riscure

driving your security forward

RISCURE VISION ON POST QUANTUM CRYPTOGRAPHY

MARC WITTEMAN

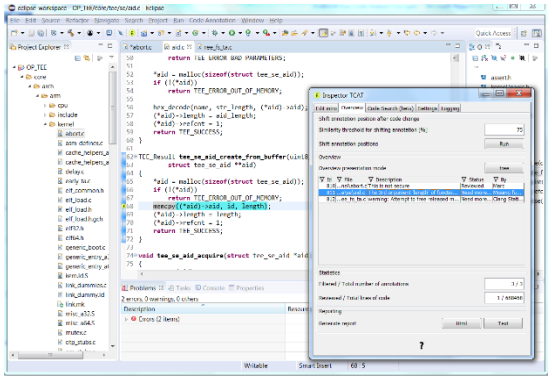
COSADE
APRIL 4, 2023

Who is Riscure?






- Security Lab founded in the Netherlands, with branch offices in US and China
- We focus on devices that must be **secure** in a hostile environment
- We serve 200+ clients worldwide with security test **tools**, **services**, and **training**
- Our work is recognized by the world's leading security authorities




CONTENT

1. Introduction PQC
2. Timelines
3. Implementation Security
4. Vulnerability Testing
5. Pre-silicon
6. Testable intermediate data in Dilithium
7. Conclusion

Tables and graphs from various sources are used and referenced at the end of the presentation

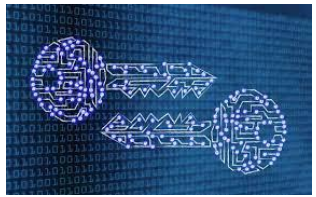
1. INTRODUCTION PQC

POST QUANTUM CRYPTO

Why is this needed?

Quantum Computers are a field of scientific research

- using a new extremely fast method of calculation
- expected to be practical in ’10’ years
- Impacting cryptographic security
  - Symmetric algorithms need longer keys, i.e. 128 bit → 256 bit
  - Popular asymmetric algorithms (RSA/ECC) can be trivially broken

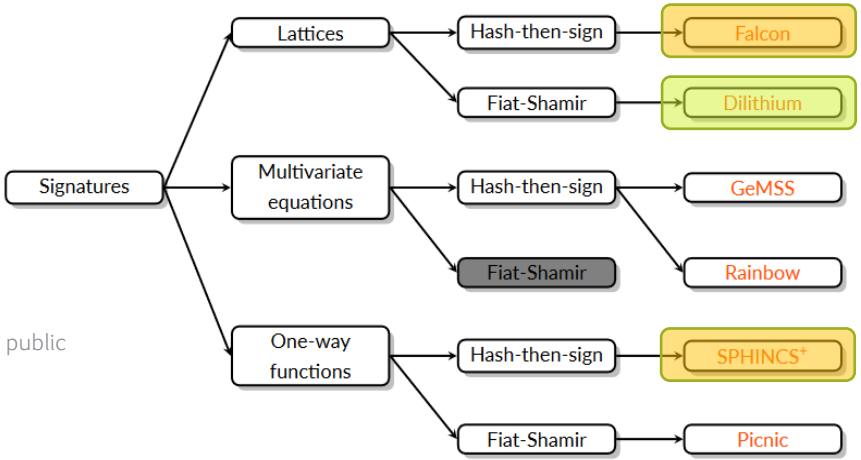


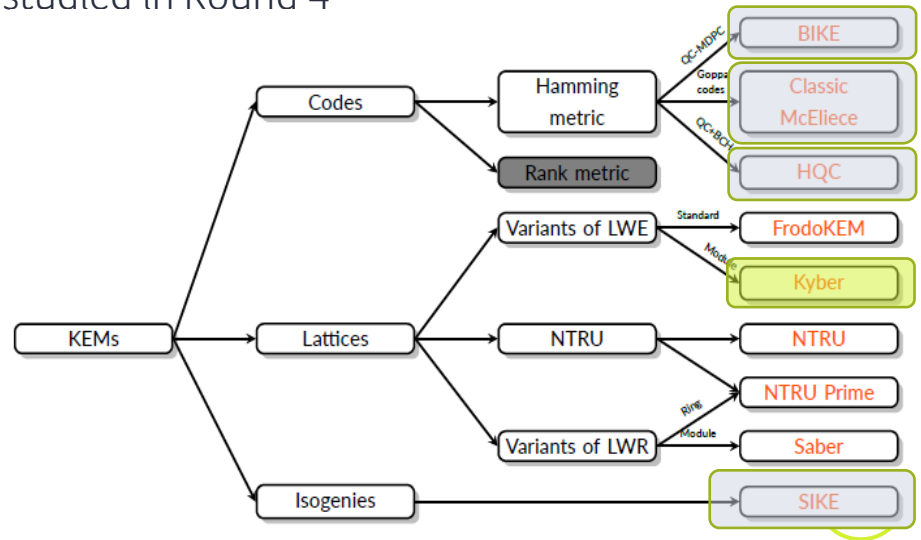
NIST

- organized (since 2016!) a contest to find the best PQC candidates
- completed the third round on in 2022
- selected algorithms for signing and key encryption, continues the search

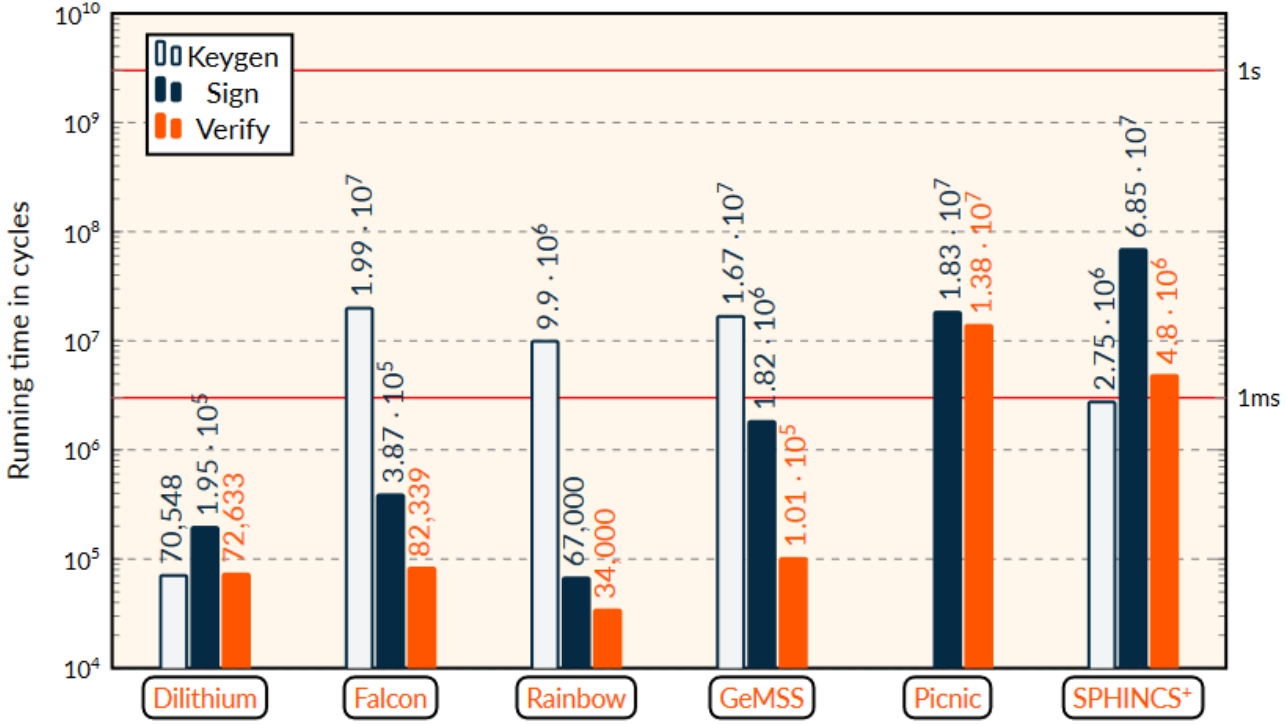
THE SELECTED POST QUANTUM ALGORITHMS

- Preferred algorithms are: Dilithium (signing) and Kyber (key encryption)
  These are fast algorithms with reasonable key/signature sizes
- 2 alternatives are given for signing: Falcon and Sphincs
  because of signature size, and to avoid total reliance on Lattices
- 4 additional Key encryption algorithms will be studied in Round 4





Quantum resistant signatures - performance



RSA-2048:
Sign: ~$2.1 * 10^6$ cycles
Verify: ~58,000 cycles

PQC algorithms will likely need hardware implementation,
but initial and low-cost implementations can be software based

IS PQC STANDARDIZATION READY NOW?

Stakes are growing, attacks continue

- Two recent attacks on SIKE
  - Hertzbleed, attack → exploits “dynamic voltage & frequency scaling”
  - Glue-and-Split attack → math can break crypto in 1 hour
- SIKE is now dead ☹, but others may live ☺
- NIST will continue the selection process

- So, how urgent is the introduction of PQC, and what are the timelines?

2. PQC TIMELINES

WHY DO PQC IF THERE'S NO QUANTUM COMPUTER YET?

Risk	Description
Store Now, Decrypt Later	Prior to the availability of a Cryptographically Relevant Quantum Computer (CRQC), motivated bad actors may harvest data and store it, with the goal of decrypting it once quantum computing capabilities become available. This attack undermines the security of data with long-lived confidentiality needs, such as corporate IP, state secrets or individual bio-data. It is widely believed that some actors are already engaging in this type of attack.
Code-signing and Digital signatures	If algorithms become vulnerable, then service authentication can be attacked, and lead to vulnerabilities in software updates.
Rewriting history	If digital signature algorithms become vulnerable, the integrity of digitally signed data can be compromised e.g. audit records, call records, contracts, other data.
Key Management Attacks	It is possible that infrastructure is used to store symmetric keys using vulnerable wrappers. Keys used for such long-term storage can therefore become vulnerable by attacking the wrapping mechanisms.

- Encryption more urgent than signing
- Early adopters most likely governments

NATIONAL TIMELINES

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
China	China Specific	CACR (2020)	Start Planning
European Commission	NIST	ENISA (2022)	Start planning and mitigation
France	NIST (but not restricted to)	ANSSI (2022)	Start planning; Transition from 2025
Germany	NIST (but not restricted to)	BSI (2022)	Start planning
Japan	Monitoring NIST	CRYPTREC	Start planning; initial timeline
South Korea	KpqC	MSIT (2022)	Start competition First round (Nov.'22-Nov.'23)
United Kingdom	NIST	NCSC (2020)	Start planning;
United States	NIST	NSA (2022)	Implementation 2023-2033

BUSINESS TIMELINES

- The Global Risk Institute issued the Quantum Threat Timeline Report, stating that there is a significant (>30%) risk of a capable Quantum Computer emerging in the next decade (by 2032)
- Commercial National Security Algorithm Suite proposes a timeline

3. IMPLEMENTATION SECURITY

IMPLEMENTATION SECURITY

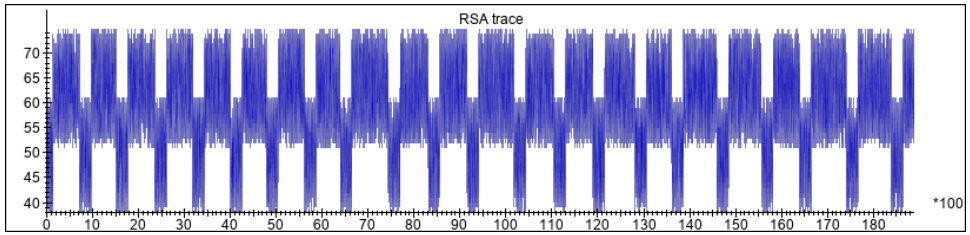
Moving to stronger algorithms only makes sense if we also address implementation security

Three levels of danger

1. Weakness → a theoretical situation of reduced strength (based on a threat)
   - Semiconductor work-related consumption of power
   - Semiconductor reliance on stable operating conditions
2. Tested vulnerability → an observable security risk (based on testing)
   - Handling of intermediate data depending on some key bits
   - Unverified output of cryptograms
3. Exploit → a practical route to compromize (based on attack)
   - CPA on S-box output
   - Horizontal Deep Learning attack on ECC

HISTORY OF RSA ATTACKS

RSA implementations have been attacked since 1997



1997

Side Channel Attacks on RSA

2022

- Timing
- SPA
- DPA
- CPA
- Montgomery reduction
- CRT recombination
- Templates
- Cross-correlation
- Horizontal
- Deep Learning

Exploits keep emerging,
When can we be sure about implementation security?

How do we avoid PQC market disruptions due to emerging attacks?

4. VULNERABILITY TESTING

EFFICIENT TESTING AND REDUCING FUTURE ATTACK RISK

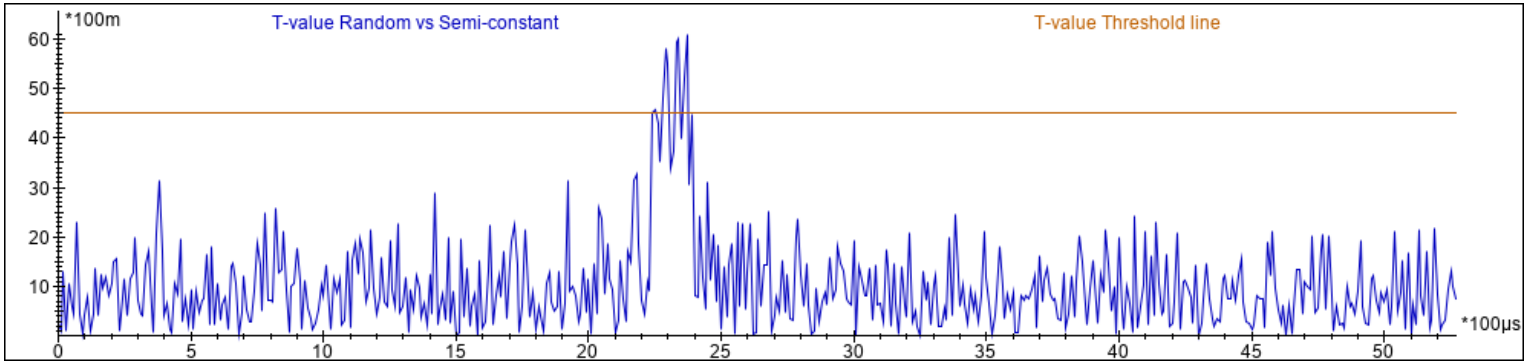
A lesson learned from certification

Focus on Vulnerabilities rather than Exploits

- Leakage assessment → TVLA
  - testing secret leakage through **Side Channel Analysis**
  - only leakage measurement, no key extraction
- Robustness assessment → FIRM
  - testing chip and software robustness against **Fault Injection**
  - only measure corruption, no key extraction
- Vulnerability testing characteristics:
  - Fast test implementation and execution
  - May find leakage that is not (yet) exploitable (can prevent future attacks!)
  - Still need to test for all potential leakage models

WHAT IS TVLA?

Test Vector Leakage Assessment, commonly used in certification



- TVLA was proposed in 2014 by Rambus as a fast method for detecting leakage
  - saves time
  - requires less expertise
- Based on Welch's T-test, using dedicated crypto inputs, maximizing leakage of intermediate data

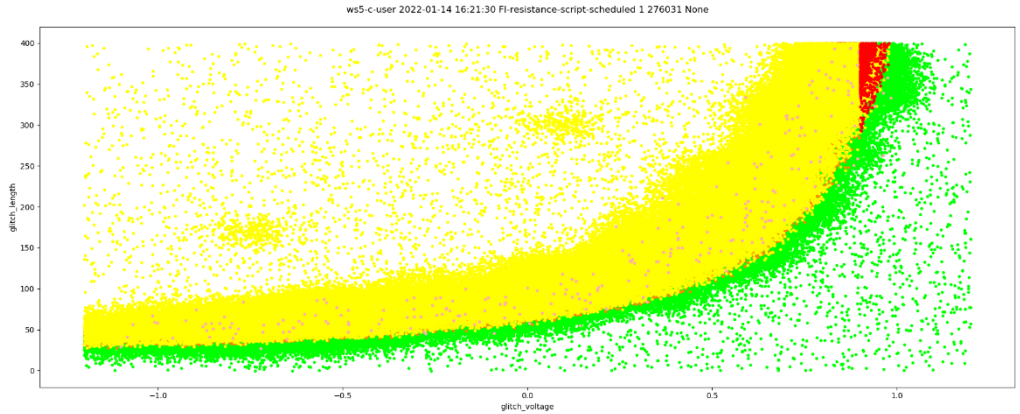
$$t(I) = \frac{X_A(I) - X_B(I)}{\sqrt{\frac{S_A^2(I)}{N_A} + \frac{S_B^2(I)}{N_B}}}$$

What is FIRM?

Fault Injection Resistance Metric, under development at Riscure to increase accuracy and speed in certification

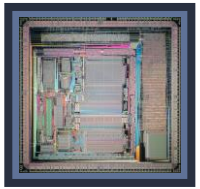
- Using dedicated target test code and test system control, testing for:
  - Wrong branch taken (if, else)
  - Instruction skipped
  - Instruction corrupted
  - Data corrupted
  - Address corrupted
  - Wild jumps due to special register (PC/RA/SP) corruption

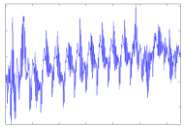
Result	Number	Percentage
Expected	71687	25.97%
Crash/Mute	115036	41.68%
CM detected	88517	32.06%
Success	791	0.29%



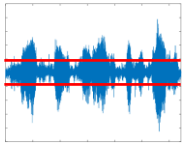
5. PRE-SILICON

POST-SILICON





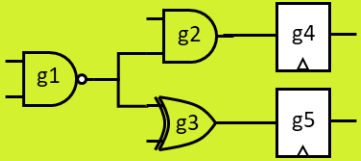
Leakage Metric



Reject

Accept

PRE-SILICON



RTL
gate-level

Gate-level Leakage Metric

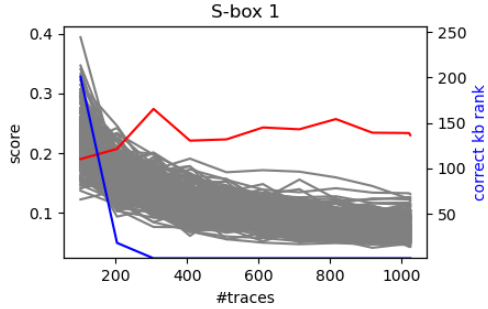
Ranking

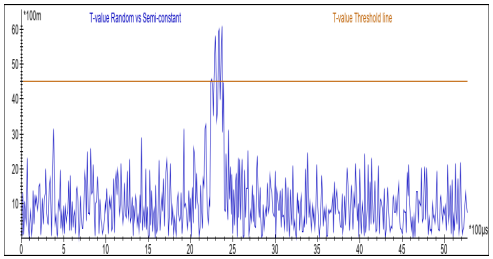
1 g4
2 g3
3 g2
4 g5
5 g1

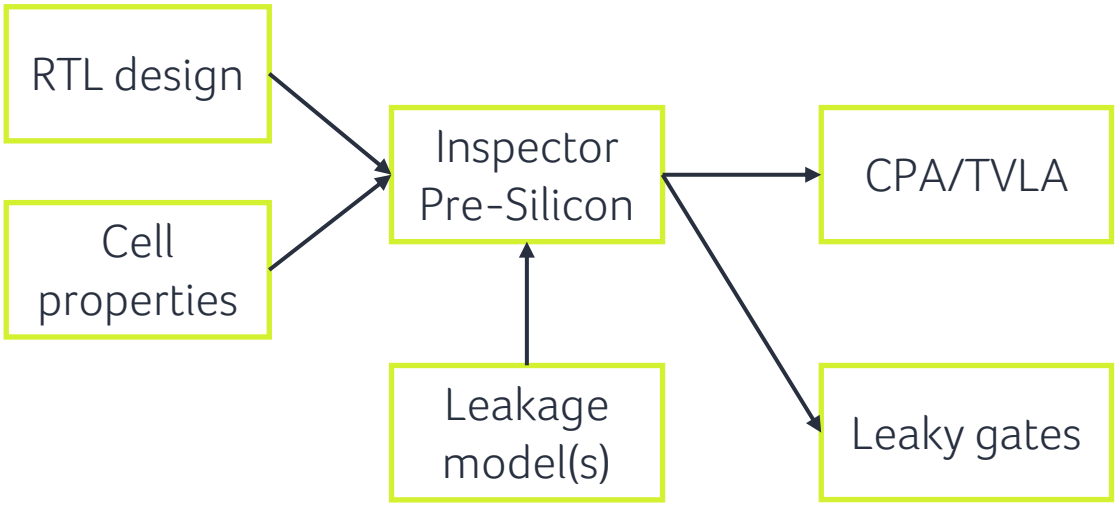
Top-N

Root Cause Analysis

SCA SIMULATION AND ROOT CAUSE ANALYSIS







g129741 aes_comp_encipher_block.v 153

```
151  function [127:0] add( input[127:0] data, input[127:0] key );
152    begin
153      add = data ^ key;
154    end
155  endfunction
```

We can simulate traces to obtain noiseless CPA plots

and do root cause analysis to find the leaky gates in RTL

6. TESTABLE INTERMEDIATE DATA IN DILITHIUM

WHICH INTERMEDIATES CAN WE TEST IN DILITHIUM?

$\underline{\mathsf{Sign}(sk, M)}$

05 $\mathbf{z} := \perp$

06 **while** $\mathbf{z} = \perp$ **do**

$\mathbf{y} \leftarrow S^{\ell}_{\gamma_1 - 1}$

08 $\mathbf{w}_1 := \mathsf{HighBits}(\mathbf{Ay}, 2\gamma_2)$

09 $c \in B_\tau := \mathrm{H}(M \parallel \mathbf{w}_1)$

$\mathbf{z} := \mathbf{y} + c\mathbf{s}_1$

11 **if** $\|\mathbf{z}\|_\infty \geq \gamma_1 - \beta$ or $\|\mathsf{LowBits}(\mathbf{Ay} - c\mathbf{s}_2, 2\gamma_2)\|_\infty \geq \gamma_2 - \beta$, then $\mathbf{z} := \perp$

12 **return** $\sigma = (\mathbf{z}, c)$

7. CONCLUSION

CONCLUSION

Riscure vision on PQC

- PQC implementation in HW and SW has started,
  but we have time to do it right!
- Vulnerability Testing is the best way to obtain security assurance
  because it provides efficiency and risk reduction
- Pre-silicon analysis is becoming available and can shorten time to market
- Are you building a PQC solution? Riscure can help
  - Avoid design flaws
  - Test implementation for side channel leakage and fault injection robustness
  - Get your solution certified!

SOURCES

1. Cryptographic Suite for Algebraic Lattices
   https://csrc.nist.gov/CSRC/media/Presentations/Crystals-Dilithium/images-media/CRYSTALS-Dilithium-April2018.pdf
2. Side-channel analysis of NIST PQC candidates
   https://pqczoo.com/sca/
3. Post Quantum Telco Network Impact Assessment Whitepaper
   https://www.gsma.com/newsroom/wp-content/uploads//PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf
4. Breaking and Protecting the Crystal: Side-Channel Analysis of Dilithium in Hardware
   https://eprint.iacr.org/2022/1410.pdf
5. Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste
   https://eprint.iacr.org/2022/1713.pdf
6. 2022 Quantum Threat Timeline Report
   https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/
7. Understanding the Upcoming NIST Post-Quantum Cryptographic Standards
   https://content.pqshield.com/hubfs/Understanding%20the%20Upcoming%20NIST%20Post-Quantum%20Standards%20-%20Final%20Feb%2021.pdf

Questions?

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
www.riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79
inforequest@riscure.com

Riscure China
Room 2030-31, No. 989, Changle Road,
Shanghai 200031
China
Phone: +86 21 5117 5435
inforcn@riscure.com

riscure

driving your security forward