Quantum Cryptanalysis of Block Ciphers: Quadratic Speedups and Beyond

André Schrottenloher
Cryptology group, CWI
Post-quantum cryptography

Asymmetric
- RSA (factorization) and ECC (discrete logarithms) become broken in polynomial time
  \[\text{[Shor]}\]
- 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

\[\Rightarrow\] should we simply “double the key size”?

---

### 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 $2^{|k|}$
  - 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 \( 2^{|k|/2} \)
  - \( \implies \) 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

André Schrottenloher (CWI)
Attacks based on Quantum Search

Attacks based on Simon’s Algorithm

Offline-Simon

The “True” Power of Offline-Simon

Quantum search

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

Classical (exhaustive) search

Repeat $\frac{|X|}{|G|}$ times

\[
\begin{align*}
\text{Sample } x & \in X \\
\text{Test if } f(x) & = 1
\end{align*}
\]

Quantum search (Grover’s algorithm)

Repeat $O\left(\sqrt{\frac{|X|}{|G|}}\right)$ times

\[
\begin{align*}
\text{Sample } x & \in X \rightarrow \text{quantumly} \\
\text{Test if } f(x) & = 1 \rightarrow \text{quantumly}
\end{align*}
\]

---

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

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

$$\frac{1}{\sqrt{|\text{all keys } k'|}} \sum_{\text{all keys } k'} |k'|$$

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 \(|\text{good key } k\rangle\).
Quantum search (ctd.)

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

A classical exhaustive search with $O(T)$ iterations

An exhaustive search with $O(T_1)$ iterations of an exhaustive search with $O(T_2)$ iterations

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

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

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

- simple linear and differential attacks
- Square and Demirci-Selçuk MITM attacks
- Boomerang (differential) attacks
- ...  

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

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

$$T < 2^{|k|/2}$$

$\implies$

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

André Schrottenloher (CWI)
Attacks based on Quantum Search

Attacks based on Simon’s Algorithm

Offline-Simon

The “True” Power of Offline-Simon

Simons’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 $\Omega\left(2^{n/2}\right)$.

Simons’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 $O(n)$ times, solves a linear system

---

Example: The Even-Mansour cipher

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

\[
x \xrightarrow{\oplus k_1} P \xrightarrow{\oplus k_2} E_{k_1,k_2}(x)
\]

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

**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 $D \ (D \leq 2^{n/2})$.

---

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 \( E_{k_1,k_2} \).

\( \implies \) the “quantum-type” Even-Mansour cipher is broken in *polynomial time*.

Quantum adversary models

**Q1 model**
- Make classical queries to $x \mapsto E_k(x)$ (and inverse)
- Do **offline** quantum computations

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

**Q2 model**
- Do quantum computations
- Can use $E_k$ as black-box **inside** the quantum algorithm

$\Rightarrow$ 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 $|k| = 2n$.

$\begin{array}{c}
\begin{array}{c}
\text{x} \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
E_k \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
k_1 \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
k_2 \\
\end{array}
\end{array}
\begin{array}{c}
\text{FX}_{k_1,k_2,k}(x)
\end{array}$

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

- $O(2^{2n}/2) = O(2^n)$ Grover iterates
- $O(n)$ sup. queries and $O(n^3)$ 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.)

\[ \sum_x |x\rangle |F_z(x) = (FX \oplus E_z)(x) \rangle \]

**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" \( \sum_x |x\rangle |\text{FX}(x)\rangle \)

\begin{align*}
\text{Test iter. 1} & \quad \begin{cases} 
\text{Run Simon's algorithm} \\
\text{Unmake the query to } E_z: \text{ back to } \sum_x |x\rangle |\text{FX}(x)\rangle 
\end{cases} \\
\text{Query } E_z: \sum_x |x\rangle |(\text{FX} \oplus E_z)(x)\rangle 
\end{align*}

\begin{align*}
\text{Test iter. 2} & \quad \begin{cases} 
\text{Run Simon's algorithm} \\
\text{Unmake the query to } E_z 
\end{cases} \\
\text{Query } E_z: \sum_x |x\rangle |(\text{FX} \oplus E_z)(x)\rangle 
\end{align*}

\begin{align*}
\text{Test iter. 3} & \quad \begin{cases} 
\text{Run Simon's algorithm} \\
\text{Unmake the query to } E_z 
\end{cases} \\
\text{Query } E_z: \sum_x |x\rangle |(\text{FX} \oplus E_z)(x)\rangle 
\end{align*}

\ldots
Attacks based on Quantum Search
Attacks based on Simon’s Algorithm
Offline-Simon
The “True” Power of Offline-Simon

Offline-Simon attack on FX

\[
E_k \quad \rightarrow \quad FX_{k_1, k_2, k}(x)
\]

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 \( |k| = 2^n \):

- creating the initial “query states” costs the codebook \( (2^n \text{ queries}) \)
  and time \( \widetilde{O}(2^n) \)
- the quantum search contains \( O\left(2^{2n/2}\right) \) iterations: time \( \widetilde{O}(2^n) \)

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)

\[
x \xrightarrow{} E_k \xrightarrow{} E'_k \xrightarrow{} \text{EFX}_{k, k_1, k_2}(x)
\]

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 \( \tilde{O}(2^n) \) (and the trade-off is the same as FX).

---

Gazi, Tessaro, “Efficient and optimally secure key-length extension for block ciphers via randomized cascading”, EUROCRYPT 2012
What is happening here?

Data/Time tradeoffs

Increased data (up to the codebook) does not help, while it helps in the FX attack.
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 \( z_0 \).

\[ \implies \text{not applicable.} \]

**“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 \( z_0 \).

\[ \implies \text{the quantum algorithm only needs an efficient “in-place” operation, not necessarily a XOR.} \]
Tweaking Offline-Simon (ctd.)

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

We have:

\[
(E'_k)^{-1}(E_{FX}(x)) \oplus E_k(x) = k_2 \oplus E_k(k_1 \oplus x) \oplus E_k(x) \quad \text{(periodic)}
\]

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 be 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!