Preparing Symmetric Crypto for the Quantum World

María Naya-Plasencia

Inria, France

ERC project QUASYModo

FSE 2019

Paris – March 26 2019

Preliminaries...

No quantum knowledge needed for following this talk

Outline

- ▶ **Introduction**

  Motivation, scenarios and evolution

- ▶ **Useful quantum tools**

- ▶ **Presentation of some results**

  - • Building new useful quantum tool: collision and k-xor algorithms

  - • Some quantum attacks (Simon +)

- ▶ **Final conclusion and Open problems**

Motivation

Cryptanalysis: Foundation of Confidence

▶ Ideal security defined by generic attacks $(2^{|K|})$. Does real security meet this ideal security? Need of continuous security evaluation.

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

▶ We are often left with an empirical measure of the security: cryptanalysis.

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.

Very Important Notion: Security Margin

▶ Best attacks determine the security margin $\Rightarrow$ Possibly with high complexities: find the highest number of rounds reached.

▶ Allows to compare primitives.

▶ The estimates of security margin need to be precise and correct in order to be meaningful.

Post-Quantum Cryptography

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 $2^{|K|} \rightarrow 2^{|K|/2}$

Double key length for equivalent ideal security.

Much to learn about cryptanalysis 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:

  • If a primitive is safe in Q_0, it will also be in Q_1.

▶ Does this mean that **(so far)** the Q_1 scenario/results are not interesting?

No!

safe = no attack better than generic attack

Model Q_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? → 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_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-Funder-Nielsen-Salvail13], [Mossayebi-Schack16], [Song-Yun17], 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.

Model Q_3

Super strong model:

Everything is broken [Roetteler-Steinwandt 15]

Too strong model!

Another scenario classification

Scenario A) With big quantum memory or

Scenario B) quantum memory limited to $poly(n)$

The first one: interesting from a theoretical point of view and for considering trade-offs,

The second one: more "realistic" scenario.

Evolution

First Results

Quantum Symmetric Cryptanalysis:

- ▶ 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]

Quantum Symmetric Cryptanalysis

▶ In 2015/2016:

[Kaplan-Leurent-Leverrier-NP16] Simon on modes/slide attacks.

[Kaplan-Leurent-Leverrier-NP16b] Diff/linear.

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]...

Recent activity from QUASYModo

- ▶ Efficient Collisions [Chailloux NP Schrottenloher Asiacrypt17],

- ▶ Quantum cryptanalysis of AEZ [Bonnetain SAC17]

- ▶ On modular additions [Bonnetain NP Asiacrypt 2018]

- ▶ k-xor problem [Grassi NP Schrottenloher Asiacrypt2018]

- ▶ AES quantum evaluation [Bonnetain NP Schrottenloher 18]

- ▶ On quantum slide attacks [Bonnetain NP Schrottenloher 18]

- ▶ Quantum security analysis of CSIDH[Bonnetain Schrottenloher18]

- ▶ Optimal merging the k-xor problem [NP Schrottenloher 19]

- ▶ Improved low-qubit hidden shift algorithms [Bonnetain 19]

Some Useful Quantum Tools

Some Quantum Tools...

...that have been useful so far.

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

Amplitude Amplification (Grover's generalization)

> *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]: $\Omega(\sqrt{\frac{2^n}{|\mathsf{supp}(f)|}})$.

In detail, we will see later: $\mathcal{O}\left(\sqrt{\frac{2^n}{|\mathsf{supp}(f)|}}(s_T + f_T)\right)$.

Quantum Counting Algorithm

Distinguish a biased distribution:
Given a Bernouilli distribution, determine with high probability whether it has a parameter $1/2$ or $1/2 + \varepsilon$.

▶ Classical complexity: $\mathcal{O}\left(\frac{1}{\varepsilon^2}\right)$.

▶ Quantum complexity:
[Brassard-Hoyer-Tapp 98] $\mathcal{O}\left(\frac{1}{\varepsilon}\right)$.

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 $\to$ scenario A. (Scenario B later)

Simon's algorithm

Simon's problem:
Given $f : \{0,1\}^n \rightarrow \{0,1\}^n$ 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]: $\widetilde{\mathcal{O}}(n)$.

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 Useful Quantum Tools

- New Quantum Collision Algorithm
- Quantum K-xor Algorithms
- Multicollisions
- Grover-meets-Simon
- Simon-meets-Kuperberg
- Framework for quantizing classical attacks
- Quantumly efficient DDT equivalent
- Miss-in-the-middle search

Collision Search

with A. Chailloux, A. Schrottenloher

Collision Search Problem

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

Many applications: *e.g.* generic attacks on hash functions.

(Multi-target preimage search can be seen as a particular case).

Best known algorithms

	Time	Queries	Qubits	Classical Memory
Pollard	$2^{n/2}$	$2^{n/2}$	0	$O(n)$
Grover	$2^{n/2}$	$2^{n/2}$	$O(n)$	0
BHT	$2^{2n/3}*$	$2^{n/3}$	$O(n)*$	$2^{n/3}$
Ambainis	$2^{n/3}$	$2^{n/3}$	$2^{n/3}$	0

Considered Model

▶ The same one as in the previous collision quantum algorithms BUT we limit the amout of quantum memory available to a small amount $\mathcal{O}(n)$: scenario B instead of A.

▶ Available small quantum computers seem like the most plausible scenario.

▶ We are interested in the theoretical algorithm and we did not take into account yet implementation aspects.

Starting Point: BHT Algorithm

- Optimal number of queries,

- $\mathcal{O}(n)$ qubits (scenario B),

- But time?

BHT: Summarized procedure

▶ Build a list L of $2^{n/3}$ elements (classical memory),

▶ Exhaustive search for finding one element that collides: With AA, the number of iterations is: $(\frac{2^n}{2^{n/3}})^{1/2} = 2^{n/3}$.

▶ Testing the membership with L for the superposition of states costs $2^{n/3}$ with n qbits:

$$\text{Time: } 2^{n/3} + 2^{n/3}(1 + 2^{n/3}) \approx 2^{2n/3}$$

Can we improve this?

Let's build the list L with distinguished points e.g. $H(x_i) = 0^u \| z$, for $z \in \{0,1\}^{n-u}$.

The cost of building the list is bigger: $2^{n/3+u/2}$.

The setup of AA is bigger: $2^{u/2}$

The membership test stays the same: $|L| = 2^{n/3}$

BUT The number of iterations is smaller: $2^{n/3-u/2}$

Time: $2^{n/3+u/2} + 2^{n/3-u/2}(2^{u/2} + 2^{n/3}) \approx 2^{2n/3-u/2} + 2^{n/3+u/2}$

With optimal parameters

The cost will be optimized for a certain size of L:
$2^v \neq 2^{n/3}$.

Time: $2^{v+u/2} + 2^{\frac{n-v-u}{2}}(2^{u/2} + 2^v)$

For $v = n/5$, $u = 2n/5$: Time: $\widetilde{\mathcal{O}}\left(2^{2n/5}\right)$

Comparison

	Time	Queries	Qubits	Classical Memory
Pollard	$2^{n/2}$	$2^{n/2}$	0	$O(n)$
Grover	$2^{n/2}$	$2^{n/2}$	$O(n)$	0
BHT	$2^{2n/3}$	$2^{n/3}$	$O(n)$	$2^{n/3}$
Ambainis	$2^{n/3}$	$2^{n/3}$	$2^{n/3}$	0
New algorithm	$2^{2n/5}$	$2^{2n/5}$	$O(n)$	$2^{n/5}$

Example of Applications

▶ Hash functions: Collision and Multi-preimages time from $2^{n/2}$ to $2^{2n/5}$ and $2^{3n/7}$ (Q1). Ex.- time and queries for $n = 128$: Pollard rho$= 2^{64}$

vs

Ours $= 2^{51}$ with less than 1GB classical.

▶ Multi-user setting.

▶ Operation modes.

▶ Bricks for Cryptanalysis.

About Parallelization

▶ What about comparison with parallel rho?
This algo provides new trade-offs.
For comparison, previous example $n = 128$:
Parallel rho$= 2^{51}$ with 2^{13} processors

vs

Ours $= 2^{51}$ with less than 1GB classical.

▶ When both parallelized: up to $2^{n/3}$ processors this algorithm is more time-efficient than parallel rho.

Conclusion - Collision

New efficient collision search algorithm with small quantum memory (nothing *scary*, new trade-offs):

First algorithm with less than $2^{n/2}$ computations in scenario B.

Many applications in symmetric cryptography.

Open question: is it possible to meet the optimal $2^{n/3}$ in time with small quantum memory?

Quantum Efficient Algorithms for the k-xor Problem (and Update)

with L. Grassi, A. Schrottenloher

k-xor problem with random functions

> Given query access to a random function $H : \{0,1\}^n \rightarrow \{0,1\}^n$, find $x_1, \ldots, x_k$ such that $H(x_1) \oplus \ldots \oplus H(x_k) = 0$.

For us, equivalent to the case with k different random functions.

Many applications (with k-sum, similar algorithms apply), ex.: attacks on FSB, XLS, SWIFFT; correlation attacks.

The 3-xor problem

Find 3 elements that xor to 0: not much better than collision in classical setting.

Classically, no exponential time acceleration, only logarithmic:

Complexity of $\widetilde{\mathcal{O}}\left(2\right)^{n/2}$.

3-xor: Scenario B Algorithm

▶ 1st approach, distinguished point: $2^v = 2^{n/8}$, $T = 2^{3n/8}$
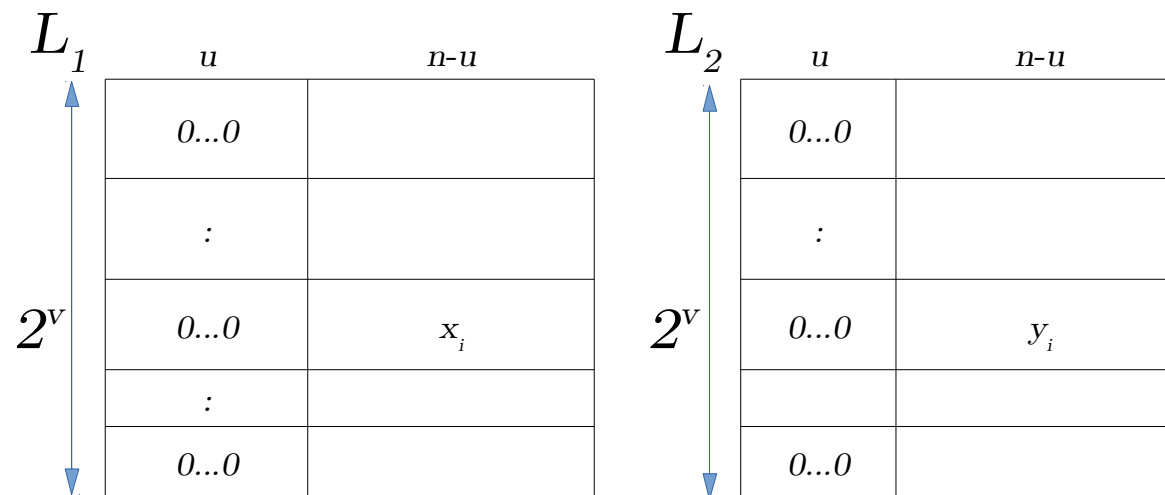
▶ Intuition: With a memory of $2^v + 2^v$ we obtain 2^{2v} potential collisions.

3-xor: Scenario B Algorithm

► 1st approach: $2^v = 2^{n/8}$, $T = 2^{3n/8}$

► 2nd approach, techniques linked to "list merging":
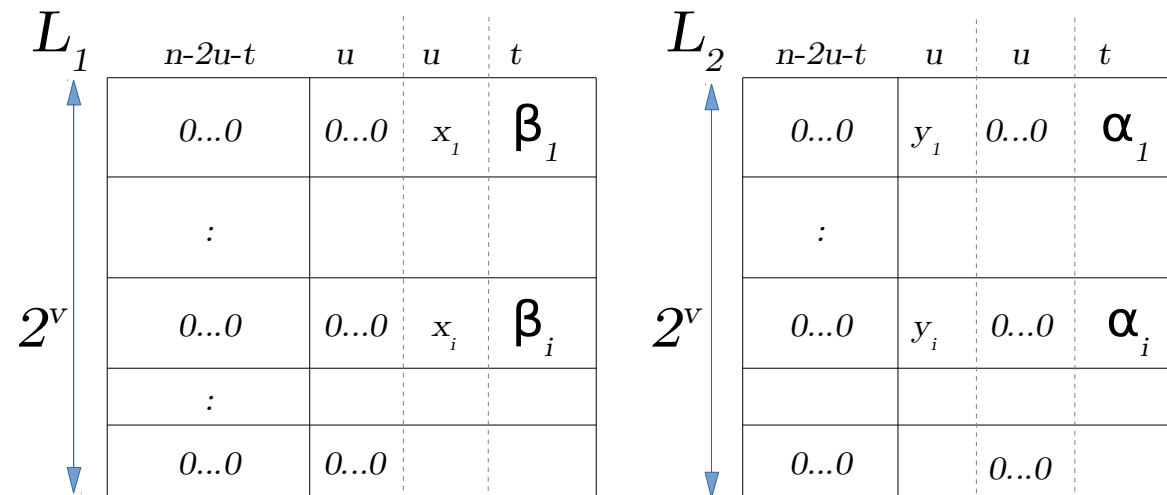
$$\text{Improved time} = 2^{5n/14}, \text{ with } 2^v = 2^{n/7}.$$

► Exponentially better than collision, contrary to classical!

3-xor: Scenario A Algorithm

- Same technique as before, but no need for a common prefix of zeroes.

- This gives
 QM$= 2^{n/5}$ and Time$= 2^{3n/10}$.

The k-xor algorithms
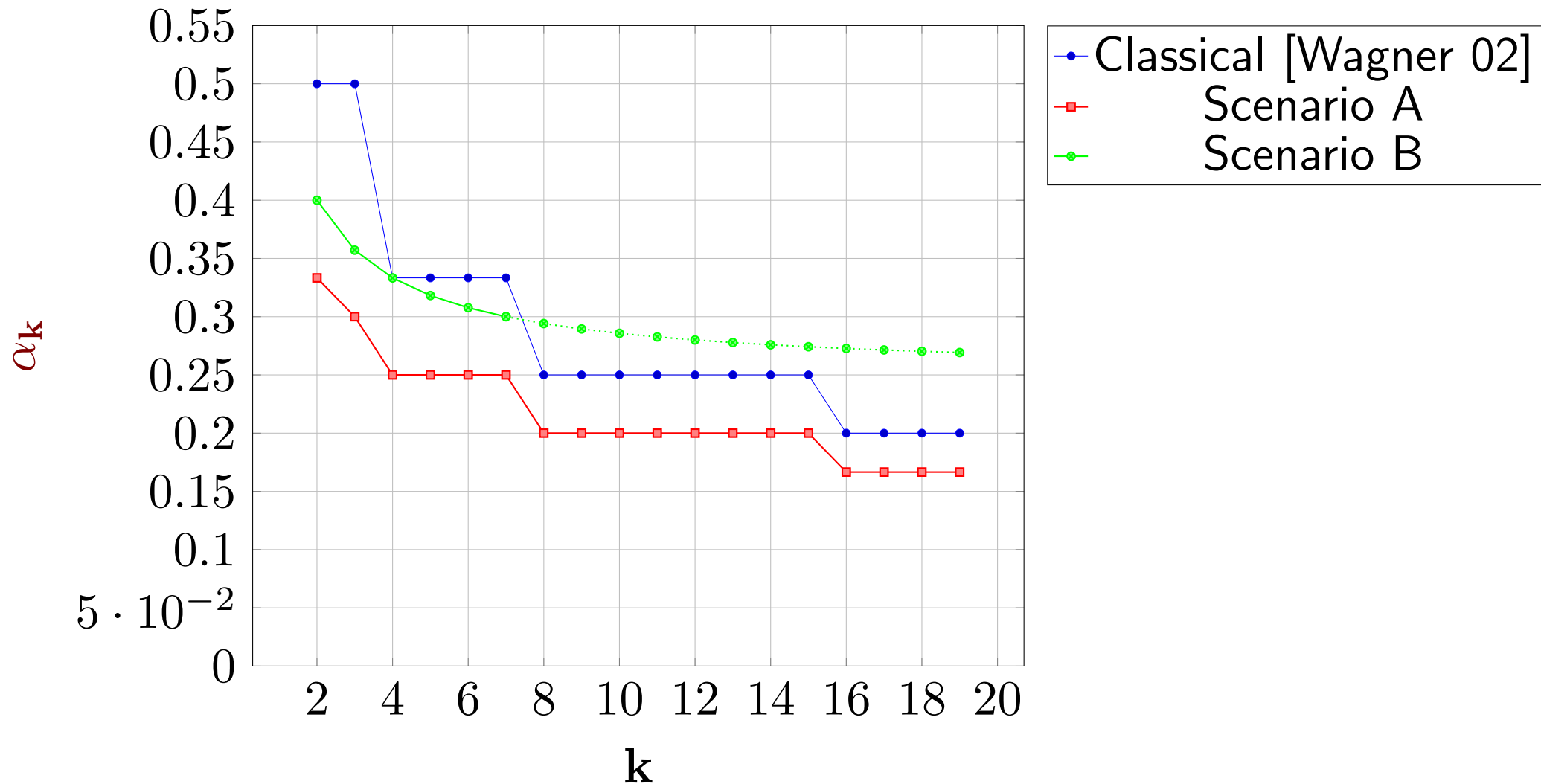
The time complexities are $\widetilde{\mathcal{O}}\left(2^{\alpha_{\mathbf{k}} n}\right)$

k-xor algorithms: Very Recent results

▶ Related to dissection: partial solutions to subproblems $n' < n$, $k' < k$ and combining them.

▶ When optimal? Not intuitive at all! $\Rightarrow$ Recursive MILP program for optimality in both scenarios.

Can we reach better complexities than $\widetilde{\mathcal{O}}\left(2^{n/(\lfloor \log_2(k) \rfloor + 2)}\right)$ when k is not a power of 2 in scenario A? Can we obtain time complexities better than classical for $k \geq 8$ in scenario B?

New Results: scenario B
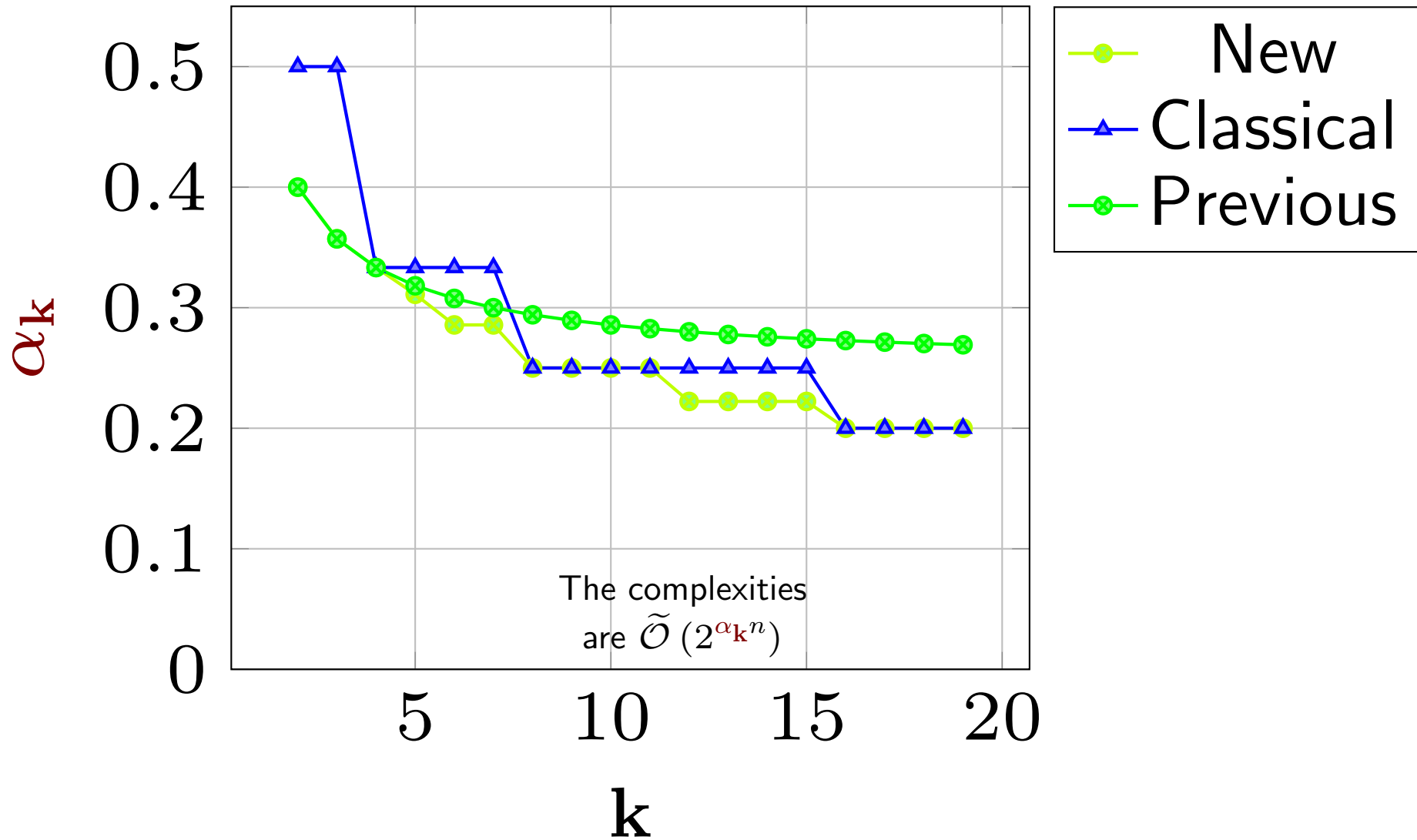
New Results: scenario A
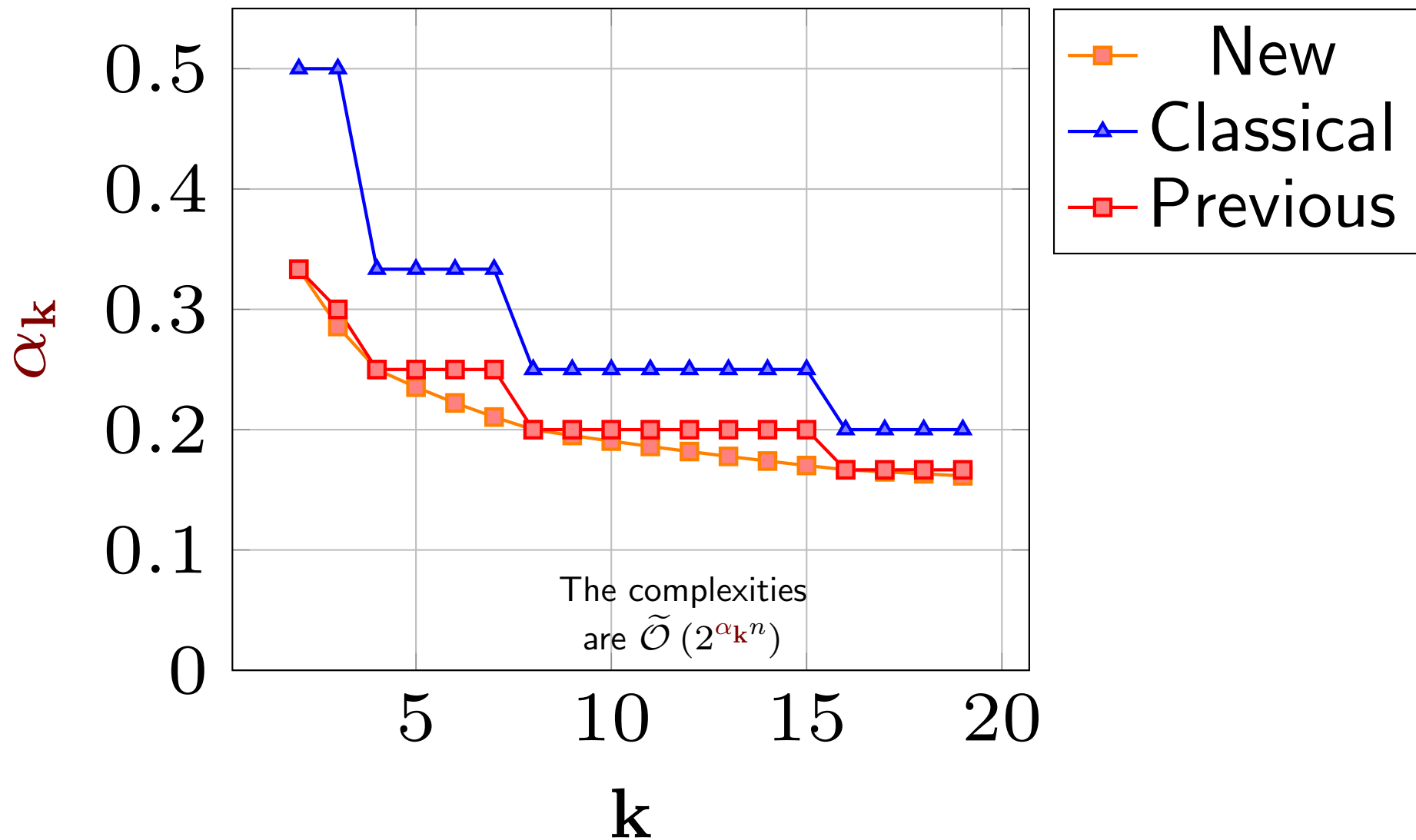
Conclusion - k-xor - Optimal Merging

- ▶ The quantum 3-xor problem is exponentially easier than the quantum collision problem (in both settings), contrary to classical.

- ▶ The time for solving the 3-xor problem in scenario A beats the lower bound for quantum collision of $2^{n/3}$

- ▶ For generic k, scenario B improves Wagner for half the values, and scenario A improves for all k (interpolated curve).

Some Results
on Quantum Attacks

New Quantum Attacks

- Differential/Linear
- Simon-based
- Kuperberg-based
- Slide attacks
- DS-MITM

And dedicated analysis:

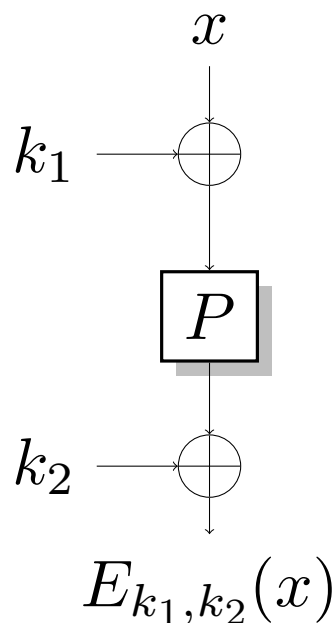- FX and Feistel constructions
- Q_2 attack on AEZ
- Q_2 attack on Poly-1305
- AES Quantum analysis

Simon and Kuperberg Attacks

with X. Bonnetain, M. Kaplan,
G. Leurent, A. Leverrier

Simon on Even-Mansour [Kuwakado Morii 12]

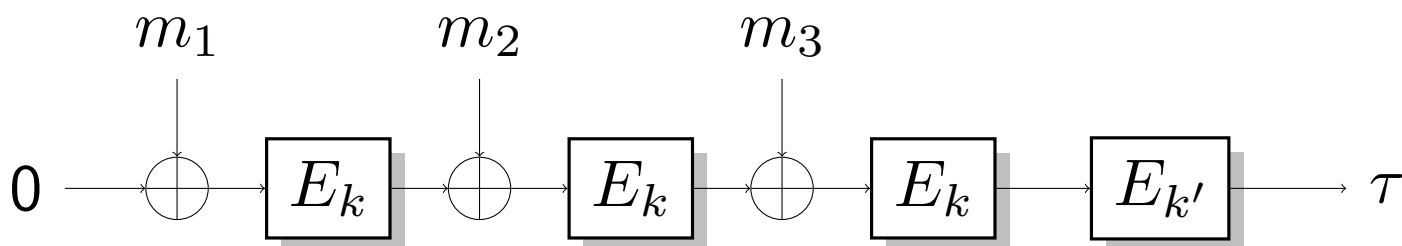▶ [Even-Mansour 97] cipher: $DT > 2^n$

$$f(x) = E_K(x) \oplus P(x) \rightarrow f(x) = f(x \oplus k_1)$$

Simon's algo on $f \Rightarrow k_1$ in $\mathcal{O}(n)$

[Kaplan-Leurent-Leverrier-NP 16]

Simon on most authentication modes + slide attacks

- ▶ For example encrypt-last-block CBC-MAC:

$$f : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$$

$$b, x \quad \mapsto \mathsf{CBCMAC}(\alpha_b\|x) = E_{k'}\big(E_k\big(x \oplus E_k(\alpha_b)\big)\big).$$

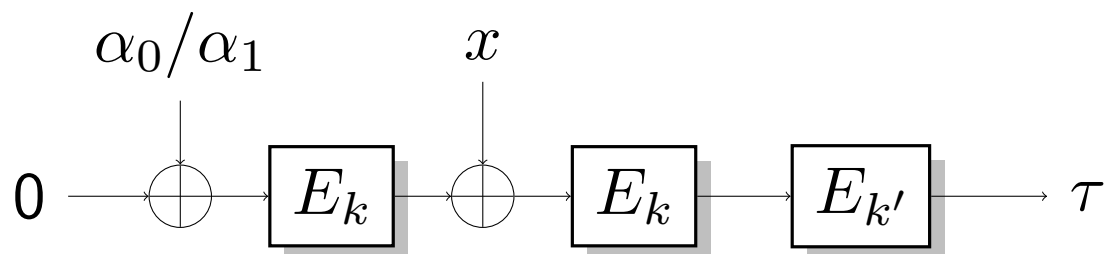$\mathsf{CBCMAC}(\alpha_1\|x \oplus E_k(\alpha_0) \oplus E_k(\alpha_1)) =$

$E_{k'}\big(E_k\big((x \oplus E_k(\alpha_0) \oplus E_k(\alpha_1)) \oplus E_k(\alpha_1)\big)\big) = \mathsf{CBCMAC}(\alpha_0\|x)$

$s = 1\|E_k(\alpha_0) \oplus E_k(\alpha_1)$

[Kaplan-Leurent-Leverrier-NP 16]

Simon on most authentication modes $+$ slide attacks

▶ For example encrypt-last-block CBC-MAC:

$$f : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$$
$$b, x \quad \mapsto \mathsf{CBCMAC}(\alpha_b \| x) = E_{k'}\big(E_k\big(x \oplus E_k(\alpha_b)\big)\big).$$

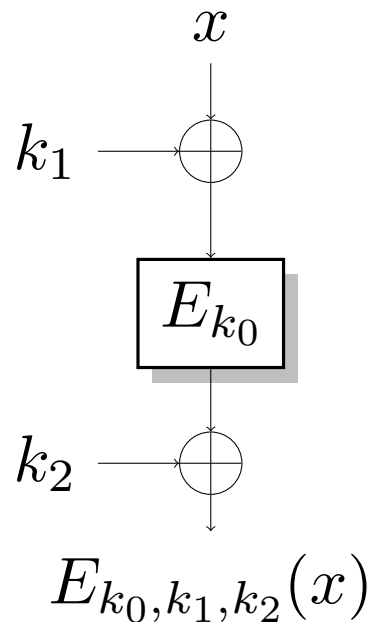$\mathsf{CBCMAC}(\alpha_1 \| x \oplus E_k(\alpha_0) \oplus E_k(\alpha_1)) =$

$E_{k'}\big(E_k\big((x \oplus E_k(\alpha_0) \oplus E_k(\alpha_1)) \oplus E_k(\alpha_1)\big)\big) = \mathsf{CBCMAC}(\alpha_0 \| x)$

$s = 1 \| E_k(\alpha_0) \oplus E_k(\alpha_1)$

Simon and Grover on FX construction

The FX construction is a natural construction for extending the key-length $n \Rightarrow 2n$.

$$x$$
$$k_1 \longrightarrow \oplus$$
$$\boxed{E_{k_0}}$$
$$k_2 \longrightarrow \oplus$$
$$E_{k_0,k_1,k_2}(x)$$

[Leander May 17] Combined Simon with Grover:
$\rightarrow$ broken in $O(2n2^{n/2})$

Tweaking to resist Simon's algo.?

▶ In [Alagic Russell 17] several proposals. Most efficient: replace xor by modular additions.

▶ Hidden shift problem in $\mathbb{Z}/(N)$.

▶ No algorithm in polynomial time: Kuperberg in $2^{O(\sqrt{n})}$

▶ Up to what point do primitives resist?

Motivation and results [Bonnetain-NP18]

- ▶ 4. Dimension symmetric primitives

- ▶ 1. More precise evaluation of Kuperberg's algorithm complexity+improvement

- ▶ 2. What about parallel modular additions?

- ▶ 3. New Quantum attacks (Feistel's slide, FX)

Improvement and Simulation

Our improvement: all the bits with one iteration.

$$O(n^2 2^{\sqrt{2\log_2(3)n}}) \Rightarrow O(n2^{\sqrt{2\log_2(3)n}})$$

Our simulations: $0.7 \times 2^{1.8\sqrt{n}}$ for recovering full s.
Code available: ask Xavier Bonnetain if interested.
`xavier.bonnetain@inria.fr`

Results - Conclusion

- Improved Kuperberg's algorithm and new algorithm for parallel modular additions.

- State size needed for 128-bit security.
  at least 5200 bits (but for FX)
  $\Rightarrow$ not very realistic.

- Might be better to just avoid vulnerable constructions, or try different patches.

- Recently: concrete security of some Isogeny-based primitives [Bonnetain-Schrottenloher]

Final Conclusion

General Conclusion (for now) 1/2

- ▶ No reason to panic, symmetric crypto seems to be holding on well

- ▶ Bigger internal states?

- ▶ Ideas from quantum analysis might improve classical analysis

- ▶ Many things yet to do to precisely evaluate security, to find best attacks, to adjust parameters...

► **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,...)

► At least: information worth knowing.

Aristotle?

Open problems

- Propose an efficient AE mode Q_2-safe
- New quantum attacks: QFT ?
- Quantum security evaluation of primitives(LW)
- Generic key-length extensions?
- Design of primitives with bigger state
- Time-memo Trade-offs for k-xor algorithms
- Evaluating quantum implementation of algorithms
- ...

Quantum-Safe Symmetric Primitives

Lots of things to do !

▶ And what about quantum asymmetric cryptanalysis??

Necessary to evaluate the concrete security of proposed primitives.

Possible links between both.

ERC QUASYModo

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

- ▶ 1 PhD position
- ▶ 1 PostDoc position