Starting transition towards products embedding post-quantum cryptography

Aline Gouget

Outine

- The dream of « Quantum computing »
- Why digital security companies should prepare for transition to post-quantum cryptography?
- Starting transition towards products embedding post-quantum cryptography, what it means?
- Hash-based signatures
- Lattice-based cryptography
- Implementation attacks
- Take out

The dream of « Quantum computing »

Hello, quantum world !

- Became a step closer to reality recently
  - 1998 – 2 qubits
  - 2000 – 4, 5, and then 7 qubits
  - 2006 – 12 qubits
  - 2011 – 14 qubits
  - 2017 –17, 49 qubits -> 56?
  - Measuring qubits is not best metric

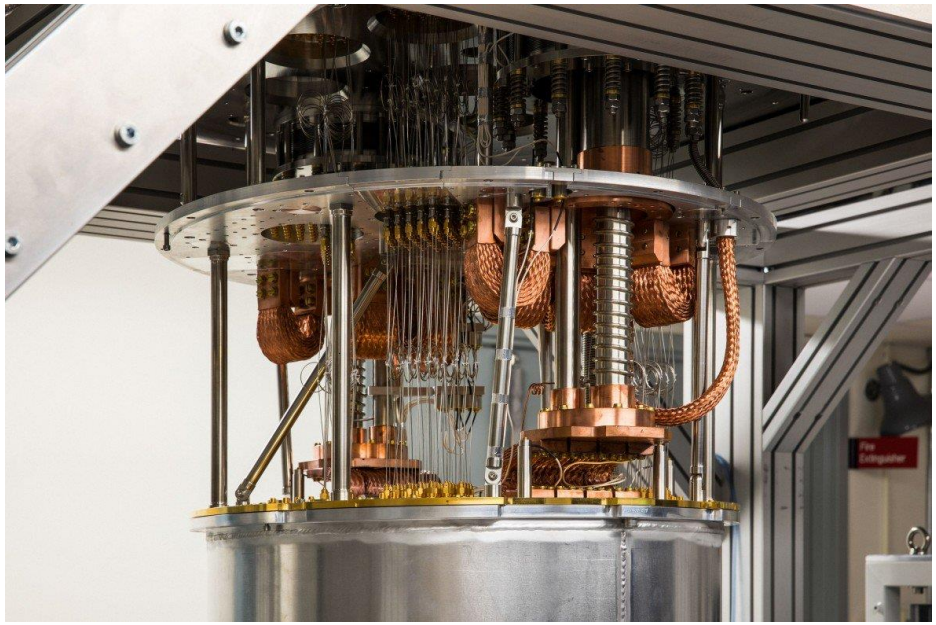
https://csrc.nist.gov/CSRC/media//Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf

  - New: 2018 - 72 qubits

gemalto

“[Quantum computing] is no longer a physicist’s dream It is an engineer’s nightmare”, Isaac Chuang, MIT

- “*We have this device that is more complicated than you can simulate on a classical computer, but it’s not yet controllable to the precision that you could do the algorithms you know how to do.*”, Jay Gambetta, MIT Technology Review 2018



Quantum computing, what for?

- *A NASA perspective on quantum computing: Opportunities and challenges*, R. Biswas et al., Parallel Computing, May 2017

  - « *For most problems, however,* ***it is currently unknown whether quantum algorithms can provide an advantage****, and if so by how much, or* ***how to design quantum algorithms*** *that realize such advantages.* »

  - « *Many of the most challenging computational* ***problems arising in the practical world are tackled today by heuristic algorithms*** *that have not been mathematically proven to outperform other approaches but have been shown to be effective empirically*. »

  - « *While quantum heuristic algorithms have been proposed, empirical testing becomes possible only as quantum computation hardware is built.* ***The next few years will be exciting*** *as empirical testing of quantum heuristic algorithms becomes more and more feasible*.»

Expected job 1 for quantum computers: boost AI

- "*There is a natural combination between the intrinsic statistical nature of quantum computing … and machine learning*", J. Otterbach, physicist at Rigetti Computing, Berkeley, California

- "*Manipulation of large matrices and large vectors are exponentially faster on a quantum computer*", S. Lloyd, physicist at the MIT

- So far, though, machine learning based on quantum matrix algebra has been demonstrated only on machines with just four qubits

- Google, Microsoft, IBM and other tech giants are pouring money into quantum machine learning

https://www.quantamagazine.org/job-one-for-quantum-computers-boost-artificial-intelligence-20180129/

Still, It could be a mirage

- Kalai, mathematician at Hebrew University in Jerusalem about quantum computing
  - « ***Quantum computing is*** *like any similar process in nature —* ***noisy****, with random fluctuations and* ***errors****. When a quantum computer executes an action, in every computer cycle there is some probability that a qubit will get corrupted.* »
  - « *We need what's known as* ***quantum error correction****. But this will require 100 or even 500 "physical" qubits to represent a single "logical" qubit of very high quality. And then to build and use such quantum error-correcting codes,* ***the amount of noise has to go below a certain*** *level, or* ***threshold****.* »
  - « *Many researchers believe that we can go beyond the threshold, and that constructing a quantum computer is merely an engineering challenge of lowering it. However,* ***our first result shows that the noise level cannot be reduced****,* ***because doing so will contradict an insight from the theory of computing about the power of primitive computational devices****.* »
  - « *So I don't need to be certain,* ***I can simply wait and see****.* »

https://www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207/

gemalto

Why digital security companies should prepare for transition to post-quantum cryptography?

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

gemalto
security to be free

NSA update on its cryptography strategy

- Back in august 2015, NSA explicitly talked about the threat of quantum computers

- "*Unfortunately, the growth of **elliptic curve** use has bumped up against the fact of continued progress in the research on quantum computing, **necessitating a re-evaluation of our cryptographic strategy**.“*

- "*we recommend not making a significant expenditure to [make the transition to Suite B] at this point but **instead to prepare for the upcoming quantum resistant algorithm transition.“***

- Then, subject tackled by NIST in 2016 with the announcement of NIST’s call for submissions on post-quantum public-key cryptography

How serious is the threat for cryptography in use?

The sky is falling?

- When will a quantum computer be built that breaks current crypto?
  - 15 years, $1 billion USD, nuclear power plant (to break RSA-2048) (PQCrypto 2014, Matteo Mariantoni)

[Dustin Moody NIST, Post-quantum Crypto 2016]
http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf

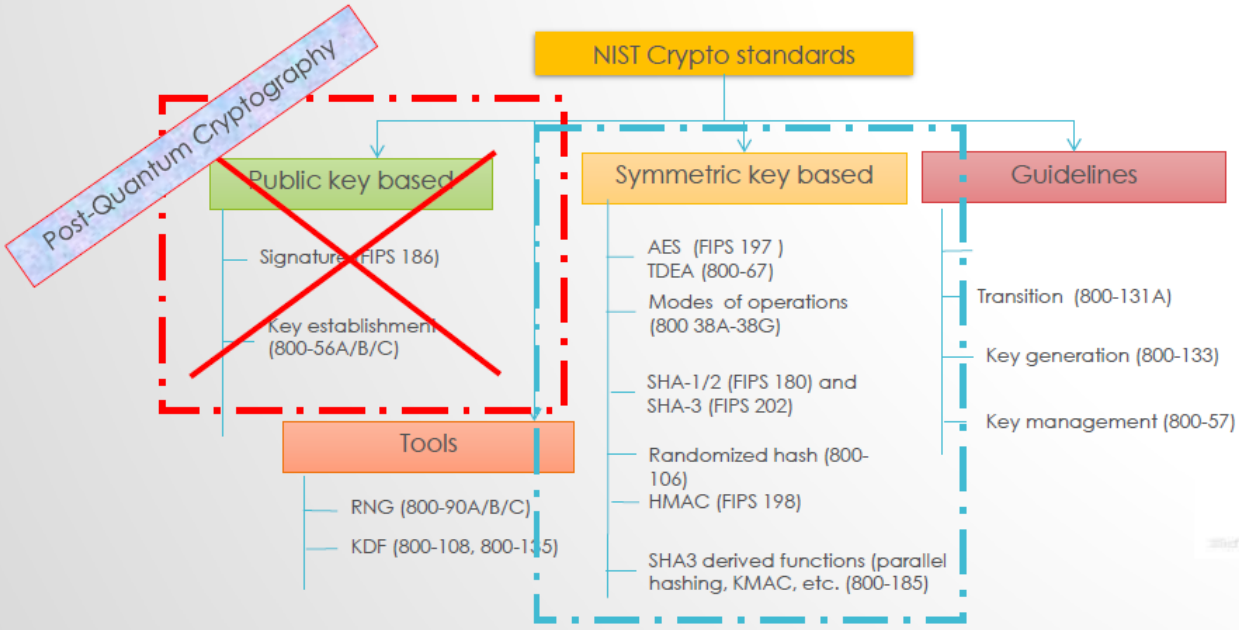
"1 in 7 chance key cryptography tools will be broken by 2026 and a 50% chance by 2031 "

Author: Michele Mosca,
Institute for Quantum Computing & Special Advisor on Cyber Security to the Global Risk Institute

gemalto

THE SKY IS FALLING?

- If a large-scale quantum computer could be built then....



https://csrc.nist.gov/CSRC/media//Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf

gemalto

THE DECISION TO MOVE FORWARD

- NIST decided **it is the time** to look into standardization
- We see our role as managing a process of achieving community consensus in a **transparent** and **timely** manner
- We do not expect to "pick a winner"
  - Ideally, several algorithms will emerge as 'good choices'

https://csrc.nist.gov/CSRC/media//Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf

NIST'S PQC ~~CONTEST~~ STANDARDIZATION PLAN

Timeline	
Nov. 30, 2017	Submission deadline
April 2018	Workshop – Submitters' presentations
3-5 years	Analysis phase - NIST reports on findings and more workshops/conferences
2 years later	Draft standards available for public comments

- NIST will post "complete and proper" submissions - Dec 2017
- NIST PQC Standardization Conference (with PQCrypto, Apr 2018)
- Initial phase of evaluation (12-18 months)
  - Internal and public review
  - No modifications allowed
- Narrowed pool will undergo a second round (12-18 months)
  - Second conference to be held
  - Minor changes allowed
- Possible third round of evaluation, if needed
- NIST will release reports on progress and selection rationale

https://csrc.nist.gov/CSRC/media//Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf

DIFFERENCES WITH AES/SHA-3 COMPETITIONS

- Post-quantum cryptography is more complicated than AES or SHA-3
  - No silver bullet - each candidate has some disadvantage
  - Not enough research on quantum algorithms to ensure confidence for some schemes
- We do not expect to "pick a winner"
  - Ideally, several algorithms will emerge as "good choices"
- We will narrow our focus at some point
  - This does not mean algorithms are "out"
- Requirements/timeline could potentially change based on developments in the field

https://csrc.nist.gov/CSRC/media//Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf

Current NIST crypto recommendations

TDEA (Triple Data Encryption Algorithm) and AES are specified in [10].
Hash (A): Digital signatures and hash-only applications.
Hash (B): HMAC, Key Derivation Functions and Random Number Generation.
The security strength for key derivation assumes that the shared secret contains sufficient entropy to support the desired security strength. Same remark applies to the security strength for random number generation.

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

All key sizes are provided in bits. These are the minimal sizes for security.

https://www.keylength.com/en/4/

ANSSI

I. ANSSI recommendations on cryptographic mechanisms

National guidelines: Référentiel Général de Sécurité

RGS version 2.0, **Annex B1**, v2.03, Feb. 2014

II. ANSSI views regarding post-quantum cryptography

III. SOG-IS guidelines (ongoing work)

Agreed Cryptographic Mechanisms

version 1.0, May 2016

http://risq.fr/pres/qsci_hg_30-01-2017.pdf

gemalto

ANSSI

RGS Annex B1 in a nutshell [3/4]

> some resulting requirements on parameter sizes

	symmetric primitives	hash functions	EC-DLOG on a subgroup of order q	RSA PB on Z/NZ	DLOG on GF(p)
recommended parameter lengths in bits	|key| ≥ 128	|hash| ≥ 256	|largest prime factor(q)| ≥ 256	|N| ≥ 3072	|p| ≥ 3072
tolerated i.e., compliant with rules **if not used beyond**	|key| ≥ 100 2020	|hash| ≥ 200 2020	|largest prime factor(q)| ≥ 200 2020	|N|≥ 2048 2030	|p|≥ 2048 2030

http://risq.fr/pres/qsci_hg_30-01-2017.pdf

gemalto

ANSSI

RGS Annex B1 in a nutshell [4/4]

- examples of other rules or recommendations
  - recommended block size for block ciphers: $n \geq 128$ bits
    - for blockciphers used beyond 2020, $n \geq 128$ bits is required
  - for encryption modes of operations
    - no IND-CPA attack of complexity less than $2^{n/2}$ must exist
    - modes supported by a proof of security are recommended
    - a combined use whith a message authentication mode is recommended
- examples of recent evolutions
  - RSA PB + DLOG: ≥ 3072 bits beyond 2030 instead of ≥ 4096 bits beyond 2020
  - DLOG on prime fields only (this was only recommended in former versions)
  - random number generators

http://risq.fr/pres/qsci_hg_30-01-2017.pdf

ANSSI

[II] Post-Quantum Cryptography (PQC)

> quantum computation threat (reminder)

- if large-scale quantum computers ever become a reality then:
  - currently deployed asymmetric cryptography will collapse [Shor95]
  - symmetric cryptography will also be to some extent affected [Grover96, Simon95]
- it is notoriously difficult to predict whether this will happen and when
  - « only a rash person would declare that there will be no useful quantum computers by the year 2050, but only a rash person would predict that there will be » [Mermin07]
  - one could replace 2050 by 2040 in the former statement
- anyway, this potential threat should obviously not be ignored
- while the issue has been debated for years, it was brought under the spotlights by the US CNSS advisory memorandum of July 2015

  « […] as we anticipate a need to shift to quantum-resistant cryptography in the near future »

http://risq.fr/pres/qsci_hg_30-01-2017.pdf

gemalto

Post-Quantum Cryptography: ANSSI views [1/2]

> the most promising medium/long term avenue to thwart the quantum threat

> however post-quantum asymmetric mechanisms proposed so far
[based on (ideal) lattices, codes, multivariate cryptography, isogenies, etc.]
are not yet sufficiently mature, well studied, standardized
to be immediately deployed as a drop-in replacement
for pre-quantum mechanisms based on the RSA, DLOG, and EC-DLOG problems

=> no short-term endorsement of such mechanisms in RGS Annex B1 is foreseen
[single potential exception: hash-based signatures]

http://risq.fr/pres/qsci_hg_30-01-2017.pdf

Post-Quantum Cryptography: ANSSI views [2/2]

> recognised symmetric mechanisms and hash functions

can be reasonably conjectured quantum-safe if their key / hash length is sufficiently large

[outside from the very strong security model of « quantum chosen message » attacks]

> hybrid mechanisms constructed over a recognised pre-quantum key exchange mechanism

while not harming the pre-quantum security of the original scheme
such hybrid mechanisms can potentially add some protection
against the quantum threat

one can distinguish two main types of hybrid key exchange mechanisms

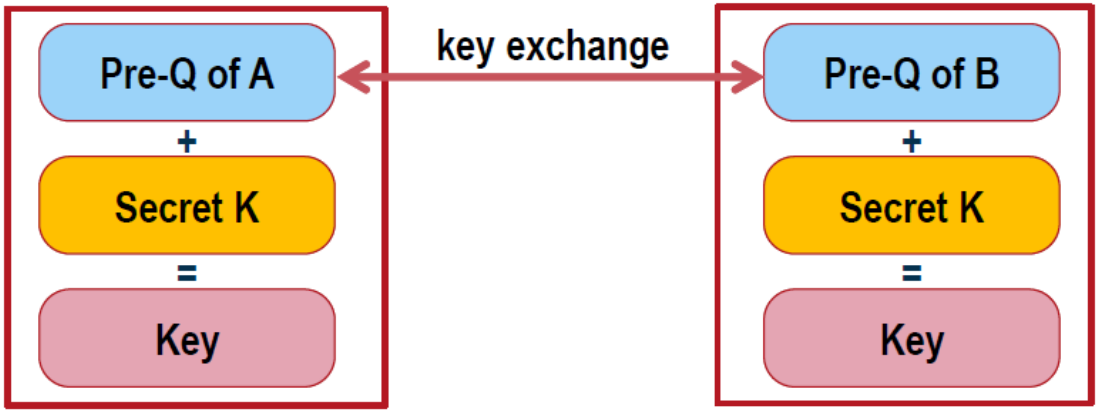
http://risq.fr/pres/qsci_hg_30-01-2017.pdf

Post-Quantum Cryptography: ANSSI views [2/2]

> recognised symmetric mechanisms and hash functions
can be reasonably conjectured quantum-safe if their key / hash length is sufficiently large
[outside from the very strong security model of « quantum chosen message » attacks]

> hybrid mechanisms constructed over a recognised pre-quantum key exchange mechanism

- type1 combines a pre-shared secret key with the key derived from the pre-quantum key exchange (⚠ this induces a strong key management constraint ⚠)



http://risq.fr/pres/qsci_hg_30-01-2017.pdf

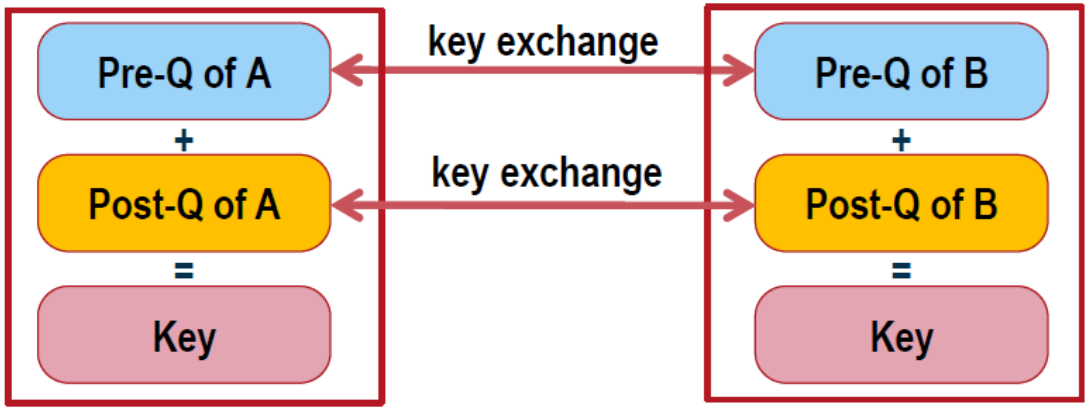
gemalto

Post-Quantum Cryptography: ANSSI views [2/2]

> recognised symmetric mechanisms and hash functions
can be reasonably conjectured quantum-safe if their key / hash length is sufficiently large
[outside from the very strong security model of « quantum chosen message » attacks]

> hybrid mechanisms constructed over a recognised pre-quantum key exchange mechanism

- type2: combines the key derived from the pre-quantum key exchange with the key derived from a post-quantum key exchange



http://risq.fr/pres/qsci_hg_30-01-2017.pdf

gemalto

Post-Quantum Cryptography: ANSSI views [2/2]

> recognised symmetric mechanisms and hash functions
can be reasonably conjectured quantum-safe if their key / hash length is sufficiently large
[outside from the very strong security model of « quantum chosen message » attacks]

> hybrid mechanisms constructed over a recognised pre-quantum key exchange mechanism
[type 1 or type 2]

while not harming the pre-quantum security of the original scheme such hybrid mechanisms can potentially add some protection against the quantum threat

⇒ RGS Annex B1 in its present form could allow to endorse the pre-quantum part of such hybrid public key mechanisms and to view their post-quantum part as an extra « in-depth » protection.

- the above approach can be transposed to other pre-quantum PK mechanisms

http://risq.fr/pres/qsci_hg_30-01-2017.pdf

Post-Quantum Cryptography: ANSSI views [3/3]

> the main focus in the next [five] years should be put on an international effort for developing, evaluating and standardizing sufficiently mature and well studied asymmetric PQC primitives
- a strong involvement of the academic community is needed
- the NIST call for proposals for quantum-safe primitives is a significant step in the right direction
- in France the RISQ project will contribute to this effort

Programme d'Investissements d'Avenir
GRANDS DÉFIS DU NUMÉRIQUE

RISQ

Regroupement de l'Industrie française pour la Sécurité Post – Quantique

"Gathering of the French Industry for Post-Quantum Security"

Industry | Certification Body | **Academia**

+ External Partners: DGA, Systematic Paris Region Digital Ecosystem

http://risq.fr/pres/qsci_hg_30-01-2017.pdf

gemalto

RISQ Collaborative project

- **Need to move to quantum-safe world**: key establishment, digital signature, asymmetrical encryption.
- **What?** secure communications (internet and mobile networks), smartcards, ID documents, embedded systems, IoT, etc.
- **Anticipated change**: norms and prototypes.

Goal of the RISQ project:

- **Academic sphere**: develop their expertise.
- **Industrial sphere**: prepare for migration.

gemalto

Post-Quantum Cryptography: ANSSI views [3/3]

> the main focus in the next [five] years should be put on an international effort for developing, evaluating and standardizing sufficiently mature and well studied asymmetric PQC primitives
  - a strong involvement of the academic community is needed
  - the NIST call for proposals for quantum-safe primitives is a significant step in the right direction

> for use cases requiring a long-lived protection of the information, e.g. ≥ 20 years
  - it is advised to start taking the quantum threat into account
  - the use of hybrid key exchange and/or of hash based signature mechanisms can be considered on a per case basis
  - however any « direct jump » to a stand-alone post-quantum asymmetric key exchange or encryption mechanism is considered premature

> for other use cases (the majority of commercial crypto)
  - this is a medium term issue: while an immediate transitioning to quantum-safe mechanisms is not requested, provisions for facilitating future evolutions of crypto mechanisms (by enhancing crypto agility, etc.) are recommended

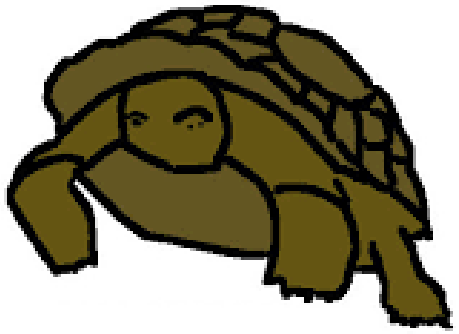
http://risq.fr/pres/qsci_hg_30-01-2017.pdf

Academic knowledge on post-quantum public-key crypto

- Under researched
- Security not sufficiently mature, for almost all public-key post-quantum schemes

  → NIST Post-quantum process foster knowledge development by independent teams of researchers!
- Big and Slow, according to EU project PQCRYPTO H2020

PQCRYPTO
ICT-645622



Starting transition towards products embedding post-quantum cryptography, what it means?

Symmetric-key cryptography

- "AES-256 & SHA-256 are **both secure beyond 2050!"**
  - ETSI GR QSC 006 V1.1.1 (2017-02) Limits to Quantum Computing applied to symmetric key sizes,
    - http://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_QSC006v010101p.pdf

- What about AES-128?
  - Breaking a 128-bit AES key costs about 2^{87} gates and takes the time of 2^{81} gate operations rather than 2^{64} operations predicted by the rule of thumb [Grassl et al., Post-Quantum Crypto 2016]

  - "***We don't know*** *that Grover's algorithm will ever be practically relevant, but if it is, doubling the key size will be sufficient to preserve security.*" [NISTIR8105, 2016]

  - "*But* ***this recommendation may be overly conservative****, as quantum computing hardware will likely be more expensive to build than classical hardware.*" [NISTIR8105, 2016]

Symmetric-key cryptography

- What about 3DES-3keys?
  - No academic publication on this topic
  - Only “Quantum attacks against iterated block ciphers” [Kaplan, QCrypt 2015]

- NIST recommendation : 3DES-3keys ok up to 2030

- Update to Current Use and Deprecation of TDEA, July 2017
  - NIST plans to reduce the maximum amount of plaintext allowed to be encrypted under a single TDEA 3-key bundle from 2^{32} to 2^{20} (64-bit) blocks.
  - NIST plans to disallow the algorithm for TLS, IPsec and possibly other protocols
  - NIST urges all users of TDEA to migrate to AES as soon as possible.

Quantum cryptanalysis of symmetric-key cryptography

- Several MAC and authenticated encryption modes can be broken with a quantum computer if an attacker has access to a *quantum implementation* of the primitive and can query it with *superpositions* [Kaplan et al., Crypto2016]

- Is it a realistic model to analyze the security?

- Anyway, **more effort on quantum cryptanalysis** of symmetric-key cryptography **is also needed**

Quantum-safe public-key signature

- Hash-based signature schemes
  - Most mature security analysis against classical/quantum computing

- A candidate for the replacement of ECDSA or RSA signature?
  - For authentication purpose?
    - Not clear: product lifetime, back-end control, risk-based authentication, revocation,…
  - For digital signature of documents with non repudiation property?
    - Not clear: blockchain-based time-stamping techniques are emerging
    - Maybe first CA keys
  - For transaction signing?
    - Maybe yes for cryptocurrency like Bitcoin
    - Not clear in general: product life-time, symmetric-key based MAC,…
  - More specific use-cases?
    - e.g. firmware update - Intel [Brickell, Post-QuantumCrypto2016]
    - Crypto agility, capability to verify a post-quantum signature

Quantum-safe public-key encryption/key exchange

- Long-term confidentiality
  - Today's encrypted communication can be stored by attackers
  - Later, could be decrypted when large scale quantum computer will be available
    - This risk is already existing w.r.t. potential advances in standard cryptanalysis
    - But, yes data protetion is becoming a key topic
  - No post-quantum PK cryptography recommended today

FACEBOOK TWITTER GOOGLE + LINKEDIN MAIL

November 30, 2016 0

Google's Post-Quantum Cryptography Experiment Successful

Quantum Computers Create A Need For New Cryptography Methods.

A few months ago, Chrome began a real-world experiment testing post-quantum cryptography. The experiment involved shipping a new TLS key-agreement method, which was designed to stand up to quantum computers.

The new key-agreement method combined a post-quantum algorithm named "New Hope" with an elliptic curve known as X25519. The resulting combination was named "CECPQ1," which stands for Combined Elliptic Curve + Post-Quantum 1.

This week, Adam Langley, an engineer working on Chrome, shared an update on the experiment's progress.

> Here the results are more concrete: we did not find any unexpected impediment to deploying something like NewHope. There were no reported problems caused by enabling it.

> None the less, if the need arose, it would be practical to quickly deploy NewHope in TLS 1.2. (TLS 1.3 makes things a little more complex and we did not test with CECPQ1 with it.)
>
> At this point the experiment is concluded. We do not want to promote CECPQ1 as a de-facto standard and so a future Chrome update will disable CECPQ1 support. It's likely that TLS will want a post-quantum key-agreement in the future but a more multilateral approach is preferable for something intended to be more than an experiment.

gemalto

Crypto agility

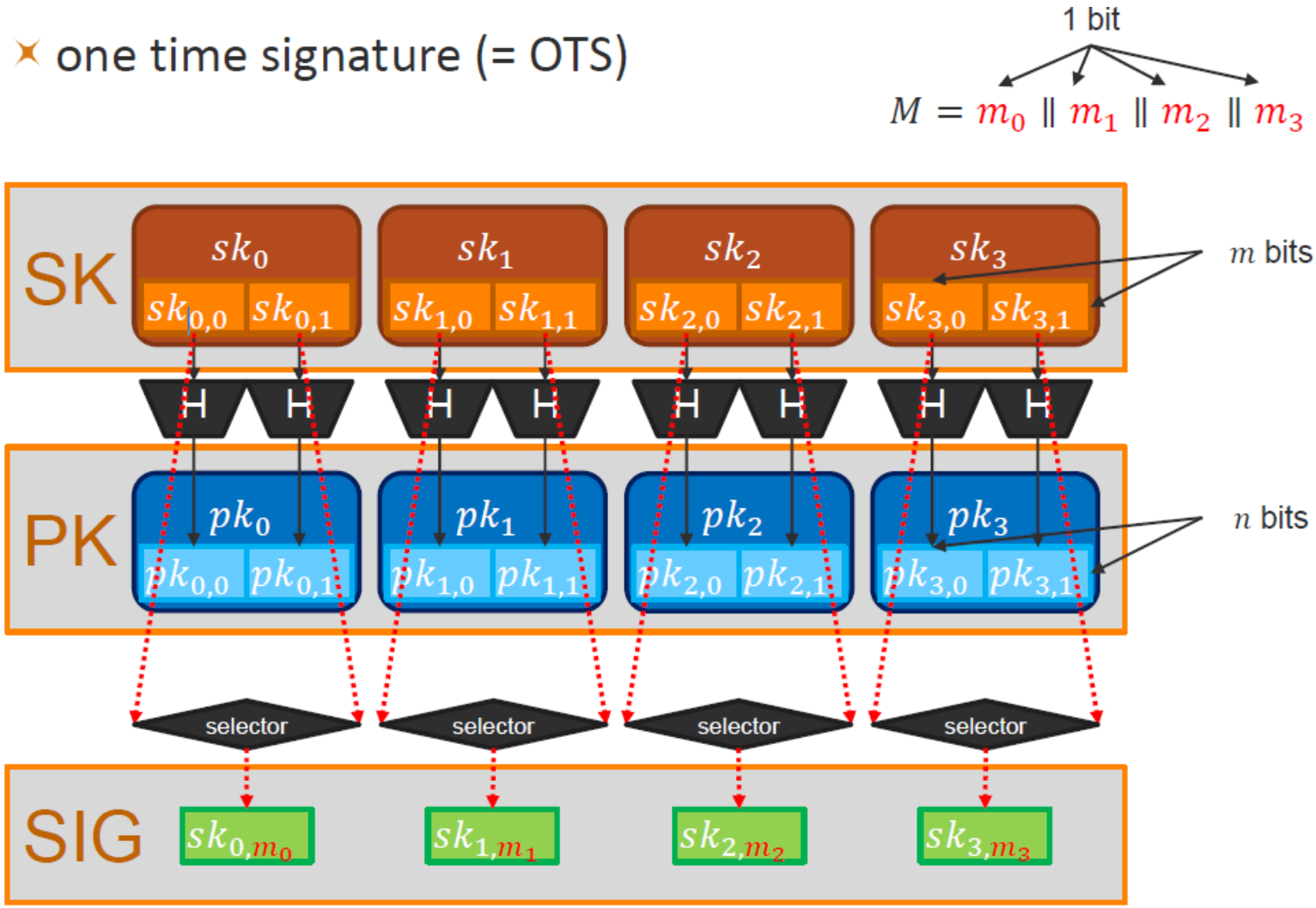
- Cryptographic agility is the capacity for an IT system to easily evolve and adopt alternatives to the cryptographic primitives it was originally designed to use

- On embedded systems, ability to swiftly switch out algorithms for newer, more secure ones
  - Secure remote loading of software for new crypto algorithm
  - Secure remote loading of keys and certificates
  - But, using hardware crypto accelerator designed for current crypto
  - Testing of side-channel/fault resistance?
  - Certification process?

Hash-based signatures

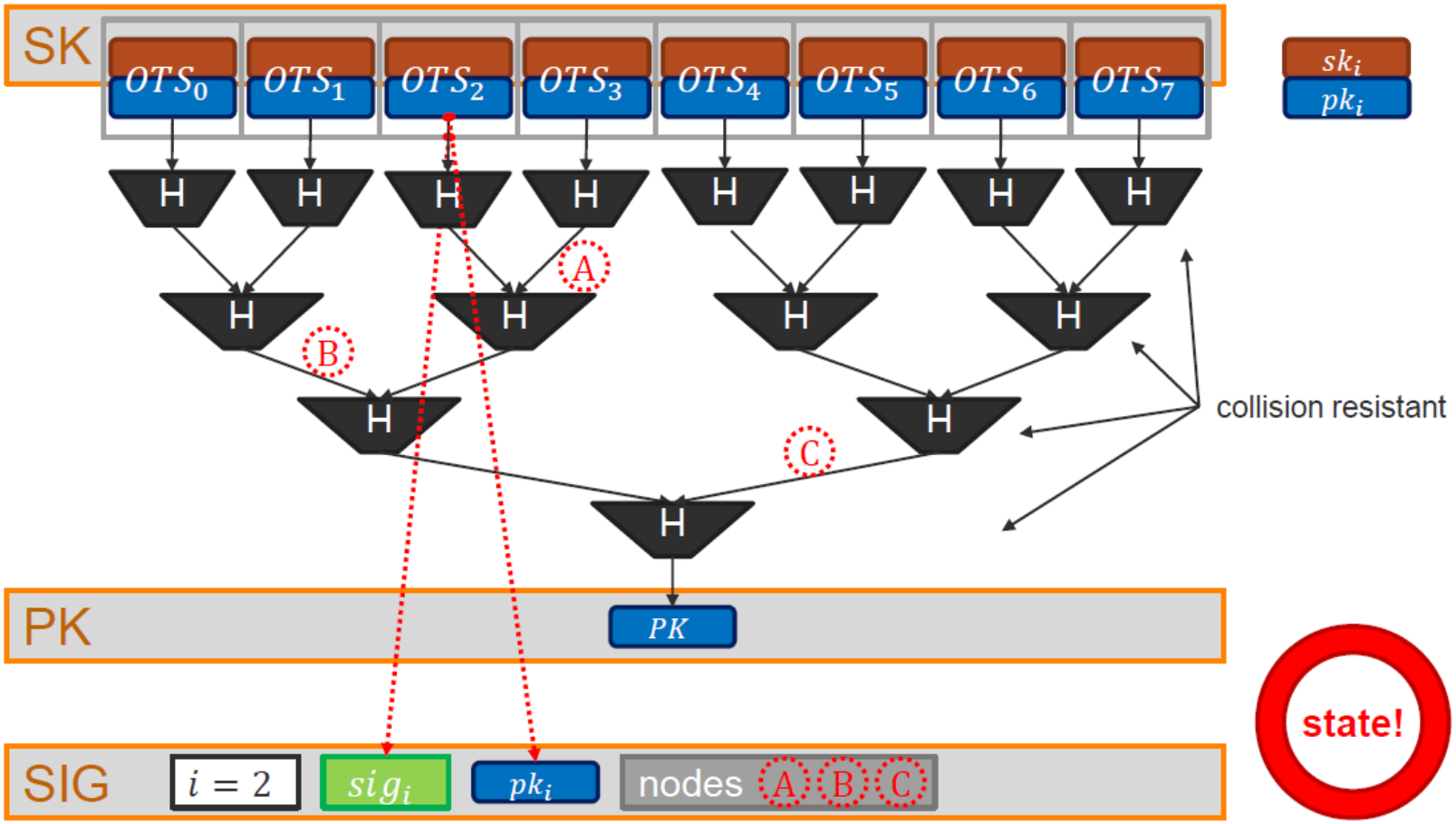
Lamport's scheme

- one time signature (= OTS)



gemalto

Merkle Tree – many time signatures



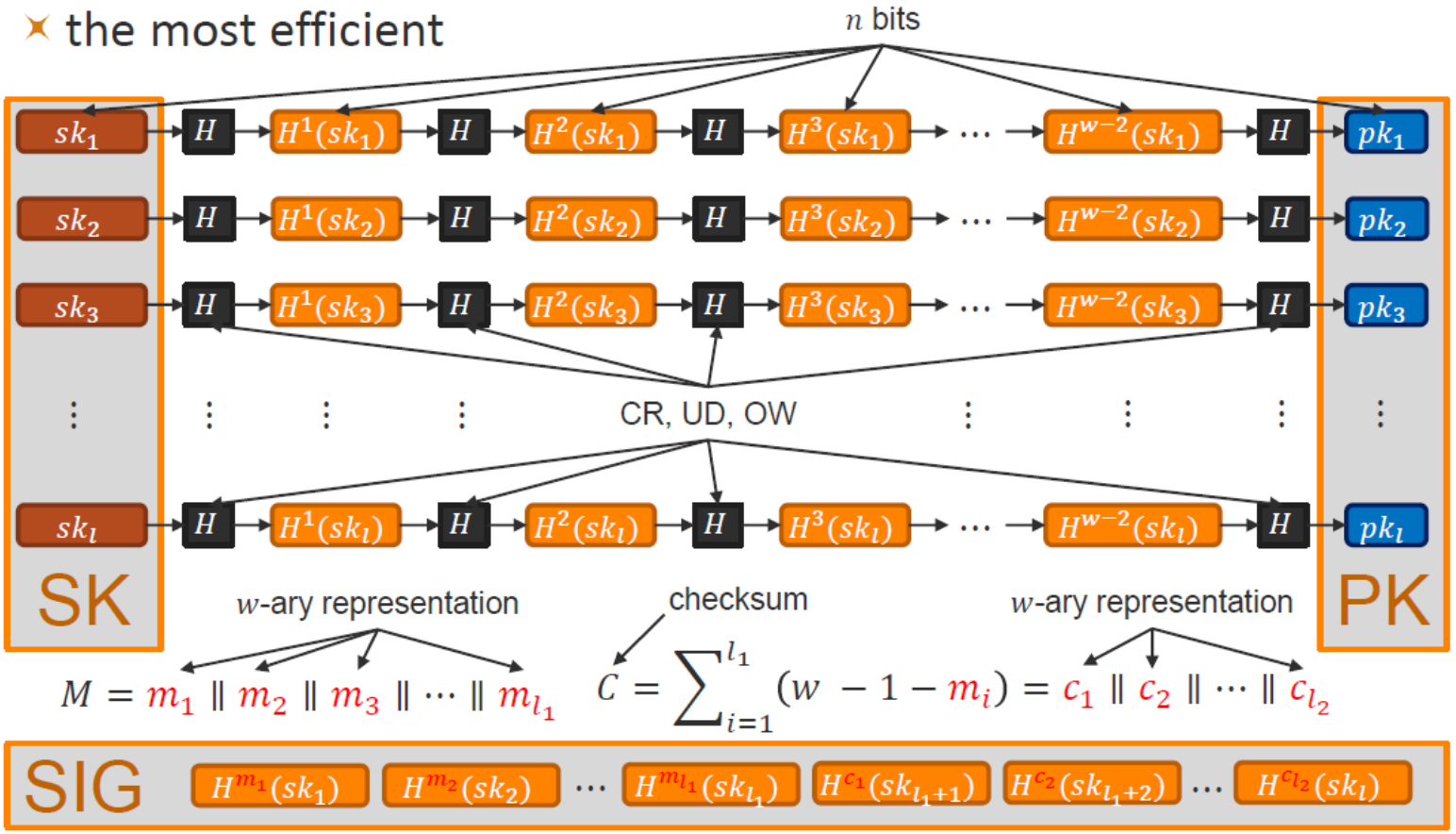
gemalto

State Management

- The same index must not be used twice to issue two different signatures
- Necessary to remember which index was used
- Secure implementation of a counter is needed
- However
  - Managing multiple signers are problematic
  - Potential privacy issue

Winternitz-OTS (= WOTS)

- the most efficient

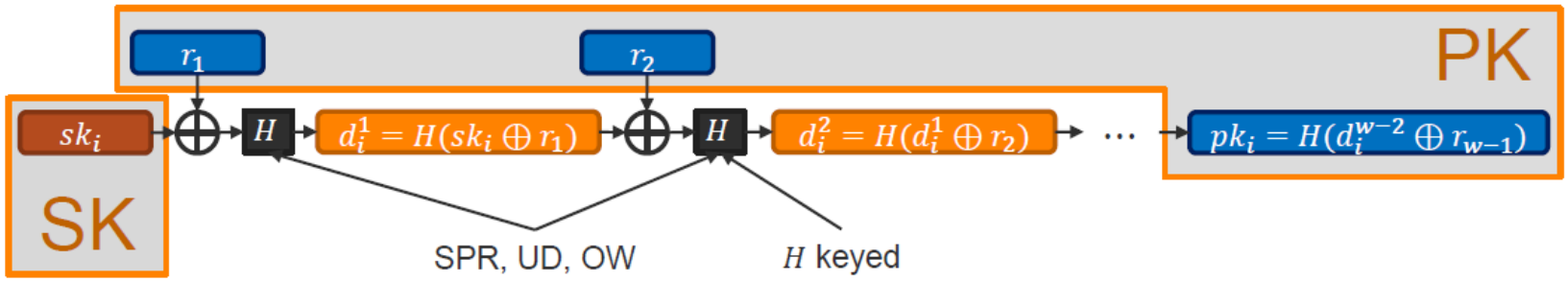


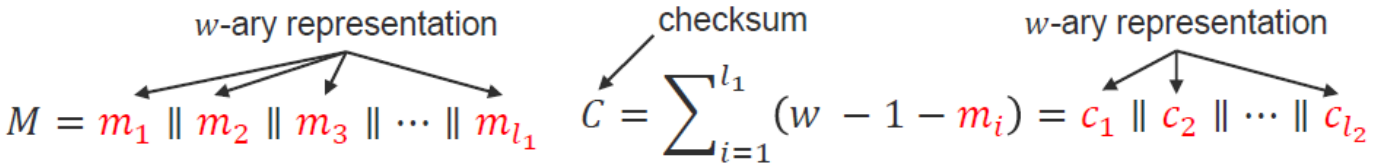
- trade-off between size and runtime

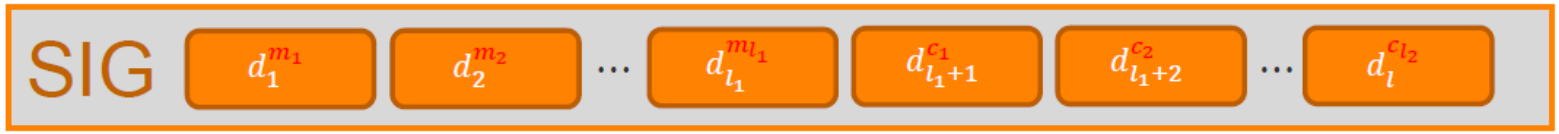
Test implementation: $w = 16; l = 67$

gemalto

WOTS+







- reduction of security requirements
  - collision resistance is replaced by second preimage resistance

gemalto

Standard for hash-based signatures

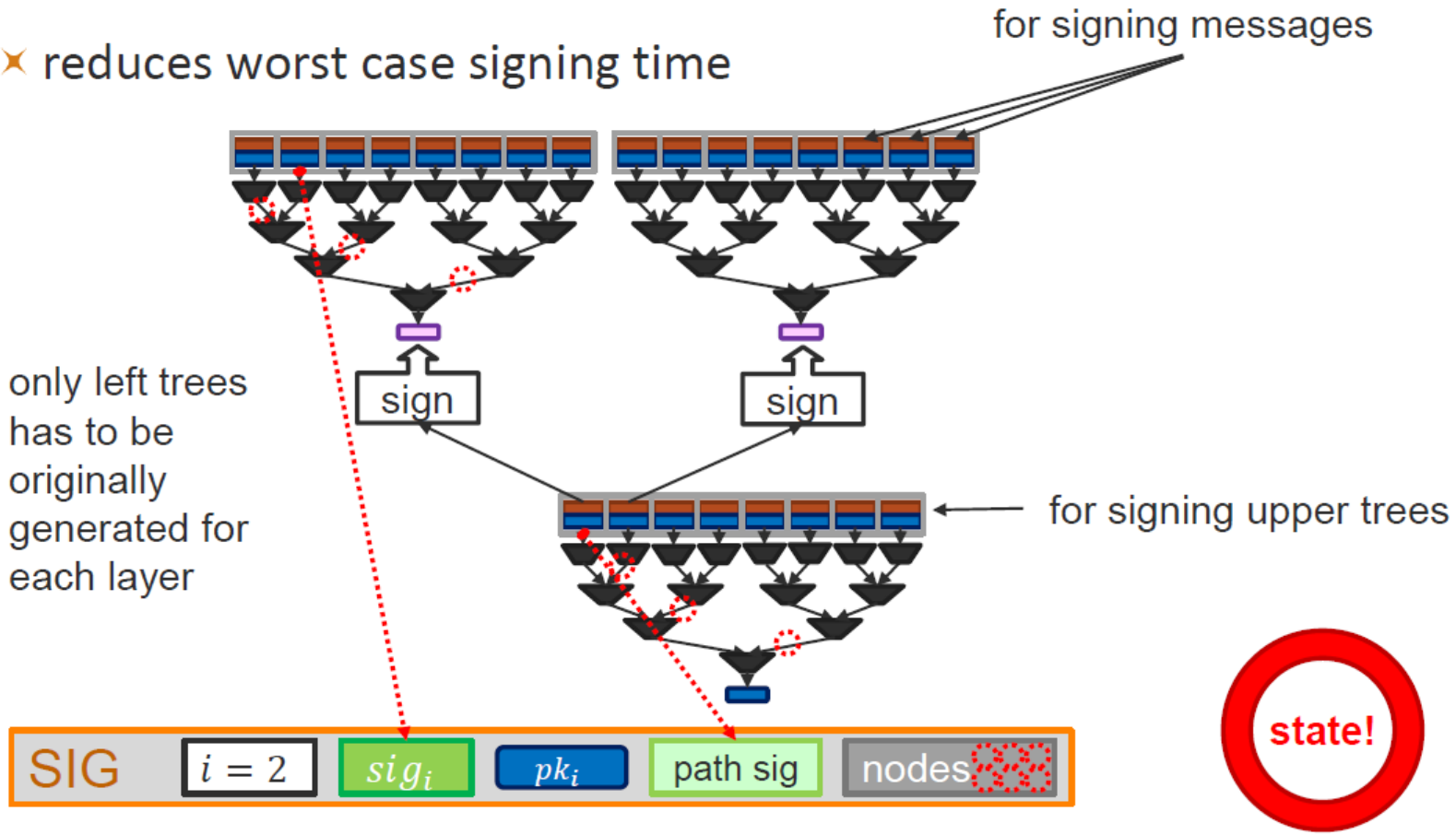
- Security of statefull hash based signatures is considered to be sufficiently mature

- LMS and XMSS are two hash based signature schemes that have been proposed in the IETF (Internet Engineering Task Force)

- Security proofs
  - XMSS: if you can generate an XMSS forgery, you must be able to generate (second) preimages
  - LMS: if the Merkle Damgård compression function acts randomly, then the probability of the attacker finding a forgery is tiny

XMSS^{MT} (= Multi Tree XMSS)

- reduces key generation time
- reduces worst case signing time



gemalto

LMS vs XMSS: Comparion of two Hash-Based Signature Standards, P. Kampanakis and S. Fluhrer

	Public Key	Signature
LMS	$24 + n$	$12 + n(p + h + 1)$
XMSS	$4 + 2n$	$4 + n(p + h + 1)$
HSS	$28 + n$	$(36d + 2nd - n - 20) + n(\Sigma p + \Sigma h)$
XMSS^{MT}	$4 + 2n$	$\lceil \Sigma h/8 \rceil + n(\Sigma p + \Sigma h + 1)$

Table 2: Sizes (in bytes) of HBS schemes based on scheme parameters.

- Parameters
  - *n*: the length of the hash. n = 32 (SHA-256)
  - *p:* the number of Winternitz chains used in a single OTS operation
  - *h:* the height of a single Merkle tree

LMS vs XMSS: Comparion of two Hash-Based Signature Standards, P. Kampanakis and S. Fluhrer

	Public Key	Signature
LMS	56	2508
XMSS	68	2500
HSS	60	5076
XMSS^{MT}	68	4963

(a) $w = 16$, $p = 67$, 2^{10} LMS / XMSS and 2^{20} HSS / XMSS^{MT} total messages (2 levels)

	Public Key	Signature
LMS	56	2828
XMSS	68	2820
HSS	60	5716
XMSS^{MT}	68	5605

(b) $w = 16$, $p = 67$, 2^{20} LMS / XMSS and 2^{40} HSS / XMSS^{MT} total messages (2 levels)

	Public Key	Signature
HSS	60	8600
XMSS^{MT}	68	8392

(c) $w = 16$, $p = 67$, 2^{60} HSS / XMSS^{MT} total messages (3 levels)

	Public Key	Signature
HSS	60	15533
XMSS^{MT}	68	14824

(d) $w = 16$, $p = 67$, 2^{60} HSS / XMSS^{MT} total messages (6 levels)

Table 3: Sizes (in B) of HBS scheme for various parameters and $n = m = 32$.

LMS vs XMSS: Comparion of two Hash-Based Signature Standards, P. Kampanakis and S. Fluhrer

Operation	LMS	XMSS	XMSS / LMS ratio
	XMSSMT_SHA2-256_W16_H20_D2		
PK Gen	0.89 s	3.26 s	3.66
Sign	1.21 ms	4.72 ms	3.90
Verify	0.339 ms	1.76 ms	5.19
	XMSSMT_SHA2-256_W16_H40_D2		
PK Gen	720 s	3340 s	4.64
Sign	1.91 ms	7.70 ms	4.03
Verify	0.350 ms	1.75 ms	5.00

Table 6: Measured time per operation for LMS and XMSS

R&D in progress

- Development of PoC in collaboration with BUs
  - To benchmark performances on embedded devices / HSM
  - To understand impact on the full key management process
- Identify potential issues with known functional requirements
- Side-channel/fault analysis
- Build crypto agility based on hash-based signatures

Lattice-based cryptography

The most promising post-quantum family?

- A claimed very good efficiency!

- But for which security assumption?
  - LWE,
  - NTRU,
  - Ring-LWE, Module-LWE, etc.

Lattice algorithms to solve LWE and ISIS

- LWE and ISIS are cases of CVP, and hence are solved using algorithms for lattice basis reduction.
- A **fundamental challenge** is to predict the running time of lattice attacks for large parameters.
- **Question:** How many people in this room consider themself an expert on floating-point LLL, enumeration algorithms, choice of block size in BKZ, Hermite factors, lattice sieving?

Conclusions

- We need a community of people who are experts in lattice reduction and worst-case reductions.
- We need to understand Ring-LWE.
- Adaptive attacks should be considered (especially for homomorphic encryption).
- Lattice signatures should be made more compact.
- Final comment: post-quantum crypto should be about greater security, not greater efficiency.

Steven Galbraith | Challenges for lattice cryptography

Steven Galbraith
Post-quantum Cryptography 2016
https://pqcrypto2016.jp/

Encryption

Scheme	Security reduction	Efficiency : time	Efficiency : space
NTRUencrypt (1998)	NTRU	Very fast	Good
Regev LWE (2005)	LWE	Disastrous	Disastrous
Lyubashevsky RLWE (2012)	Ring-LWE	Fast	Good
Lizard (2016)	LWE, LWR	$5* \leq$ RLWE	$5* \geq$ RLWE
Kyber (2017)	MLWE	Fast	Good

Key exchange

Scheme	Security reduction	Efficiency : time	Efficiency : size
NTRU KE (2013)	NTRU	Fast	Good
New Hope (2015)	RLWE	Very fast	Good
Frodo (2017)	LWE	$2* \leq$ New Hope	$5* \geq$ New Hope

Internship of Maxime Plançon, 2017

BLISS Signature

Signature

To sign a message m :

- Step 1 : Generate y_1, y_2 from a centered discrete Gaussian distribution of public standard deviation and a random bit $b \in \{0, 1\}$.
- Step 2 : Compute the hash $c = H(P_k y \mod 2q, m)$.
- Step 3 : Compute $z_1 = y_1 + (-1)^b s_1 c$, $z_2 = y_2 + (-1)^b s_2 c$.
- Step 4 : Check that the $\mathcal{L}_2$ and $\mathcal{L}_\infty$ norms of z_1, z_2 do not leak the information about the secret key (Rejection sampling). Otherwise restart.
- Step 5 : Compress z_2 and return (c, z_1, z_2).

Verification

The signing process requires a message, signature $m, (c, z_1, z_2)$.

- Check that z_1, z_2 were meant to pass rejection sampling test.
- Check the equality of c and $H(\xi h z_1 + \xi q c \mod 2q + z_2 \mod q, m)$.

Internship of Maxime Plançon, 2017

Multiple use of noise

We assume that an attacker is provided 2 signatures

$$\begin{cases} \text{sign}(m_1) = (c_1, z_{11}, z_{21}) \\ \text{sign}(m_2) = (c_2, z_{12}, z_{22}) \end{cases}$$

with

$$\begin{cases} y_1 = \sum_{j=0}^{N-1} y_{11j} X^j \\ y_2 = \sum_{j=0}^{l-1} y_{11j} X^j + \sum_{j=l}^{N-1} y_{12j} X^j \end{cases}$$

Internship of Maxime Plançon, 2017

Fake twins

We assume that for one message of signature (c, z_1, z_2), the ℓ first coefficients of y_1 and y_2 are the same. More formally :

$$y_1 = \sum_{i=0}^{N-1} y_{1i} X^i \ , \ y_2 = \sum_{i=0}^{\ell-1} y_{1i} X^i + \sum_{i=\ell}^{N-1} y_{2i} X^i$$

$$z_1 = y + y_1 + (-1)^b cf, \ z_2 = y + y_2 + (-1)^b c(2g+1).$$

Where y_1, y_2 non zero coefficients are greater than some integer ℓ, and y degree is at most ℓ.

Important practical issue with lattice-based signatures

- The rejection sampling step
- It will reject the candidate for signature with a non-negligible probability
- Not possible for practical use-cases with strong timing limitation
  - EMV contactless payment
  - Access control for transport application
- For this type of use-case, it is needed to guarantee that the full transaction will be performed in less than, e.g. 300ms
- How to choose parameters of lattice-based signatures to be able to guarantee that?

Lattice-based signature submitted to NIST process

	Signature size (Bytes)	Public key size (Bytes)	Rejection sampling	Assumption
Crystals-Dilithium	2044	1184	**Yes**	Module-LWE
DRS	**8530**	**5,000,000**	No, but **not constant time**	GDD/BDD/ uSVP
Falcon	**617**	**897**	**Yes**	SIS on NTRU
pqNTRUSign	1408/2048	2048/2048	**Yes**	uSVP on NTRU
qTesla	3104	4128	**Yes**	R-LWE

- For specific use-cases, some criteria could be unavoidable, e.g. the maximum execution time is guaranteed to be less than 300 ms, let's say with probability $1-1/2^{128}$

Many lattice-based key encapsulation mechanism

- Compact LWE
- Crystals-Kyber
- Emblem
- FrodoKEM
- Giophantus
- HILA5
- KCL
- Kindi
- LAC
- Lepton
- LIMA
- Lizard
- Lotus
- NewHope
- NTRUEncrypt
- NTRU-HRSS-KEM
- NTRU Prime
- Odd Manhattan
- Round 2
- Three Bears
- Titanium

Priority order based on security problem?

BDD

- Odd Manhattan

NTRU

- NTRUEncrypt
- NTRU-HRSS-KEM

Module-LWE

- Crystals-Kyber
- Kindi

LWE

- FrodoKEM
- KCL
- Lotus

LWR

- Round 2

Ring-LWE

- HILA5
- LAC
- LIMA
- NewHope

Implementation attacks

Implementing a cryptographic scheme

- Low cost embedded devices represents a highly constraint environment that challenges all post-quantum cryptographic schemes

- First step is to choose a « secure » cryptographic scheme and suitable for identified functional requirements
  - With security proof, or
  - Extensive study & no known attack

- Second step is to implement the selected cryptographic scheme
  - Naive implementation → leakage on secret values
  - Secure implementation → suitable countermeasures to protect the secret values

- 2 main families of implementation attacks
  - Side-channel analysis: e.g. timing, power consumption, electromagnetic emanation
  - Fault analysis

Main information leakages

Passive

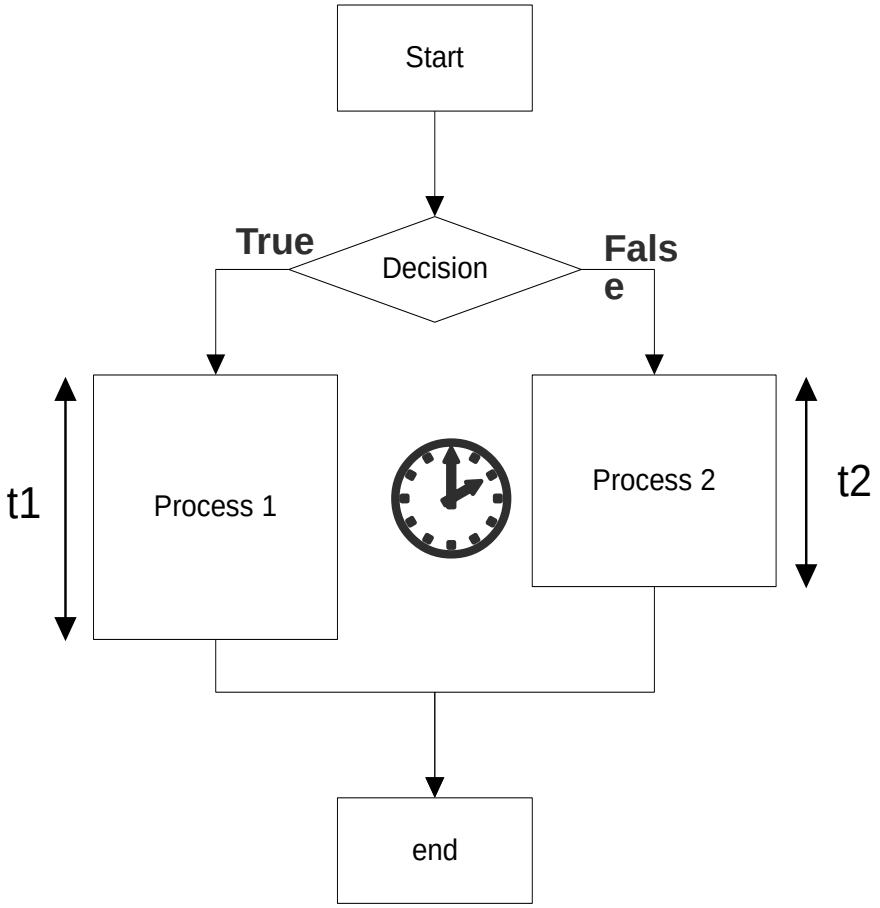
- Timing analysis: when execution timing depends on manipulated data
- Power consumption analysis: when power consumption depends on the type of instruction or on manipulated data
  - Single Power Analysis (SPA), Differential Power Analysis (DPA)
- Electromagnetic emanation analysis: when electromagnetic emanation depends on the instruction or on manipulated data
  - SEMA, DEMA

Active

- Fault analysis : when the effect of a fault can be used to deduce information on secret values using input/output values of the crypto function
  - Differential Fault Analysis (DFA), Ineffective Fault Analysis (IFA)

Timing Analysis

- Introduced at CRYPTO'96 par Paul Kocher
- Principle of the attack
  - Secret data are manipulated in a crypto device
  - Execution time
    - Depends on secret values
    - Leaks information on secret values
    - Can be measured, or at least the difference between 2 executions
- Basic material to conduct this type of attack



Most well-known timing analysis (1/2)

Pseudo-code for "VerifySecret“ cmd

- IN
  - P = PIN code value stored in the card
  - C = Challenge (proposed value for the PIN)
- OUT
  - ‘KO’ or ‘OK’
- VERIFY SECRET
  - For b = 0 to 7
    - If C[b] != P[b]
      - then return ‘KO’
  - Return 'OK’

Constant time implementation for sensitive part!

Important but not enough

Most well-known timing analysis (2/2)

- *Security flaws induced by CBC padding, application to SSL, IPSEC, WTLS*, Serge Vaudenay, Crypto 2002

- Given a ciphertext, the goal of the attack is to is to recover a plaintext

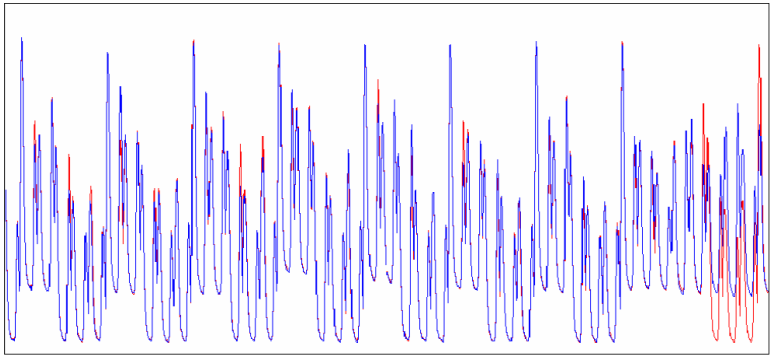
- Timing attack, e.g.
  - Premature stop: e.g. if the padding is invalid then the MAC is not checked while if the padding is valid the MAC check is done
  - Specific reaction: e.g. plaintext-dependent sanity check followed later by assigning a zero value to the plaintext message length in the case this sanity check fails

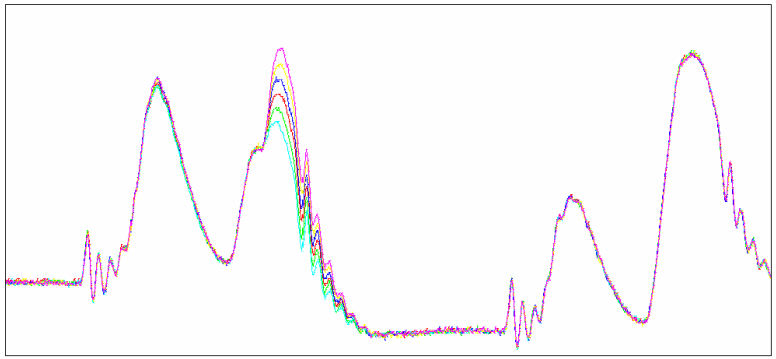
  - Detailed error messages, different status words

gemalto

Power consumption analysis

- Introduced at Crypto'99 by Paul Kocher *et al.*
- Power consumption on microprocessor reflects the internal activity of the component
  - It results essentially from the sum of consumptions at its different gates
- Power consumption depends on
  - Instructions executed
  - Data manipulated
- The simple analysis (SPA) of the consumption makes the assumption that the shape of a curve depends directly on the operations carried out





Fault Analysis

- Active implementation attack

- Faults can be maliciously injected into specific operations so that the faulty output carries some information about the secret key
  - Spacial dimension: fault injected at a specific location using a laser
  - Temporal dimension: fault injected at a specif clock-cycle by reducing the supply voltage and/or increasing the operating frequency

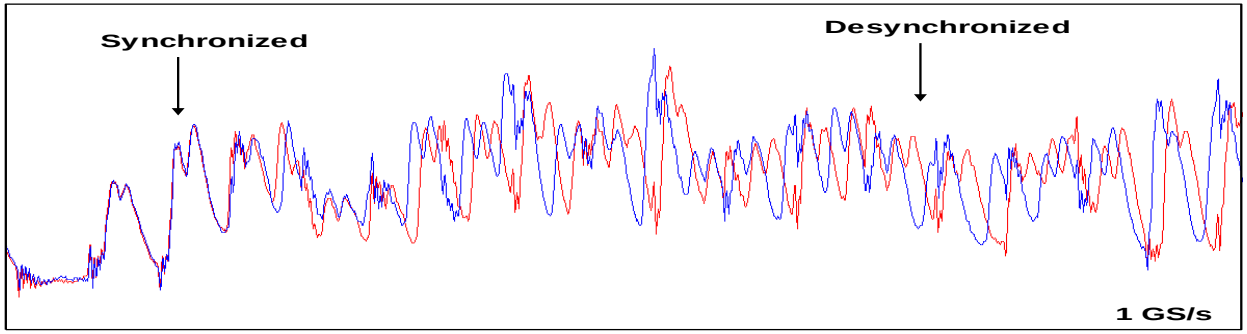
- Differential Fault Analysis (DFA)
  - Faulty output(s) can be analyzed against the correct one
  - Mathematical techniques for cryptanalysis depend on the cryptographic scheme

Countermeasures

- Suitable hardware and software countermeasures must be used
  - To reduce information leakages on secret values
  - To prevent the exploitation of leakage to retrieve secret values

- Non-invasive attacks (passive) cannot be detected by the hardware device whereas invasive attacks (active) can be in some cases
  - Modern hardware components have a memory erase mechanism when an attack is detected

- Examples of countermeasures
  - Noise generator: module that consumes electricity randomly
  - Masking
  - Detector of frequency, voltage or electronic intensity variations, thermometer, light sensor
  - Active shield: metal cover fed continuously throughout the circuit (probing detection)
  - Detection, e.g computing the same result twice and compare them



gemalto

Implementation attacks on post-quantum cryptography

- Hash-based signature
  - Secure implementation of hash function → many studies available
  - Secure implementation of PRNG → many studies available
  - State management → new but related to secure implementation of counter
  - Side-channel vulnerability of XMSS
    - A. Hülsing, D. Butin, S.-L. Gazdag, and A. Mohaisen. XMSS: Extended Hash-based Signatures,July 2017. Work in Progress - https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmsshash-based-signatures/.
  - Fault Attack on XMSS^{MT}
    - Physical Attack Vulnerability of Hash-Based Signature Schemes, Master-Thesis von Matthias Julius Kannwischer, 2017
      - https://www.cdc.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_CDC/Documents/theses/Matthias_Kannwischer.master.pdf

Implementation attacks on post-quantum cryptography

- Code-based cryptography
  - Mc Eliece encryption scheme
    - The secret key is a selected error-correcting code
    - The public key is a random-looking version of that code
    - Messages are treated as codewords multiplied by the public key and augmented by random noise
  - Side-channel analysis applies on decryption/decoding phase
    - Most widely used decoding scheme for Goppa codes is the Patterson algorithm
      - Timing analysis [Strenzke et al, PKC2008] on the error locator polynomial phase to retrieve the message, but not the secret key. Further analysis lead to key recovery [Strenzke, PQCryoto 2013]
      - Power analysis on implementation secure against timing attack [Heyse et al. PQCrypto2010]
  - Fault analysis
    - Inherent error-correction capability
    - No result yet

Implementation attacks on post-quantum cryptography

- Lattice-based cryptography
  - Power attacks against NTRU cryptosystem
    - Atici, Batina, Gierlichs and Verbauwhede, 2008
    - Wang, Zheng and Wang, 2013
    - Zheng, Wang and Wei, 2013
  - Timing attacks against NTRU Encrypt
    - Silverman and Whyte, 2007
    - Vizev, 2007
  - Fault attacks against NTRU
    - Kamal and Youssef, 2012

  - More recent work
    - Bindel, Buchmann and Krämer. *Lattice-based signature schemes and their sensitivity to fault attacks*, 2016.
    - Espitau, Fouque, Gérard and Tibouchi, *Loop-abort faults on lattice-based fiat–shamir and hash-and-sign signatures*, 2016.
    - Espitau, Fouque, Gerard and Tibouchi, *Side-channel attacks on bliss lattice-based signatures – exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers*, 2017.
    - R. Primas, P. Pessl and Mangard, *Single-trace side-channel attacks on masked lattice-based encryption*, 2017.

Implementation attacks on post-quantum cryptography

- Still few effort in evaluating the security of post-quantum schemes against implementation attack
- Also, very few studies on suitable hardware accelerator for post-quantum cryptography
- More to come, hopefully

Take out

Take out

- Symmetric-key cryptography only (but no forward-security) for use-cases that require long-term data confidentiality/authenticity
  - Slight impact on performances for AES-256
  - SHA-256 is already in use
- Hybrid mechanisms pre-quantum & post-quantum
  - Significant additional cost « by design », can be acceptable when
    - long-term confidentiality is needed
    - long-term non-repudiation is needed, e.g. using blockchain-based technologies
- Hash-based signatures
  - PoC in progress
- Preparing for the management of crypto agility
- Side-channel/fault analysis