Beyond Quadratic Speedups in Quantum Attacks on Symmetric Schemes

Xavier Bonnetain André Schrottenloher Ferdinand Sibleyras

ePrint 2021/1348

A quick view of Quantum cryptanalysis

Polynomial attacks

RSA, discrete log, some symmetric schemes *in the Q2 model*...

A quick view of Quantum cryptanalysis

Polynomial attacks

RSA, discrete log, some symmetric schemes *in the Q2 model*...

Superpolynomial gains

Ordinary isogenies, CSIDH...

A quick view of Quantum cryptanalysis

Polynomial attacks

RSA, discrete log, some symmetric schemes *in the Q2 model*...

Superpolynomial gains

Ordinary isogenies, CSIDH...

At-most-quadratic gains

- Most of the rest, including symmetric schemes in the Q1 model
- Most attacks are quantum improvements over classical attacks

A reassuring idea

Quantum attacks on symmetric schemes

- Exhaustive search has a quadratic speedup
- Grover-accelerated classical attacks have a speedup at most quadratic

A quantum lower bound?

Assuming attack speedups are at most quadratic, if no classical attack beats classical exhaustive search, no quantum attack can beat quantum exhaustive search.

Outline

1. Introduction
2. Attack on Even-Mansour
3. The offline Simon's algorithm
4. Breaking the quadratic barrier
5. Conclusion

Simon's algorithm

Simon's problem

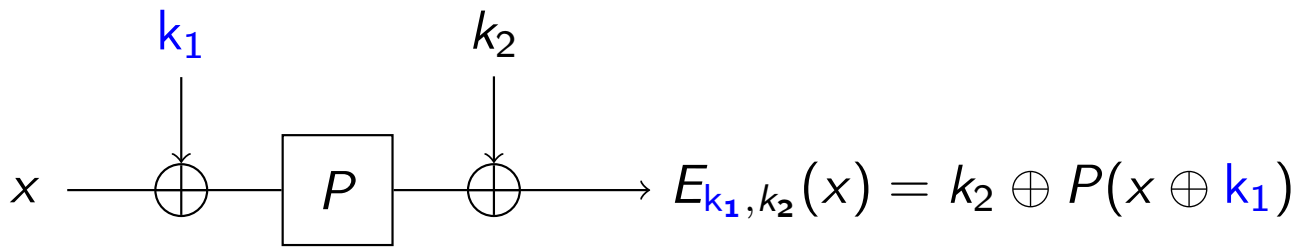
- $f : \{0,1\}^n \to \{0,1\}^n$
- $s \in \{0,1\}^n, f(x) = f(x \oplus s)$
- Goal: find s

Simon's algorithm

- Quantum queries to f : $\sum |x\rangle |0\rangle \mapsto \sum |x\rangle |f(x)\rangle$.
- Sample y: $s \cdot y = 0$.
- Repeat $O(n)$ times and solve a linear system.

The Even-Mansour Cipher

Built from a random permutation $P : \{0,1\}^n \to \{0,1\}^n$.

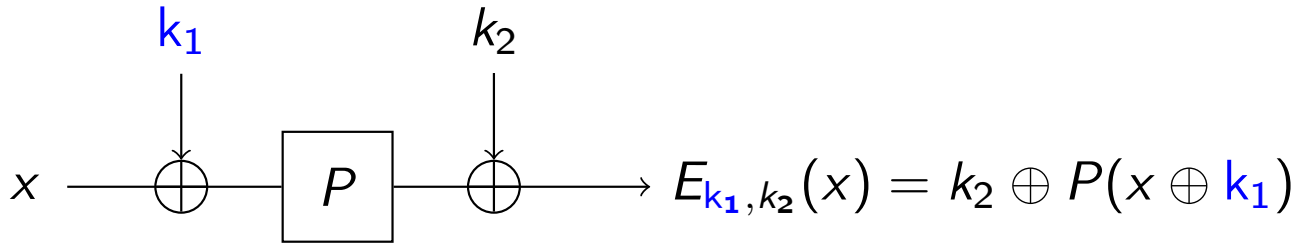


Classical security

Any attack needs Time $\times$ Data $\geq 2^n$

The Even-Mansour Cipher

Built from a random permutation $P : \{0,1\}^n \to \{0,1\}^n$.



Classical security

Any attack needs Time $\times$ Data $\geq 2^n$

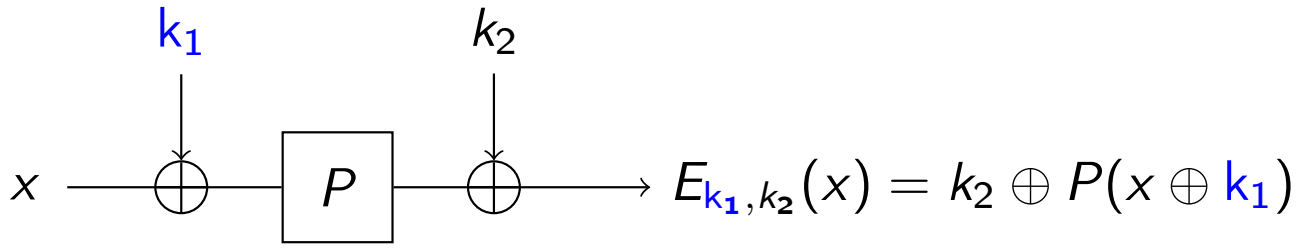
Quantum attack [KM12]

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

Simon's algorithm breaks Even-Mansour in polynomial time.

The Even-Mansour Cipher

Built from a random permutation $P : \{0,1\}^n \to \{0,1\}^n$.



Classical security

Any attack needs Time $\times$ Data $\geq 2^n$

Quantum attack [KM12]

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

Simon's algorithm breaks Even-Mansour in polynomial time.
Requires quantum queries

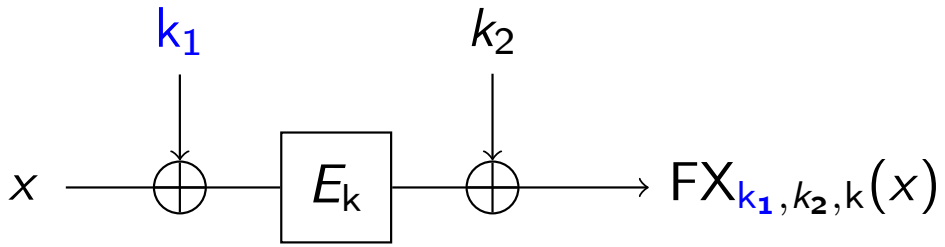
We need

$\sum |x\rangle |0\rangle \mapsto \sum |x\rangle |f(x)\rangle$

In general, we have

$(x_0, f(x_0)), (x_1, f(x_1)) \ldots$

The FX construction



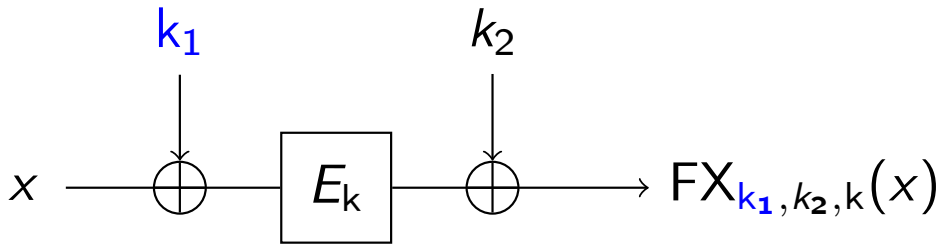
Classical security

Any classical attack statisifies $TD \geq 2^{n+|k|}$.

Attack example

- Create a list with 2^{n-u} $\mathrm{FX}_{k_1,k_2,k}(x) \oplus \mathrm{FX}_{k_1,k_2,k}(x \oplus 1)$
- For each candidate key $\hat{k}$:
  - Query 2^u times $E_{\hat{k}}(x) \oplus E_{\hat{k}}(x \oplus 1)$
  - A collision gives a guess for (k_1, k)

The FX construction



Classical security

Any classical attack statisifies $TD \geq 2^{n+|k|}$.

Quantum attack: "Grover-meet-Simon" [LM17]

- Quantum search for k
- Checking: previous quantum attack works $\iff$ the guess of k is correct

Total time is $\underbrace{poly(n)}_{\text{Simon's algo}} \times \underbrace{2^{|k|/2}}_{\text{Grover's iterates}}$.

A remark on FX [BHNSS19]

The function:

$$f_z(x) = \mathrm{FX}_{\mathsf{k_1},k_2,\mathsf{k}}(x) \oplus E_z(x)$$

has $f_z(x \oplus \mathsf{k}_1) = f_z(x)$ **if** $z = \mathsf{k}$ **(the good one)**.
f_z is a sum:

$$f_z(x) = \underbrace{\mathrm{FX}_{\mathsf{k_1},k_2,\mathsf{k}}(x)}_{\substack{\textbf{Independent of z: online function f}}} \oplus \underbrace{E_z(x)}_{\substack{\textbf{Grover search space: offline function } g}}$$

For one query to f_z

- Do one quantum query to $\mathrm{FX}_{\mathsf{k_1},k_2,\mathsf{k}}(x)$ (fixed!)
- Add $E_z(x)$ (only depends on public information)

A new attack on FX

The queries to $\mathrm{FX}_{k_1,k_2,k}(x)$ are made beforehand.

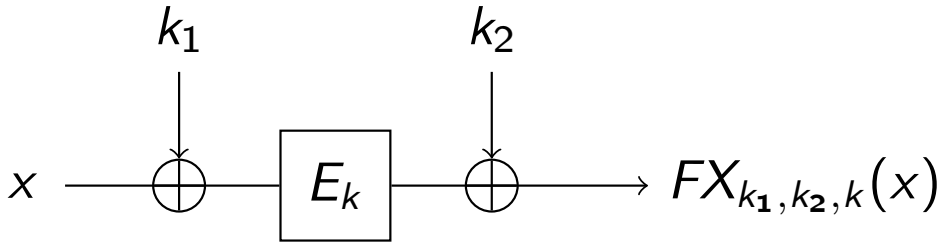
Test function

- Fetch the sample states $\sum_{x\in\{0,1\}^n} |x\rangle\,|\mathrm{FX}_{k_1,k_2,k}(x)\rangle$
- Create the Simon states $\sum_{x\in\{0,1\}^n} |x\rangle\,|\mathrm{FX}_{k_1,k_2,k}(x)\oplus E_z(x)\rangle$
- Test if there is a period
- **Revert** the operations and get back the sample states

Attack cost

- Time unchanged
- Queries reduced from $\mathcal{O}\left(n2^{|k|/2}\right)$ to $\mathcal{O}(n)$
- Needs $\mathcal{O}\left(n^2\right)$ Qubits

Removing the quantum queries



Producing the sample states with *classical* queries is possible... with 2^n time and data, with the whole codebook.

Attack cost

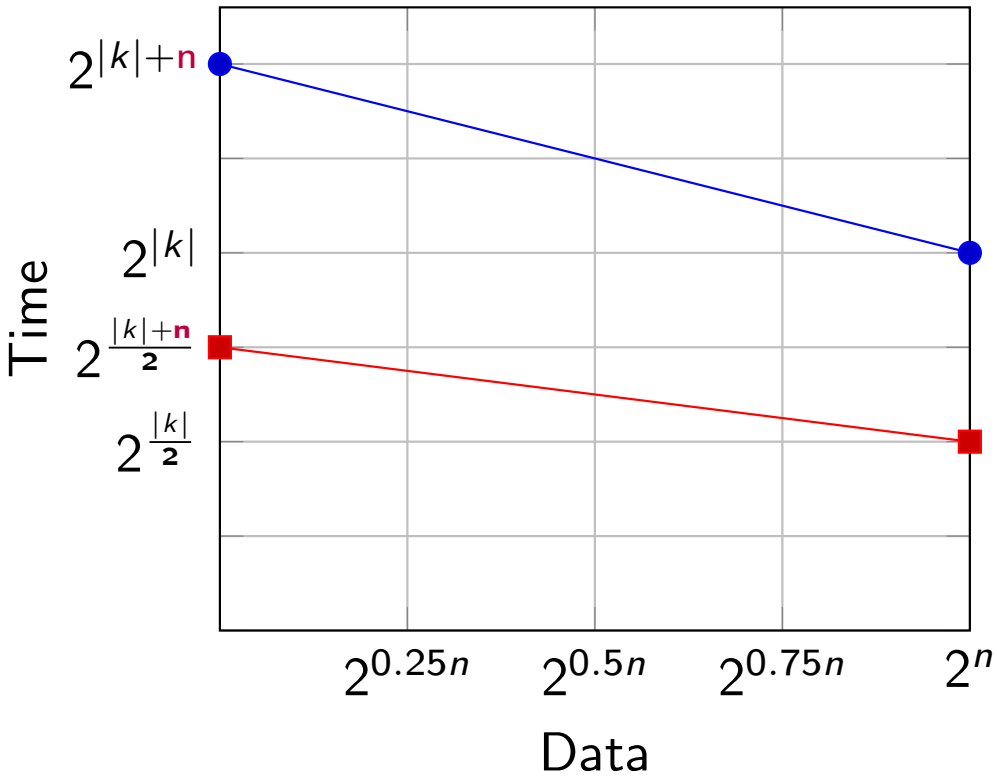
- Setup: 2^n data
- Search: $2^{|k|/2}$ time

Time/Data Tradeoff

Period size reduction

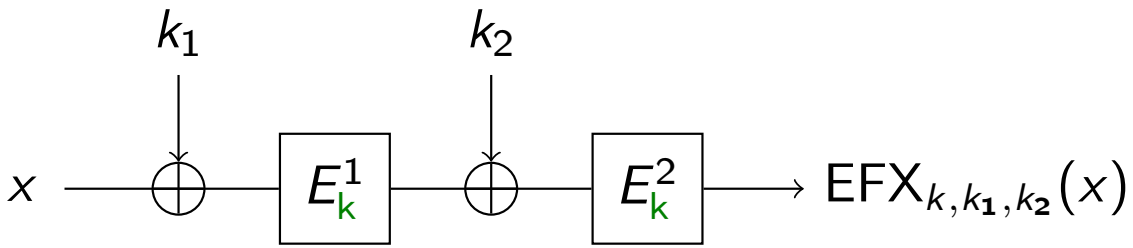
We can guess part of the period to reduce the data requirement.

- Setup: 2^{n-u} data
- Search: $2^{(|k|+u)/2}$ time

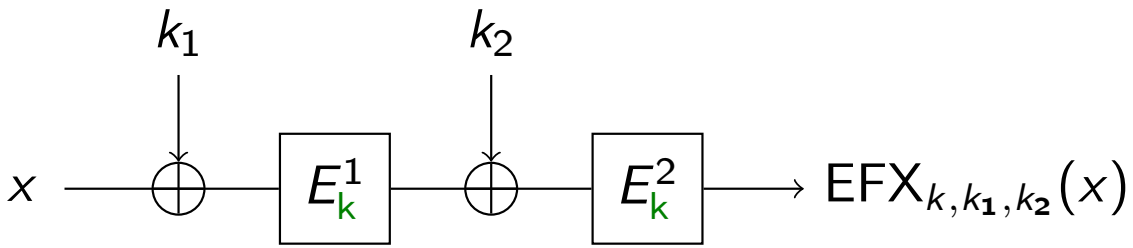


- Quadratic speedup
- Plus memory gain

Extended-FX



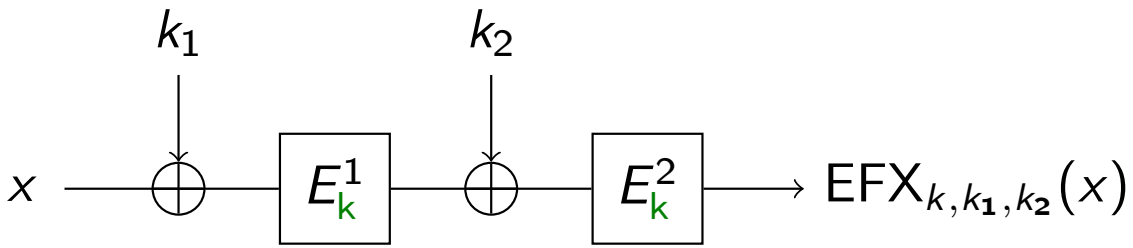
Extended-FX



Classical security

- Time $\times$ Data $\geq 2^{n+|k|}$
- Time $\geq 2^{n/2+|k|}$

Extended-FX

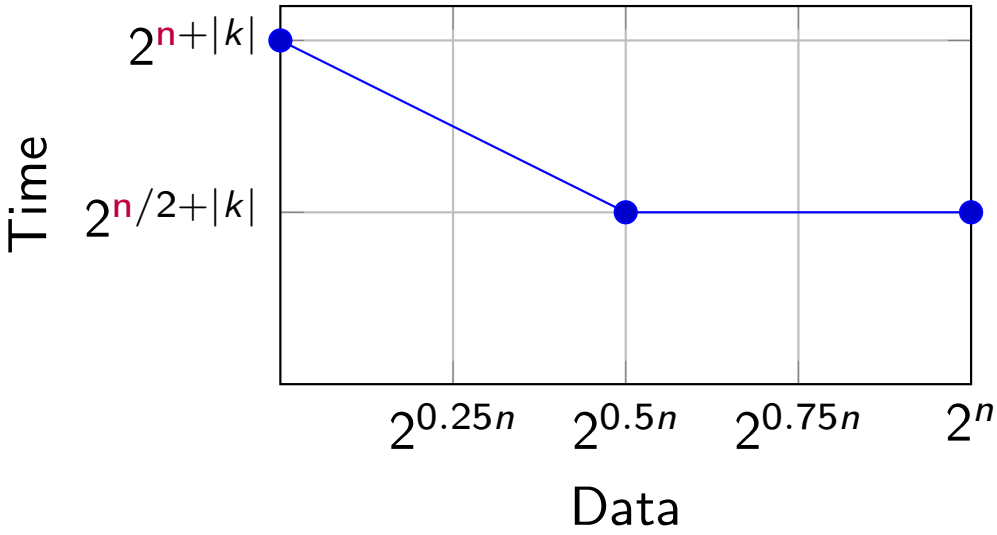


Classical security

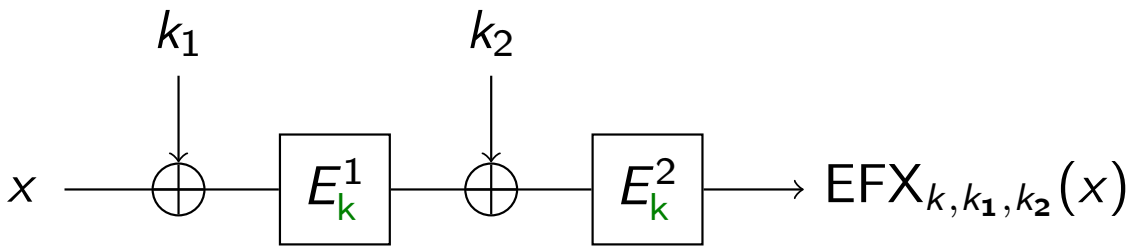
- Time $\times$ Data $\geq 2^{n+|k|}$
- Time $\geq 2^{n/2+|k|}$

Classical attack

- Apply the FX attack
- For all candidate key $\hat{k}$:
  - Invert E_k^2
  - Look for a collision



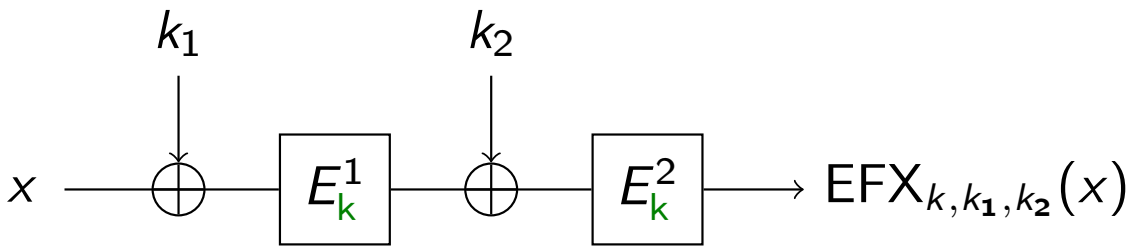
Quantum attack on Extended-FX



A new test function

$f_z(x) = (E_z^2)^{-1}(\mathrm{EFX}_{k,k_1,k_2}(x)) \oplus E_z^1(x)$ periodic if $z = k$

Quantum attack on Extended-FX



A new test function

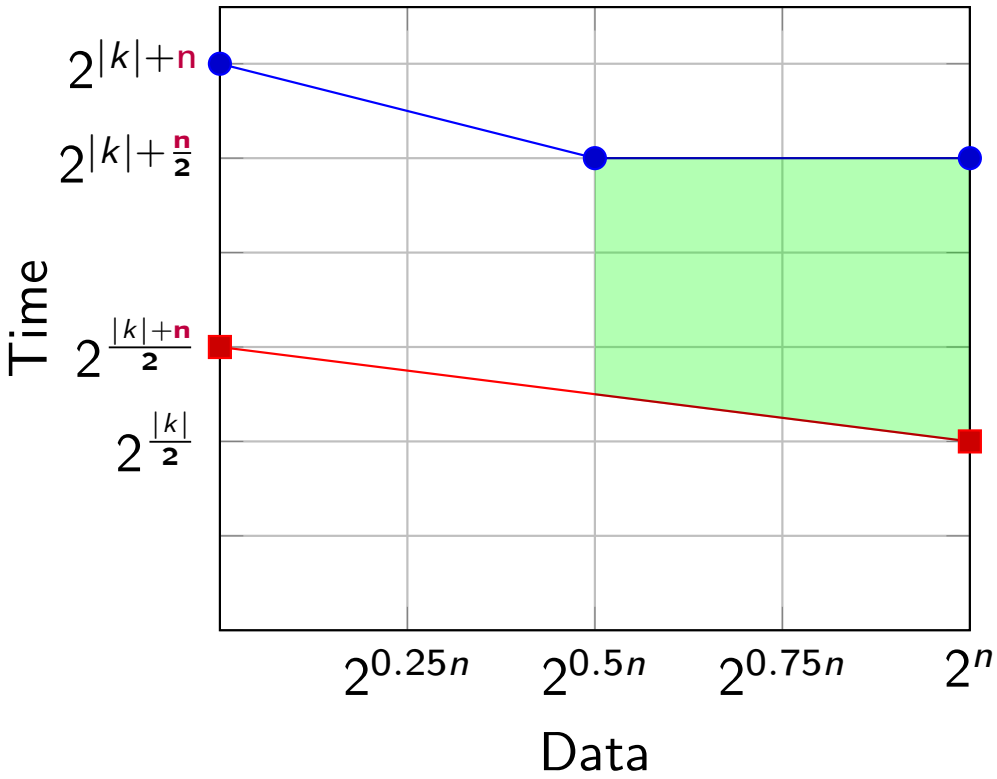
$f_z(x) = (E_z^2)^{-1}(\mathrm{EFX}_{k,k_1,k_2}(x)) \oplus E_z^1(x)$ periodic if $z = k$

Applying the Offline Simon's algorithm

Same principle as FX to compute $f_z(x)$:

- A fixed part: $\mathrm{EFX}_{k,k_1,k_2}(x)$
- A publicly computable part:
  - Transform reversibly the fixed part to $(E_z^2)^{-1}(\mathrm{EFX}_{k,k_1,k_2}(x))$
  - Add $E_z^1(x)$

Quantum gap for Extended-FX



- Gap larger than quadratic if Data $\geq 2^{n/2}$
- Maximal gap 2.5, with $|k| = 2n$

Conclusion

On Extended-FX

- Such constructions do appear in actual cryptosystems.
- The gap with unlimited data is tight.
- Extended-FX offers no increase in quantum security.

On the attack

- More than quadratic speedups are achievable in symmetric cryptography, *with classical queries*, *in the ideal model*.
- 2.5 is optimal for this algorithm.
- A $\oplus$ is enough for meaningful applications of HS algorithms.

Open questions

- Quantum lower bound with limited data?
- More than quadratic gap before the birthday bound?
- Can we extend the gap with another approach? (cubic?)