qCPA Security Game

Adversary

Encryption Queries:

(In any order)

Challenge Query:

b''

Wins if $b'' = b'$.

Challenger

$b' \leftarrow_\$ \{0, 1\}$

$K \leftarrow \mathrm{KGen}$

$N \leftarrow_\$ \{0,1\}^\kappa$

N

(M, AD), possibly in superposition

$(C, T) \leftarrow \mathrm{Enc}_K(N, AD, M)$

(C, T)

$N \leftarrow_\$ \{0,1\}^\kappa$

N

$(M_0, AD), (M_1, AD)$, classical values

$(C^*, T^*) \leftarrow \mathrm{Enc}_K(N, AD, M_{b'})$

(C^*, T^*)

Breaking AES-OTR‘s IND-qCPA Security

Specifications of AES-OTR

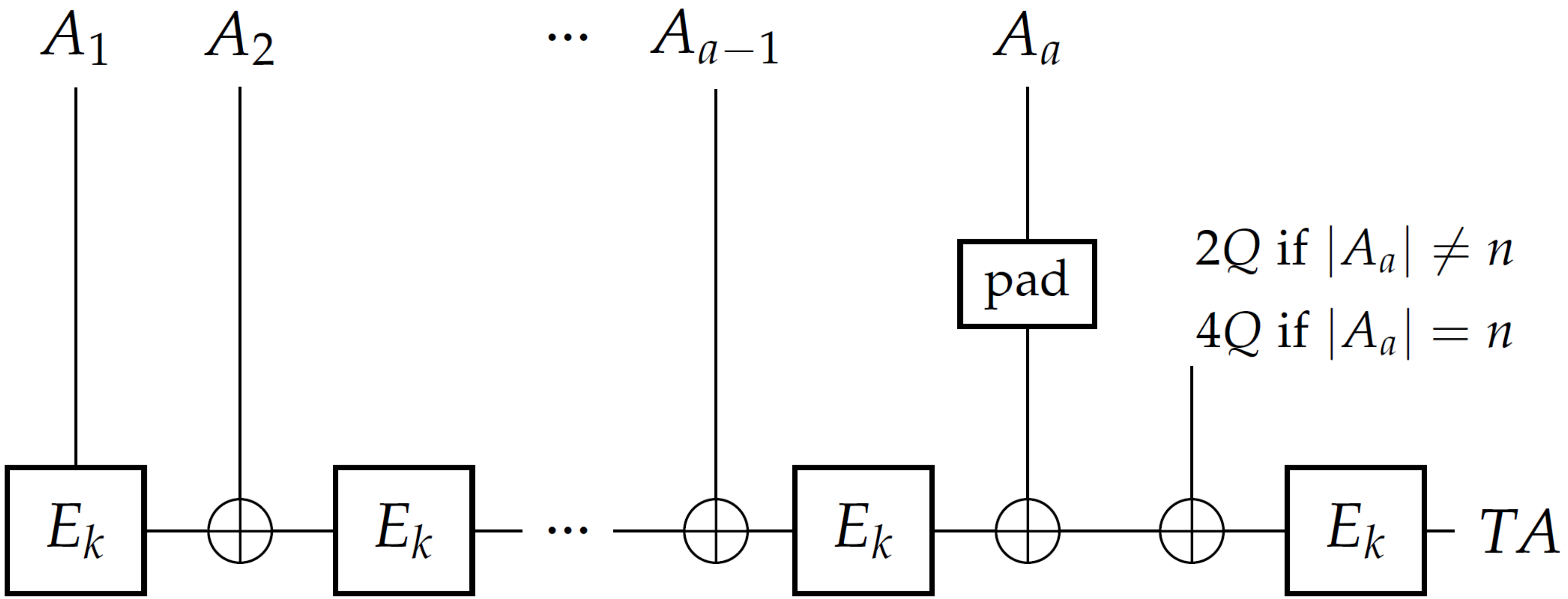
Algorithm OTR-$\mathcal{E}_{K,s}(N, A, M)$

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

AD Processing

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

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



Specifications of AES-OTR

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

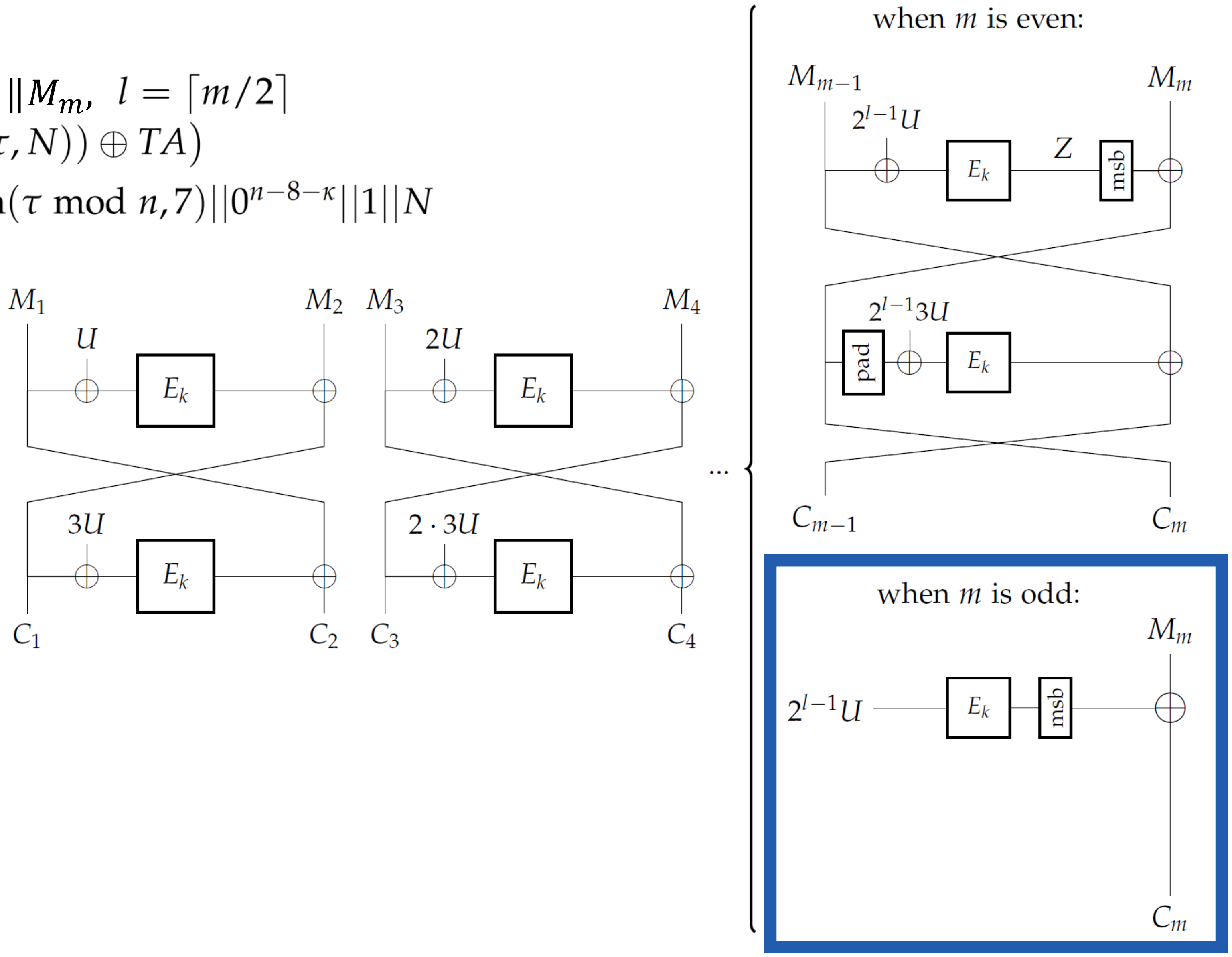
if $A \neq \varepsilon$ **then**
    $TA \leftarrow \text{AF-S}_K(A)$
else $TA \leftarrow 0^n$
$(C, TE) \leftarrow \text{EF-S}_{K,\tau}(N, M, TA)$
$T \leftarrow \text{msb}_\tau(TE)$
return (C, T)

AD Processing

Encryption Core

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

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



Specifications of AES-OTR

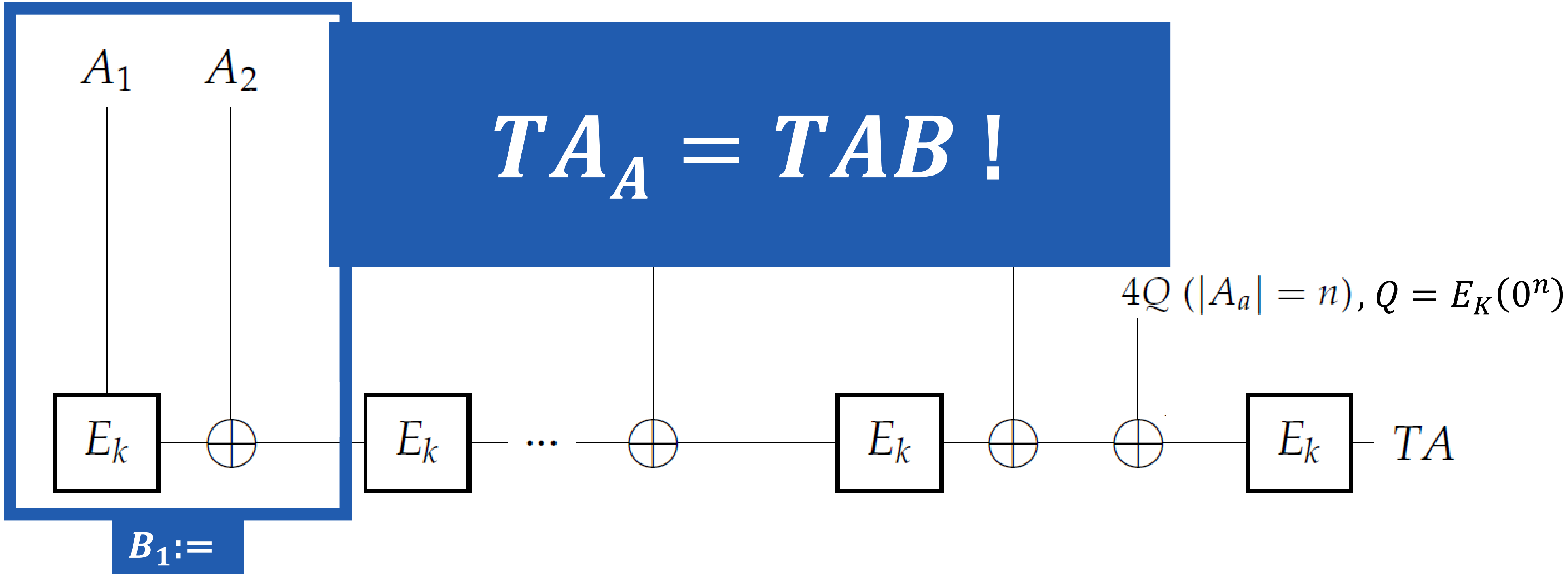
Algorithm 2 OTR-$\mathcal{E}_{K,s}(N, A, M)$

```
if A ≠ ε then
    TA ← AF-S_K(A)                      AD Processing
else TA ← 0^n
(C, TE) ← EF-S_{K,τ}(N, M, TA)          Encryption Function
T ← msb_τ(TE)                           Tag Computation
return (C, T)
```

$$
\begin{array}{l}
\textbf{if } A \neq \varepsilon \textbf{ then} \\
\quad TA \leftarrow \text{AF-S}_K(A) \qquad \textbf{AD Processing} \\
\textbf{else } TA \leftarrow 0^n \\
(C, TE) \leftarrow \text{EF-S}_{K,\tau}(N, M, TA) \qquad \textbf{Encryption Function} \\
T \leftarrow \text{msb}_\tau(TE) \qquad \textbf{Tag Computation} \\
\textbf{return } (C, T)
\end{array}
$$

Finding Collisions in Serial AD Processing

- High-level attack on <u>unforgeability</u> first described by Kaplan *et al.* (Crypto 2016).
  - Detailed attack followed by Chang *et al.* (Symmetry 2022).
- AD $A = A_1 \| \ldots \| A_a$ with $A_i \in \{0,1\}^n$
- Define AD $B = B_1 \| \ldots \| B_{a-1}$ 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 $f_2 : \{0,1\}^{n+1} \to \{0,1\}^\tau$

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

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

depends on AD

- Where

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

Period of f_2 only depends on TA_D!

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

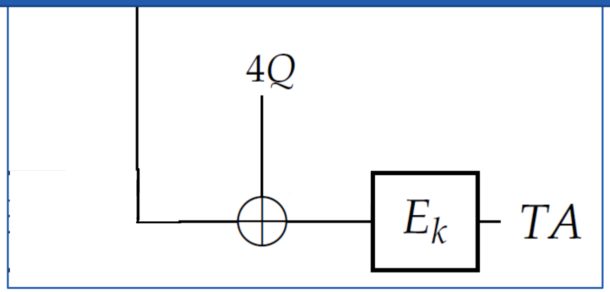
- Define new function $g : \{0,1\}^{n+1} \to \{0,1\}^n$, (inner function of f_2)

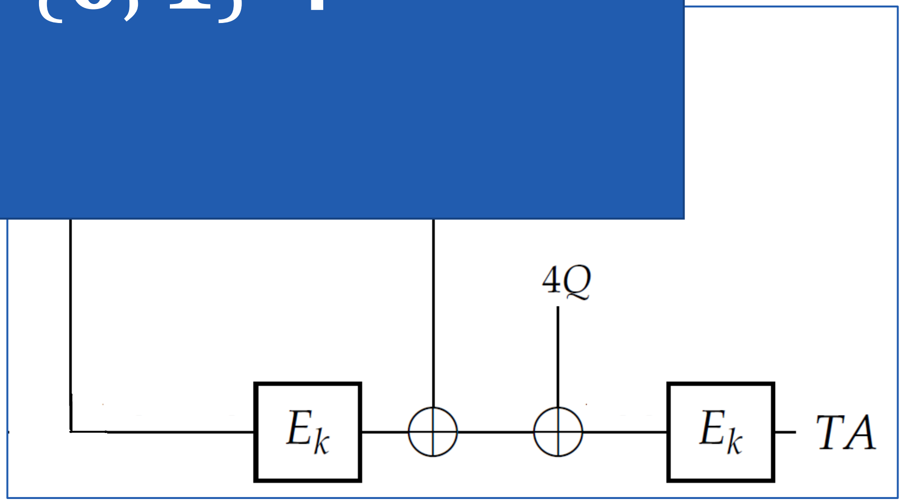
$$\begin{cases} \text{AE-S}_K(B||A) & \text{if } b = 0 \end{cases}$$

- **Claim**: g (and th

$g(0||A \oplus$ $= g(0||A)$

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

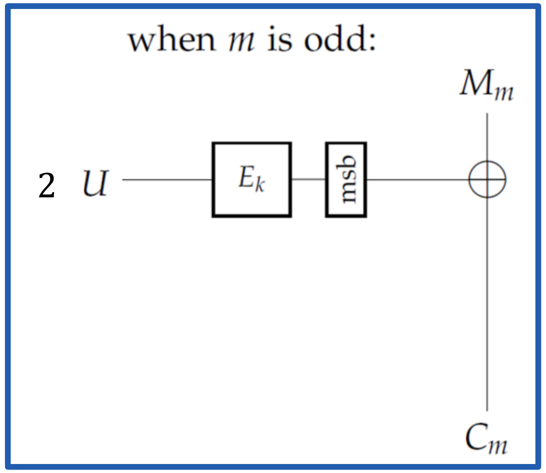




IND-qCPA Attack on AES-OTR with Serial AD Processing

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
$$V = E_K\Big(2 \cdot E_K(\mathrm{Format}(\tau, N))\Big)$$
in $2\mathcal{O}(n)$ quantum encryption queries
3. Output the bit $b'' = b'$ if $M_{b'} = C^* \oplus V$



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

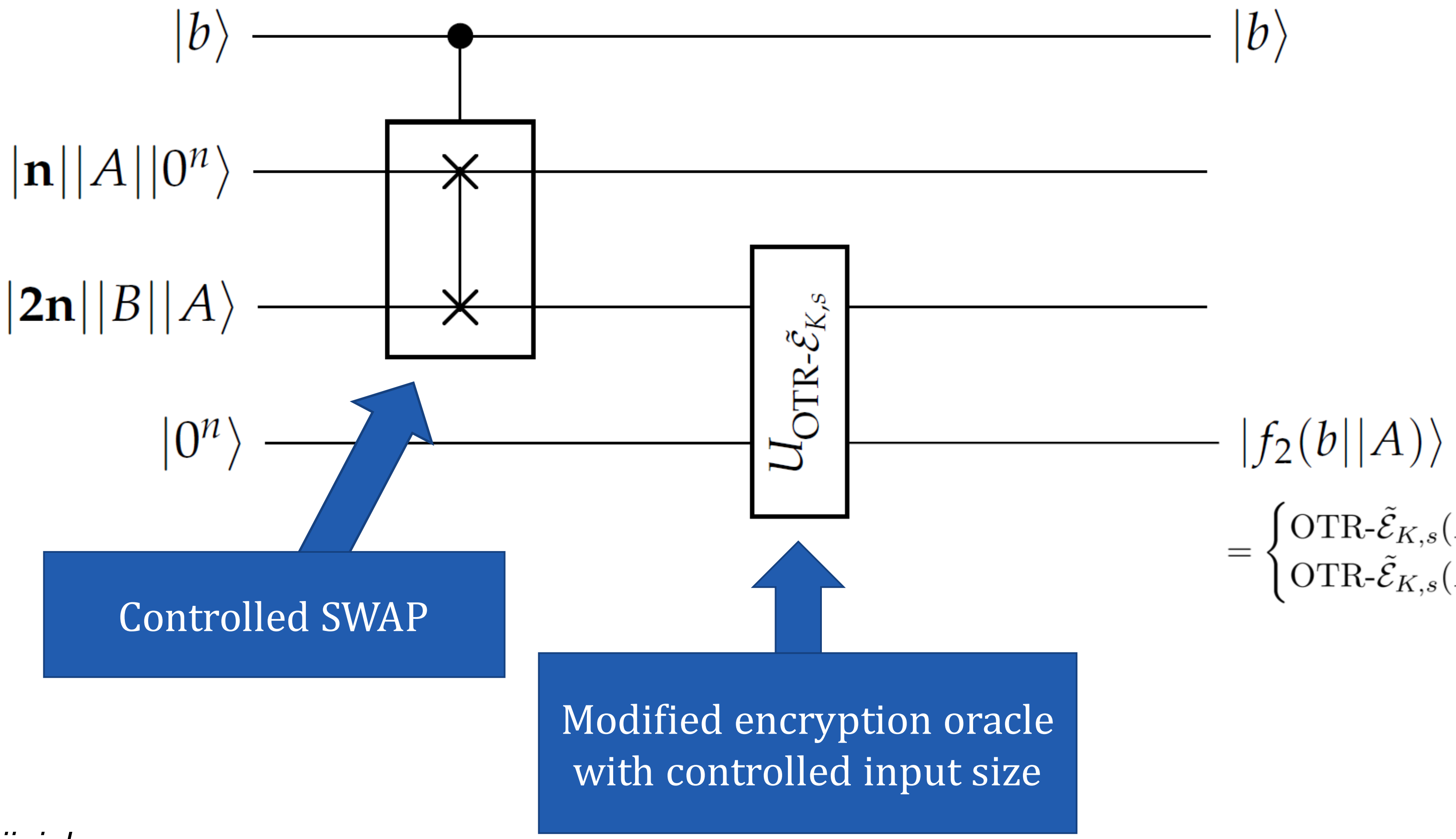
Why does this work?

→ For empty AD and single block message:

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

Superposition Over **Unequal-Length** Data

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



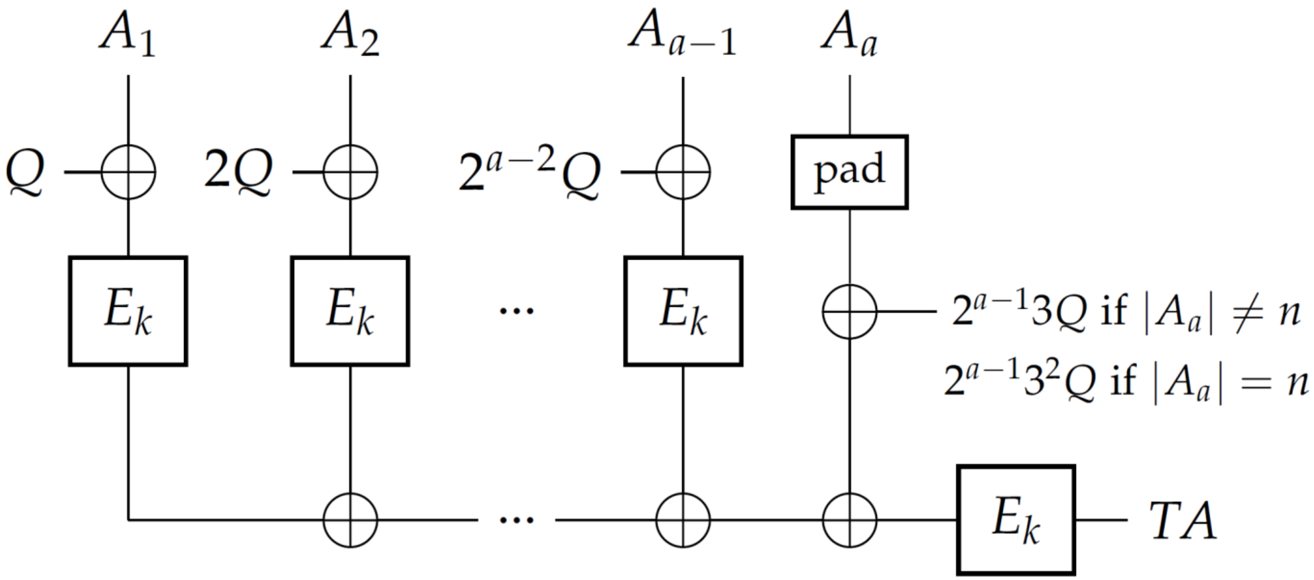
$$= \begin{cases} \text{OTR-}\tilde{\mathcal{E}}_{K,s}(N, \text{bin}(2n, n)||B||A, \varepsilon) & \text{if } b = 0. \\ \text{OTR-}\tilde{\mathcal{E}}_{K,s}(N, \text{bin}(n, n)||A||0^n, \varepsilon) & \text{if } b = 1. \end{cases}$$

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.



AD processed in parallel

Quantum Key-Recovery Attack on OPP

Specifications of OPP (simplified)

- **Offset Public Permutation** Mode

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

1: $X \leftarrow \mathrm{pad}^0_{n-\kappa-k}(N)$ — **Zero padding**

2: $C, S \leftarrow \mathrm{OPPEnc}(K, X, M)$ — **Encryption Core**

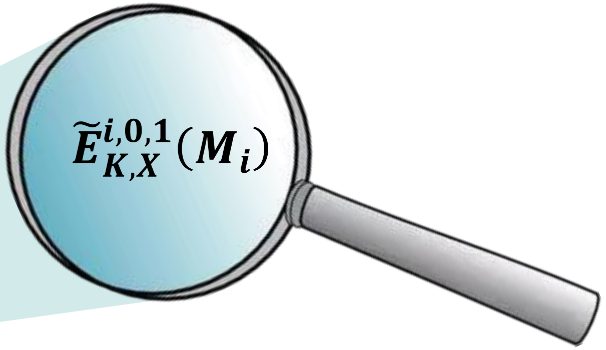
3: $T \leftarrow \mathrm{OPPAbs}(K, X, AD, S)$ — **Authentication Core** (not relevant for the attack)

4: **return** C, T

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

Algorithm $\mathrm{OPPEnc}(K, X, M)$

$M_0||...||M_{m-1} \leftarrow M$, s.t. $|M_i| = n$
$C \leftarrow \varepsilon$
$S \leftarrow 0^n$
for $i \in \{0, ..., m-1\}$ **do**
    $C_i \leftarrow \widetilde{E}^{i,0,1}_{K,X}(M_i)$
    $C \leftarrow C||C_i$
    $S \leftarrow S \oplus M_i$
return $C, \widetilde{E}^{m-1,2,1}_{K,X}(S)$



Checksum: Xor of all plaintext blocks

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

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

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

Key

$$\tilde{E}(K, X, \bar{i}, M) = P\big(\underbrace{\delta(K, X, \bar{i})}_{\gamma^{i_2} \circ \beta^{i_1} \circ \alpha^{i_0}(P(X \parallel K))} \oplus M\big) \oplus \delta(K, X, \bar{i})$$

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

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

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

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

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

Quantum Key-Recovery Attack on OPP: Preparation

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

What if we can recover

$$\boldsymbol{\Omega = P(X||K)}?$$

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 $g : \{0,1\}^{(2n+1)n+\tau} \to \{0,1\}^{(n+1)n}$

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

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

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

- $\tilde{f}_N$ 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 $y = (y_1, \ldots, y_n) \in \{0,1\}^{n^2}$ orthogonal to **each** of the periods <u>with a single quantum qu</u>
- We get n linear equ

  which we are able t
- P is a public, efficie

We recover the key!

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:

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

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

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