Quantum Attacks on Symmetric Constructions

André Schrottenloher

Inria Rennes

Quantum computing

Quantum state (**n** qubits):

- $|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$
- α_x are complex numbers (**amplitudes**)
- Measurement outputs x with prob. $|\alpha_x|^2$

- We transform the state using **unitary operations**, then measure
- **Partial** measurements will reduce the superposition

Quantum computing

Quantum state (**n** qubits):

- $|\psi\rangle = \sum_{x \in \{0,1\}^{\mathbf{n}}} \alpha_x |x\rangle$
- α_x are complex numbers (**amplitudes**)
- Measurement outputs x with prob. $|\alpha_x|^2$

- We transform the state using **unitary operations**, then measure
- **Partial** measurements will reduce the superposition

(Typical) operations:

- Classical **reversible** operations "in superposition": transform each bit-string $|x\rangle \mapsto |\mathcal{A}(x)\rangle$
- Fourier transforms over the amplitudes, for example the Hadamard transform:

$$\sum_x f(x) |x\rangle \to \left(\sum_y (-1)^{x \cdot y} f(y) \right) |x\rangle \text{ where } f : \{0,1\}^{\mathbf{n}} \to \mathbb{C}$$

The two quantum adversaries

Consider a cipher E_K.

The two quantum adversaries

Consider a cipher E_K.

"Standard" access (Q1)

$$x \longrightarrow \boxed{E_K} \longrightarrow E_K(x)$$

- Adversary is quantum
- Black-box is classical

"Superposition" access (Q2)

$$|x\rangle\,|0\rangle \longrightarrow \boxed{E_K} \longrightarrow |x\rangle\,|E_K(x)\rangle$$

- Adversary is quantum
- Black-box **is quantum**

The two quantum adversaries

Consider a cipher E_K.

"Standard" access (Q1)

$$x \longrightarrow \boxed{E_K} \longrightarrow E_K(x)$$

- Adversary is quantum
- Black-box is classical

"Superposition" access (Q2)

$$|x\rangle\,|0\rangle \longrightarrow \boxed{E_K} \longrightarrow |x\rangle\,|E_K(x)\rangle$$

- Adversary is quantum
- Black-box **is quantum**

- Q1 / Q2 only concerns **keyed black-boxes**
- **Primitive queries** (random oracle, ideal cipher) are **always quantum**

Example: Grover's search

Time $T \rightarrow \sqrt{T}$ for exhaustive search **if**:

- sampling the search space
- testing the sampled value

are quantum algorithms.

Example: Grover's search

Time $T \rightarrow \sqrt{T}$ for exhaustive search **if**:

- sampling the search space
- testing the sampled value

are quantum algorithms.

Consider an authenticated cipher $E_K : x \rightarrow y, t$.

Key search

- Find **K** that matches known plaintext-ciphertexts
- In quantum time $2^{|K|/2}$, **Q1**

Forgery

- Find y, t such that t **passes verification**
- In quantum time $2^{|t|/2}$, **Q2**

Q1 security and primitive queries

If all oracles have classical access, then classical information-theoretic proofs trivially lift to the Q1 setting.

$\implies$ We must at least allow quantum primitive access.

Aaronson, Ambainis, "The need for structure in quantum speedups." Theory Comput. 2014

Yamakawa, Zhandry, "Verifiable Quantum Advantage without Structure." FOCS 2022

Q1 security and primitive queries

If all oracles have classical access, then classical information-theoretic proofs trivially lift to the Q1 setting.

$\Longrightarrow$ We must at least allow quantum primitive access.

With a random oracle

- The Aaronson-Ambainis conjecture: for any **distinguishing** problem relative to a RO, quantum queries give at most a **polynomial** speedup **[AA14]**
- The Yamakawa-Zhandry result: exponential gap is achievable for a **search** problem **[YZ22]**

Aaronson, Ambainis, "The need for structure in quantum speedups." Theory Comput. 2014

Yamakawa, Zhandry, "Verifiable Quantum Advantage without Structure." FOCS 2022

Summary: Q1 and Q2 security

- Many cipher / MAC / AE constructions are **broken** in Q2
- Even these "broken" constructions can be **secure** in Q1
- But Q1 security is not automatic as long as non-classical oracles are involved
- Best quantum / classical gap known in the Q1 setting on real-life constructions is $T \to T^{2/5}$ (not Grover search!)

Simon's Algorithm (and Attacks)

Simon's algorithm

Simon's problem

Let $f : \{0,1\}^{\mathbf{n}} \to \{0,1\}^{\mathbf{n}}$ be a 2-to-1 function such that $\exists \mathbf{s}, \forall x, f(x \oplus \mathbf{s}) = f(x)$. Find $\mathbf{s}$.

Simon, "On the power of quantum computation", FOCS 1994

Simon's algorithm

Simon's problem

Let $f : \{0,1\}^{\mathbf{n}} \to \{0,1\}^{\mathbf{n}}$ be a 2-to-1 function such that $\exists \mathbf{s}, \forall x, f(x \oplus \mathbf{s}) = f(x)$. Find $\mathbf{s}$.

Simon's problem in cryptography

Same, but f is a random periodic function.

Simon, "On the power of quantum computation", FOCS 1994

Simon's algorithm (subroutine)

1. Start from $|0\rangle$
2. Hadamard transform: $\sum_x |x\rangle$
3. **Compute** f: $\sum_x |x\rangle |f(x)\rangle$
4. Measure $f(x)$: $\sum_{x|f(x)=a} |x\rangle = |x\rangle + |x \oplus \mathbf{s}\rangle$
5. Hadamard transform: $\sum_y \left((-1)^{x\cdot y} + (-1)^{(x\oplus \mathbf{s})\cdot y}\right) |y\rangle$

If $y \cdot \mathbf{s} = 1$, then:

$$(-1)^{x\cdot y} + (-1)^{(x\oplus \mathbf{s})\cdot y} = (-1)^{x\cdot y}\left(1 + (-1)^{\mathbf{s}\cdot y}\right) = 0$$

$\implies$ one can only measure y such that $y \cdot \mathbf{s} = 0$.

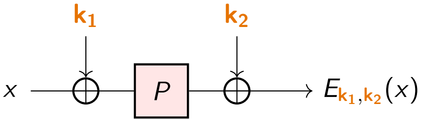
$\implies$ $\mathcal{O}(\mathbf{n})$ queries to succeed

Simon's algorithm for the cryptanalyst

1. Using our oracles (construction, primitives), define a periodic function
2. Run Simon's algorithm
3. Use the information recovered to break some property

- Access to a black-box cipher: find the secret key (break PRP security)
- Access to a black-box AE / MAC: find an **internal state** value which allows to produce some forgeries

Example: Even-Mansour cipher

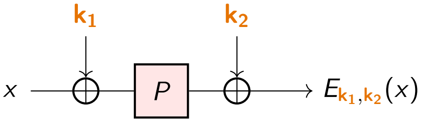


$$E_{\mathbf{k_1},\mathbf{k_2}}(x) = \mathbf{k_2} \oplus P(x \oplus \mathbf{k_1})$$

Kuwakado, Morii, "Security on the quantum-type even-mansour cipher", ISITA 2012

Alagic, Bai, Katz, Majenz, "Post-Quantum Security of the Even-Mansour Cipher", EUROCRYPT 2022

Example: Even-Mansour cipher



$$E_{\mathbf{k_1},\mathbf{k_2}}(x) = \mathbf{k_2} \oplus P(x \oplus \mathbf{k_1})$$

Consider the function:

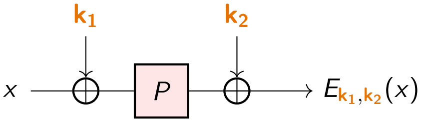
$$f(x) = E_{\mathbf{k_1},\mathbf{k_2}}(x) \oplus P(x) \implies f(x \oplus \mathbf{k_1}) = \mathbf{k_2} \oplus P(x \oplus \mathbf{k_1}) \oplus P(x) = f(x) \ .$$

In Q2, finding $\mathbf{k_1}$ is an **easy** quantum problem.

Kuwakado, Morii, "Security on the quantum-type even-mansour cipher", ISITA 2012

Alagic, Bai, Katz, Majenz, "Post-Quantum Security of the Even-Mansour Cipher", EUROCRYPT 2022

Example: Even-Mansour cipher



$$E_{\mathbf{k_1},\mathbf{k_2}}(x) = \mathbf{k_2} \oplus P(x \oplus \mathbf{k_1})$$

Consider the function:

$$f(x) = E_{\mathbf{k_1},\mathbf{k_2}}(x) \oplus P(x) \implies f(x \oplus \mathbf{k_1}) = \mathbf{k_2} \oplus P(x \oplus \mathbf{k_1}) \oplus P(x) = f(x) \ .$$

In Q2, finding $\mathbf{k_1}$ is an **easy** quantum problem.

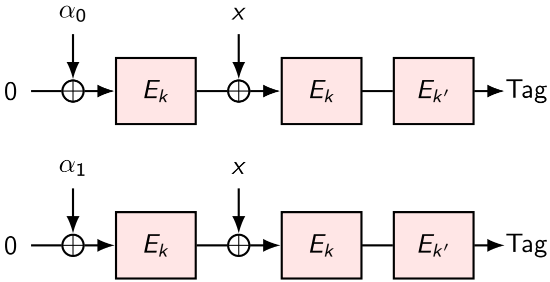
But it's Q1-secure **[ABKM22]**

Kuwakado, Morii, "Security on the quantum-type even-mansour cipher", ISITA 2012

Alagic, Bai, Katz, Majenz, "Post-Quantum Security of the Even-Mansour Cipher", EUROCRYPT 2022

Example: ECBC-MAC

From a block cipher E_k and two keys k, k'.



Fix a pair of values α_0, α_1 for the first block. Define:

$$f(x) := MAC_{k,k'}(\alpha_0, x) \oplus MAC_{k,k'}(\alpha_1, x) \ .$$

$$\implies f(x) = f(x \oplus E_k(\alpha_0) \oplus E_k(\alpha_1)) \ .$$

Kaplan, Leurent, Leverrier, Naya-Plasencia, "Breaking Symmetric Cryptosystems Using Quantum Period Finding", CRYPTO 2016

Example: ECBC-MAC (ctd.)

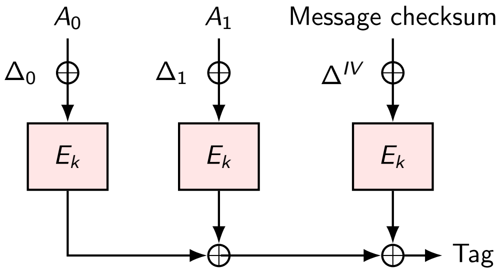
$\Longrightarrow$ using Simon's algorithm, we can recover $\mathbf{s} = E_k(\alpha_0) \oplus E_k(\alpha_1)$ with $\mathcal{O}(\mathbf{n})$ queries

Forgeries

For each message that starts with α_0: $\alpha_0||m_1||m_2 \ldots m_\ell$, we know that $\alpha_1||m_1 \oplus \mathbf{s}||m_2 \ldots m_\ell$ **has the same tag**.

From this point onwards, we output two valid $\{\text{message}, \text{tag}\}$ per query.

Example: OCB3 MAC



- The offsets $\Delta_0, \Delta_1, \Delta^{IV}$ are secret-dependent
- Only Δ^{IV} depends on the IV

$$MAC_k(IV, A_0, A_1) = F_{k,IV} \oplus E_k(\Delta_0 \oplus A_0) \oplus E_k(\Delta_1 \oplus A_1)$$

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

Example: OCB3 MAC (ctd.)

$$MAC_k(IV, A_0, A_1) = F_{k,IV} \oplus E_k(\Delta_0 \oplus A_0) \oplus E_k(\Delta_1 \oplus A_1)$$

$$\implies MAC_k(IV, A_0, A_1) = MAC_k(IV, A_1 \oplus \mathbf{s}, A_0 \oplus \mathbf{s}) \ ,$$

where $\mathbf{s} = \Delta_0 \oplus \Delta_1$.

- But IV changes at each query: we cannot compute (quantumly) twice the same function.

Example: OCB3 MAC (ctd.)

$$MAC_k(IV, A_0, A_1) = F_{k,IV} \oplus E_k(\Delta_0 \oplus A_0) \oplus E_k(\Delta_1 \oplus A_1)$$
$$\implies MAC_k(IV, A_0, A_1) = MAC_k(IV, A_1 \oplus \mathbf{s}, A_0 \oplus \mathbf{s}) \ ,$$

where $\mathbf{s} = \Delta_0 \oplus \Delta_1$.

- But IV changes at each query: we cannot compute (quantumly) twice the same function.

- Simon's subroutine **uses a single query** and the result **depends only on s**
- It works as long as **s** stays the same!

First summary of attacks

When a controlled value (i.e. message block) is XORed to a secret value (key, offset, internal state ...), we can:

- embed a **hidden boolean shift** between two queries;
- recover it with Simon's algorithm;
- use it to break a security property.

Interlude

What if the **period** changes at each query, but the **function** is the same?

Bonnetain, S., "Single-Query Quantum Hidden Shift Attacks". ToSC 2024

Interlude

What if the **period** changes at each query, but the **function** is the same?

Single-query (kind of) shift-finding

- If Q2 access to $x \mapsto g(x \oplus \mathbf{s})$ where $g \ : \{0,1\}^{\mathbf{n}} \to \{0,1\}$ is known
- Find **s** in a single Q2 query to $g(x \oplus \mathbf{s})$ (**with some probability**)
- Requires either:
  - $\widetilde{\mathcal{O}}(2^{n/2})$ Q2 queries to g
  - $\mathcal{O}(2^n)$ queries to g in precomputation
  - g to be "simple"

$\Longrightarrow$ applied to AEGIS-type AEs, but no "generic" mode so far.

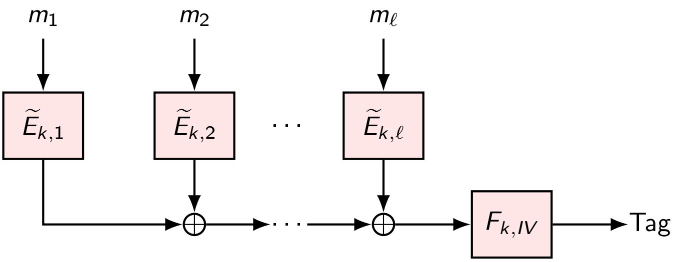
Bonnetain, S., "Single-Query Quantum Hidden Shift Attacks". ToSC 2024

Quantum Linearization Attack

New example: a kind of parallel MAC

Like the OCB MAC, but:

- Use a generic TBC
- Use post-processing by a function F
- With or without IVs, yields classically secure MACs such as LightMAC and PMAC



There is still a periodic function

Restrict the inputs so that each block takes only two values: $m_1 = b_1||0, \ldots, m_\ell = b_\ell||0$ and make a function:

$$\begin{cases} G_{k,IV} \ : \{0,1\}^\ell \to \{0,1\}^{\mathbf{n}} \\ (b_1||\cdots||b_\ell) \mapsto F_{k,IV}\left(\underbrace{\bigoplus_{1\leq i\leq \ell} \widetilde{E}_{k,i}(b_i||0)}_{:=H(b_1||\cdots||b_\ell)}\right) \\ \end{cases}$$

There is still a periodic function

Restrict the inputs so that each block takes only two values: $m_1 = b_1||0, \ldots, m_\ell = b_\ell||0$ and make a function:

$$\begin{cases} G_{k,IV} & : \{0,1\}^\ell \to \{0,1\}^{\mathbf{n}} \\ (b_1||\cdots||b_\ell) \mapsto F_{k,IV}\Bigg(\underbrace{\bigoplus_{1\le i\le \ell} \widetilde{E}_{k,i}(b_i||0)}_{:=H(b_1||\cdots||b_\ell)} \Bigg) \end{cases}$$

- If you flip b_i, you XOR $\widetilde{E}_{k,i}(b_i||0) \oplus \widetilde{E}_{k,i}(b_i||1)$ to the output of H

$\Longrightarrow$ H is an affine function of its input $(b_1||\cdots||b_\ell)$

There is still a periodic function

Restrict the inputs so that each block takes only two values:
$m_1 = b_1||0, \ldots, m_\ell = b_\ell||0$ and make a function:

$$\begin{cases} G_{k,IV} : \{0,1\}^\ell \to \{0,1\}^{\mathbf{n}} \\ (b_1||\cdots||b_\ell) \mapsto F_{k,IV}\Bigg(\underbrace{\bigoplus_{1\le i\le\ell} \widetilde{E}_{k,i}(b_i||0)}_{:=H(b_1||\cdots||b_\ell)}\Bigg) \end{cases}$$

- If you flip b_i, you XOR $\widetilde{E}_{k,i}(b_i||0) \oplus \widetilde{E}_{k,i}(b_i||1)$ to the output of H

$\implies$ H is an affine function of its input $(b_1||\cdots||b_\ell)$

$$H(b_1||\cdots||b_\ell)$$

$$= \underbrace{\Big((\widetilde{E}_{k,1}(0) \oplus \widetilde{E}_{k,1}(1)) \quad \cdots \quad (\widetilde{E}_{k,\ell}(0) \oplus \widetilde{E}_{k,\ell}(1))\Big)}_{M_\ell:\text{ binary matrix, } \mathbf{n} \text{ rows and } \ell \text{ columns}} \times \begin{pmatrix} b_1 \\ \ldots \\ b_\ell \end{pmatrix} \oplus \bigoplus_i \widetilde{E}_{k,i}(0) .$$

The periodic function

When $\ell \geq \mathbf{n} + 1$, the kernel of M_ℓ is non-trivial. Each of its elements α is an ℓ-bit string such that:

$$\forall x, H(x \oplus \alpha) = H(x)$$

$$\implies G_{k,IV}(x) = F_{k,IV}(H(x)) = G_{k,IV}(x \oplus \alpha) \ .$$

- We recover such an α with Simon's algorithm
- α is information on the internal state, which allows to forge tags

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

Consequences of linearization attacks

Polynomial-time Q2 attacks on most parallel MACs (LightMAC, PolyMAC), BBB parallel MACs, and any construction that:

- processes the input blocks **independently**
- computes one or more XOR-linear functions of these processed input blocks
- computes the tag from the outputs of these functions

Maybe the Real Treasure was the Proofs we made Along the Way

Methods for Q2 security

Proofs of security in the Q2 setting use different tools:

- One-way-to-hiding lemma(s)
- Recording of random oracle queries

There may be two common issues:

- Difficulty to obtain tight proofs;
- Impossible to prove something which has been broken

Making modes Q2-secure

- Tweaking the block cipher / permutation / RO calls using an IV
  - The IV changes at each query $\Longrightarrow$ each query is "with a different function"
- IV-based key derivation **[LL23]**
- Replace offset-based TBC (like OCB3) by a generic TBC

$\Longrightarrow$ this places the burden of security on the primitive

Lang, Lucks, "On the Post-quantum Security of Classical Authenticated Encryption Schemes", AFRICACRYPT 2023

Proving Q1 security instead

Since Q2 security is difficult and / or not achievable and / or not tight, let's prove Q1 security instead?

- Tight results for Even-Mansour and tweakable EM
- Results on Ascon

Alagic, Bai, Katz, Majenz, "Post-Quantum Security of the Even-Mansour Cipher", EUROCRYPT 2022

Alagic, Bai, Katz, Majenz, Struck, "Post-quantum Security of Tweakable Even-Mansour, and Applications.", EUROCRYPT 2024

Conclusion

- A lot of modes were broken with Q2 attacks (the situation seems settled now?)
- Saving the Q2 security of some modes is possible (using the classical nature of IVs and keys)
- For all broken modes (in the ideal model), Q1 security is an interesting target

Conclusion

- A lot of modes were broken with Q2 attacks (the situation seems settled now?)
- Saving the Q2 security of some modes is possible (using the classical nature of IVs and keys)
- For all broken modes (in the ideal model), Q1 security is an interesting target

Thank you!