Quantum Security of Symmetric Cryptosystems

André Schrottenloher

Inria, France

Post-quantum cryptography

Asymmetric

- RSA (*factorization*) and ECC (*discrete logarithms*) become broken in polynomial time [Shor]
- **Post-quantum crypto** = "we don't use them anymore"

Symmetric

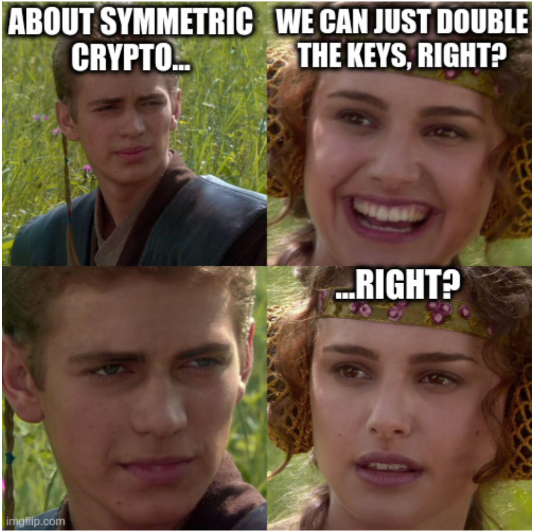
- Grover's algorithm accelerates exhaustive search of the key:

$\Longrightarrow$ from $\sqrt{2^{|k|}} = 2^{|k|/2}$

Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", FOCS 1994

Grover, "A Fast Quantum Mechanical Algorithm for Database Search", STOC 1996

Post-quantum symmetric crypto?



. . . right?

Let's take a block cipher: E_k a family of permutations of $\{0,1\}^n$ indexed by a key k. For example, AES-256.

On an ideal cipher, $\underbrace{\text{exhaustive search}}_{\text{Resp. Grover's search}}$ finds the key in $\underbrace{\text{time } 2^{|k|}}_{\text{Resp. } 2^{|k|/2}}$

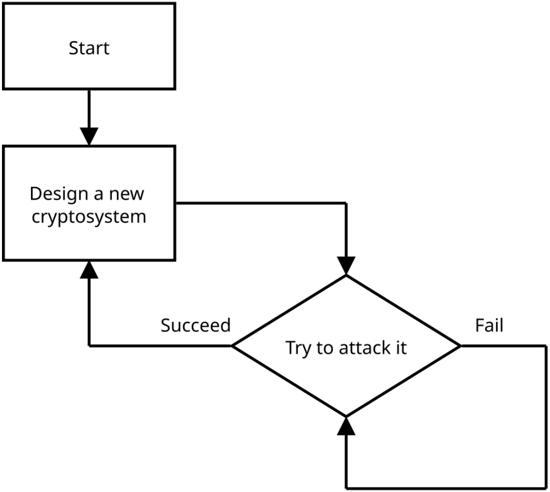
Except that there are no ideal ciphers: only **ciphers which behave as ideal.***

The cipher behaves as ideal if there is no better way to find the key than exhaustive search (resp. Grover's search).

* As far as we know.

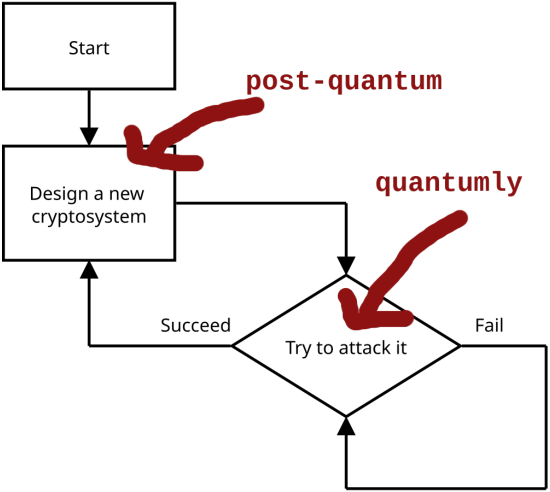
The cycle of cryptanalysis

How do we know that ciphers are secure?



The cycle of cryptanalysis, updated

How do we know that cryptosystems are quantum-secure?



What is an attack?

- A **key-recovery attack** = an algorithm that finds the key faster than exhaustive search (resp. Grover)
- If we find one, **the cipher is broken**

- If we can't break the entire cipher, we **weaken it** and try again
- "How many rounds broken" (10/14 for AES-256) gives a **security margin**

We're leaving out other types of attacks, other attacker models, other primitives, etc.

Quantum vs. classical cryptanalysis

Everything is possible!

1. No classical attack ($= 2^{|k|}$) and no quantum attack ($= 2^{|k|/2}$)
2. A classical attack ($< 2^{|k|}$) but no quantum attack ($= 2^{|k|/2}$)
3. A classical attack ($< 2^{|k|}$) and a quantum attack ($< 2^{|k|/2}$)
4. No classical attack ($= 2^{|k|}$) but a quantum attack ($< 2^{|k|/2}$)

Case 4 is the most problematic for us. So far only specific examples. . . and not AES-256.

Outline

1. Attacks based on Quantum Search
2. Simon's Algorithm and Superposition Attacks
3. Super-quadratic Q1 Attacks

Attacks based on Quantum Search

Quantum search

X a search space, $f : X \to \{0,1\}$ with $G = f^{-1}(1) \subseteq X$, find $x \in G$.

Classical (exhaustive) search:

$$\text{Repeat } \frac{|X|}{|G|} \text{ times } \begin{cases} \text{Sample } x \in X \\ \text{Test if } f(x) = 1 \end{cases}$$

Quantum (Grover's) search:

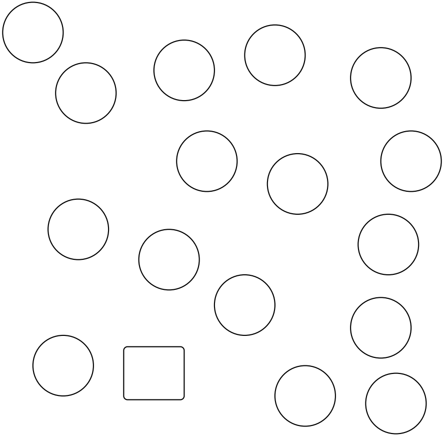
$$\text{Repeat } \simeq \sqrt{\frac{|X|}{|G|}} \text{ times } \begin{cases} \text{Sample } x \in X \to \text{quantumly} \\ \text{Test if } f(x) = 1 \to \text{quantumly} \end{cases}$$

Grover, "A fast quantum mechanical algorithm for database search", STOC 96

Brassard, Høyer, Mosca, Tapp, "Quantum amplitude amplification and estimation", Contemp. Math. 2002

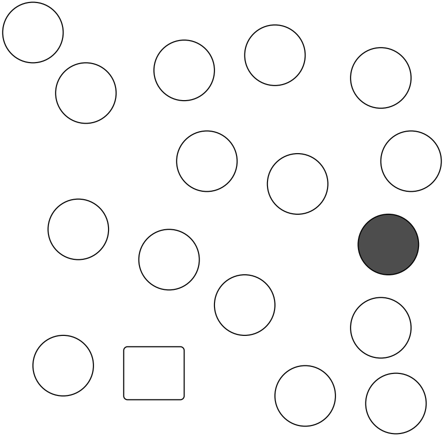
Exhaustive key search

We test keys k' at random until we find one that agrees with a few pairs $(x, E_k(x))$.



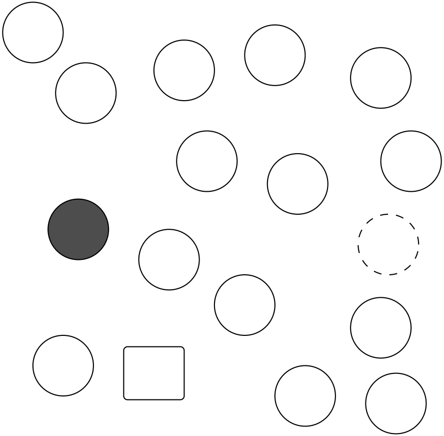
Exhaustive key search

We test keys k' at random until we find one that agrees with a few pairs $(x, E_k(x))$.



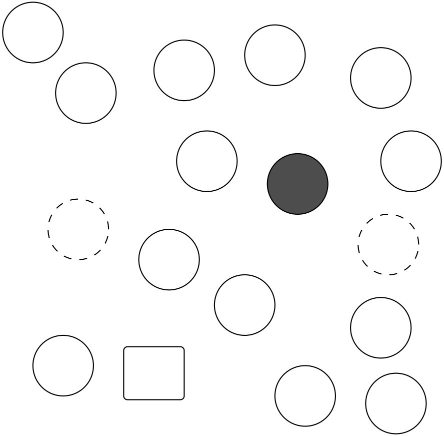
Exhaustive key search

We test keys k' at random until we find one that agrees with a few pairs $(x, E_k(x))$.



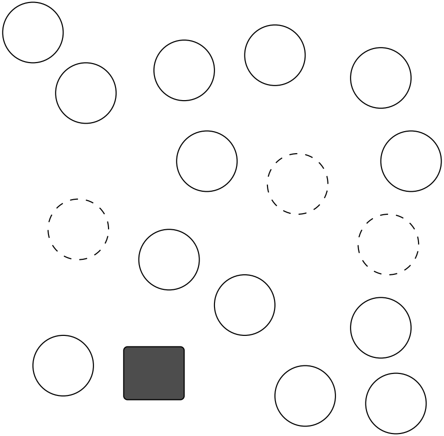
Exhaustive key search

We test keys k' at random until we find one that agrees with a few pairs $(x, E_{k}(x))$.



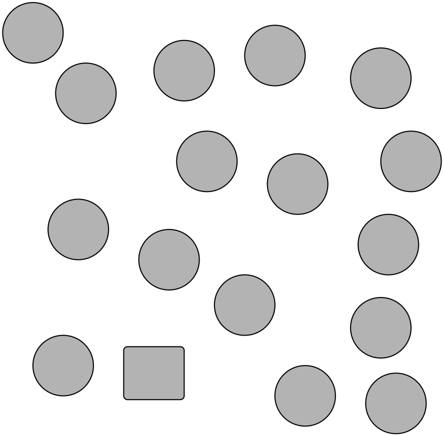
Exhaustive key search

We test keys k' at random until we find one that agrees with a few pairs $(x, E_k(x))$.



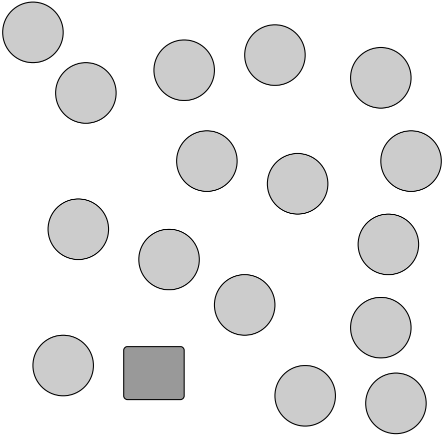
Quantum search (ctd.)

We move globally (statefully) from $X = \{\text{all keys}\}$ to $G = \{\text{good key } \mathbf{k}\}$.



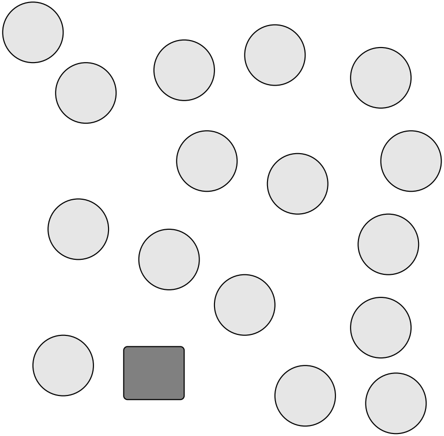
Quantum search (ctd.)

We move globally (statefully) from $X = \{\text{all keys}\}$ to $G = \{\text{good key } \mathbf{k}\}$.



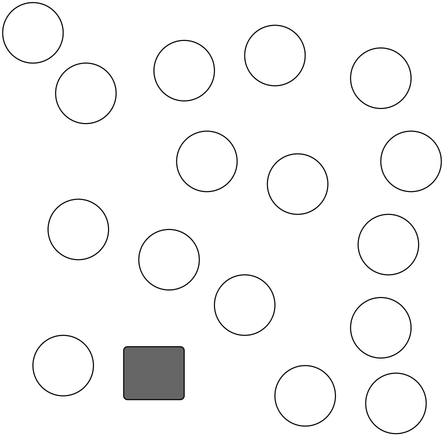
Quantum search (ctd.)

We move globally (statefully) from $X = \{\text{all keys}\}$ to $G = \{\text{good key } \mathbf{k}\}$.



Quantum search (ctd.)

We move globally (statefully) from $X = \{\text{all keys}\}$ to $G = \{\text{good key } \mathbf{k}\}$.



Example: key search

Needs a few classical pairs $x, E_k(x)$ for known x.

Classical: guess k', compute $E_{k'}(x)$ and compare, until it matches.

Quantum: run Grover's search; to test a key k', compute $E_{k'}(x)$ and compare.

- Needs a quantum circuit to test k', i.e., a quantum implementation of E

Implementing E is not easy: for AES the 2^{64} Grover's search iterates cost $\geq 2^{80}$ quantum gates.

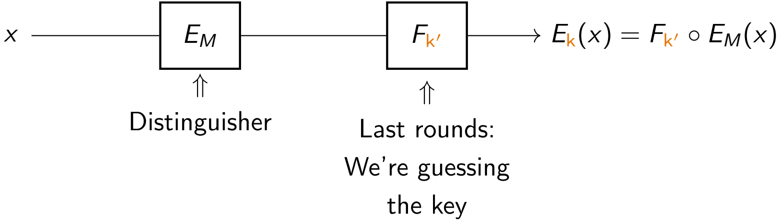
Jaques, Naehrig, Roetteler, Virdia, "Implementing Grover oracles for quantum key search on AES and LowMC", EUROCRYPT 2020

Correspondence of attacks

Many classical attacks can be "turned quantum":

- Linear and differential attacks [KLLN16]
- Square and Demirci-Selçuk MITM attacks [BNS19]
- Boomerang (differential) attacks [FNS21]
- ...

Typically due to the "distinguisher rounds + key-recovery rounds" structure.



Correspondence of attacks (ctd.)

Typical key-recovery attack:

- Guess subkey k'
- Remove the last rounds and use the distinguisher

$\Longrightarrow$ if it works, guess is correct

Classical time:

$$2^{|k'|} \times \text{ running the distinguisher}$$

Quantum time:

$$2^{|k'|/2} \times \text{ running the distinguisher}$$

$\Longrightarrow$ if the distinguisher **is a search**, we have a quantum attack:

$$2^{|k'|} \times T < 2^{|k|} \implies 2^{|k'|/2} \times \sqrt{T} < 2^{|k|/2}$$

Examples

Linear cryptanalysis: construct a pair of masks α, β such that:

The Boolean function $x \mapsto \alpha \cdot x \oplus \beta \cdot E_M(x)$ is more biased for E_M than a random permutation.

Differential cryptanalysis: construct a pair of differences Δ_i, Δ_o such that:

A pair of plaintexts $x, x \oplus \Delta_i$ maps to $E_M(x), E_M(x) \oplus \Delta_o$ with probability bigger than for a random permutation.

In both cases the distinguisher can be accelerated:

- **Estimate** the bias faster using Amplitude Estimation
- **Find** a difference pair faster using Grover search

Kaplan, Leurent, Leverrier, Naya-Plasencia, "Quantum Differential and Linear Cryptanalysis", ToSC 2016

Correspondence of attacks (ctd.)

But there are much more complex attacks, and not everything admits a quadratic speedup.

A typical issue starts when the attack needs a large memory (e.g., precomputed table of 2^{80} entries: already bigger than Grover's limit).

On AES, quantum attacks break **less rounds** so far.

Simon's Algorithm and Superposition Attacks

Simon's algorithm

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a function with a hidden period:

$$f(x \oplus s) = f(x), \text{ find } s.$$

Classical resolution:

Find a **collision**: $(x, y), x \neq y$ such that $f(x) = f(y)$, and hope that:

$$x \oplus s = y \implies s = x \oplus y$$

In time $\simeq 2^{n/2}$.

Simon's algorithm (ctd.)

Start with 2n qubits	$\|0\rangle\|0\rangle$
Apply $H^{\otimes n}$ and f	$\sum_x \|x\rangle\|f(x)\rangle$
Measure the second register	$\|x_0\rangle + \|x_0 \oplus s\rangle$
Apply $H^{\otimes n}$	$\sum_y \left((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus s)\cdot y}\right)\|y\rangle$
	$= \sum_y (-1)^{x_0 \cdot y}\left(1 + (-1)^{s \cdot y}\right)\|y\rangle$

Measure y such that $1 + (-1)^{s \cdot y} \neq 0 \iff s \cdot y = 0$

- With $\geq n$ values $y_1, \ldots y_m$, we obtain either a linear system in s, or a system of full rank (no period)
- Works in the "typical crypto" case of a random periodic f

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

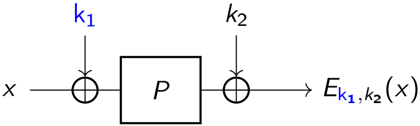
Simon's algorithm (simplified)

Query f in superposition $\rightarrow$ quantum magic $\rightarrow$ random y such that $s \cdot y = 0$.

$\implies$ repeat this $\simeq n$ times, solve a linear system to find s.

Example: the Even-Mansour cipher

Built from a public permutation $P : \{0,1\}^n \to \{0,1\}^n$ and $2n$ bits of key.



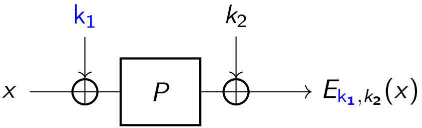
$$E_{k_1,k_2}(x) = k_2 \oplus P(x \oplus k_1)$$

Classical security:
If P is a random permutation, an adversary performing T queries to P and D queries to E_{k_1,k_2} needs $T \cdot D = 2^n$ to recover the key.

Even, Mansour, "A Construction of a Cipher from a Single Pseudorandom Permutation", J. Cryptol. 1997

Dunkelman, Keller, Shamir, "Slidex Attacks on the Even-Mansour Encryption Scheme", J. Crypto 2015

Simon-based attack on Even-Mansour



Define: $f(x) = E_{k_1,k_2}(x) \oplus P(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$

Quantum attack:

- f satisfies $f(x \oplus k_1) = f(x)$.
- With **quantum access** to f, find k_1 with Simon's algorithm.
- A query to f contains a query to E_{k_1,k_2}.

$\Longrightarrow$ complete break!

Kuwakado, Morii, "Security on the quantum-type Even-Mansour cipher", ISITA 2012

Quantum adversary models

Q1 model:

- Make classical queries to $x \mapsto E_k(x)$
- Do quantum computations

$\implies$ realistic, less powerful. “Store now, decrypt later”.

Only **quadratic** speedups **at most so far**?

Q2 model:

- Do quantum computations
- Queries E_k in superposition (e.g. standard oracle)

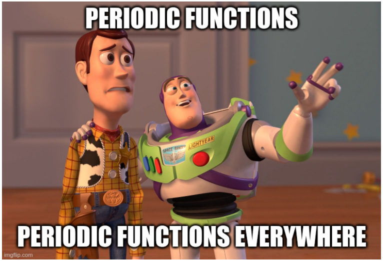
$\implies$ theoretical, strictly more powerful, but non trivial.

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

A long list of Q2 breaks

- Even-Mansour cipher, self-similar key-alternating / Feistel ciphers
- CBC-MAC, OCB... **[KLLN16]**
- LightMAC(+), PolyMAC, GCM-SIV(2), Poly1305, PMAC(+)... **[BLNS21]**

$\Longrightarrow$ many good modes (encryption & MACs) get broken

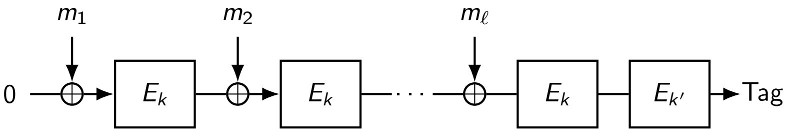


Kaplan, Leurent, Leverrier, Naya-Plasencia, "Breaking Symmetric Cryptosystems Using Quantum Period Finding", CRYPTO 2016

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

A Q2 break on CBC-MAC

From a block cipher E_k and two keys k, k'. **Integrity & authenticity protection.**



Use the MAC with two blocks:

$$\mathrm{MAC}_{k,k'}(m_1, m_2) = E_{k'} \circ E_k(m_2 \oplus E_k(m_1)) \ .$$

Fix m_1 to a pair of values $\{\alpha_0, \alpha_1\}$:

$$\underbrace{\mathrm{MAC}_{k,k'}(\alpha_0, x)}_{:= f(x)} = \underbrace{\mathrm{MAC}_{k,k'}\Big(\alpha_1, x \oplus E_k(\alpha_0) \oplus E_k(\alpha_1)\Big)}_{:= g(x \oplus \mathrm{E_k}(\alpha_0) \oplus \mathrm{E_k}(\alpha_1))} \ .$$

CBC-MAC (ctd.)

The boolean **hidden shift** problem is not harder than the **hidden period** problem. Simply define:

$$F(b, x) = \begin{cases} f(x) \text{ if } b = 0 \\ g(x) \text{ if } b = 1 \end{cases}$$

then F has a **hidden period** $1||\mathsf{E_k}(\alpha_0) \oplus \mathsf{E_k}(\alpha_1)$.

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

For any message that starts with α_0: $\alpha_0||m_1||m_2 \dots m_\ell$, the message $\alpha_1||m_1 \oplus \mathsf{s}||m_2 \dots m_\ell$ **has the same tag**.

$\Longrightarrow$ **breaks authenticity** as it allows the adversary to output new valid $\{\text{message}, \text{tag}\}$ pairs

Wrapping up

- Despite these breaks, Q2-secure MAC / encryption remains possible

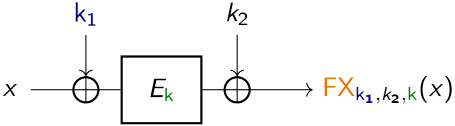
  ...and Q1-secure is fine as well
- On primitives, only specific ones are broken (not AES)

Going back to the "realistic" Q1 setting, all algorithms / attacks had a **quadratic** speedup at most. Is this a strong limitation?

Super-quadratic Q1 Attacks

Grover meets Simon: the FX attack

FX = Even-Mansour with a cipher E_k instead of the public P



Superposition attack on FX: "Grover-meet-Simon"

- Search k with Grover's algorithm
- To test a guess z, do the Even-Mansour attack

$\Longrightarrow$ attack fails: $z \neq k$

$\Longrightarrow$ attack succeeds: $z = k$

GMS problem: "among all the functions $x \mapsto (FX \oplus E_z)(x)$, find the single z which gives a periodic function"

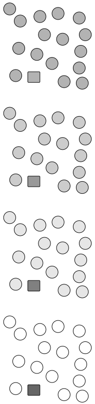
Leander, May, "Grover Meets Simon - Quantumly Attacking the FX-construction", ASIACRYPT 2017

Running the FX attack

- If $|k| = 2n$, $2^{2n/2} = 2^n$ Grover iterates
- n sup. queries and n^3 computations at each iterate

0. Setup Grover's initial state $\sum_z |z\rangle$
1. Iteration 1 $\begin{cases} \textbf{Test current state} \\ \text{Apply Grover's diffusion transform} \end{cases}$
2. Iteration 2 $\begin{cases} \textbf{Test current state} \\ \text{Apply Grover's diffusion transform} \end{cases}$
3. Iteration 3 $\begin{cases} \textbf{Test current state} \\ \text{Apply Grover's diffusion transform} \end{cases}$

...



Running the FX attack (ctd.)

Test iter. 1 $\begin{cases} \text{Make the queries } \sum_x |x\rangle\,|F_z(x) = (\mathsf{FX} \oplus \mathsf{E}_z)(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the queries} \end{cases}$

Test iter. 2 $\begin{cases} \text{Make the queries } \sum_x |x\rangle\,|F_z(x) = (\mathsf{FX} \oplus \mathsf{E}_z)(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the queries} \end{cases}$

Test iter. 3 $\begin{cases} \text{Make the queries } \sum_x |x\rangle\,|F_z(x) = (\mathsf{FX} \oplus \mathsf{E}_z)(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the queries} \end{cases}$

E_z varies between the iterates, but FX **is always the same**!

Improving the FX attack (ctd.)

Setup $\{$ Make the "offline query states" $\sum_x |x\rangle\,|\mathsf{FX}(x)\rangle$

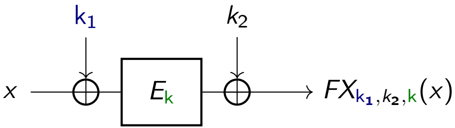
Test iter. 1 $\left\{\begin{array}{l}\text{Query } \mathsf{E_z}\text{: } \sum_x |x\rangle\,|(\mathsf{FX} \oplus \mathsf{E_z})(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the query to } \mathsf{E_z}\text{: back to } \sum_x |x\rangle\,|\mathsf{FX}(x)\rangle\end{array}\right.$

Test iter. 2 $\left\{\begin{array}{l}\text{Query } \mathsf{E_z}\text{: } \sum_x |x\rangle\,|(\mathsf{FX} \oplus \mathsf{E_z})(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the query to } \mathsf{E_z}\end{array}\right.$

Test iter. 3 $\left\{\begin{array}{l}\text{Query } \mathsf{E_z}\text{: } \sum_x |x\rangle\,|(\mathsf{FX} \oplus \mathsf{E_z})(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the query to } \mathsf{E_z}\end{array}\right.$

...

Offline-Simon attack on FX



In looking for the single z such that $FX \oplus E_z$ is periodic, we can make the queries to FX **only once**, **"offline"**.

If $|k| = 2n$:

- creating the initial "query states" costs the codebook (2^n queries) and time $\simeq 2^n$
- the quantum search contains $2^{2n/2}$ iterations: time $\simeq n^3 2^n$

Bonnetain, Hosoyamada, Naya-Plasencia, Sasaki, and S., "Quantum Attacks Without Superposition Queries: The Offline Simon's Algorithm", ASIACRYPT 2019

(Almost) a super-Grover speedup

Classical time:

$$2^{|k|} \times \underbrace{\text{attacking EM}}_{2^{n/2}}$$

Quantum time:

$$2^{|k|/2} \times \underbrace{\text{attacking EM}}_{n^3}$$

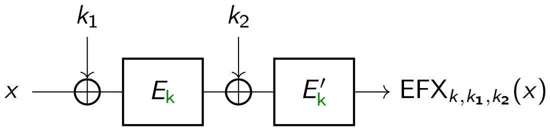
Unfortunately, we also have a better classical attack on FX $\rightarrow$ speedup remains quadratic.

What if...

. . . there existed a way to **strengthen** the FX construction such that:

- the classical security improves
- the offline-Simon attack has the same complexity?

Extended FX (a.k.a. 2-XOR-Cascade)



Still assuming: $|k| = 2n$:

Any classical adversary must make $2^{5n/2}$ queries to E, E' to distinguish.

A quantum adversary can recover all the keys in time $\simeq n^3 2^n$.

Gaži, Tessaro, "Efficient and optimally secure key-length extension for block ciphers via randomized cascading", EUROCRYPT 2012

Tweaking Offline-Simon

We are given the codebook of $\mathsf{EFX}[E, E']_{\mathsf{k},k_1,k_2}$ for some keys.

$$\mathsf{EFX}[E, E']_{\mathsf{k},k_1,k_2} = E'_{\mathsf{k}}\big(k_2 \oplus E_{\mathsf{k}}(k_1 \oplus x)\big)$$

Previous Offline-Simon problem:
Find the unique z such that $F_z = \mathsf{f} \oplus \mathsf{g}_\mathsf{z}$ is periodic.

$\implies$ not applicable.

"True" Offline-Simon problem:
Find the unique z such that $F_z = \pi_\mathsf{z} \circ \mathsf{f}$ is periodic.

$\implies$ replaces the XOR by any permutation π_z that we can compute.

Tweaking Offline-Simon (ctd.)

Setup: Make the "offline query states" $\sum_x |x\rangle |f(x)\rangle$

Test iter. 1
- Apply π_z in-place: $\sum_x |x\rangle |\pi_z \circ f(x)\rangle$
- Run Simon's algorithm
- Apply ${\pi_z}^{-1}$: back to $\sum_x |x\rangle |f(x)\rangle$

Test iter. 2
- Apply π_z in-place: $\sum_x |x\rangle |\pi_z \circ f(x)\rangle$
- Run Simon's algorithm
- Apply ${\pi_z}^{-1}$: back to $\sum_x |x\rangle |f(x)\rangle$

Test iter. 3
- Apply π_z in-place: $\sum_x |x\rangle |\pi_z \circ f(x)\rangle$
- Run Simon's algorithm
- Apply ${\pi_z}^{-1}$: back to $\sum_x |x\rangle |f(x)\rangle$

...

Tweaking Offline-Simon (ctd.)

$$\mathsf{EFX}[E, E']_{\mathsf{k},k_1,k_2} = E'_{\mathsf{k}}\big(k_2 \oplus E_{\mathsf{k}}(k_1 \oplus x)\big) \ .$$

We have:

$$\pi_{\mathsf{k}}(\mathsf{EFX}(x)) := (\mathsf{E}'_{\mathsf{k}})^{-1}\Big(\mathsf{EFX}(x)\Big) \oplus \mathsf{E}_{\mathsf{k}}(\mathsf{x}) =$$

$$k_2 \oplus E_{\mathsf{k}}(k_1 \oplus x) \oplus E_{\mathsf{k}}(x) \qquad \text{(periodic)}$$

is periodic or random.

Conclusion

Conclusion

So far in quantum symmetric cryptanalysis:

1. many attacks with quadratic (Grover-style) speedups
2. many Q2 breaks of constructions / modes of operation
3. super-quadratic speedups (up to 2.5) on specific cases

$\Longrightarrow$ improvement comes from the super-quadratic distinguisher (e.g., Even-Mansour)

What is the largest speedup?

Conclusion

There is no "largest" speedup for attacks in symmetric crypto.

[YZ22]: there exists a PRF construction that is:

- provably secure in the Random Oracle model (i.e., without any crypto "trapdoor")
- invertible in quantum polynomial time

Fortunately, good symmetric crypto primitives (e.g., AES) seem to remain as good in the quantum setting.

Thank you!

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

Bonus: hash functions

A function $h\ :\{0,1\}^* \to \{0,1\}^{\mathsf{n}}$ that "behaves like a random function".

- Preimage search: $2^{\mathsf{n}} \to 2^{\mathsf{n}/2}$ (Grover)
- Collision search: $2^{\mathsf{n}/2} \to 2^{\mathsf{n}/3}$ (*)

The subquadratic speedup of collision search is optimal (for a random function).

$\implies$ if the attack has a typical quadratic speedup:

$$\sqrt{T} \simeq 2^{\mathsf{n}/3} \iff T \simeq 2^{2\mathsf{n}/3} > 2^{\mathsf{n}/2}$$

$\implies$ this wouldn't be a classical attack, but it can be a quantum one **[HS20]**

(*) Depends on the memory available (model and quantity).

Hosoyamada, Sasaki, "Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound", EUROCRYPT 2020