New Results on Symmetric Quantum Cryptanalysis and Perspectives

María Naya-Plasencia
Inria, France

ERC project QUASYModo

Indocrypt 2021 - 14 Dec 2021

Outline

- Introduction
  On Quantum-Safe Symmetric Cryptography

- Quantum Cryptanalysis - Illustrative Case
  Even-Mansour and FX:
  Best Classical and Quantum attacks

- Open Problems and Conclusion

Symmetric Cryptography

Classical Cryptography

Enable secure communications even in
the presence of malicious adversaries.

Asymmetric (e.g. RSA) *(computationally costly)*

Security based on well-known hard mathematical problems (e.g. factorization).

Symmetric (e.g. AES) *(key exchange needed BUT efficient.)*

Ideal security defined by generic attacks ($2^{|K|}$).

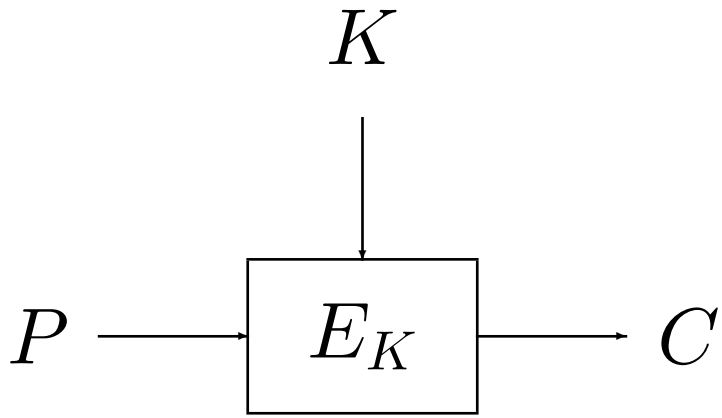
Need of continuous security evaluation (cryptanalysis).

$\Rightarrow$ Hybrid systems! (e.g. in SSH)

Symmetric primitives

- Block ciphers, (stream ciphers, hash functions..)

Message decomposed into blocks, each transformed by the same function E_K.



E_K is composed of a round transform repeated through several similar rounds.

Generic Attacks on Ciphers

- Security provided by an ideal block cipher defined by the best generic attack: exhaustive search for the key in $2^{|K|}$.

  $\Rightarrow$ typical key sizes $|K| = 128$ to 256 bits.

- Recovering the key from a secure cipher must need at least $2^{|K|}$ operations.

Cryptanalysis: Foundation of Confidence

- Ideal security defined by generic attacks.
  Does real security meet this ideal one?
  Need of continuous security evaluations

> Any attack better than the generic one
> is considered a "break".

- We are often left with an empirical measure of the security: Cryptanalysis.

Current scenario

- Competitions (AES, SHA-3, eSTREAM, CAESAR, LW..).
- New needs: Lightweight, FHE-friendly, easy-masking.

$\Rightarrow$ Many good proposals/candidates.

- How to choose?
- How to be ahead of possible weaknesses?
- How to keep on trusting the chosen ones?

Cryptanalysis: Foundation of Confidence

When can we consider a primitive as secure?

- A primitive is secure as far as no attack on it is known.
- The more we analyze a primitive without finding any weaknesses, the more reliable it is.

Design new attacks + improvement of existing ones:

- essential to keep on trusting the primitives,
- or to stop using the insecure ones!

Very Important Notion: Security Margin

If no attack is found on a given cipher,
what can we say about its robustness?

The security of a cipher is not a 1-bit information:

- Round-reduced attacks.
- Analysis of components.

$\Rightarrow$ determine and adapt the security margin, which is the highest number of rounds reached by an attack.

On high complexities

When considering large keys, sometimes attacks breaking the ciphers might have a very high complexity far from practical *e.g.*. 2^{120} for a key of 128 bits.
Still dangerous because:

- Weak properties not expected by the designers.
- Experience shows us that attacks only get better.
- Other existing ciphers without the "ugly" properties.

- When determining the security margin:
  Allows to compare primitives and to anticipate problems.

Post-Quantum Symmetric Cryptography

Post-Quantum Cryptography

Adversaries have access to **quantum computers.**

Asymmetric (e.g. RSA):

Shor's algorithm: Factorization in polynomial time

$\Rightarrow$ current systems not secure!

Solutions: lattice-based, code-based cryptography...

Symmetric (e.g. AES):

Grover's algorithm: Exhaustive search from $2^{|K|}$ to $2^{|K|/2}$.

Double the key length for equivalent ideal security.

Much to learn about cryptanalysis of current ciphers when having quantum computing available.

Post-Quantum Cryptography

Problem for present existing long-term secrets.
$\Rightarrow$ start using quantum-safe primitives NOW.

Important tasks:

- Conceive the cryptanalysis algorithms for evaluating the security of symmetric primitives in the P-Q world.

- Use them to evaluate and design symmetric primitives for the P-Q world.

On Quantum Attacks

- Compare to best generic attack,
- generic attack is accelerated, so
- broken classical primitive might be unbroken in a quantum setting:

e.g. a primitive might not have 256-bits security against a classical adversary but might have 128-bit security against a quantum one.

Scenarios and Models

Considered Scenarios

- **Model Q_0**
  classical attacks with classical computers.
- **Model Q_1**
  Q_0 + access to a quantum computer.
- **Model Q_2**
  Q_1 + superposition queries to a quantum cryptographic oracle (QCO).
- **Model Q_3**
  Q_1 + superposition queries with the differences of a secret key in a QCO.

Model Q_0

Nothing new here.

Model Q_1

- So far, the best we have obtained is a quadratic speed-up, but it can be smaller.
  Regarding exhaustive search:
  - If a primitive is safe[1] in Q_0,
    it will also be in Q_1.
- Does this mean that (so far) these Q_1 scenario/results are not interesting?

No!

[1] safe = no attack better than generic attack

Model Q_1

- Until recently, the best we have obtained was a quadratic speed-up, but it can be smaller.
  Regarding exhaustive search:
  - If a primitive is safe in Q_0,
    it will also be in Q_1.
- Are Q_1 scenario/results not interesting?

No!

Model Q_1

1) In a post-quantum future:

- Classical or quantum surnames will disappear:
  Expected security given by their best generic attack (*e.g.* Grover).
  And security margin? $\rightarrow$ determined by the highest number of rounds cryptanalyzed with any attack more performant than generic.
- Q_1 results: important information needed for determining the unique and future security margin.

Model Q_1

2) Regarding Collisions this is a bit different, as quantum collision speed-up is less than quadratic:

Hosoyamada and Sasaki 2020: showed that we could build quantum rebound attacks on hash functions that reach more rounds than classical attacks!

Model Q_2

Very powerful, BUT...

Many good reasons to study security in this scenario:

- Simple: used in security proofs.
- Non-trivial: Many constructions still seem resistant.
- Inclusive of all intermediate scenarios: protocols, obfuscation, hybrid machines, incompetent users...

Model Q_2

Defined and used in many results:

[Zhandry12], [Boneh-Zhandry13], [Damgård et al13], [Mossayebi-Schack16], [Song-Yun17], [Ito et al19], [Cid et al20], Simon's attacks, FX, AEZ...

An attack in this model $\Rightarrow$ we need to be extra careful when implementing the primitive in a quantum computer and using it in certain applications.

Ideas have proved useful for improving Q_1 attacks.

Model Q_3

Super strong model:

Everything is broken [Roetteler-Steinwandt 15]

Too strong model!

Another scenario classification

Different types of memory:

- Classical memory,
- Small amount of qubits,
- QRAM memories (QRACM or QRAQM).

Less complex memory, less amount $\Rightarrow$
more realistic scenario

Evolution

First Results

- Quantum analysis of CubeHash [Leurent 10]
- Simon on 3-round Feistel [Kuwakado Morii 10]
- Simon on Even-Mansour [Kuwakado Morii 12]
- Quantum MITM iterated ciphers [Kaplan14]
- Quantum Related-Key [Roetteler-Steinwandt15]
- Simon on modes+slides[Kaplan-Leurent-Leverrier-NP16b][Santolli-Schaffner17]
- Difflinear [Kaplan-Leurent-Leverrier-NP16b]

Quantum Symmetric Cryptanalysis

Many new results since:

FX [Leander-May17], parallel multi-preim. [Banegas-Bernstein17], Multicollision [Hosoyamada-Sasaki-Xagawa17], Mitm Q1 [Hosoyamada Sasaki 18], DS Mitm Feistel [Hosoyamada Sasaki 18], Miss-in-the-middle [Xie, Yang 18], Feistel key-recovery [Dong, Wang 18], CCA on Feistel [Ito et al 19], Quantum Rebounds [Hosoyamada Sasaki 20], Simon's evaluations [Bonnetain, Jacques20] [Shi21] , Q1 better than quadratic[Bonnetain, Schrottenloher, Sibleyras21] ...

Main activity from QUASYModo

- Efficient Collisions [Chailloux NP Schrottenloher Asiacrypt17],
- On modular additions [Bonnetain NP Asiacrypt 2018]
- K-xor [Grassi NP Schrottenloher Asiacrypt2018] [NP Schrot EC20]
- AES quantum evaluation [Bonnetain NP Schrottenloher ToSC18]
- On quantum slide attacks [Bonnetain NP Schrottenloher SAC18]
- Off-line Simon [Bonnetain Hosoyamada NP Schrott. Sasaki AC19]
- Algos subset-sum [Bonnetain Bricout Schrottenloher Shen AC20]
- Saturnin[Canteaut Duval Leurent NP Perrin Pornin Schrot.ToSC20]
- QCB [Bhaumik Bonnet. Chailloux Leurent NP Schrot SeurinAC21]
- Q linearization attacks [Bonnetain Leurent NP Schrot. AC21]

Most Useful Quantum Tools

Some Quantum Tools...

...that have been useful so far.

- Amplitude Amplification (AA) /Grover
- Quantum Collisions
- Simon
- Kuperberg

Amplitude Amplification

Exhaustive search:
Given $f : \{0,1\}^n \to \{0,1\}$, find one element $x \in \{0,1\}^n$ such that $f(x) = 1$.

- Classical complexity: $\Omega(\frac{2^n}{|\mathsf{supp}(f)|})$.
- Quantum complexity [Brassard-Hoyer 97]: $\mathcal{O}\left(\sqrt{\frac{2^n}{|\mathsf{supp}(f)|}}\right)$.

Quantum Collision Algorithms

Collision problem: Given a random function $H : \{0,1\}^n \to \{0,1\}^n$, find $x, y \in \{0,1\}^n$ with $x \neq y$ such that $H(x) = H(y)$.

- Classical complexity: $\Omega(2^{n/2})$.
- Quantum complexity: [Brassard-Hoyer-Tapp 97] $\mathcal{O}\left(2^{n/3}\right)$ in queries, in time and in quantum memory

Simon's algorithm

Simon's problem:

Given $f : \{0,1\}^n \to \{0,1\}^n$ such that
$\exists s \mid f(x) = f(y) \iff [x = y \text{ or } x \oplus y = s]$,
find s.

- Classical complexity: $\Omega(2^{n/2})$.
- Quantum complexity [Simon 94]:
  $T = \mathcal{O}\left(n^3\right), D = \mathcal{O}\left(n\right)$

Kuperberg's algorithm

Hidden Shift Problem with modular addition:
Let f, g be two injective functions, $(\mathbb{G}, +)$ a group. Given the promise that there exists $s \in \mathbb{G}$ such that, for all x, $f(x) = g(x + s)$, retrieve s.

- Classical complexity: $\Omega(2^{n/2})$.
- Quantum complexity: [Kuperberg 05] $2^{\widetilde{\mathcal{O}}(\sqrt{n})}$.

Some new Results
New useful Quantum Tools

Some New Tools

New quantum tools for cryptanalysis:

- New Quantum Collision Algorithm
- Quantum K-xor Algorithms
- Multicollisions
- Grover-meets-Simon
- Off-line Simon
- Simon-meets-Kuperberg
- Framework for quantizing classical attacks
- Quantumly efficient DDT equivalent...

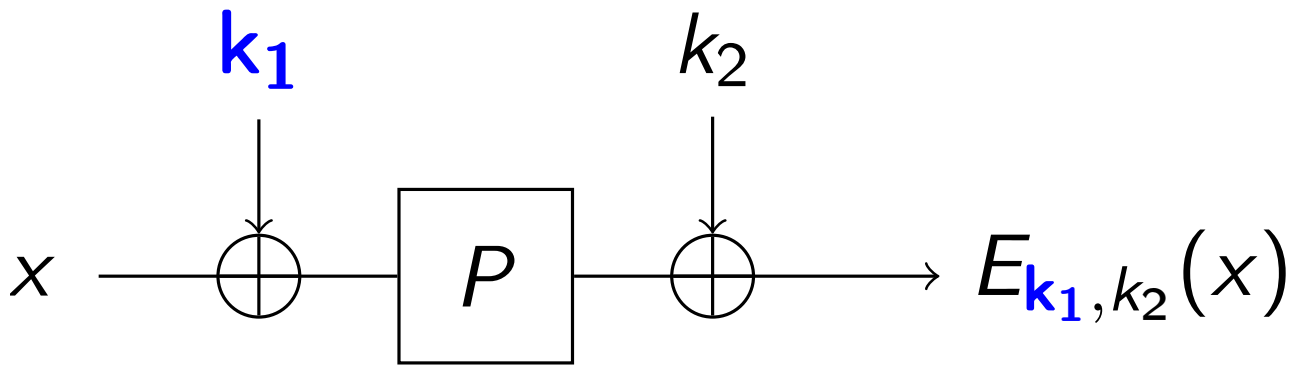
Recent Quantum Cryptanalysis: Illustrative Case

Outline of the case

- Even-Mansour Construction
- Best generic classical attacks
- Best quantum attacks in Q1 and Q2
- FX construction - Grover-meets-Simon Q2
- Reducing the queries
- Off-line Simon.
- Better than quadratic in Q1.

Even-Mansour [EM97]

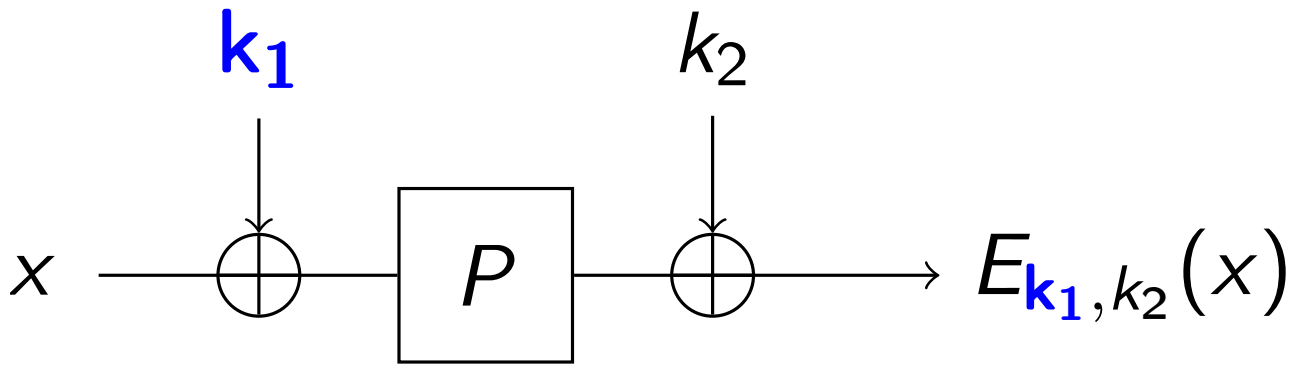
From a public random permutation
$P : \{0,1\}^n \to \{0,1\}^n$ and
$2n$ bits of key, k_1 and k_2:



Even-Mansour [EM97]

Any classical attack requires $T \times D \geq 2^n$.

Ex1) Guess $k_1 \Rightarrow k_2$: $D = 2$ and $T = 2^n$.



Ex2)Collision search on f:

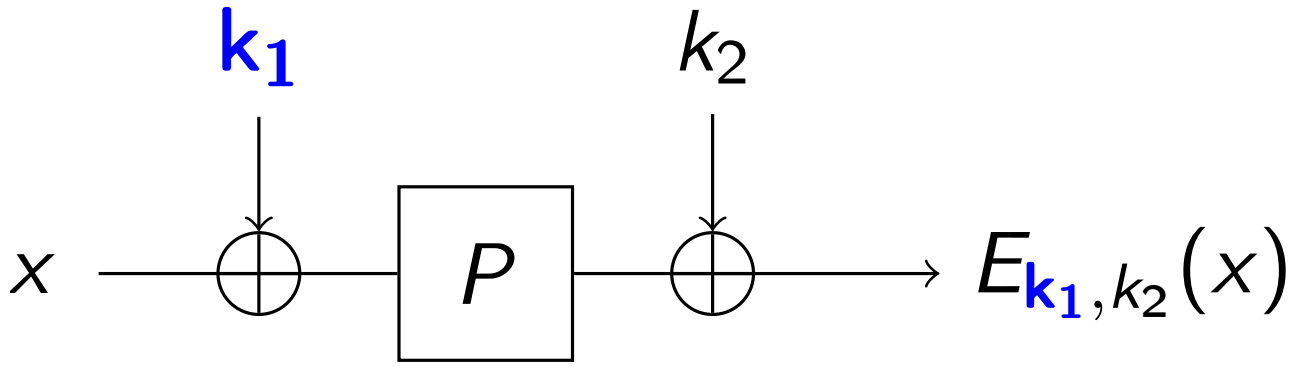
$f(x) = E_{k_1,k_2}(x) \oplus P(x) = k_2 \oplus P(x) \oplus P(x \oplus k_1)$

as $f(x) = f(x \oplus k_1)$, with $T = D = 2^{n/2}$.

All calls to f are queries $\rightarrow D \geq 2^{n/2}$

Even-Mansour [EM97]

Any classical attack requires $T \times D \geq 2^n$.

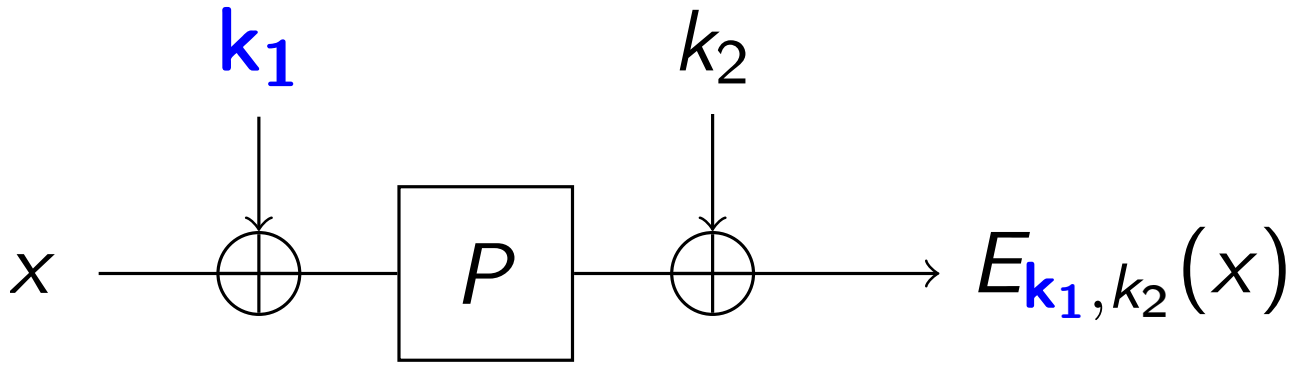


Ex3)We can define $h(x)$ and $g(x)$ [Daemen 91]:

$h(x) = E_{k_1,k_2}(x) \oplus E_{k_1,k_2}(x \oplus 1)$ and
$g(x) = P(x) \oplus P(x \oplus 1)$ (not queries).
We have $\forall x, g(x \oplus k_1) = h(x)$.
Complexity: D and $T = 2^n/D$

Even-Mansour [EM97]

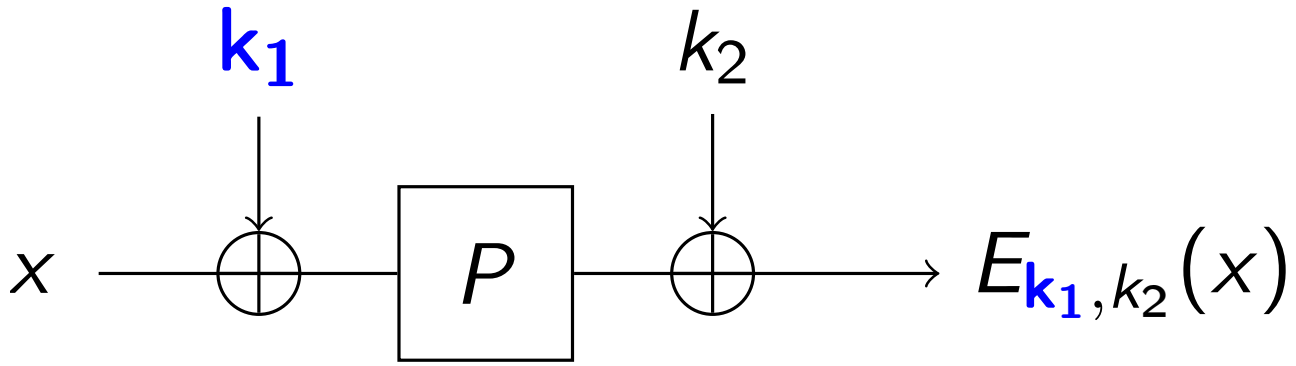
And quantumly?



Even-Mansour Q1 A [KM12]

And quantumly?

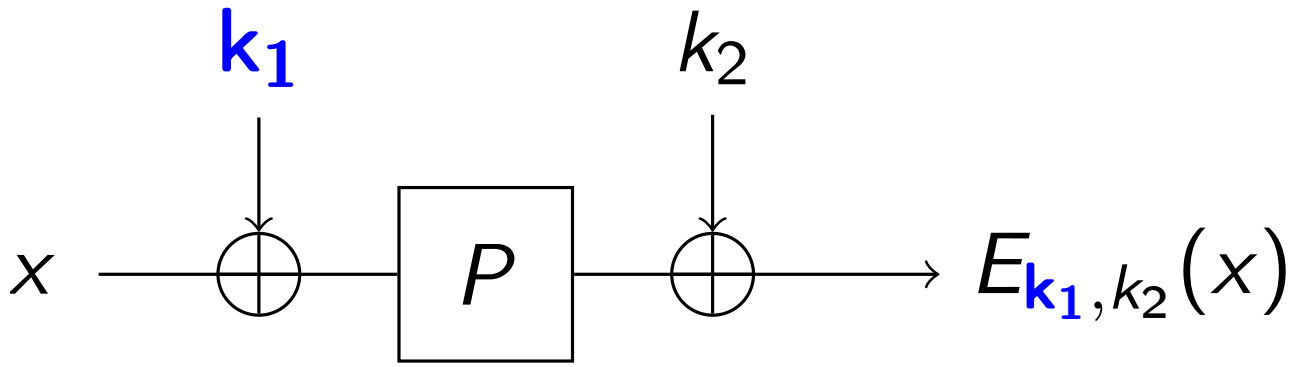
We could use BHT with h and g:
$D \times T^2 = 2^n$ needs D qRAM.



Even-Mansour Q1 B [HS18]

And quantumly?

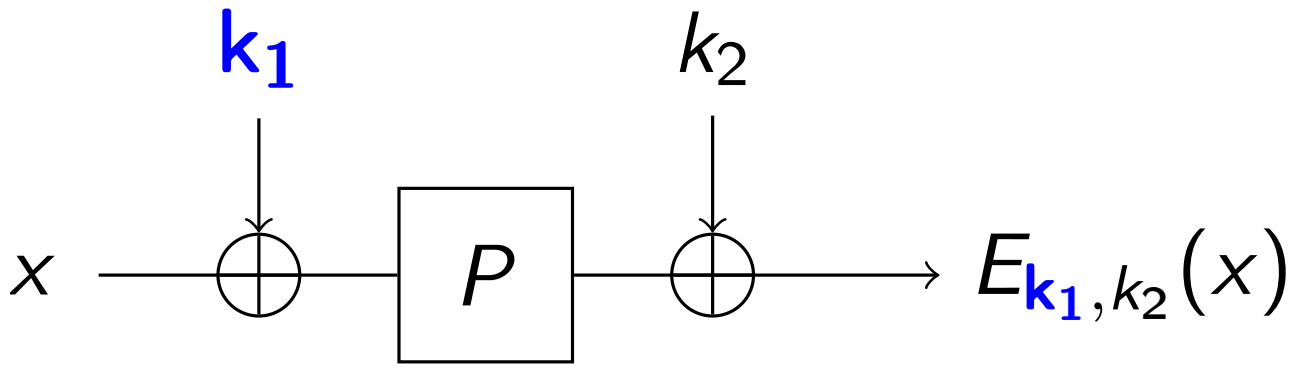
We could use [CNPS17] and no qRAM (but classical memo$= 2^{n/7}$):
$D = T = 2^{3n/7}$



Even-Mansour Q2 [KM12]

And quantumly?

In Q2 we can directly use Simon on f:



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

that has a secret period k_1: we can recover it in polynomial time.

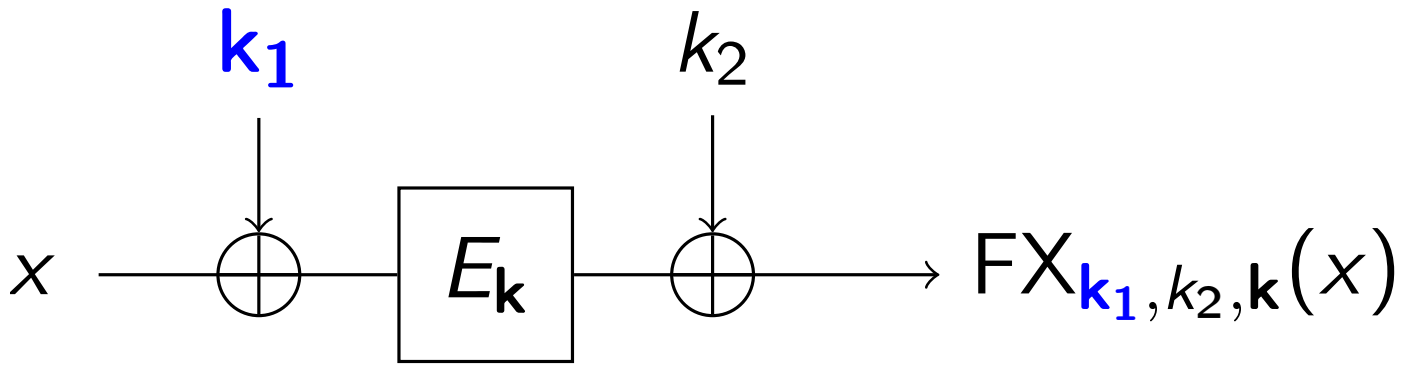
Even-Mansour

Previously open questions:

- Could we improve previous attacks?
- Could we use Simon's algorithm in Q_1?

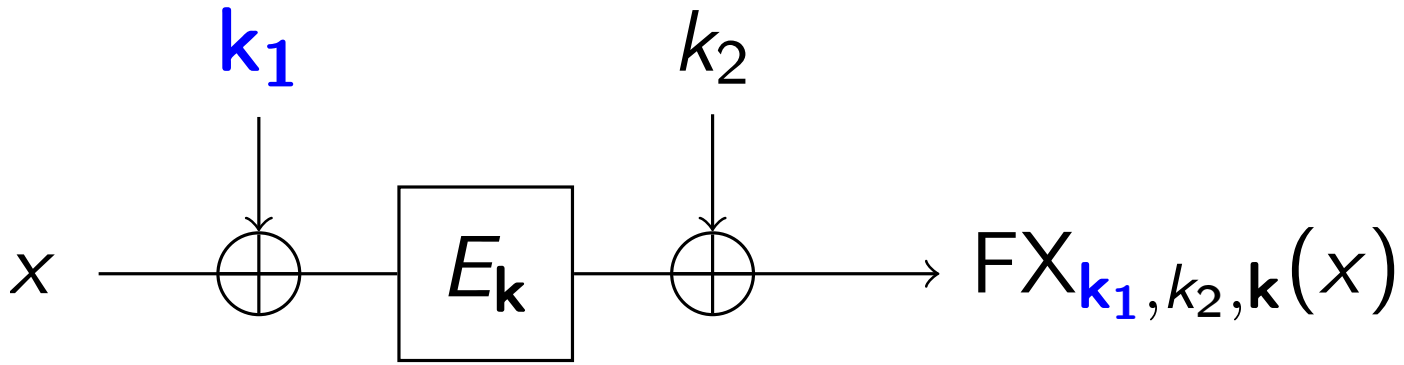
Let us have a look at FX first...

The FX construction



Classically, verifies $T \times D \geq 2^{2n}$.

Grover meets Simon [LM17]

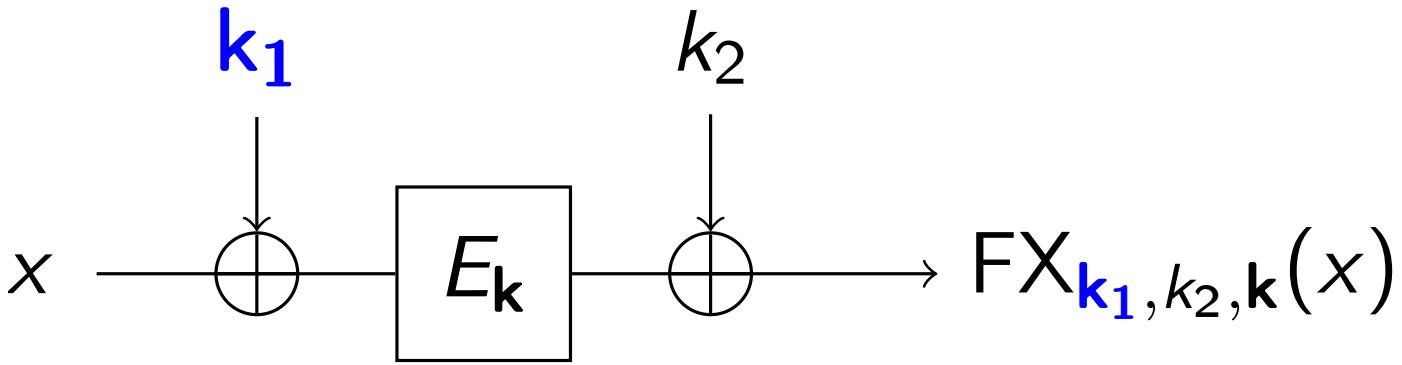


In Q2: Grover search on the cipher key k with variable k' and use as a test Simon's attack on Even-Mansour to check if the corresponding function $f_{k'}$ has a period:

$f_{k'}(x) = FX_{k,k_1,k_2}(x) \oplus E_{k'}(x)$

$T = n^3 \times 2^{n/2}$ $D = n \times 2^{n/2}$

Reducing D: Idea [BHNPSS19]



$f_{k'}(x) = FX_{k,k_1,k_2}(x) \oplus E_{k'}(x)$

Depends on encryption oracle, but not on k'

Depends on guess k' but not on encryption oracle

In order to reduce D, makes sense to make only one superposition query to FX_{k,k_1,k_2} and reuse it.

Reducing D: Idea [BHNPSS19]

$$f_{k'}(x) = FX_{k,k_1,k_2}(x) \oplus E_{k'}(x)$$

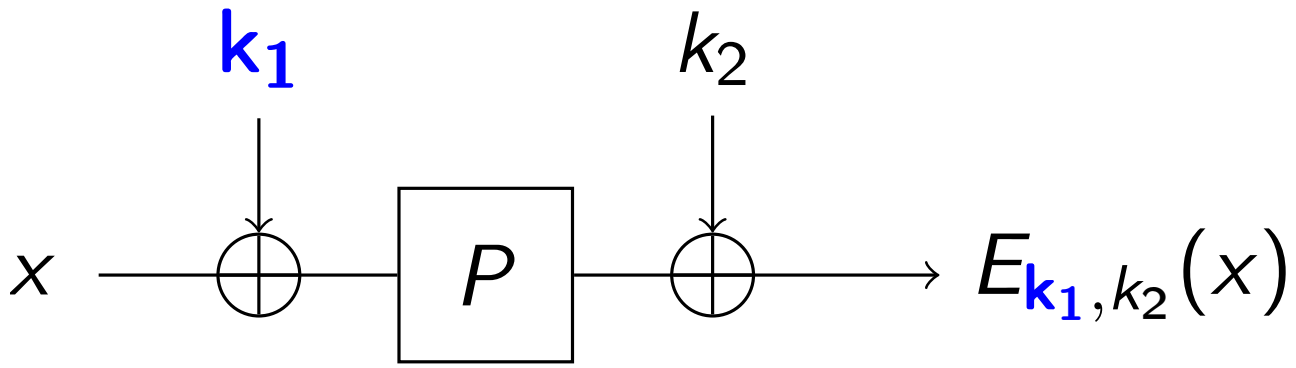
Precompute $\mathcal{O}(n)$ states with a superposition query to $FX_{k,k_1,k_2}(x)$.

Grover iteration test: compute the superposition of the $E_{k'}(x)$, on the precomputed states,
check with Simon if it's periodic,
and next un-do the computation to go back to the original states.

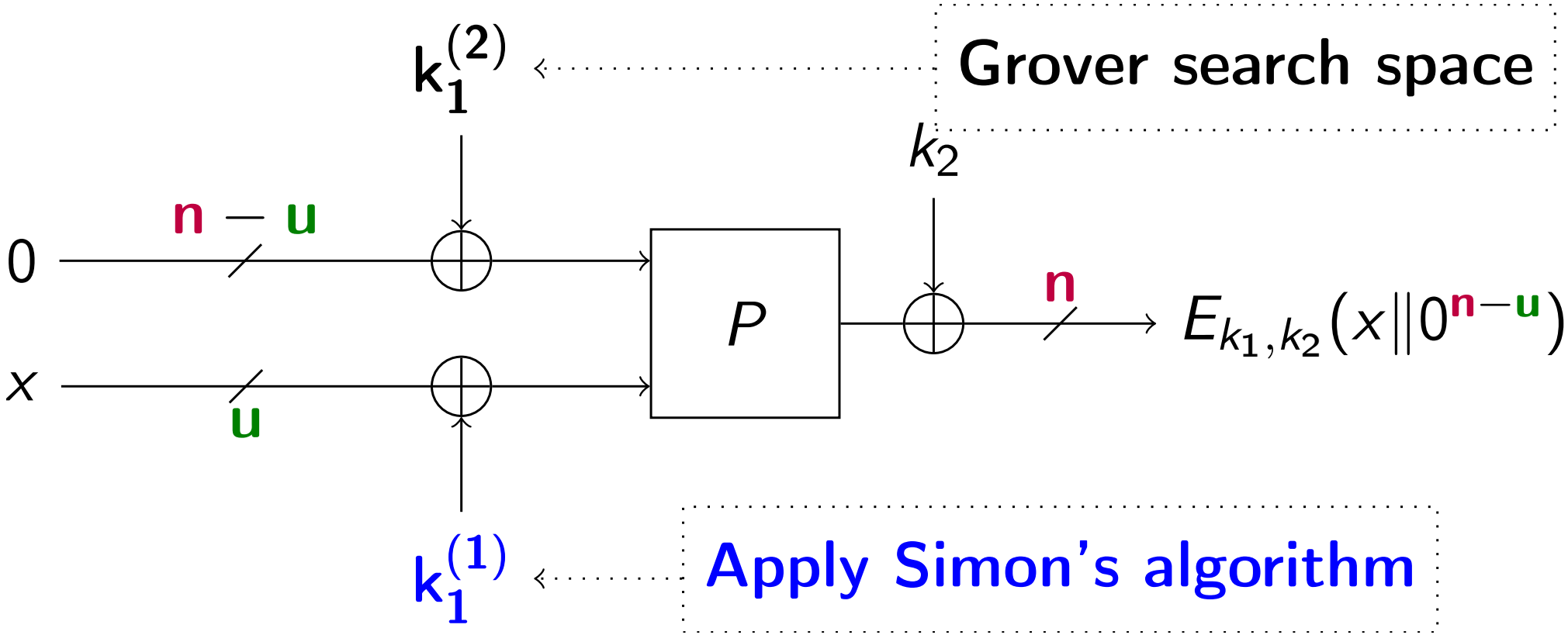
$D = \mathcal{O}(n)$ instead $D = 2^{n/2}$ with the same $T = \mathcal{O}(n)\, 2^{n/2}$.

Simulating Q2 queries

Can we apply Simon in Q1?
First ideas: We could perform classical queries and superpose them later simulating a Q2 query.
BUT it would need 2^n D and T
$\Rightarrow$ not very interesting.

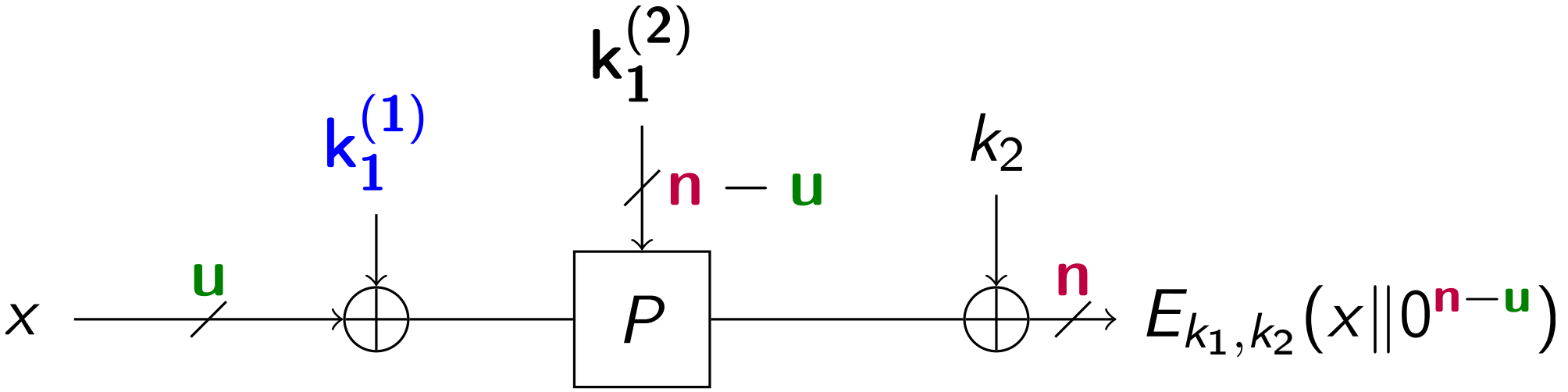


Off-line Simon



Off-line Simon [BHNPSS19]

$(n-u)$ k_1 bits guessed with Grover.
The remaining u bits: Simon's secret period.
We can simulate the superposition query in 2^u



$D = 2^u$ and $T = 2^u + 2^{(n-u)/2}$ which implies $DT^2 = 2^n$

Comparison [BHNPSS19]

EM:

Model	Queries	Time	Q-memory	C-memory	Reference
Q2	$\mathcal{O}(n)$	$\mathcal{O}(n^3)$	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$	[KM12]
Q1	$\mathcal{O}(2^{n/3})$	$\mathcal{O}(2^{n/3})$	$\mathcal{O}(2^{n/3})$	$\mathcal{O}(2^{n/3})$	[KM12]
Q1	$\mathcal{O}(2^{3n/7})$	$\mathcal{O}(2^{3n/7})$	$\mathcal{O}(n)$	$\mathcal{O}(2^{n/7})$	[HS18]
Q1	$\mathcal{O}(2^{n/3})$	$\mathcal{O}(n^3 2^{n/3})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	[BHNPSS19]

FX:

Q2	$\mathcal{O}(n2^{m/2})$	$\mathcal{O}(n^3 2^{m/2})$	$\mathcal{O}(n^2)$	0	[LM17]
Q2	$\mathcal{O}(n)$	$\mathcal{O}(n^3 2^{m/2})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	[BHNPSS19]
Q1	$\mathcal{O}(2^{3(m+n)/7})$	$\mathcal{O}(2^{3(m+n)/7})$	$\mathcal{O}(n)$	$\mathcal{O}(2^{(m+n)/7})$	[HS18]
Q1	$\mathcal{O}(2^{(m+n)/3})$	$\mathcal{O}(n^3 2^{(m+n)/3})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	[BHNPSS19]

Conclusion [BHNPSS19]

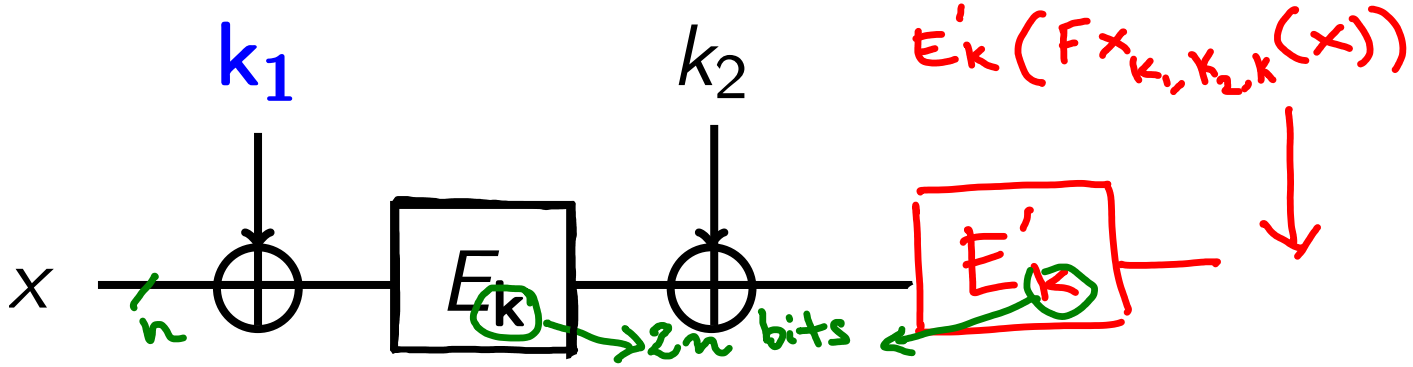
- Best known attacks on Q1 and Q2 for EM and FX (improves memory and queries).
- Simon in Q1
- There are other applications (slides, related-key in Q1)

Is a better than quadratic speed-up possible?

$\Rightarrow$ YES [Bonnetain, Schrottenloher, Sibleyras 21].

Q_1 Better than quadratic [BSS21]

- 2-xor Cascade [Gazi Tessaro EC 2012]



Classical security: $2^{2n}2^{n/2} = 2^{2.5n}$

Quantum security [Bonnetain Schrottenloher Sibleyras 21]:

off-line Simon, we have 2^n computations and 2^n classical queries.

Open Problems

Many Open problems

- New quantum attacks: QFT and linear cryptanalysis ?
- Quantum security evaluation of primitives(LW)
- Design of primitives with bigger states
- Generic key-length/state extensions?
- Improved quantum attacks on hash functions?
- Evaluating quantum implementation of algorithms
- Integral/Saturation cryptanalysis...

Final Conclusion

General Conclusion (for now) 1/2

- No reason to panic, symmetric crypto seems to be holding on well
- Bigger internal states/keys? How?
- Ideas from quantum analysis might improve classical analysis
- Many things yet to do to precisely evaluate security, to find best attacks, to adjust parameters...

General Conclusion (for now) 2/2

- What about Q2? No consensus:
  Surprising-scary results vs useless model?

- IMHO: Very strong model but when possible, better to avoid Q2 attacks: symmetric modus operandi works well in part because we are never too paranoid: (attacks on 2^{200} declare ciphers broken,...)

- Q2 attacks have improved Q1 attacks.

Quantum-Safe Symmetric Primitives

Lots of things to do !

[1]Many thanks to André Schrottenloher, Xavier Bonnetain, Anne Canteaut, Gaetan Leurent, Anthony Leverrier...

ERC QUASYModo

https://project.inria.fr/quasymodo/