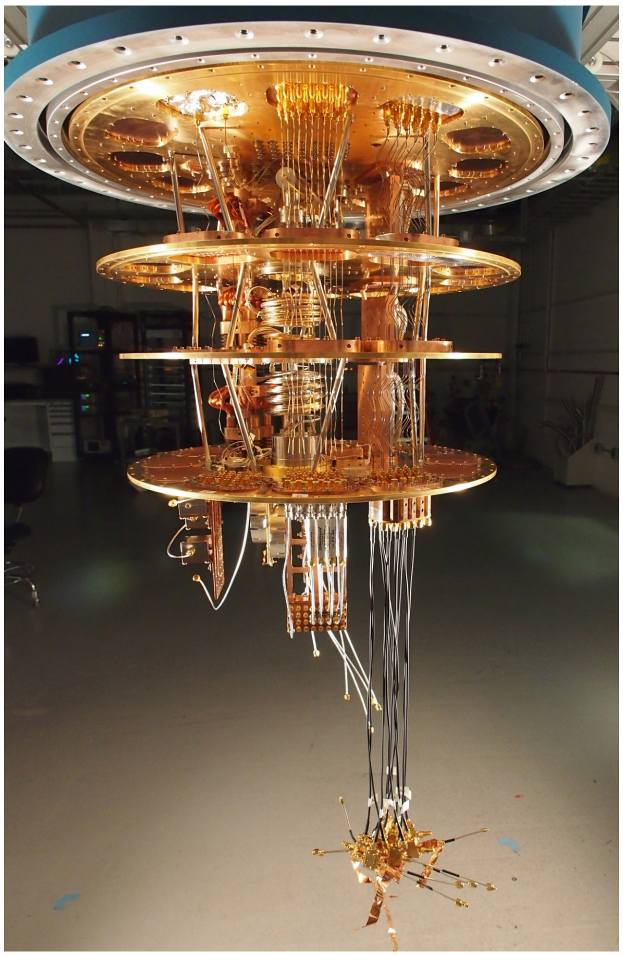
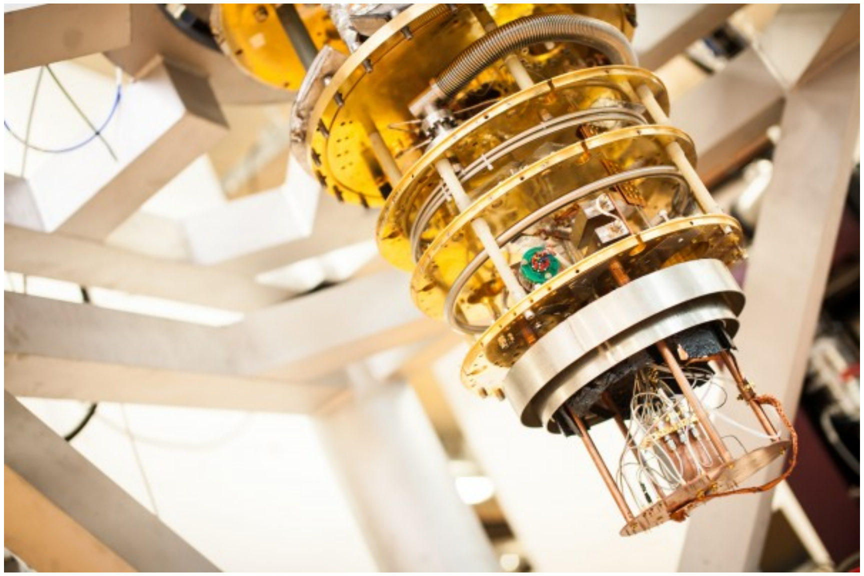
Post-Quantum Cryptography in Reconfigurable Hardware: Challenges, Opportunities, & State-of-the-Art



Kris Gaj, Ahmed Ferozpuri, Viet Dang, Duc Nguyen, Farnoud Farahmand, & Jens-Peter Kaps

ECE Department
George Mason University

Quantum Computers



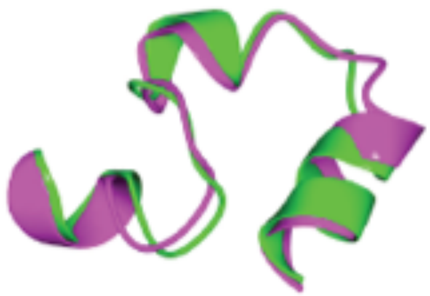
- **One of ten breakthrough technologies of 2017**
- Substantial investments by: Google, IBM, Intel, Microsoft, Alcatel-Lucent, NTT
- Quantum computers based on superconducting circuits operating in the temperature close to absolute 0 (~0.01 K)

- **November 2017: IBM's 50-qubit chip**
- **January 2018: Intel's 49-qubit chip, "Tangle-Lake"**
- **March 2018: Google's 72-qubit chip "Bristlecone"**

Photos: https://www.technologyreview.com

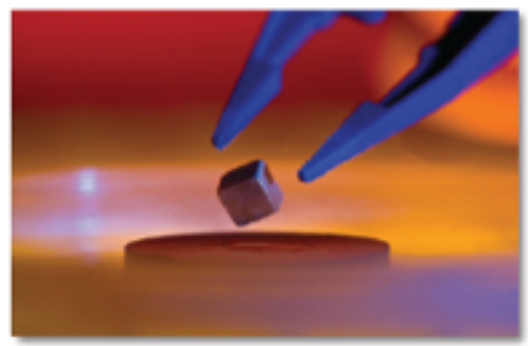
What Quantum Computers Can Do?

Model complex molecules



Health: Quantum chemistry for medicine

Model complex materials



Energy: Room-temperature superconductivity

Solve complex math problems

Security: factoring **and code breaking**

Nobel 2012 citation: *"The quantum computer may **change our everyday lives** in this century in the same radical way as the classical computer did in the last century."*

Source: Vandersypen, PQCrypto 2017

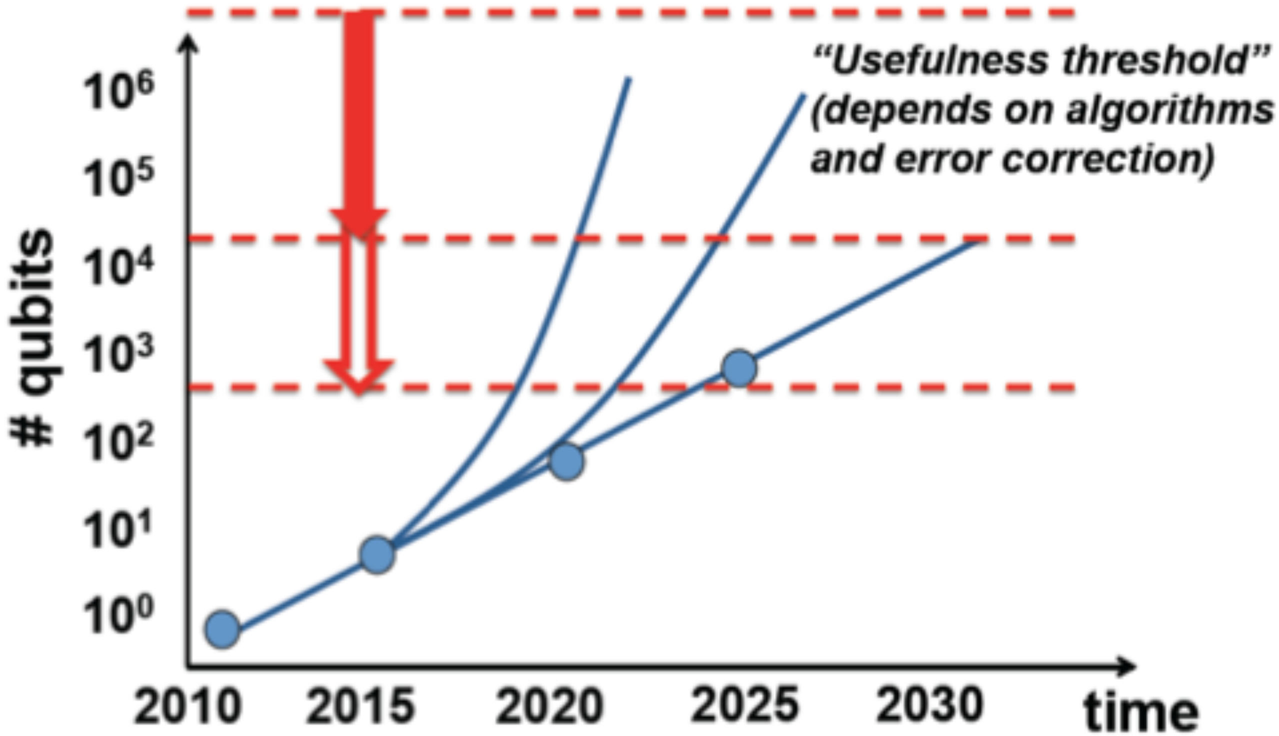
Quantum Computers & Cryptography

1994: Shor's Algorithm, breaks major public key cryptosystems based on

Factoring:	RSA
Discrete logarithm problem (DLP):	DSA, Diffie-Hellman
Elliptic Curve DLP:	Elliptic Curve Cryptosystems

independently of the key size
assuming
a sufficiently powerful and reliable quantum computer available

How Real Is the Danger?



"There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."
Dr. Michele Mosca
Deputy Director of the Institute for Quantum Computing, University of Waterloo
April 2015

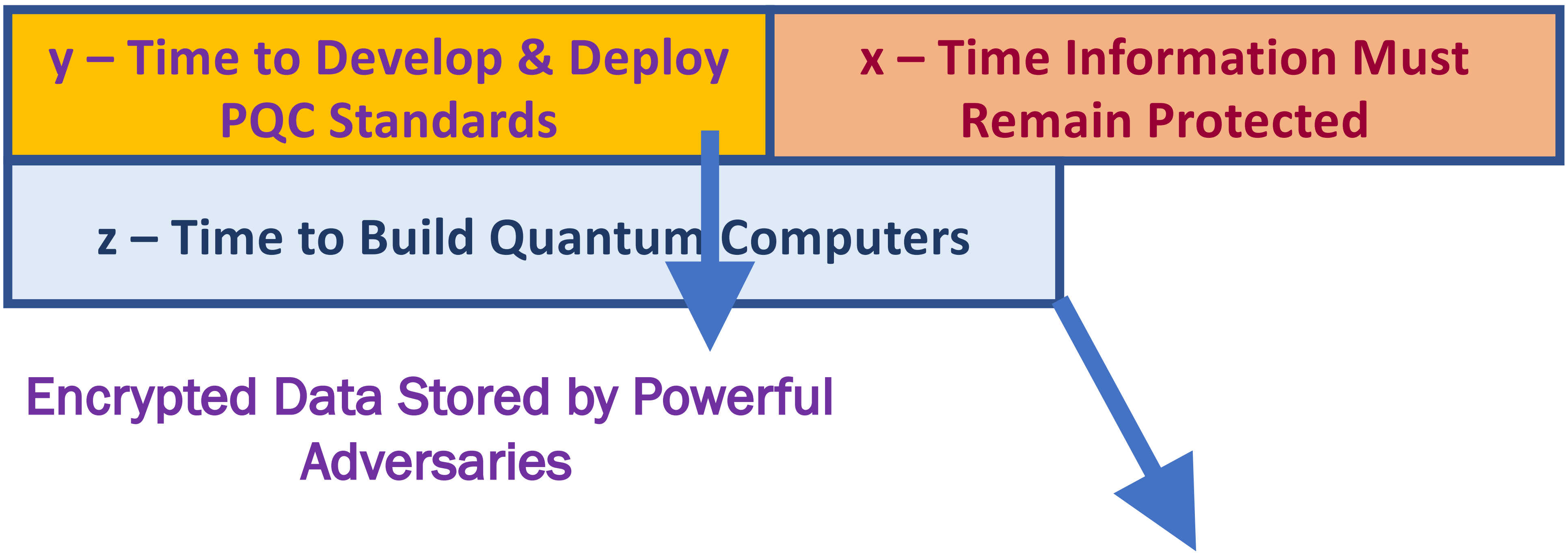
Source: Vandersypen, PQCrypto 2017

Post-Quantum Cryptography (PQC)

- Public-key cryptographic algorithms for which there are no known attacks using quantum computers
  - Capable of being implemented using any traditional methods, including software and hardware
  - Running efficiently on any modern computing platforms: PCs, tablets, smartphones, servers with FPGA accelerators, etc.
- Term introduced by Dan Bernstein in 2003
- Equivalent terms: quantum-proof, quantum-safe or quantum-resistant
- Based entirely on traditional semiconductor VLSI technology!

“Theorem” by Mosca

If $z < y + x$, then worry!



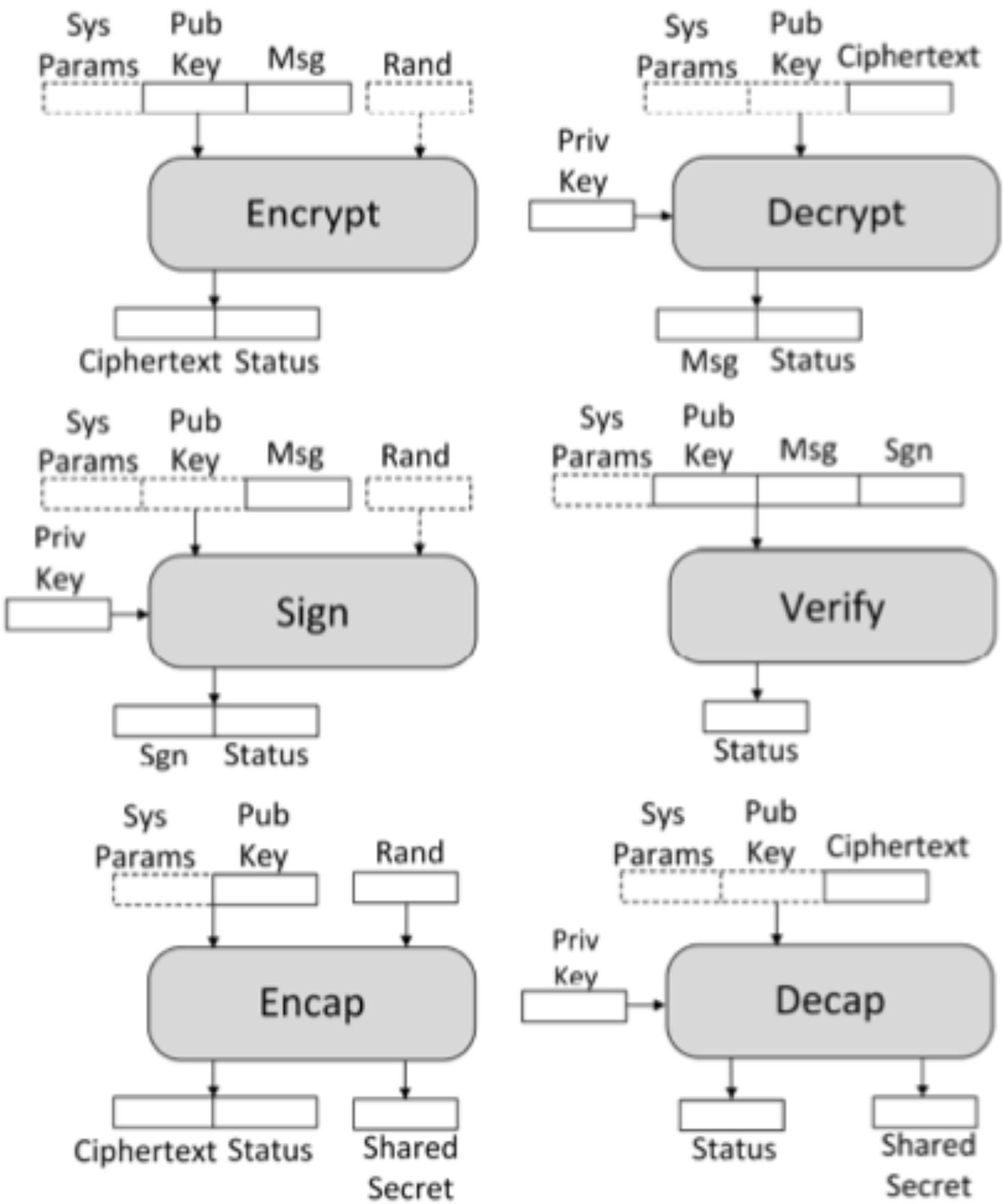
Encrypted Data Stored by Powerful Adversaries

No Announcement when Quantum Computer Available to NSA, Foreign Governments, or Organized Crime

NIST PQC Standardization Process

- **Feb. 2016:** NIST **announcement of standardization plans** at PQCrypto 2016, Fukuoka, Japan
- **Dec. 2016:** NIST **Call for Proposals** and Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms
- **Nov. 30, 2017: Deadline** for submitting candidates
- **Dec. 2017:** Announcement of the **First Round Candidates**
- **Apr. 2018:** The First **NIST PQC Standardization Conference**

Three Types of PQC Schemes



1. Public Key Encryption

2. Digital Signature

3. Key Encapsulation Mechanism (KEM)

Five Security Categories

Level	Security Description
I	At least as hard to break as AES-128 using exhaustive key search
II	At least as hard to break as SHA-256 using collision search
III	At least as hard to break as AES-192 using exhaustive key search
IV	At least as hard to break as SHA-384 using collision search
V	At least as hard to break as AES-256 using exhaustive key search

Leading PQC Families

Family	Encryption/ KEM	Signature
Hash-based		XX
Code-based	XX	X
Lattice-based	XX	X
Multivariate	X	XX
Isogeny-based	X	

XX – high-confidence candidates,   X – medium-confidence candidates

Round 1 Candidates

69 accepted as complete, 5 since withdrawn
26 Countries, 260 co-authors

Family	Signature	Encryption/KEM	Overall
Lattice-based	5	22	27
Code-based	2	16	18
Multivariate	7	2	9
Hash-based	2		2
Isogeny-based		1	1
Other	3	4	7
Total	19	45	64

Status of Round 1 Submissions

- 12 considered broken, 8 in need of serious tweaks

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqNTRUSign. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some attack scripts already posted causing total break or serious tweaks. Many more receiving detailed analysis.

Sources: Lange, ICMC May 2018 & pqc-comments@nist.gov

Risks of Early Hardware Implementations

GMU Team Implementation Developed in Fall 2017-Spring 2018. Preliminary Results Presented at the Code-Based Cryptography Workshop in April 2018.

Attack against the published parameter set announced on May 16

An efficient structural attack on NIST submission DAGS

Élise Barelli*[1] and Alain Couvreur†[1]

[1]INRIA & LIX, CNRS UMR 7161
École polytechnique, 91128 Palaiseau Cedex, France.

Abstract

We present an efficient key recovery attack on code based encryption schemes using some quasi–dyadic alternant codes with extension degree 2. This attack permits to break the proposal DAGS recently submitted to NIST.

keywords : Code-based Cryptography, McEliece encryption scheme, Key recovery attack, Alternant codes, Quasi–dyadic codes, Schur product of codes.

Comparison to Previous Contests

Similarities:

- Evaluation to be performed in **rounds** (12-18 months each)
- A **pool of candidates narrowed down** after each round
- Small **tweaks** allowed at the beginning of each round
- **Optimized software** implementation developed for various platforms
- **No** immediate **plans for obligatory hardware** implementations

Differences:

- Candidates not qualified to the next round (and not withdrawn by the authors) may be considered at a later date
- Taking into account quantum attacks, possible only on the platforms that do not exist at the time of the standard development
- Security analysis much more challenging and often controversial

Adi Shamir's Proposal

After the initial evaluation period (e.g., 3 years) the division of all schemes into the following categories:

- **2 Productions Schemes:** Recommended for actual wide-scale deployment. Highly Trusted.
- **4 Development Schemes:** Time-Tested, Trusted.

  At least 15 years of analysis behind them.

  Intended for initial R&D by industry.
- **8 Research Schemes:** Promising Properties, Good Performance. May contain some high-risk candidates. Main Goal: Concentrate the effort of the research community.

PQCRYPTO Consortium

11 universities and companies
Funded by European Commission under the H2020 program

TU/e technische universiteit eindhoven
BUNDESDRUCKEREI
DTU Danmarks Tekniske Universitet
Inria INVENTEURS DU MONDE NUMÉRIQUE
KU LEUVEN
NXP
50 Jahre RUB
Radboud Universiteit
TECHNISCHE UNIVERSITÄT DARMSTADT
University of Haifa
ACADEMIA SINICA

Initial Recommendations published in 2015
Co-authors of 22 Submissions

The Most Trusted Schemes – Encryption/KEM

Classical McEliece

- Proposed **40 years ago** as an alternative to RSA
- **Code-based** family
- Based on **binary Goppa codes**
- **No patents**
- **Conservative parameters (Category 5, 256-bit security)**:
  a) length n=6960, dimension k= 5413, errors=119
  b) length n=8192, dimension k= 6528, errors=128
- **Complexity of the best attack identical after 40 years of analysis, and more than 30 papers devoted to thorough cryptanalysis**
- **Sizes:**
  Public key: **a) 1,047,319 bytes, b) 1,357,824 bytes**
  Private key: a) 13,908 bytes, b) 14,080 bytes
  Ciphertext: a) 226 bytes, b) 240 bytes
- **Efficient Software** (Haswell, larger parameter set)
  - 295,930 cycles for encryption, 355,152 cycles for decryption
  - Constant time
- **Efficient Hardware** (Yale University & Fraunhofer Institute SIT, Germany): open-source, targeting FPGAs; CHES'17, PQCrypto'18

The Most Trusted Schemes – Signatures

Hash-based Schemes:

Security based on the security of
a single underlying primitive: hash function

Representatives:

SPHINCS-256 => SPHINCS+, Gravity-SPHINCS

Features:

Relatively large signatures (~ tens of kilobytes)

Signing more time consuming than verification

No reported hardware implementations

Likely Development Schemes – Lattice-based

- **NTRUEncrypt** – proposed in 1996, published in 1998; standardized by IEEE, ANSI, EESS; **no proof of security**
- **New Hope, CRYSTALS-KYBER, CRYSTALS-DILITHIUM, etc.** – New lattice-based schemes with **extended security proof**, smaller key sizes, and better efficiency

Reported Hardware Implementations:

- **Ring-LWE, BLISS, NewHope:** Ruhr University of Bochum, Germany
- **NewHope:** National Taiwan University, Academia Sinica, Taiwan
- **LWE:** Queen's University Belfast, ALaRI, RUB, Thales UK
- **Ring-LWE:** ESAT/COSIC KU Leuven, Belgium
- **Ring-LWE:** Universidad del Valle, Colombia
- **Binary RLWE:** The University of Texas at Austin, USA
- **NTRUEncrypt:** Technical University Munich, Germany
- **NTRUEncrypt:** George Mason University, USA

etc.

Major Implementation Challenges

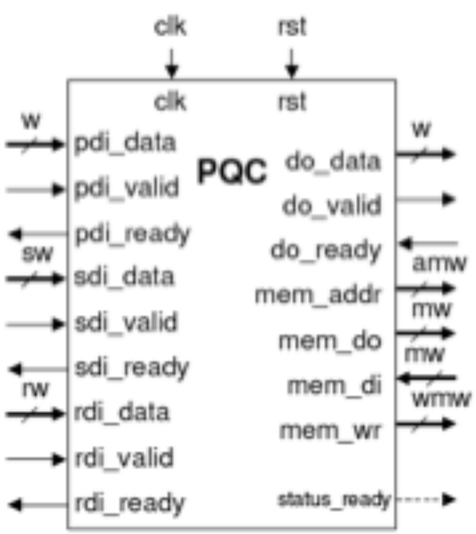
- **Mathematical complexity**
- Large amount of **man-power** required
- Large **keys and internal states**
- **Hardware resources** required for full parallelization
- New types of **basic operations**
- Need for **Random Sampling** not only from uniform but also from Discrete Gaussian distributions
- **Constant-time** implementations
- Need for **new SCA (Side-Channel Attack) countermeasures** against power and electromagnetic analysis
- **Plug-and-play replacement** for current public-key cryptography units
- Intermediate use of **Hybrid Systems**

PQC Hardware API proposed by GMU

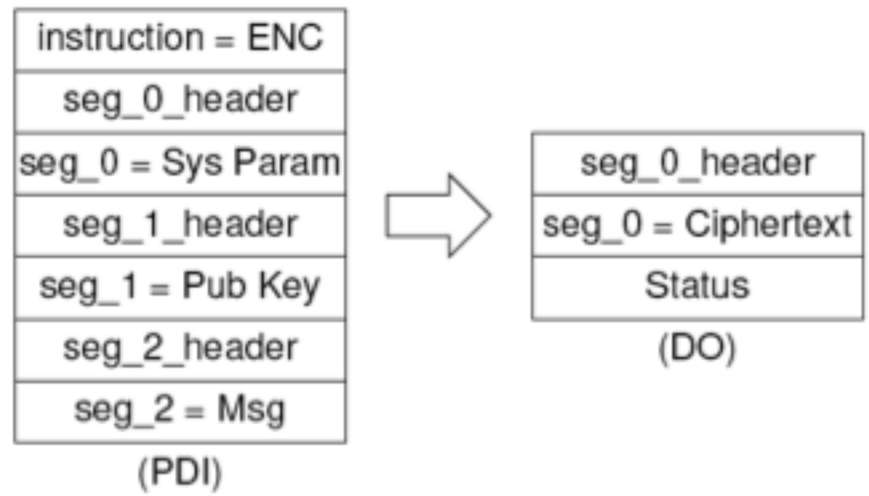
1. Minimum Compliance Criteria

- Encryption & decryption, Signature generation & verification
- Maximum message size
- Padding
- Permitted data port widths, etc.

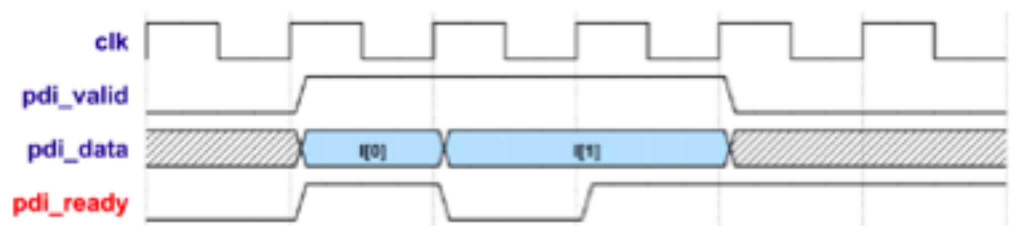
2. Interface



3. Communication Protocol



4. Timing Characteristics

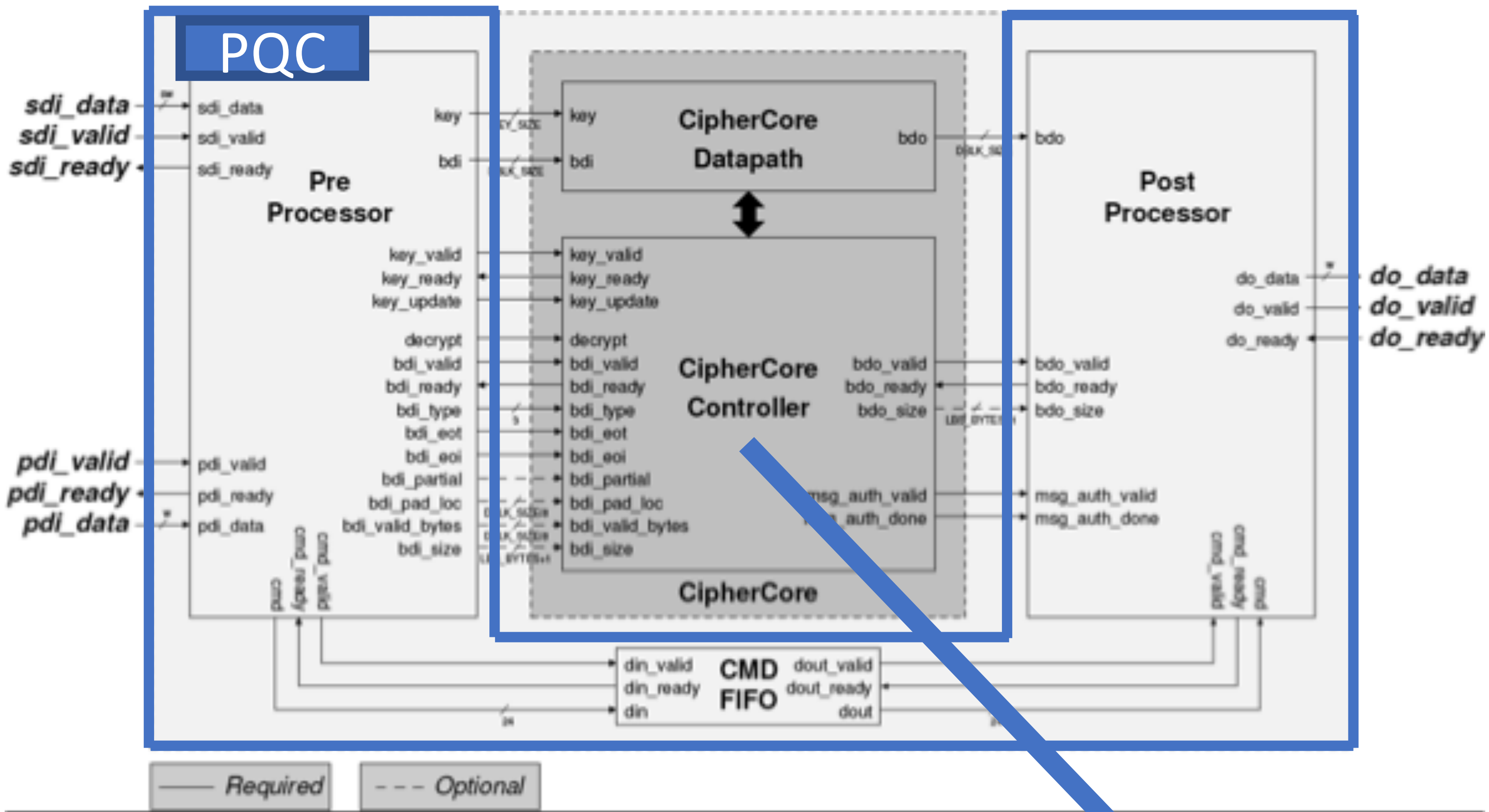


v1: October 2016 (ENC & SIG), v2: April 2018 (+ KEM & lessons)

PQC Development Package

Universal Testbench (HDL)

Pre- and PostProcessors Common for All Candidates (HDL)



Test Vector Generator (Python)

Library of Most Common Operations (HDL)

Major Optimization Targets

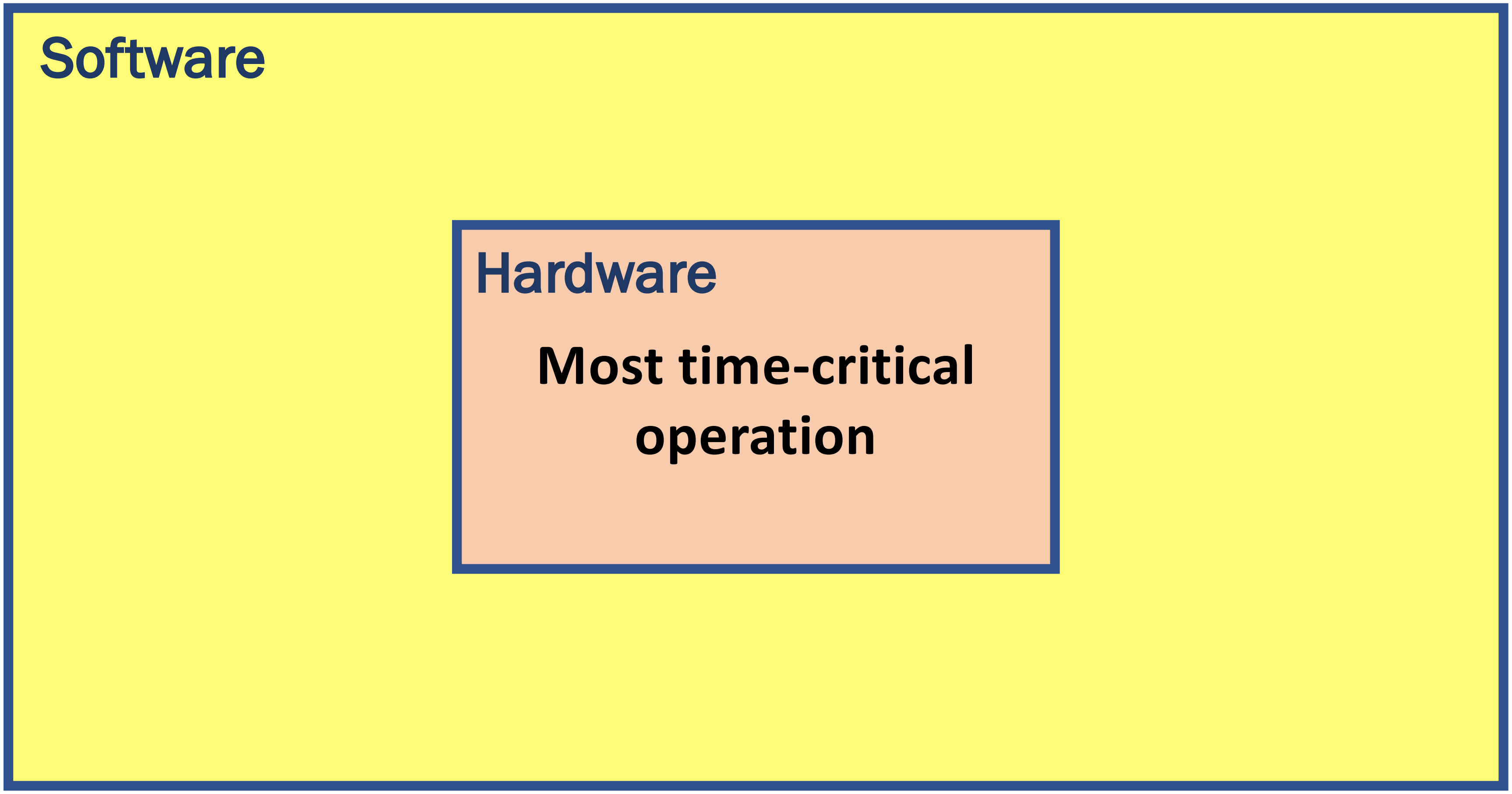
High-Speed

- Parallel processing
- Constant-time
- Parametric code

Lightweight

- Small area, power, energy per bit
- Resistance to power & electromagnetic analysis

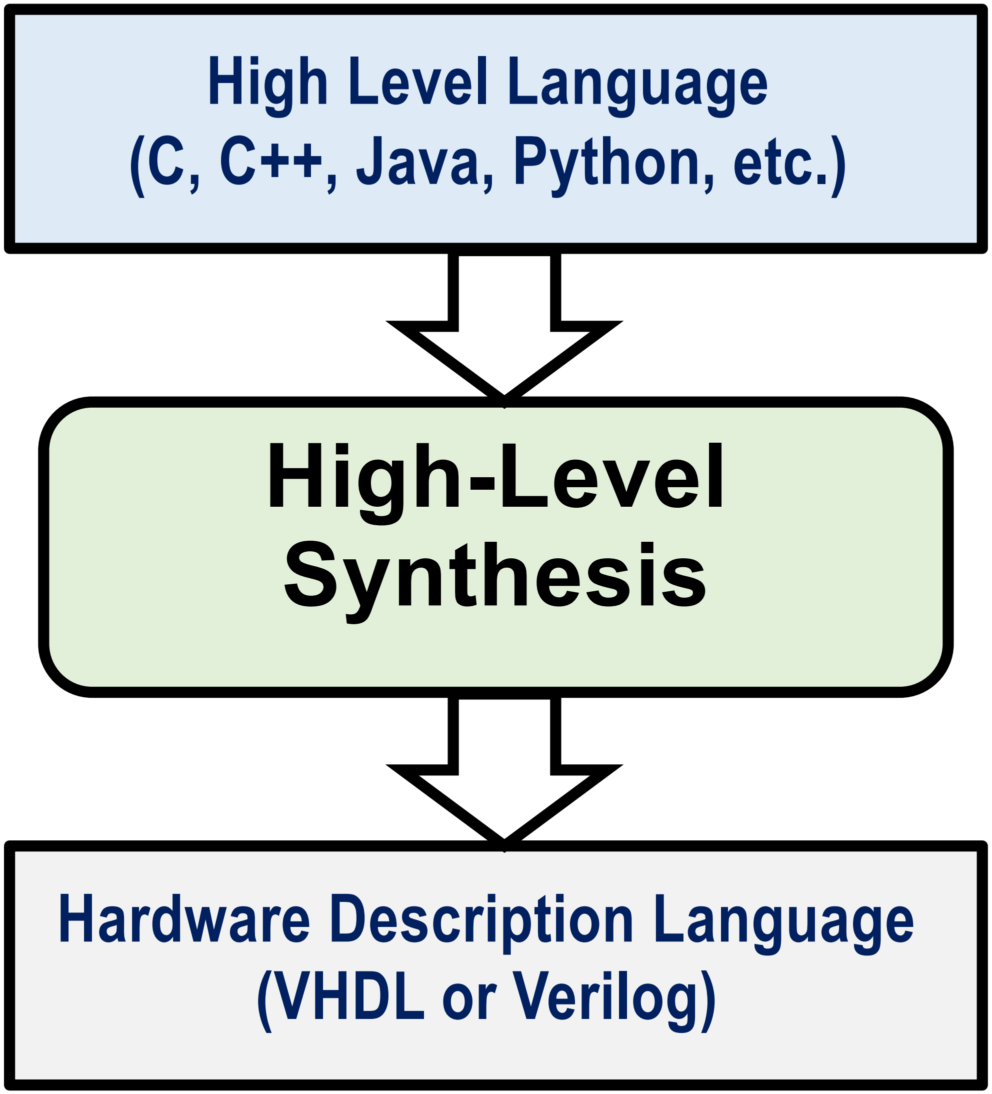
Software/Hardware Implementations



Possible Environments:

- Xilinx SDSoC
- Intel SoC Embedded Development Suite

High-Level Synthesis (HLS)



Case for High-Level Synthesis

- All submissions include **reference implementations in C**
- **Development time** potentially **decreased several times**
- **All candidates** can be **implemented by the same** group, and even the same **designer**, reducing the bias
- Results from High-Level Synthesis could have a **large impact in early stages of the competitions** and help narrow down the search (saving thousands of man-hours of cryptanalysis)
- Potential for quickly **detecting suboptimal code written manually**

Popular HLS Tools

Commercial (FPGA-oriented):

- Vivado HLS: Xilinx

Academic:

- Bambu: Politecnico di Milano, Italy
- DWARV: Delft University of Technology, The Netherlands
- GAUT: Universite de Bretagne-Sud, France

Academic & Commercial:

- LegUp: University of Toronto, Canada

Timeline of the NIST Standardization Effort

- **By Nov. 30, 2018:** Allowing/encouraging similar submissions to merge
- **Early 2019:** Beginning of Round 2
  - Candidates withdrawn or judged unsuitable by NIST
  - Candidates qualified to Round 2
  - Candidates left for future consideration
- **Aug. 2019:** Second NIST PQC Conference
- **Early 2020:** Beginning of Round 3
  - Candidates selected for standardization
  - Candidates withdrawn or judged unsuitable by NIST
  - Candidates qualified to Round 3
  - Candidates left for future consideration
- **2021-2024:** Possible future rounds
- **Possible parallel efforts by IETF, IEEE, ANSI, ETSI, ISO/IEC**

PQC Opportunities & Challenges

- The biggest **revolution in cryptography**, since the invention of public-key cryptography in 1970s
- Efficient **hardware implementations** in FPGAs and ASICs **desperately needed** to prove the candidates suitability for high-performance applications and constrained environments. **Collaboration sought by submission teams!**
- Likely **extensions to Instruction Set Architectures** of multiple major microprocessors
- **Start-up & new-product opportunities**
- **Once in the lifetime opportunity! Get involved!**

Q&A

Thank You!

Questions?

Comments?

Suggestions?

CERG: http://cryptography.gmu.edu

ATHENa: http://cryptography.gmu.edu/athena