QCB: Efficient Quantum-secure Authenticated Encryption

Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, Yannick Seurin

ASIACRYPT 2021

Introduction

From a block cipher to authenticated encryption

Block cipher

Family of permutations $E_K : \{0,1\}^n \to \{0,1\}^n$ with fixed n, indexed by a key K of fixed size (e.g. 256 bits for both).

Authenticated encryption

A function: $\mathrm{Enc}_K : IV, M, A \to C, T$

- IV is the **initial value** (or nonce) that avoids resend attacks
- M is a message of any length
- C is a ciphertext of same length
- T is an **authentication tag**
- A is the associated data (only used for the tag computation)

The decryption function first **verifies** the tag and then decrypts; if the tag is wrong it fails.

Lightweight AE from a block cipher

One option for AE is to handle the Encryption and Authentication tasks separately, e.g. encrypt-then-MAC:

1. first, encrypt M securely into C (e.g. with CTR)
2. second, authenticate C with a secure MAC (e.g., NMAC / HMAC)

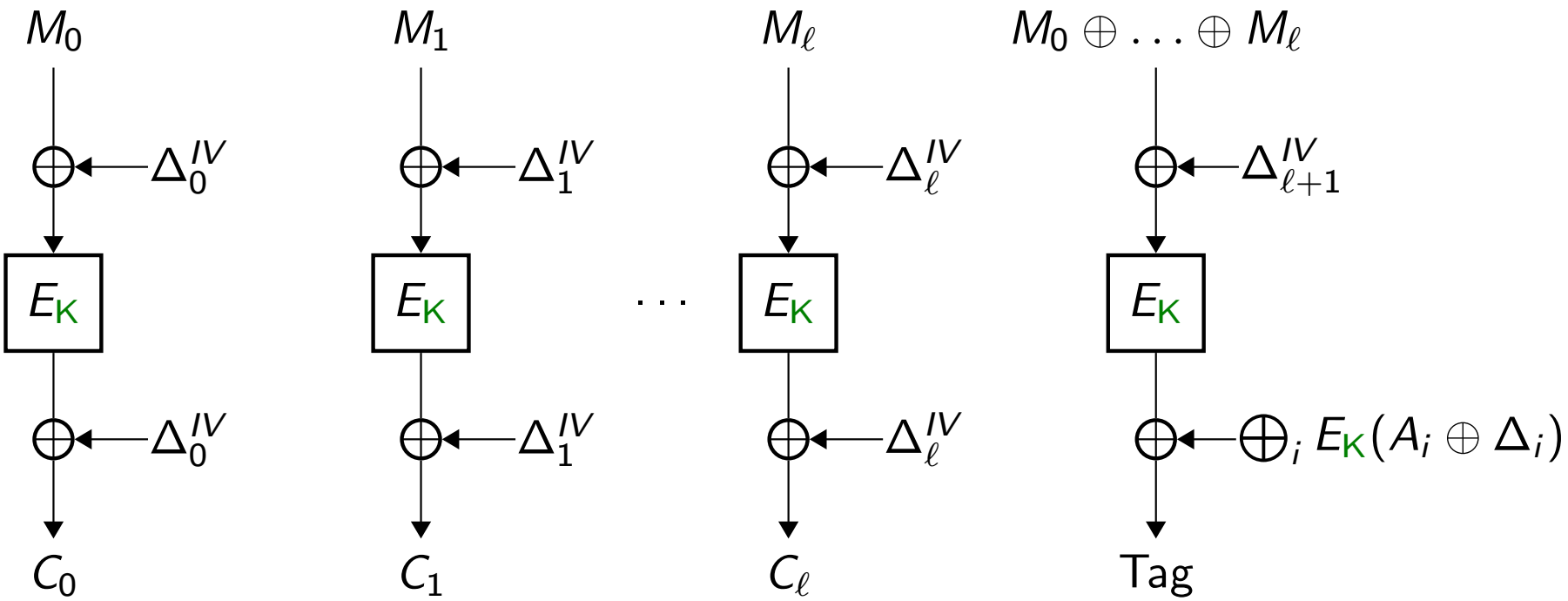
CTR mode

Cut M into blocks $M_0, \ldots, M_\ell$, produce the ciphertext blocks as: $C_i = E_K(IV \oplus i) \oplus M_i$.

This approach (used in Saturnin) yields a mode of **rate 2**: 2 block cipher calls per message block. We would like to reach rate 1.

 Canteaut, Duval, Leurent, Naya-Plasencia, Perrin, Pornin, Schrottenloher, "Saturnin: a suite of lightweight symmetric algorithms for post-quantum security"

Example: OCB3 (offset codebook)



$\Delta_i^{IV} = \Delta^{IV} \oplus \Delta_i$, Δ^{IV} and Δ_i depend on K

Krovetz, Rogaway, "The Software Performance of Authenticated-Encryption Modes", FSE 2011

Quantum security in symmetric crypto

Classical query model

- Make classical queries to the encryption function
- Do quantum computations

$\Longrightarrow$ realistic, less powerful.

Only ~~quadratic~~ **2.5** speedups **at most so far**.

Superposition query model

- Do quantum computations
- Can use black-box **inside** the quantum algorithm

$\Longrightarrow$ theoretical, strictly more powerful, but non trivial.
$\Longrightarrow$ also **more suited for provable security.**

Exponential speedups (total breaks) **become possible**.


Bonnetain, Schrottenloher, Sibleyras, "Beyond quadratic speedups in quantum attacks on symmetric schemes" ePrint 2021/1348

Quantum security of OCB

In the **superposition query model**, OCB is broken and no secure rate-1 AE mode is known.

What is in superposition?

- The adversary sets a certain maximal length ℓ and queries a quantum oracle for the AE with messages of length ℓ.
- The IV is not controlled by them, and it remains **classical**.
- We will consider IVs chosen u.a.r. at each oracle query

- If we are happy with rate-2, we can use the CTR + NMAC / HMAC composition.
- Can we fix OCB to make it quantum-resistant?

Repairing OCB (or not)

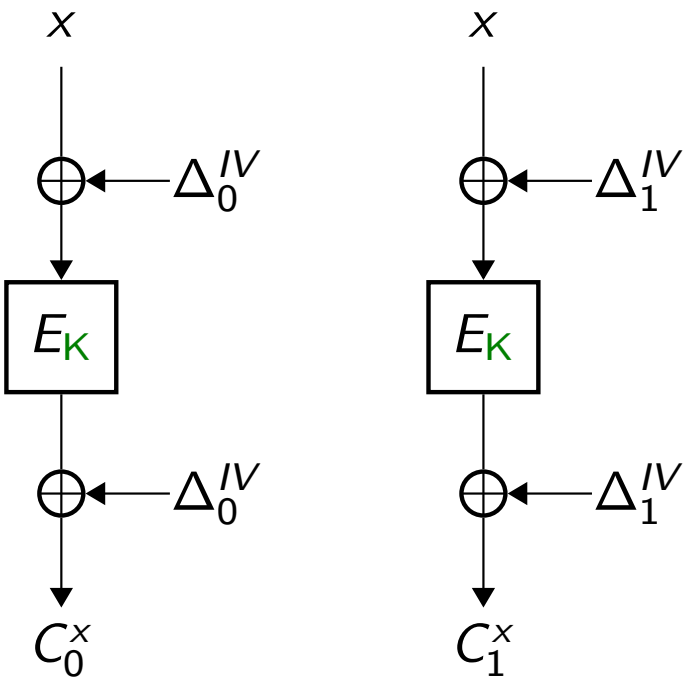
Simon-based attacks on OCB

Simon's algorithm

If we are able to (superposition) query an n-bit periodic function: $f(x \oplus s) = f(x)$ for some secret s, we can recover s in polynomial time.

- With one query and some computations, we recover a vector orthogonal to s
- Do this $\mathcal{O}(n)$ times, solve a linear system to get s

OCB3: Periods everywhere



Attack on ciphering part

We take two equal message blocks and XOR the ciphertext blocks:

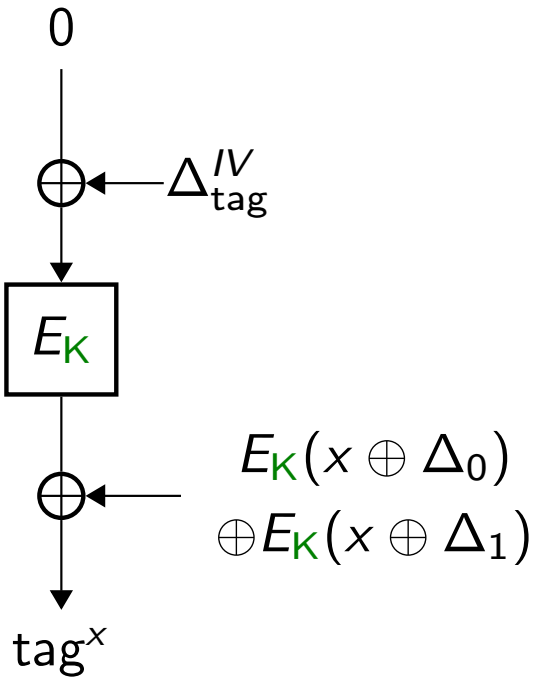
$$f(x) = C_0^x \oplus C_1^x = \Delta_0^{IV} \oplus E_K(\Delta_0^{IV} \oplus x) \oplus \Delta_1^{IV} \oplus E_K(\Delta_1^{IV} \oplus x)$$

$\Longrightarrow$ **periodic** with period $\Delta_0^{IV} \oplus \Delta_1^{IV}$

- $\Delta_0^{IV} \oplus \Delta_1^{IV} = (\Delta^{IV} \oplus \Delta_0) \oplus (\Delta^{IV} \oplus \Delta_1) = \Delta_0 \oplus \Delta_1$
- $x \mapsto C_0^x \oplus C_1^x$ is a periodic function, that we can query multiple times to recover $\Delta_0 \oplus \Delta_1$

Kaplan, Leurent, Leverrier, Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period-finding", CRYPTO 2016

OCB3: Periods everywhere (ctd.)



Attack on tag part

We take two equal AD blocks and look at the tag:

$$f(x) = \text{tag}^x = E_K(\Delta^{IV}_{\text{tag}}) \oplus E_K(x \oplus \Delta_0) \oplus E_K(x \oplus \Delta_1)$$

$\Longrightarrow$ **periodic** with period $\Delta_0 \oplus \Delta_1$

- Since the IV changes at each query, each (superposition) query is made to a **different function**
- But Simon's attack only needs the **period** to be always the same (we still sample vectors orthogonal to it), so we can recover $\Delta_0 \oplus \Delta_1$

OCB3: Forgery Attack using $\Delta_0 \oplus \Delta_1$

One-query forgery attack

- Take two AD blocks A_0 and A_1 with $A_0 \oplus A_1 \neq \Delta_0 \oplus \Delta_1$
- For some IV and a message M query $(IV, (A_0, A_1), M)$ and get ciphertext-tag pair (C, T)
- Produce (C, T) as forge of $(IV, (A_1 \oplus \Delta_0 \oplus \Delta_1, A_0 \oplus \Delta_0 \oplus \Delta_1), M)$

$$T = [\text{function of } (IV, M)] \oplus E_K(A_0 \oplus \Delta_0) \oplus E_K(A_1 \oplus \Delta_1)$$

Fixing OCB

Our initial idea

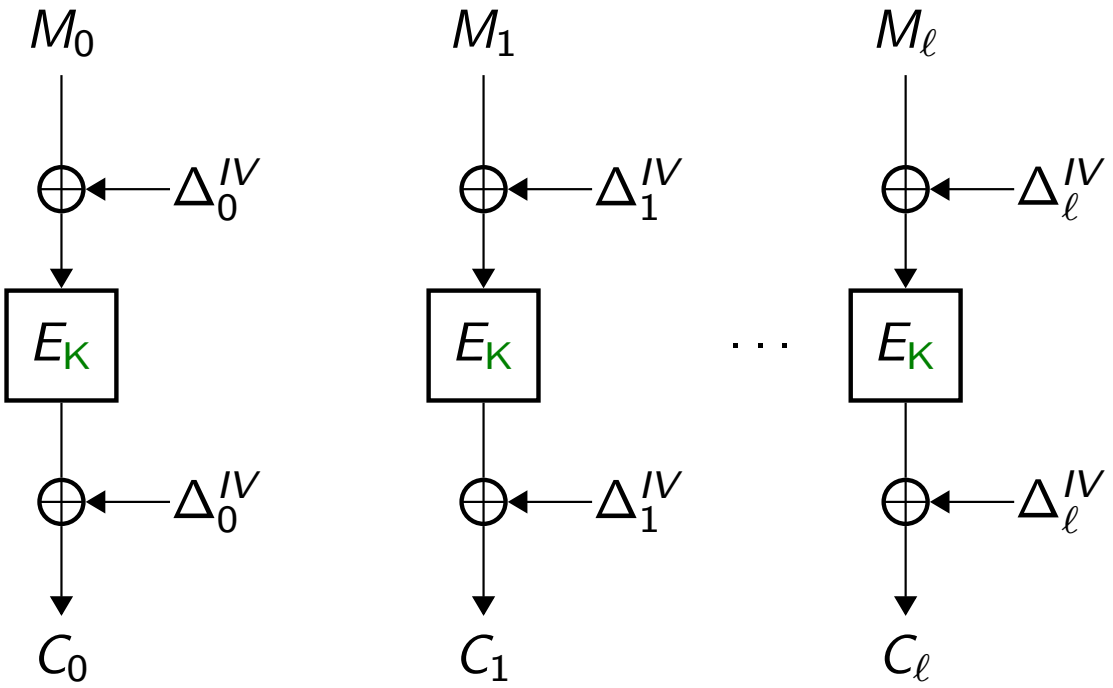
Change the definition of offsets so that $\Delta_0^{IV} \oplus \Delta_1^{IV}$ remains IV-dependent. Example: $\Delta_0^{IV} = i \cdot E_K(IV)$.

- Simon-based attack with a **single query** still works: it samples vectors y_i such that $y_i \cdot (\Delta_{i_1}^{IV} \oplus \Delta_{i_2}^{IV}) = 0$ for non-overlapping pairs (i_1, i_2) of our choice (e.g., $(1,2),(3,4),\ldots,(n-1,n)$).
- We can extract enough data to solve for $E_K(IV)$.

The problem in OCB is the "O". Using the **offsets** makes the system vulnerable to period-finding.

What is OCB without the offsets? **ΘCB**.

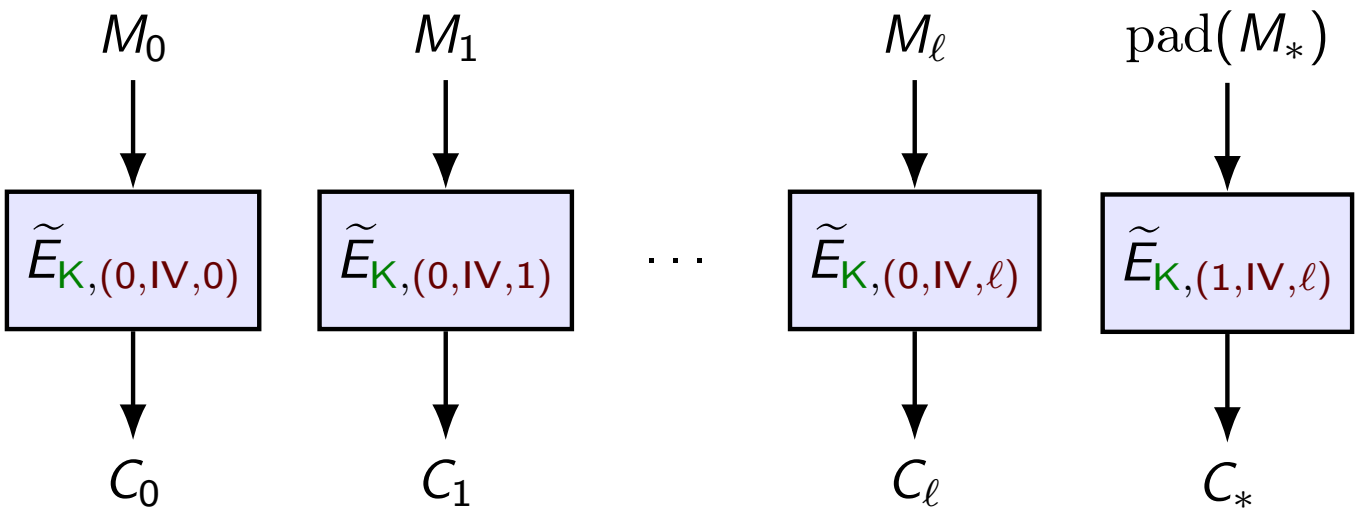
Tweakable block ciphers



- We can think of the offsets Δ_i^{IV} as **tweaks** that modify each blockcipher call
- Ideally, we would like to have a **family of independent block ciphers** indexed by the block number
  $\Longrightarrow$ this is a Tweakable Block Cipher: a block cipher $\widetilde{E}_{K,t}$ with an additional non-secret **tweak** input t

QCB: encryption

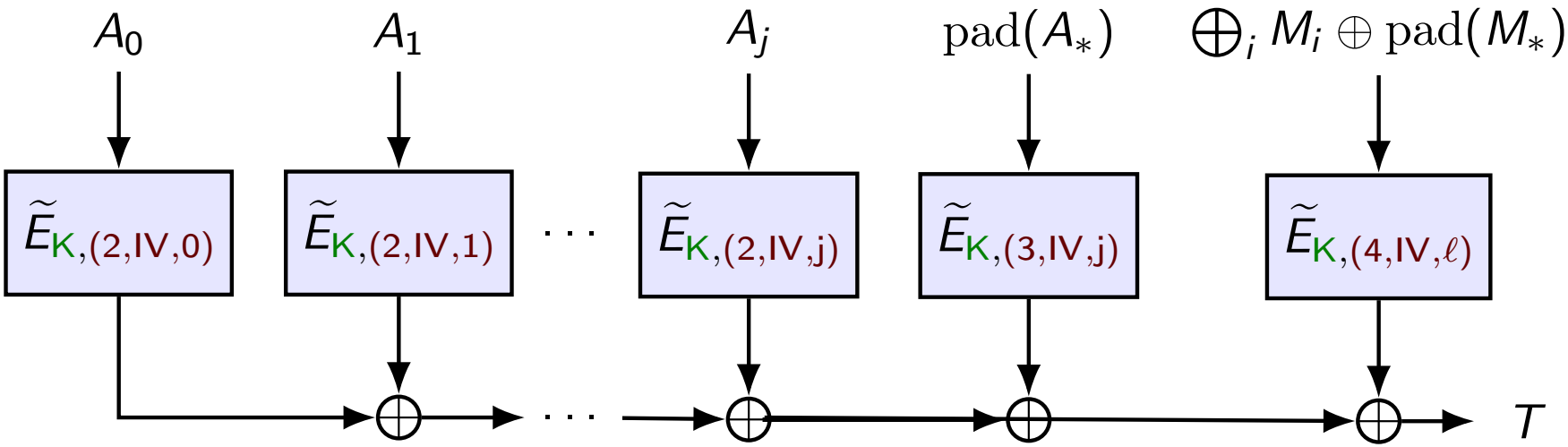
There is no change with ΘCB here (we just need to specify the independent tweak values).



QCB: tag

There is an **important change here:** the tweaks must depend on the IV.

- if they don't, we are exposed to a quantum linearization attack



Bonnetain, Leurent, Naya-Plasencia, Schrottenloher, "Quantum Linearization Attacks", ASIACRYPT 2021

Proving Security

TBC security

Quantum-secure TBC (ideal definition)

The adversary cannot distinguish $\widetilde{E}_{K,t}$ for random K from a random family of permutations Π_t, with:

- classical tweak inputs
- superposed messages / ciphertexts

In the ideal definition of a secure TBC, the classical tweaks can be chosen adaptively by the adversary

QCB security with ideal TBC

Confidentiality: IND-qCPA

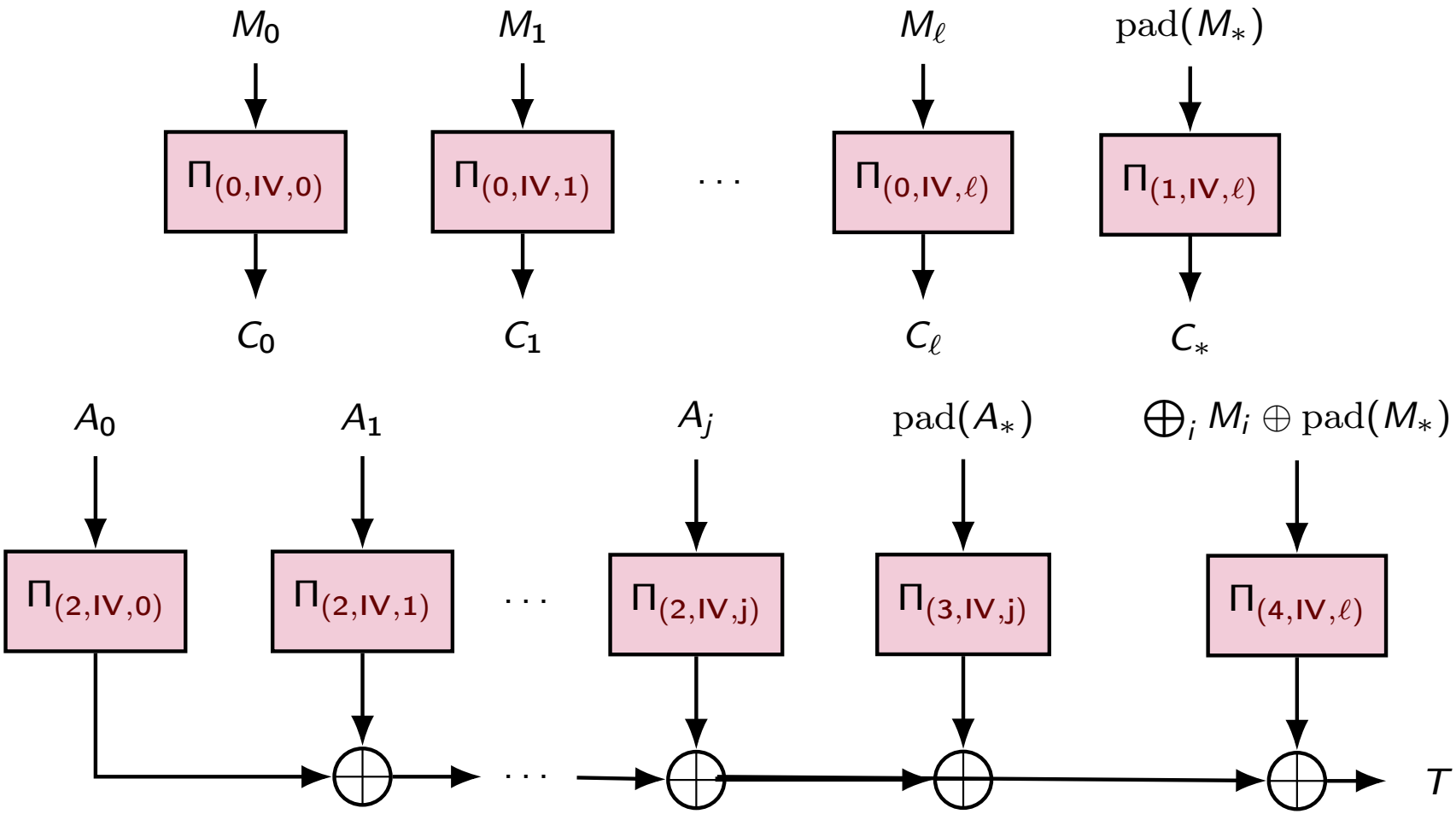
- Query Phase: The adversary makes q encryption queries with adaptive classical IVs and M, A (possibly) in superposition
- Challenge Phase: Must distinguish between encryptions of two classical messages

Authenticity: BZ

- Query Phase: The adversary makes q encryption queries with adaptive classical IVs and M, A (possibly) in superposition
- Forging Phase: Must output $q + 1$ valid tuples (A, IV, C, T)

QCB security with ideal TBC: Proof

The proofs start by replacing the TBC by random permutations Π_t.



QCB security with ideal TBC: Proof (ctd.)

Confidentiality

- Since IVs are not repeated, the random permutations in the challenge phase are independent of the random permutations in the query phase
- Adversary can guess no better than random

Authenticity

- We classify the forging attempt into cases depending on whether there is a new IV, a new ciphertext block, or a new AD
- In each case, we show that the adversary must solve one of two difficult puzzles:
  - Produce an input-output pair for a Π_i without ever querying Π_i
  - Produce two input-output pairs for a Π_i after only querying Π_i once (possibly in superposition)

Instantiating the TBC

Building a quantum-secure TBC from a block cipher

- with three block cipher calls: construction of Hosoyamada & Iwata
- for a rate-1 instantiation of TBC, we can only afford one block cipher call per TBC call
- we only found the key-tweak insertion TBC:

$$\widetilde{E}_{K,t}(x) = E_{K \oplus t}(x)$$

TBC Security

- we could not prove ideal TBC security
- we prove security when the tweaks are **non-adaptive**
- we modify the security goals of QCB accordingly

 Hosoyamada, Iwata, "Provably quantum-secure tweakable block ciphers", ToSC 2021

QCB security: modified goals

Modified IND-qCPA

- The IVs are random or specified in advance (not adversary-controlled)
- Query Phase: The adversary makes q encryption queries (superposed M, A)
- Challenge Phase: Must distinguish between two **classical** messages encrypted by the challenger

Modified BZ

- The IVs are random or specified in advance (not adversary-controlled)
- Query Phase: The adversary makes q **quantum** encryption / tag queries (superposed M, A)
- Forging Phase: Must output $q + 1$ valid tuples (A, IV, C, T)

QCB security: modified proofs

- Mostly follows the proof for the ideal TBC case
- q queries to QCB contain at most: $q(2\ell + 3)$ queries with a set of $5(\ell + 1)q$ **uncontrolled classical** tweaks (so non-adaptive)

Caveat

- Proof for BZ requires additional TBC queries to verify the forging attempts, which is not captured by the strictly non-adaptive tweaks
- We modify the TBC security game to allow a number of non-adaptive classical queries in the end, without any significant change to the proof

Conclusion

Summary: two results

If the TBC is secure (indistinguishable) with queries using:

- Classical tweaks
- Superposed messages / ciphertexts

then QCB is IND-qCPA and BZ-secure.

But we didn't manage to prove this TBC security in full generality for a rate-1 block cipher-based TBC.

If the TBC is the key-tweak insertion $\widetilde{E}_{K,t}(x) = E_{K \oplus t}(x)$, QCB is IND-qCPA and BZ-secure (in the ideal cipher model).

- This goes through a complicated security definition
- The IC model is very strong

Open questions

- IND-qCCA security (under a proper definition)
- replacing BZ by BU (more recent definition)
- prove the key-tweak insertion quantum security under classical tweak queries (without restrictions)
- without the IC model (standard PRP security), can we have:
  - a quantum-secure TBC?
  - rate-one parallelizable AE?

Full version: ePrint 2020/1304

Thank you!