Quantum Cryptanalysis of Block Ciphers: Quadratic Speedups and Beyond

André Schrottenloher
Cryptology group, CWI

75 YEARS 1946 - 2021 CWI

European Research Council
Established by the European Commission

Post-quantum cryptography

Asymmetric

- RSA (*factorization*) and ECC (*discrete logarithms*) become broken in polynomial time [Shor]
- Unfortunately, they are the most widely used today (replacements are on the way)

Symmetric

- Grover's algorithm accelerates exhaustive search of the key (square-root speedup)
- Most generic attacks admit quantum replacements

$\Longrightarrow$ should we simply **"double the key size"?**

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

Security of block ciphers

E_k is a family of permutations of $\{0,1\}^n$ indexed by a key k.

Generic key-recovery

Given some queries to a black-box $x \mapsto E_k(x)$, find k.

- **classical:** $2^{|k|}$ (try all keys)

The **classical** security of a given cipher is a **computational conjecture**:

- we conjecture that there is no key-recovery faster than $2^{|k|}$

  $\implies$ if there is, the cipher is broken
- we try to invalidate this conjecture: **cryptanalysis**
- we consider weakened (reduced-round) variants to estimate the **security margin**

  ex.: AES-256 key-recoveries reach 9 / 14 rounds

Post-quantum security of block ciphers

E_k is a family of permutations of $\{0,1\}^n$ indexed by a key k.

Generic key-recovery

Given some queries to a black-box $x \mapsto E_k(x)$, find k.

- **quantum:** $2^{|k|/2}$ (with Grover's algorithm)

The **quantum** security of a given cipher is a **computational conjecture**:

- we conjecture that there is no key-recovery faster than $2^{|k|/2}$

  $\Longrightarrow$ if there is, the cipher is broken
- we try to invalidate this conjecture: **quantum cryptanalysis**
- we consider weakened (reduced-round) variants to estimate the **quantum security margin**

Quantum vs. classical cryptanalysis

Being classically and quantumly attacked are two different properties:

- **we might have classical, but not quantum** (nothing below $2^{|k|/2}$)
- **we might have both**
- **we might have quantum** (below $2^{|k|/2}$) but not classical

When do the classical attacks **become quantum attacks?**

When are the quantum attacks **better than the classical ones?**

Outline

1. Attacks based on Quantum Search
2. Attacks based on Simon's Algorithm
3. Offline-Simon
4. The "True" Power of Offline-Simon

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 search (Grover's algorithm)

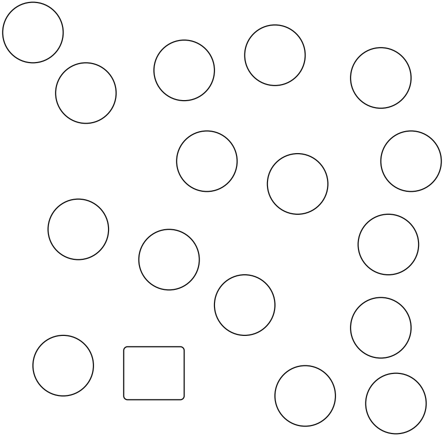
$$\text{Repeat } \mathcal{O}\left(\sqrt{\frac{|X|}{|G|}}\right) \text{ times } \begin{cases} \text{Sample } x \in X \to \text{quantumly} \\ \text{Test if } f(x) = 1 \to \text{quantumly} \end{cases}$$

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

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

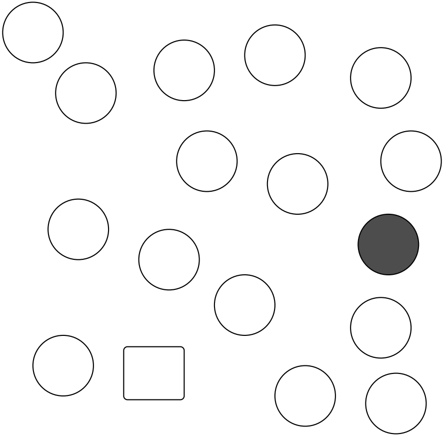
Classical search

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



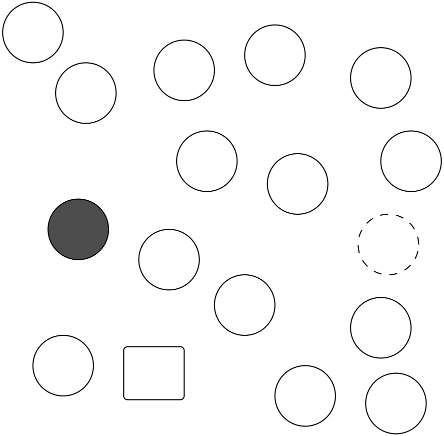
Classical search

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



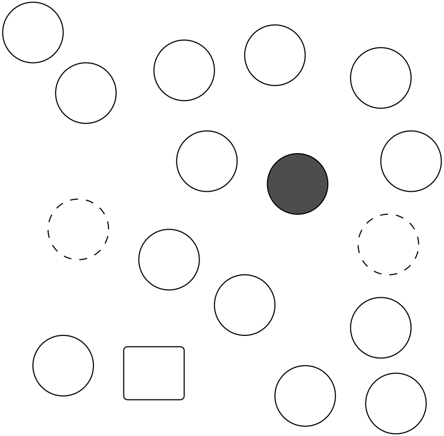
Classical search

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



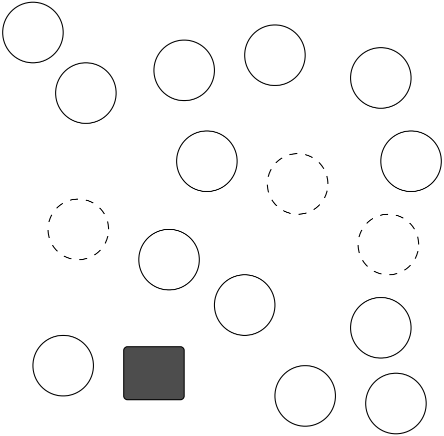
Classical search

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



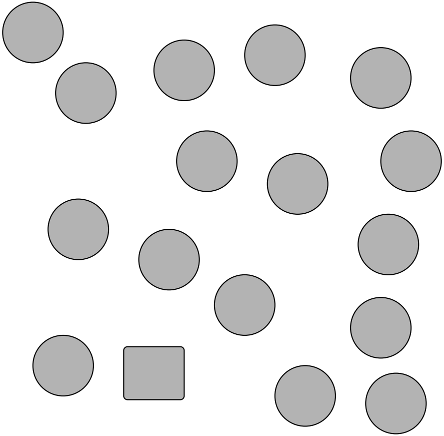
Classical search

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



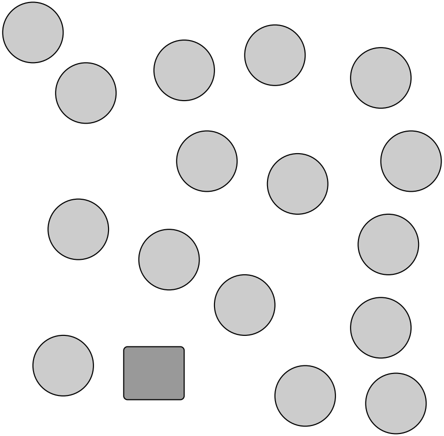
Quantum search (ctd.)

We move globally (statefully) from $\frac{1}{\sqrt{|\text{all keys } k'|}} \sum_{\text{all keys } k'} |k'\rangle$ to $|\text{good key k}\rangle$.



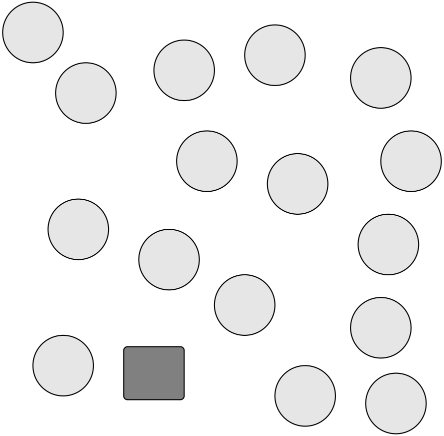
Quantum search (ctd.)

We move globally (statefully) from $\frac{1}{\sqrt{|\text{all keys } k'|}} \sum_{\text{all keys } k'} |k'\rangle$ to $|\text{good key } \mathrm{k}\rangle$.



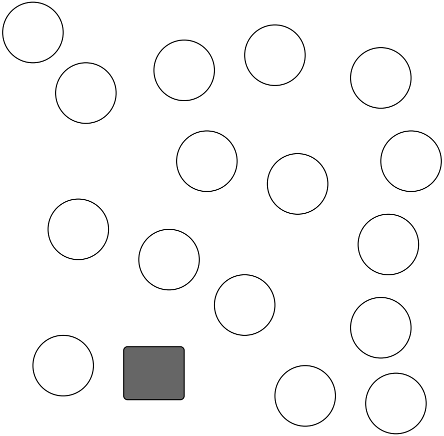
Quantum search (ctd.)

We move globally (statefully) from $\frac{1}{\sqrt{|\text{all keys } k'|}} \sum_{\text{all keys } k'} |k'\rangle$ to $|\text{good key k}\rangle$.



Quantum search (ctd.)

We move globally (statefully) from $\frac{1}{\sqrt{|\text{all keys } k'|}} \sum_{\text{all keys } k'} |k'\rangle$ to $|\text{good key } k\rangle$.



Classical-quantum search correspondence

A classical exhaustive search with $\mathcal{O}(T)$ iterations

A quantum search with $\mathcal{O}(\sqrt{T})$ iterations

An exhaustive search with $\mathcal{O}(T_1)$ iterations **of an exhaustive search** with $\mathcal{O}(T_2)$ iterations

A quantum search with $\mathcal{O}(\sqrt{T_1})$ iterations **of a quantum search** with $\mathcal{O}(\sqrt{T_2})$ iterations

Correspondence of attacks

Many classical attacks can be rephrased with combinations of exhaustive searches:

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

Ex.: differential last-rounds attack

Let $E_k = E_1 \circ E_2$ where: $\Pr(E_1(x \oplus \Delta) = E_1(x) \oplus \Delta') = 2^{-h} >> 2^{-n}$

- Guess the subkey of E_2
- Check a guess by searching for differential pairs
  - if the guess is correct, then we find them more often

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

Bonnetain, Naya-Plasencia, S., "Quantum Security Analysis of AES", ToSC 2019

Frixons, Naya-Plasencia, S., "Quantum Boomerang Attacks and Some Applications", SAC 2021

Correspondence of attacks (ctd.)

If a classical attack is "based on exhaustive search" **and** the iteration terms are dominant, then there exists a corresponding quantum attack:

$$T < 2^{|k|} \implies \sqrt{T} < 2^{|k|/2}$$

Breaking less rounds!

The "quantum search correspondence" **works both ways.**

A quantum key-recovery of time $\mathcal{O}(T)$, using memory M, **based on quantum search** $T < 2^{|k|/2}$	$\Longrightarrow$	A classical key-recovery of time $\mathcal{O}(T^2)$, using memory M, **based on classical search** $T^2 < 2^{|k|}$

- Quantum attacks based on quantum search are **always convertible to classical**
- This makes the security margin (equal or) **higher** in the quantum setting.

Still, if $2^{|k|/2}$ becomes our primary security level, then our primary attack goal is to go below.

Example: AES-128

Example on AES-128:

- **Classical 7-round DS-MITM / impossible differential** ($\leq 2^{128}$)
- **Quantum 6-round Square** (of complexity $\leq 2^{64}$) [BNS19]

- 7-round DS-MITM attack on AES-128 **[DFJ13]** starts by precomputing a table of size 2^{80}

  $\implies$ larger than 2^{64} anyway

Breaking more rounds quantumly means doing more than quantum search.

Derbez, Fouque, Jean, "Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting", EUROCRYPT 2013

Bonnetain, Naya-Plasencia, S., "Quantum Security Analysis of AES", ToSC 2019

Attacks based on Simon's Algorithm

Simon's algorithm

Let $f : \{0,1\}^n \rightarrow \{0,1\}^n$ be a function with a hidden period: $f(x \oplus s) = f(x)$, find s.

Classical resolution

Find a collision, in $\Omega\left(2^{n/2}\right)$.

Simon's algorithm

- Requires **superposition / quantum queries** that build states of the form:

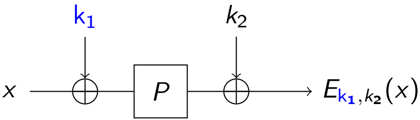
$$\sum_{x \in \{0,1\}^n} |x\rangle \, |f(x)\rangle$$

  with cost 1.
- Samples a random orthogonal y: $s \cdot y = 0$
- Repeats $\mathcal{O}(n)$ times, solves a linear system

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

Example: The Even-Mansour cipher

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



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

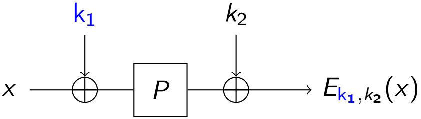
Classical security

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.

It's tight, with an attack in time $D + \frac{2^n}{D}$ and memory D ($D \leq 2^{n/2}$).

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}.

$\Longrightarrow$ the "quantum-type" Even-Mansour cipher is broken in **polynomial time.**

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

Quantum adversary models

Q1 model

- Make classical queries to $x \mapsto E_k(x)$ (and inverse)
- Do **offline** quantum computations

$\implies$ realistic, less powerful.
Typical: Grover

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

Q2 model

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

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

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

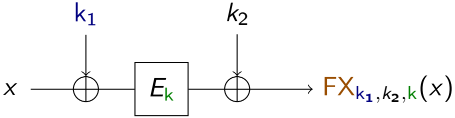
Many Q2 attacks on ciphers & more complex constructions have been designed, all using Simon's and other structure-finding algorithms.

Offline-Simon

With Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki

Grover meets Simon: the FX attack

Let's replace the public P of Even-Mansour by a block cipher E_k, with $|k| = 2n$.



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

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

$\Longrightarrow$ among all the functions $x \mapsto (FX \oplus E_z)(x)$, find the single z which gives a periodic function.

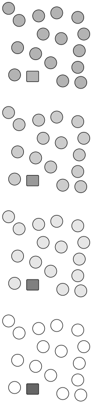
- $\mathcal{O}\left(2^{2n/2}\right) = \mathcal{O}\left(2^n\right)$ Grover iterates
- $\mathcal{O}\left(n\right)$ sup. queries and $\mathcal{O}\left(n^3\right)$ computations at each iterate

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

Running the FX attack

0. Setup Grover's initial state (**"sample"**)
1. Iteration 1 { **Test current state** / Apply Grover's diffusion transform (**"sample"**) }
2. Iteration 2 { **Test current state** / Apply Grover's diffusion transform (**"sample"**) }
3. Iteration 3 { **Test current state** / Apply Grover's diffusion transform (**"sample"**) }

. . .



Running the FX attack (ctd.)

Test iter. 1
- Make the "query states" $\sum_x |x\rangle |F_z(x) = (FX \oplus E_z)(x)\rangle$
- Run Simon's algorithm
- Unmake the "query states"

Test iter. 2
- Make the "query states" $\sum_x |x\rangle |F_z(x) = (FX \oplus E_z)(x)\rangle$
- Run Simon's algorithm
- Unmake the "query states"

Test iter. 3
- Make the "query states" $\sum_x |x\rangle |F_z(x) = (FX \oplus E_z)(x)\rangle$
- Run Simon's algorithm
- Unmake the "query states"

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

Improving the FX attack (ctd.)

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

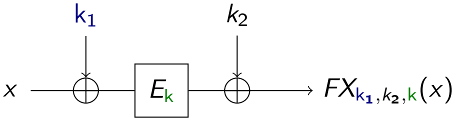
Test iter. 1 {
- Query E_z: $\sum_x |x\rangle |(FX \oplus E_z)(x)\rangle$
- Run Simon's algorithm
- Unmake the query to E_z: back to $\sum_x |x\rangle |FX(x)\rangle$

Test iter. 2 {
- Query E_z: $\sum_x |x\rangle |(FX \oplus E_z)(x)\rangle$
- Run Simon's algorithm
- Unmake the query to E_z

Test iter. 3 {
- Query E_z: $\sum_x |x\rangle |(FX \oplus E_z)(x)\rangle$
- Run Simon's algorithm
- Unmake the query to E_z

...

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 $\widetilde{\mathcal{O}}(2^n)$
- the quantum search contains $\mathcal{O}\left(2^{2n/2}\right)$ iterations: time $\widetilde{\mathcal{O}}(2^n)$

At this point, the classical attack still costs $T = 2^{2n}$ (square-root speedup).

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

The "True" Power of Offline-Simon

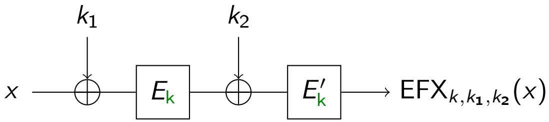
With Xavier Bonnetain, Ferdinand Sibleyras

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)



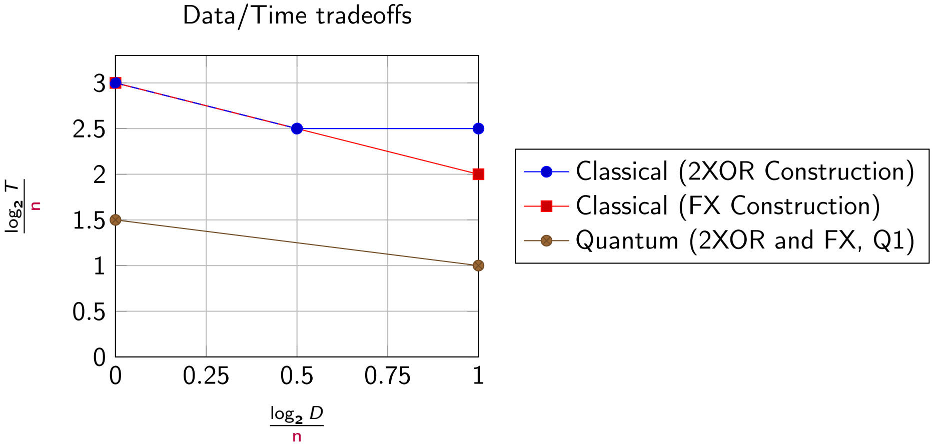
Still assuming: $|k| = 2n$.

Any classical adversary must make $2^{5n/2}$ queries to E, E' to distinguish, **even if** he knows the entire codebook.

Given the codebook of size 2^n, a quantum adversary can recover all the keys in time $\widetilde{\mathcal{O}}(2^n)$ (and the trade-off is the same as FX).

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

What is happening here?



Increased data (up to the codebook) does not help, while it helps in the FX attack.

Tweaking Offline-Simon

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

$$EFX[E, E']_{k,k_1,k_2} = E'_k(k_2 \oplus E_k(k_1 \oplus x))$$

Previous Offline-Simon problem

Let F_z be a family of functions, $F_z(x) = f(x) \oplus g_z(x)$, with a single z_0 such that F_{z_0} is periodic. Find z_0.

$\Longrightarrow$ not applicable.

"True" Offline-Simon problem

Let F_z be a family of functions, $F_z(x) = \pi_z \circ f(x)$, with a single z_0 such that F_{z_0} is periodic. Find z_0.

$\Longrightarrow$ the quantum algorithm only needs an **efficient "in-place" operation**, not necessarily a XOR.

Tweaking Offline-Simon (ctd.)

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

We have:

$$(E'_k)^{-1}\Big(EFX(x)\Big) \oplus E_k(x) =$$

$$k_2 \oplus E_k(k_1 \oplus x) \oplus E_k(x) \qquad \text{(periodic)}$$

and otherwise a random function.

Conclusion

Conclusion

Several attack families with different implications.

"Quantum search" attacks

- Likely the most common
- Many "dedicated" attack techniques can adapted
- Security margin (relative to exhaustive search) is not reduced

Structural superposition attacks (Q2)

- Some constructions become irremediably "broken"
- But there are no practical security implications for now
- So far no "dedicated" cryptanalysis in this model

Conclusion (ctd.)

"Offline" attacks

- Structural attacks, but with classical queries
- So far, up to 2.5 time speedup and cubic improvement on the time-memory product
- Conjectured cubic time speedup at best using offline-Simon: is this a generic limit?

ePrint 2021/1348

Thank you!