Quantum cryptanalysis of block ciphers: an overview

André Schrottenloher

Cryptology group, CWI

June 4, 2021

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

$\implies$ 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 access 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 $2^{|k|}$

  $\Longrightarrow$ 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 access to a black-box $x \mapsto E_k(x)$, find k.

- **quantum:** $2^{|k|/2}$ (use quantum search)

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**

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

- **quantum:** $2^{|k|/2}$ (use quantum search)

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**

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" and Beyond

Attacks based on Quantum Search

Quantum computing in a single slide

- n bits $x \to n$ qubits $|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$
- We have logical gates (quantum gates) to act on $|\psi\rangle$
- Measuring $|\psi\rangle$ yields x with probability $|\alpha_x|^2$)
- The computation modifies the amplitudes α_x
- We try to "move the amplitude" towards some good x
- **Only then,** measuring the state gives us a meaningful result

(We'll be just be using black-boxes anyway)

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)

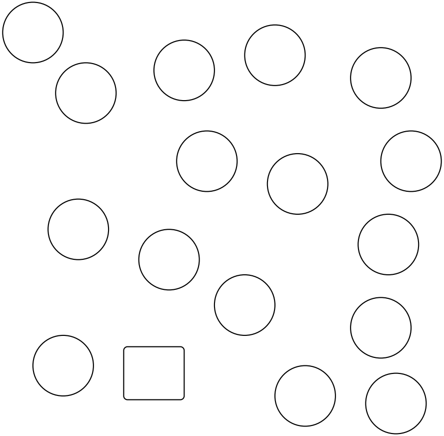
$$\text{Repeat } \mathcal{O}\left(\sqrt{\frac{|X|}{|G|}}\right) \text{ times} \begin{cases} \text{Sample } x \in X \to \text{quantumly} \\ \text{Test if } f(x) = 1 \to \text{quantumly} \end{cases}$$

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

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

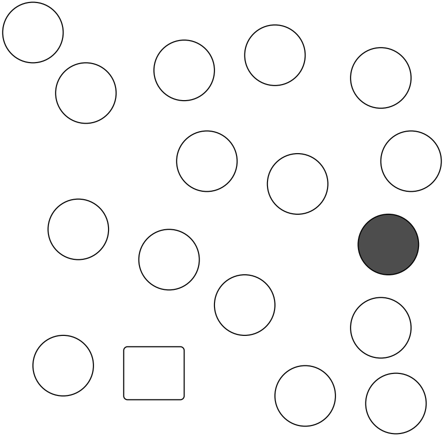
Classical search (ctd.)

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



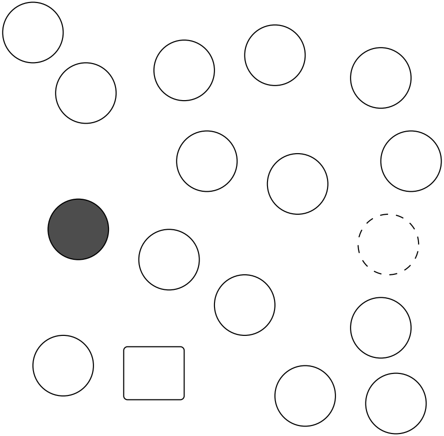
Classical search (ctd.)

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



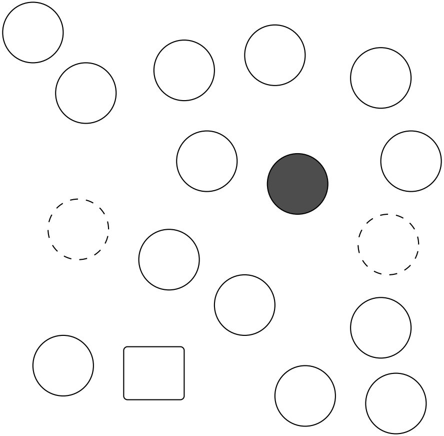
Classical search (ctd.)

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



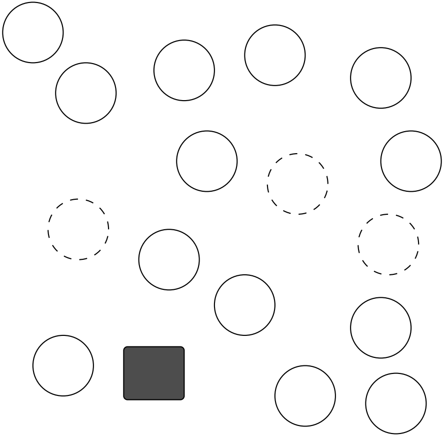
Classical search (ctd.)

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



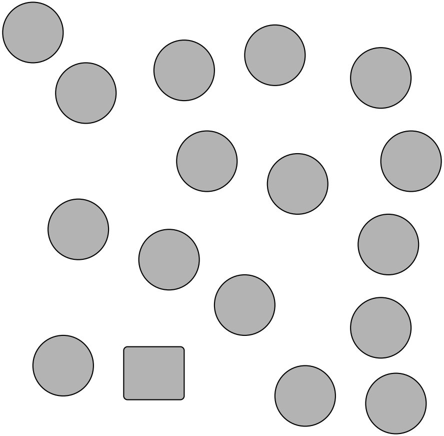
Classical search (ctd.)

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



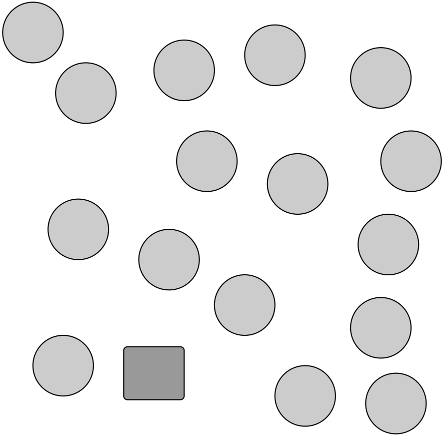
Quantum search (ctd.)

In the quantum realm, we move globally (statefully) from $X = \{\text{all keys}\}$ to $G = \{\text{good key}\}$.



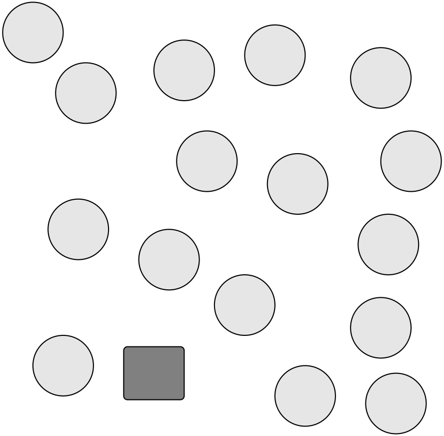
Quantum search (ctd.)

In the quantum realm, we move globally (statefully) from $X = \{\text{all keys}\}$ to $G = \{\text{good key}\}$.



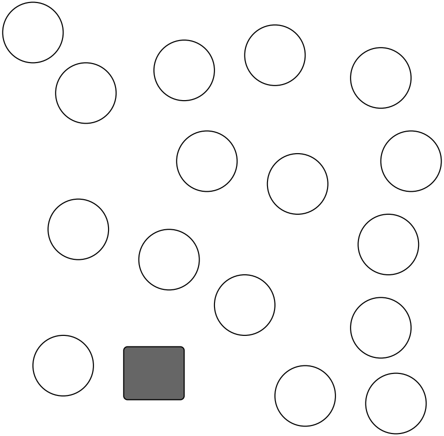
Quantum search (ctd.)

In the quantum realm, we move globally (statefully) from $X = \{\text{all keys}\}$ to $G = \{\text{good key}\}$.



Quantum search (ctd.)

In the quantum realm, we move globally (statefully) from $X = \{\text{all keys}\}$ to $G = \{\text{good key}\}$.



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

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

Example: key-recovery attacks on AES

A classical attack

- Key-recovery below time $2^{|k|}$

Some attacks (not all) can be phrased as combinations of exhaustive searches.

Best **classical** attacks:

- AES-128: 7-round Impossible Differential
- AES-256: 9-round Demirci-Selçuk-MITM

A quantum attack

- Key-recovery below time $2^{|k|/2}$

Some attacks (not all) admit quantum counterparts.

Best **quantum** attacks:

- AES-128: 6-round Quantum Square
- AES-256: 8-round Demirci-Selçuk-MITM

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

Key-recovery attacks (ctd.)

So far, the security margin of AES is **higher** in the quantum setting.

- Because of all the attacks that "do not work anymore".

Example: AES-128

Example of 7-round DS-MITM attack from [DFJ13]:

1. precompute 2^{48} limited birthday pairs for the black-box (time 2^{113}):
2. **precompute a table** of size 2^{80} for an internal 4-round distinguisher
3. perform a search over 9 key bytes (72 bits of key)

Classically below 2^{128} encryptions, but not below 2^{64} quantumly (Step 2).

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

When can we break more rounds?

The "quantum search correspondence" **works in both directions.**

A quantum key-recovery of time $\mathcal{O}(T)$, using memory M, **based on quantum search**

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

A quantum attack based on quantum search can only break as many rounds as the best classical attack.

When can we break more rounds? (ctd.)

This limitation is artificial:

- we are mimicking classical attacks
- we are considering a very restricted set of algorithms

When can we **break more rounds** quantumly?

1. When the generic problem does **not** have a quadratic speedup

   $\implies$ see Akinori's talk

2. When we use other tools than quantum search

Attacks based on Simon's Algorithm

Simon's algorithm

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

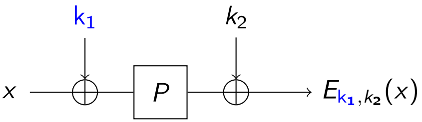
$$\sum_{x \in \{0,1\}^n} |x\rangle \, |f(x)\rangle$$

  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 $P : \{0,1\}^n \to \{0,1\}^n$ and $2n$ bits of key.



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

Classical security

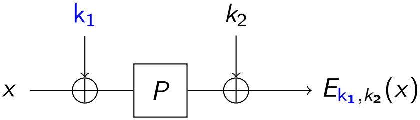
If P is a random permutation, an adversary performing T queries to P and D queries to E_{k_1,k_2} needs $T \cdot D = 2^n$ to recover the key.

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

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}.

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

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

On the superposition query model (Q2)

Q1

The adversary makes **classical** queries to the black-box.

$\Longrightarrow$ he can also observe the current traffic, and record for later breaks

$\Longrightarrow$ this is our primary concern in post-quantum crypto

Q2

The secret-key oracle is **part of** the adversary's quantum computations.

$\Longrightarrow$ this has no implication on current cryptosystems (which are still classical!)

- Some adversaries may have stronger control on the block cipher than black-box oracle access (white-box? obfuscation?)
- Q2 security is stronger, more flexible, and **not too difficult to achieve**
  - actually, most block ciphers seem fine (e.g., AES)
- Q2 attacks might be a first step in designing better Q1 versions

Summary: what we have seen so far

Quantum search attacks

- **Setting:** Q1
  and sometimes Q2
- **Requires:** a search-based classical key-recovery
- **Security:** same security margin

⇓

Surprising results are unlikely

Simon-based attacks

- **Setting:** **Q2 (quantum queries)**
- **Requires:** a periodicity property
  - happens in many designs
  - but **does not** happen in many designs

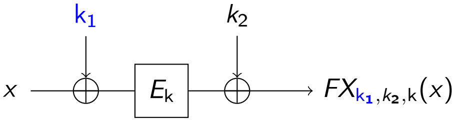
⇓

Currently, all more-than-quadratic speedups happened in this setting.

Can we use Simon's algorithm with classical queries?

"Offline-Simon" and Beyond

Grover meets Simon: the FX attack



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

- Search k with Grover's algorithm
- To check a guess z, run Kuwakado and Morii's attack

- Time: $\underbrace{n^3}_{\text{Simon's runtime}} \times \underbrace{2^{|k|/2}}_{\text{Grover's iterates}}$
- Queries: $\underbrace{n}_{\text{Simon's queries}} \times \underbrace{2^{|k|/2}}_{\text{Grover's iterates}}$

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

A closer look at the FX attack

The function:

$$f_z(x) = FX_{k_1, k_2, k}(x) \oplus E_z(x)$$

has $f_z(x \oplus k_1) = f_z(x)$ **iff** $z = k$ **is the good guess**.

The "Grover-meet-Simon" problem

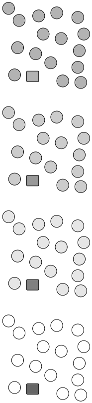
Let F be a family of functions, $F(z) = f_z$, indexed by z, with a single z_0 such that f_{z_0} is periodic. Find z_0.

$$\text{Here } f_z(x) = \underbrace{FX_{k_1, k_2, k}(x)}_{\textbf{Independent of z: online function } f} \oplus \underbrace{E_z(x)}_{\textbf{Grover search space: offline function } g_z}$$

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 $\begin{cases} \text{Make the "query states" } \sum_x |x\rangle |f_z(x) = (f \oplus g_z)(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the "query states"} \end{cases}$

Test iter. 2 $\begin{cases} \text{Make the "query states" } \sum_x |x\rangle |f_z(x) = (f \oplus g_z)(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the "query states"} \end{cases}$

Test iter. 3 $\begin{cases} \text{Make the "query states" } \sum_x |x\rangle |f_z(x) = (f \oplus g_z)(x)\rangle \\ \text{Run Simon's algorithm} \\ \text{Unmake the "query states"} \end{cases}$

g_z varies between the iterates, but f **is always the same**!

Improving the FX attack (ctd.)

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

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

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

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

...

Offline-Simon

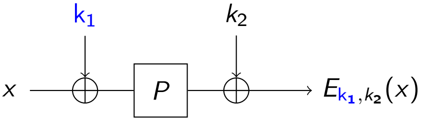
"Offline-Simon" problem

Let F be a family of functions, $F(z) = f_z = f \oplus g_z$, indexed by z, with a single z_0 such that f_{z_0} is periodic. Find z_0.

- We need to make the queries to f only once, at the beginning (hence "offline").
- With FX, reduces the queries from $\mathcal{O}\left(n2^{|k|/2}\right)$ to $\mathcal{O}\left(n\right)$

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

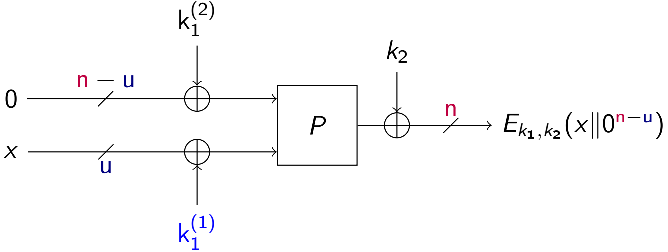
Back to the Even-Mansour cipher

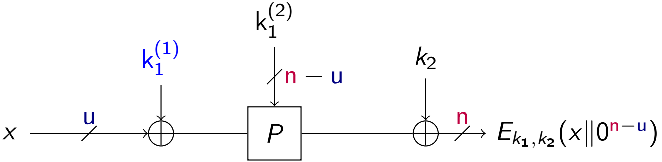


- We would like to use only classical queries . . .
- . . . but the queries in Simon's algorithm contain the 2^n inputs!

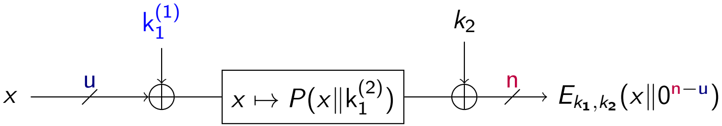
The solution is to turn Even-Mansour into an FX instance.

Offline-Simon attack on Even-Mansour





Offline-Simon attack on Even-Mansour (ctd.)



Define $f(x) = E_{k_1,k_2}(x \| 0^{\mathsf{n}-\mathsf{u}}) \oplus P(x \| \mathsf{k}_1^{(2)})$. **It has period $\mathsf{k}_1^{(1)}$**.

1. Produce the sample states $\sum_x |x\rangle \, |E_{k_1,k_2}(x \| 0^{\mathsf{n}-\mathsf{u}})\rangle$
2. (Grover) search the good $\mathsf{k}_1^{(2)}$ ($\mathsf{n} - \mathsf{u}$ bits)

Data: 2^{u}

Time: $2^{\mathsf{u}} + 2^{(\mathsf{n}-\mathsf{u})/2} \implies D \cdot T^2 = 2^{\mathsf{n}}$ for $D \leq 2^{\mathsf{n}/3}$

Memory: n^2 qubits

Classical-quantum comparison

Classical

Data-time trade-off: $D \cdot T = 2^{n}$ ($D \leq 2^{n/2}$)

$\implies T = \frac{2^{n}}{D}$

Memory: D for all $D < 2^{n/2}$

Quantum

Data-time trade-off: $D \cdot T^2 = 2^{n}$ ($D \leq 2^{n/2}$)

$\implies T = \sqrt{\frac{2^{n}}{D}}$

Memory: poly(n) **all the time**

Cons

- Still a square-root speedup!

Pros

- The memory has been removed: "quantum search alone" cannot do that

Follow-ups

- Bonnetain & Jaques: offline-Simon applied to actual designs (e.g. Chaskey)
- Frixons & S.: offline-Kuperberg when replacing the $\oplus$ by a $+$
  - It can be used to attack the Legendre PRF
- ...

Bonnetain, Jaques, "Quantum Period Finding against Symmetric Primitives in Practice", ePrint 2020/1418

Frixons, S., "Quantum security of the Legendre PRF", ePrint 2021/149

Conclusion

Conclusion

Several attack families with different implications.

"Quantum search" attacks

- Likely the most common
- Many "dedicated" attack techniques can adapted
- Suffer from the same limitations as classical attacks

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

"Offline" attacks

- Somehow using a Q2 vulnerability in a Q1 setting
- Exponential memory reductions can be a powerful practical advantage

Thank you!

References

Kaplan, Leurent, Leverrier, and Naya-Plasencia
Quantum Differential and Linear Cryptanalysis
In *IACR Trans. Symmetric Cryptol. 2016.*

Bonnetain, Naya-Plasencia, and S.
Quantum Security Analysis of AES
In *IACR Trans. Symmetric Cryptol. 2019.*

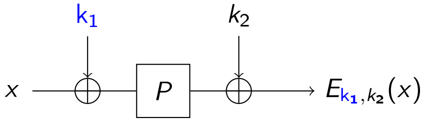
Kuwakado and Morii
Security on the quantum-type Even-Mansour cipher.
In *ISITA 2012.*

Kaplan, Leurent, Leverrier, and Naya-Plasencia
Breaking Symmetric Cryptosystems Using Quantum Period Finding
In *CRYPTO 2016.*

Leander and May
Grover Meets Simon - Quantumly Attacking the FX-construction
In *ASIACRYPT 2017.*

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

Classical trade-off



Let $g(y) = P(y) \oplus P(y \oplus 1)$, $h(x) = E_{k_1,k_2}(x) \oplus E_{k_1,k_2}(x \oplus 1)$, then

$$\forall x, g(x \oplus k_1) = h(x)$$

Attack

- Collect D values of $h(x)$ in a database $\mathcal{D}$
- Find y such that $g(y) \in \mathcal{D}$, in time $2^n/D$
- With good probability $y = x \oplus k_1$

The attack needs $T = D + 2^n/D$ and D memory.