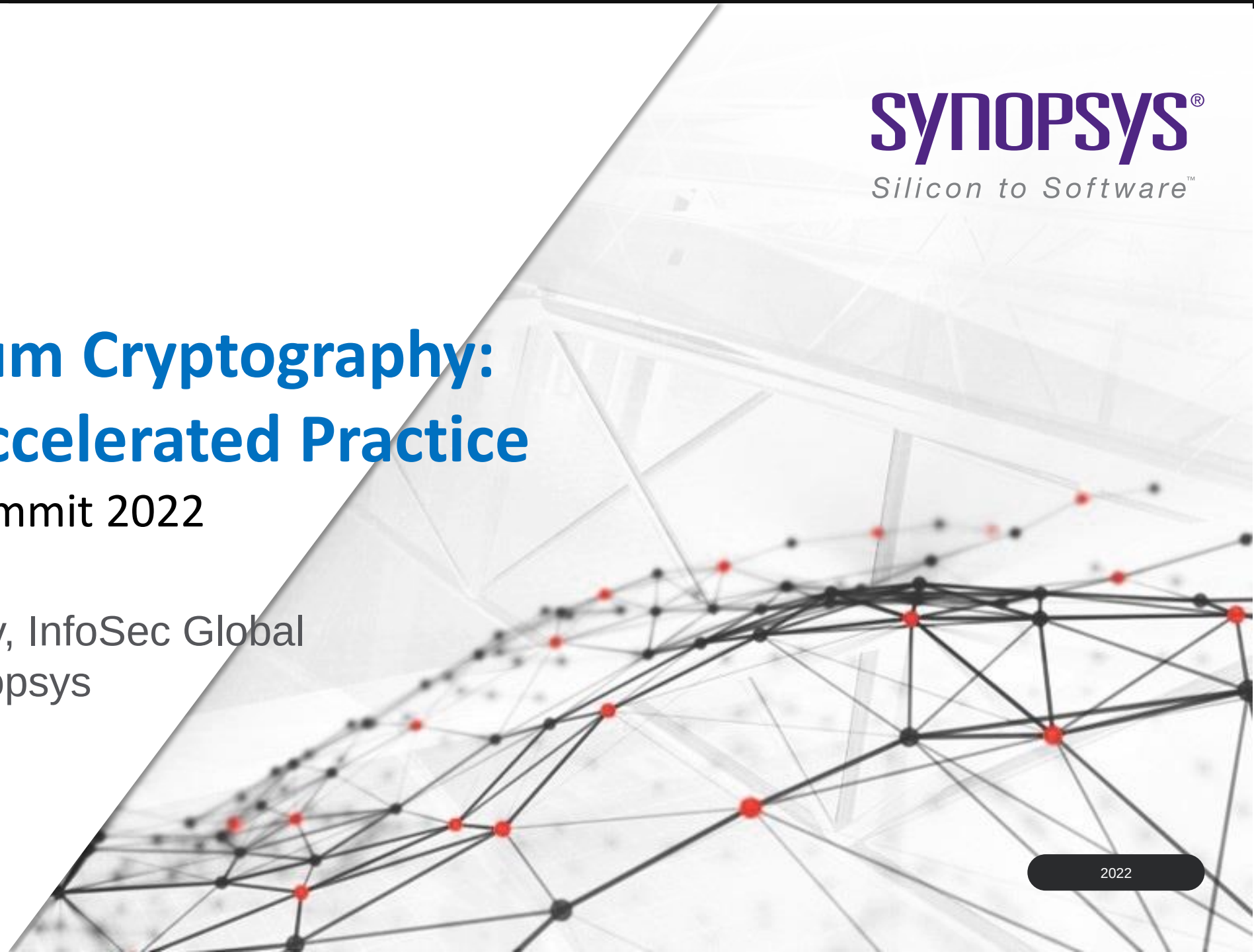
INFOSEC GLOBAL

SYNOPSYS®
Silicon to Software™

# Post-Quantum Cryptography: Theory to Accelerated Practice

ARC Processor Summit 2022

Vladimir Soukharev, InfoSec Global
Ruud Derwig, Synopsys



2022

# Abstract

## Post-Quantum Cryptography: Theory to Accelerated Practice

Post-Quantum Cryptography has received a fair amount of attention over the past few years, especially with the quantum threat becoming a closer reality. NIST's PQC standardization process is fully underway. Just recently, a big milestone on the path where the PQC algorithms are gradually becoming the cryptographic default was achieved – NIST announced the first set of standardized PQC algorithms. This means that it will be used as widely or possibly even more than the current conventional cryptography shortly. This talk will provide:

- An overview of PQC, the standardization process, and current and next practical steps to prepare for the transition to PQC. For this transition, there are several challenges to overcome. It will require crypto agility in protocols and implementations such that today's algorithms can be seamlessly replaced with the PQC alternatives. Agility in software via firmware updates is much easier than agility in hardware. However, just like for today's algorithms, HW acceleration and HW implementations are required for PQC to meet the performance as well as security targets.
- Explain how the acceleration of PQC algorithms can be done in a flexible way, such that a single accelerator can be used for traditional algorithms as well as for various PQC algorithms.
- A view 'from software to silicon' by covering end-to-end aspects of managing the PQC transition using a service-based architecture to perform the provisioning and security management of the agile crypto solutions embedded in connected devices.

# Agenda

- Introduction
- PQC Overview
- Implementation & Acceleration
- End-to-End: Trust Authority for Agile Crypto Management
- Conclusions

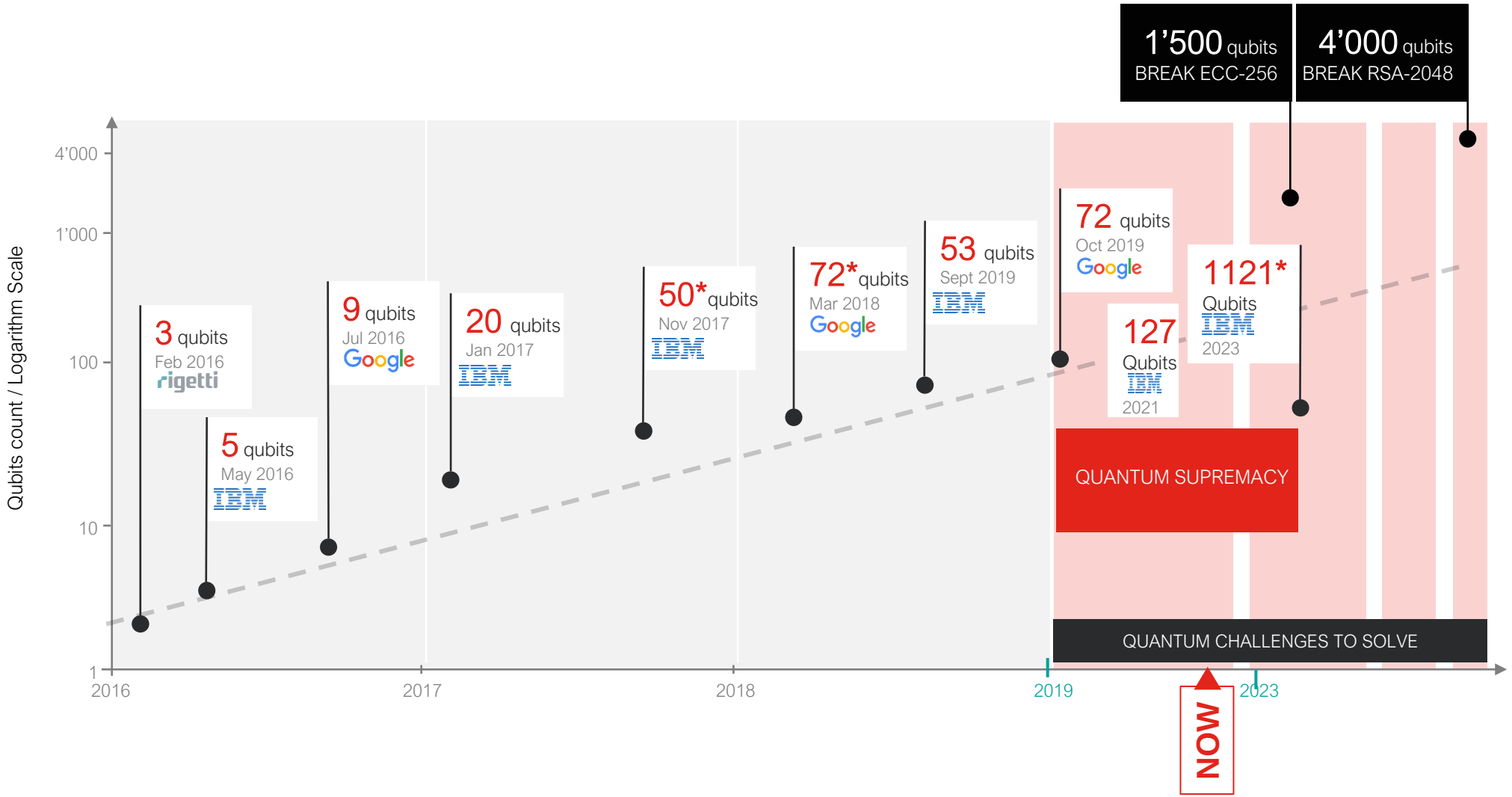
# Introduction

- **InfoSec Global** & **Synopsys** have a partnership working on Cryptographic Agility
- **Vladimir Soukharev:** Vladimir Soukharev is the Principal Cryptographic Technologist & Chief Post-Quantum Researcher at InfoSec Global. He is leading innovations and optimizations in modern cryptography, the path to cryptographic agility, and working on cryptographic lifecycle management. He is also conducting post-quantum cryptographic research and influencing and contributing to product development. Dr. Soukharev is actively working with *NIST on new post-quantum standards and with NCCoE on migration to PQC project*. He was part of the Centre of Applied Cryptographic Research and CryptoWorks21. Received his Ph.D. in Cryptography, Security, and Privacy from David R. Cheriton School of Computer Science at the University of Waterloo.
- **Ruud Derwig:** Ruud Derwig has 25+ years of experience with system architectures for embedded systems. Key areas of expertise are hardware and software IPs for security, operating systems, and other low-level platform software. He holds a master's degree in computing science and a professional doctorate in engineering from the Eindhoven University of Technology. Ruud worked at Philips Research and NXP Semiconductors and is currently Security & Systems Architect in Synopsys' Solutions Group. Ruud has contributed to various industry consortia, such as the CE Linux Forum, Linux Foundation, EEMBC, Zephyr RTOS, Eurosmart, and various European innovation projects.

# Agenda

- Introduction
- **PQC Overview**
- Implementation & Acceleration
- End-to-End: Trust Authority for Agile Crypto Management
- Conclusions

# Quantum Computer | History



# Quantum Security Levels

From NIST Talk

| Level | Security Description |
|---|---|
| I | At least as hard to break as AES128 (exhaustive key search) |
| II | At least as hard to break as SHA256 (collision search) |
| III | At least as hard to break as AES192 (exhaustive key search) |
| IV | At least as hard to break as SHA384 (collision search) |
| V | At least as hard to break as AES256 (exhaustive key search) |

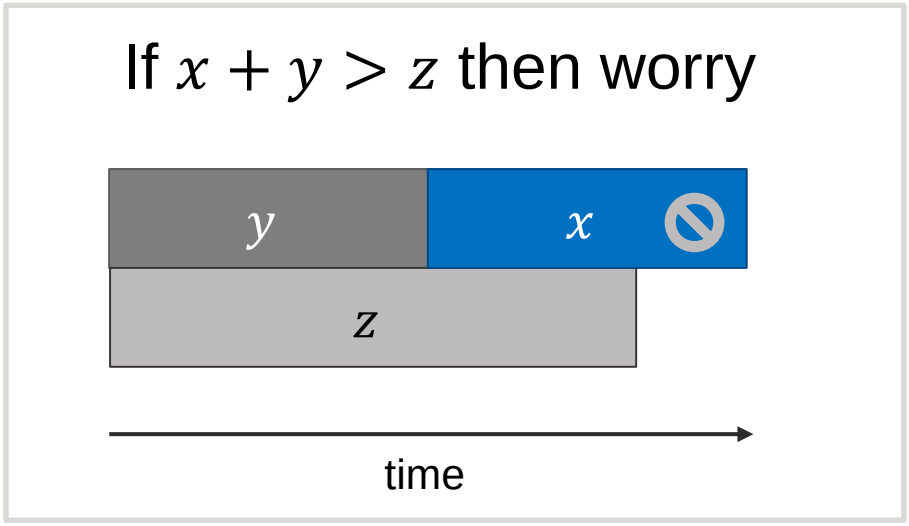
# Quantum Computer Threat

| Classical Crypto | Post-Quantum Status |
|---|---|
| **AES –** Symmetric Encryption | Larger key size needed |
| **SHA-2/3 –** Cryptographic Hashing | Larger output size needed |
| **RSA –** Asymmetric Encryption | **Broken** |
| **Diffie Hellman –** Key Exchange | **Broken** |
| **ECDSA –** Digital Signature | **Broken** |

# Do You Need to Worry?

By: Michele Mosca, https://eprint.iacr.org/2015/1075.pdf

- How long does your information need to be secure ($x$)
- How long to deploy quantum safe solutions ($y$)
- How long until a large-scale quantum computer ($z$)



# PQC | NIST PQC Timeline

| | |
|---|---|
| Feb 24-26, **2016** | NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016), Dustin Moody* |
| April 28, **2016** | NIST releases NISTIR 8105, Report on Post-Quantum Cryptography |
| Dec 20, **2016** | Formal Call for Proposals |
| Nov 30, **2017** | Deadline for submissions |
| Dec 4, **2017** | NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition", Dustin Moody* |
| Dec 21, **2017** | Round 1 algorithms announced (69 submissions accepted as "complete and proper") |
| Apr 11, **2018** | NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition", Dustin Moody* |
| April 11-13, **2018** | First PQC Standardization Conference - Submitter's Presentations |
| January 30, **2019** | Second Round Candidates announced (26 algorithms) |
| March 15, **2019** | Deadline for updated submission packages for the Second Round |
| August 22-24, **2019** | Second PQC Standardization Conference |
| July 22, **2020** | Third Round Candidates announced (15 algorithms) |
| October 1, **2020** | Deadline for updated submission packages for the Third Round |
| October 7, **2020** | Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms |
| June 7-9, **2021** | Third PQC Standardization Conference |
| July 7, **2021** | Comments for NCCoE document on Migrating to Post-Quantum Cryptographic Algorithms due |
| **July 2022** | First part of standards available AND call by NCCoE for solution to PQC migration and agility |
| **July 2022** | NCCoE, Industry Partners Create Center to Ease Migration Into Post-Quantum Cryptographic Era |
| **November 2022** | Fourth PQC Standardization Conference (Virtual) |
| **2023/2024** | Complete set of PQC Standards available |

NOW

INFOSEC GLOBAL SYNOPSYS Silicon to Software

# Crypto 101

- **Key Agreement (KA)**
  - A method when two parties exchange public keys and then each one uses his own private key and the other party's public key to produce a session key.
- **Public-Key Encryption (PKE)**
  - A method when sending party uses public key of the receiving party to encrypt the message. The receiving party uses its own private key to decrypt the message.
- **Key Encapsulation Mechanism (KEM)**
  - A method similar to PKE, but instead of a message, the sending party generates and encrypts the session key.
- **Digital Signatures (DS)**
  - A method when a signing party used its own private key to sign the message. Any party with the knowledge of the signer's public key can verify the validity of the signature.

- Cryptography requires difficult math problems. It should be computationally infeasible:
  - For any non-participating party to be able to obtain the session key
  - For any outside party to decrypt the message
  - For any party, who is not a signer, to forge (valid) signatures
  - For any party to be able to obtain a private key based on the knowledge of the public key

# Post-Quantum Cryptosystems

CO **Code** Based Cryptosystems

Security is based on the difficulty of decoding linear codes. It's famous for being the oldest public key encryption scheme that is potentially quantum safe.

HA **Hash** Based Cryptosystems

Security is based on hash functions. The most famous schemes are XMSS and SPHINCS.

✓

LA **Lattice** Based Cryptosystems

Security is based on the shortest vector problem in a lattice. The most famous schemes include Kyber or cryptosystems based on MLWE

✓

IS **Isogeny** Based Cryptosystems

Security is based on the problem of finding an isogeny between super singular elliptic curves. The most famous scheme is SIDH.

MU **Multivariate** Based Cryptosystems

Security is based on the problem of solving a set of non-linear equations. The most famous scheme is the Hidden Field Equations cryptosystems.

✗

# NIST Competition – Candidates

## Round 1 vs Current (Standardized + Round 4)

| | Round 1 | Standard | Round 4 |
|---|---|---|---|
| Lattice-based | 27 | 3 | 0 |
| Code-based | 22 | 0 | 3 |
| Multivariate | 9 | 0 | 0 |
| Symmetric/Hash-based | 3 | 1 + 2* | 0 |
| Isogeny-based | 1 | 0 | 1 |
| Other | 7 | 0 | 0 |
| Total | 69 | 4 + 2* | 4 |

*From parallel track for stateful hash-based digital signatures.

# Next Steps: Post-Quantum and Need for Crypto Agility

## NIST PQC Selected Schemes

- 3 lattice-based schemes – **Kyber, Dilithium, Falcon**
- 1 hash-based scheme (stateless) – **SPHINCS+**
- 2 hash-based schemes (stateful) – **XMSS, LMS**

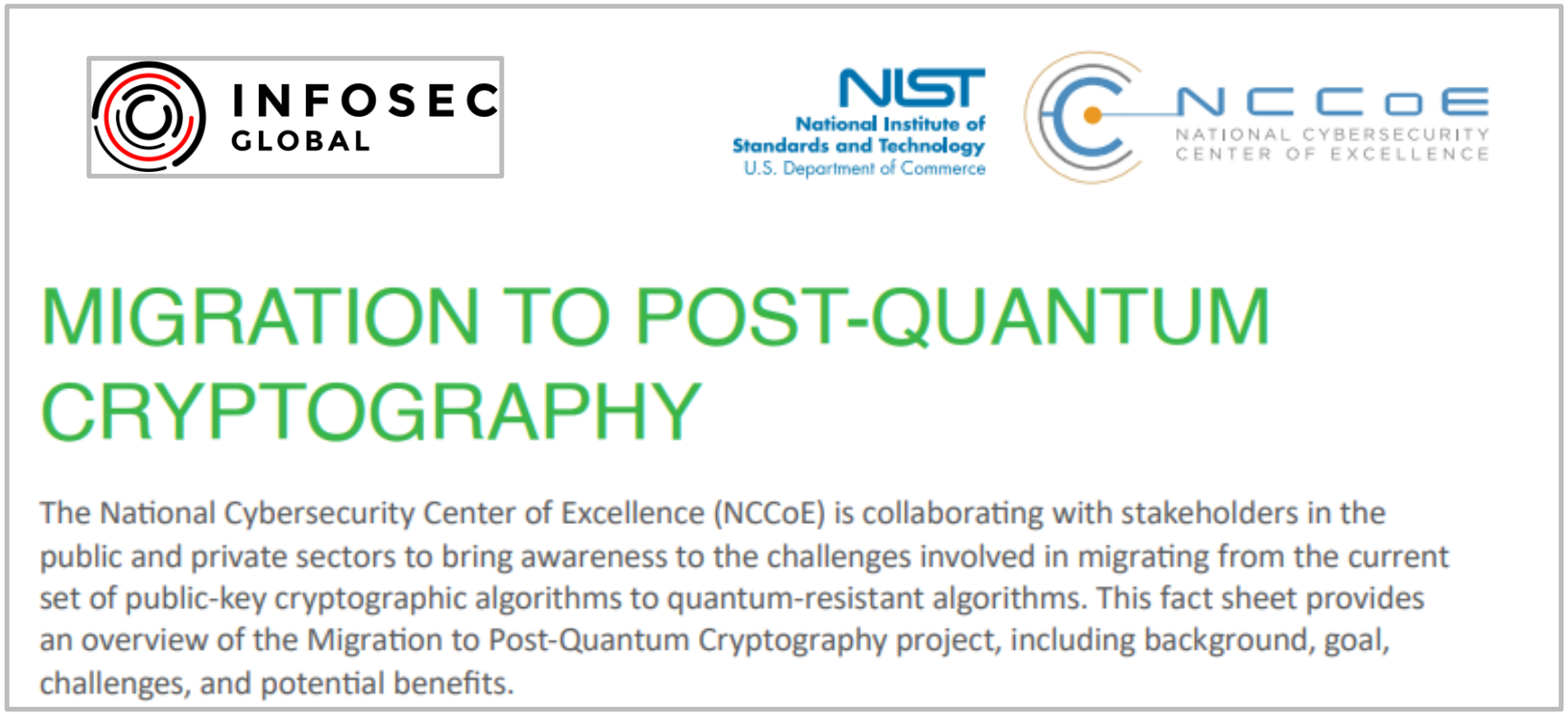
## NIST PQC Schemes to be Selected

- 1 code-based scheme – one of **BIKE, HQC, Classic McEliece**
- 1 isogeny-based scheme? – Current candidate **SIKE** is broken, but there could be **other isogeny-based schemes**
- Another track launched for more digital signatures!
- More KEMs?

## Other Standards

- IETF
- CFRG
- …

# PQC Initiative | NCCOE PQC Migration

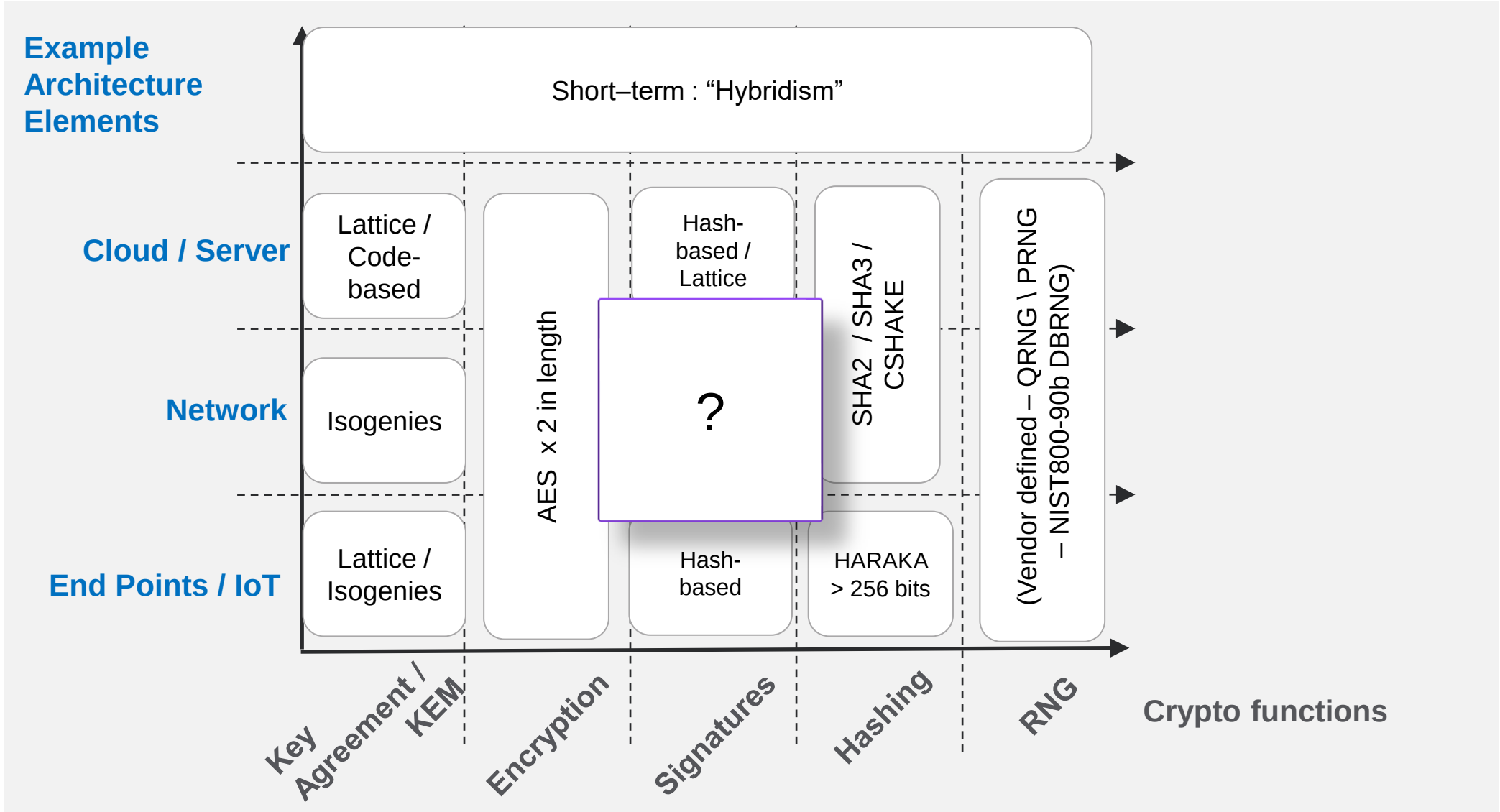



https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

## Goals

| | | | |
|---|---|---|---|
| Support identification of Public Keys algorithms usage | Provide migration tools, guidelines and practices. | Help protect Sensitive Data with PQC | Support Developers migrate to PQC |

# Agility Allows for Choices: Quantum-Safe



# Crypto Agility | Architecture

APPLICATIONS

PLATFORM

HARDWARE | FIRMWARE | DRIVERS | OS | RUNTIME | APPLICATIONS

## Crypto Agility | SDK

### Crypto Agility API

### Crypto Providers

- Provider **Classical**
- Provider **FIPS 140-2**
- Provider **PQC**
- Provider **PKCS-11**
- Provider **Hybrid***
- Wrapper **LibOQS**
- Wrapper **OpenSSL**
- Extension **API**

- Crypto **Policy**
- Crypto **Vault**

**Platform Integration**: Side-channel counter-measures | Optimizations | TEE | TPM | Other

*Recommended to be used until the final PQC standard is available

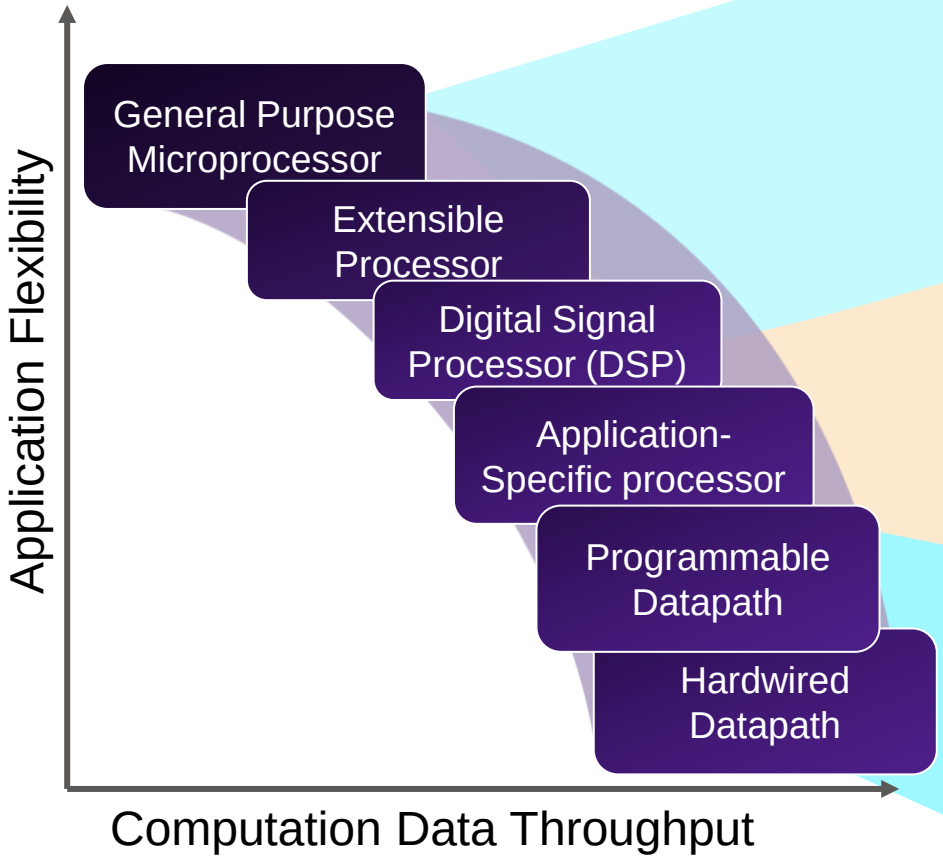
INFOSEC GLOBAL SYNOPSYS® Silicon to Software™

# Agenda

- Introduction
- PQC Overview
- **Implementation & Acceleration**
- End-to-End: Trust Authority for Agile Crypto Management
- Conclusions

# Synopsys Processing Solutions *for Security Algorithms*

## IP & Tools Address Broadest Range of Processing Requirements



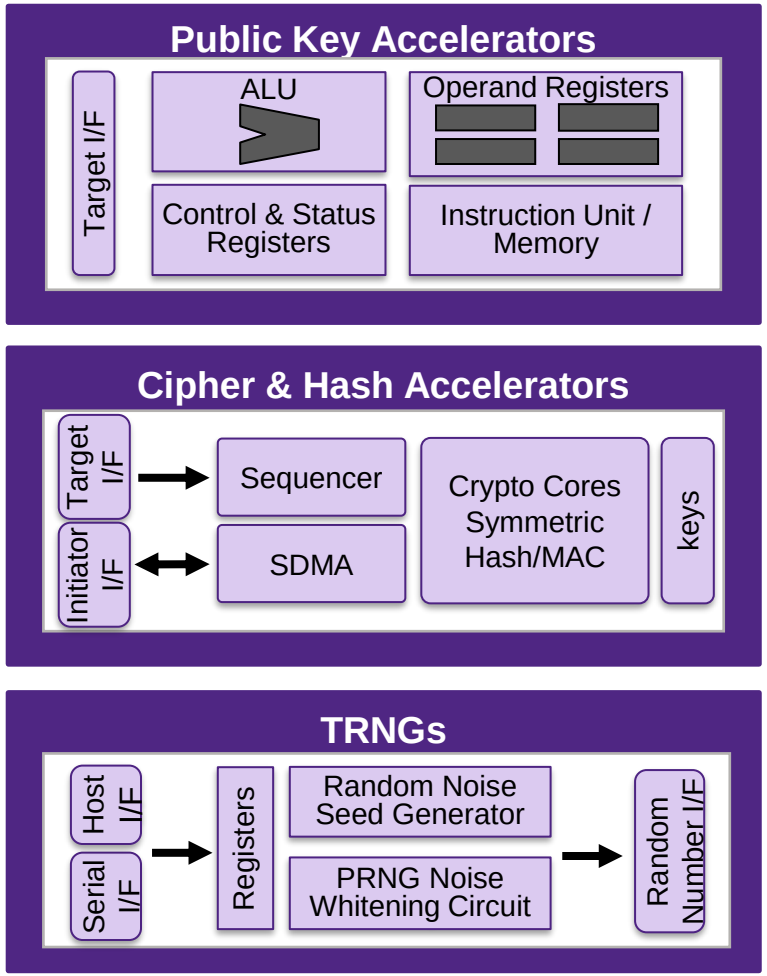

- ARC® Processor IP
  - Performance-Power-Area optimized for embedded applications
  - Highly configurable and extensible architecture
  - Based on common, code-compatible ISA & ecosystem
- ASIP Designer Tool
  - Automates creation of application-specific instruction-set processors (ASIPs)
  - User-designed, software programmable processors tailored to a specific application
- Security IP Hardware Crypto Engines
  - Highly integrated, standards-based solutions
  - Enable the most efficient silicon design and highest levels of security

INFOSEC GLOBAL

SYNOPSYS® Silicon to Software™

# Hardware Acceleration for PQC

Support for Traditional and Post-Quantum Crypto Algorithms




**Existing symmetric/hash engines and TRNG remain effective solutions**

- Quantum safe with larger keys
- Support hash-based PQC and key generation, binomial distributions

**Requirements for Public Key Accelerator IP for PQC**

**Next Gen Public Key Accelerators**

- PQC algorithms
- ECC & RSA
- Hybrid Crypto
- Crypto agility
- High performance
- Scalable
- Simple integration
- Full offload from processor
- Physical Security

INFOSEC GLOBAL

SYNOPSYS® Silicon to Software™

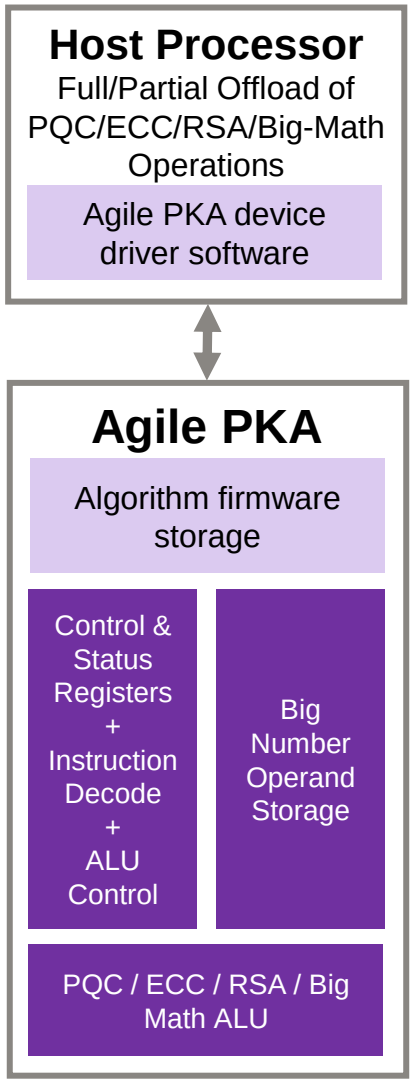
# Compute Intensive Math in PQC Systems

Looking at the PQC systems by composite functions allows us to determine which functions are overlapping as candidates for hardware or firmware implementations.

| Operation | PQC System |
|---|---|
| Addition | Dilithium (Keygen, Sign, Verify),<br>Falcon (Keygen, Sign, Verify) |
| Subtraction | Dilithium (Keygen, Sign, Verify),<br>Falcon (Keygen, Sign, Verify) |
| Multiplication | Kyber (KeyGen, Encrypt, Decrypt),<br>Dilithium (Keygen, Sign, Verify),<br>Falcon (Keygen, Sign, Verify) |
| Matrix Multiplication | Dilithium (Keygen, Sign, Verify),<br>Falcon (Keygen, Sign, Verify) |
| Extended Euclidean Algorithm | Falcon (KeyGen) |
| Polynomial Inversion | Falcon (KeyGen) |
| Polynomial Matrix Multiplication under NTT | Kyber(KeyGen, Encrypt, Decrypt), Dilithium(Keygen, Sign, Verify) |
| Polynomial Addition under NTT | Kyber(KeyGen, Encrypt, Decrypt), Dilithium(Keygen, Sign, Verify) |

# How We Approach Next Gen Agile PKA

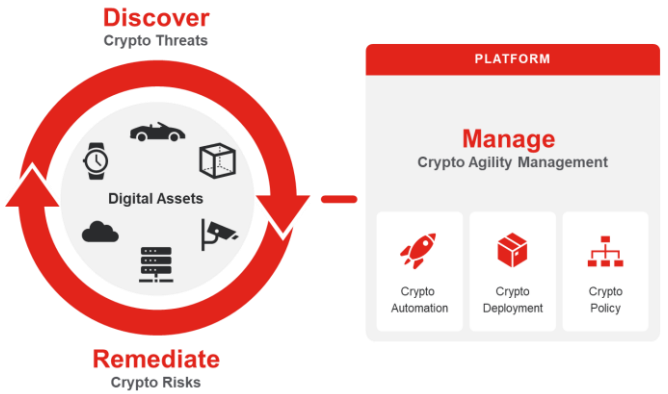
- Supported Algorithms
  - Hybrid ECC/RSA + PQC
  - Base primitive algorithms (modular exp, point multiplication, polynomial multiplication, big math)
  - End-to-end application algorithms (signatures, encrypt/decrypt, key generation)
- Hardware + Embedded Firmware
  - Programmable design with algorithms in firmware library to run on big math ALU hardware
  - Firmware offers flexibility for known/new/changing algorithms
  - Hardware offers scalability and configurability for various PPA targets
- Host Software
  - Device driver and integration into Synopsys DWC Crypto Software Library
  - Integration into ISG AgileSec Crypto SDK and Trust Authority Provisioning/Crypto Management
- Complete Synopsys Security Product
  - Not just efficient algorithm implementation: Secure Key Port,  Physical Security: DPA, FI, etc.
  - Simple SoC integration: standard bus I/F, configurable product, fully verified, testbench incl., etc.



# Agenda

- Introduction
- PQC Overview
- Implementation & Acceleration
- **End-to-End: Trust Authority for Agile Crypto Management**
- Conclusions

# Vision | One Stop Shop For Managing Cryptography




Customer Specific Crypto Requirements

**Secure Operations**

- Secure process/workflow to manage IC chip life cycle
- Secure process/workflow to manage crypto assets
- Secure framework for external applications to use crypto services

**Secure Software**

- PQ Cryptography
- Crypto Agility Management Platform to manage crypto assets and life cycle

INFOSEC GLOBAL

**Secure Hardware**

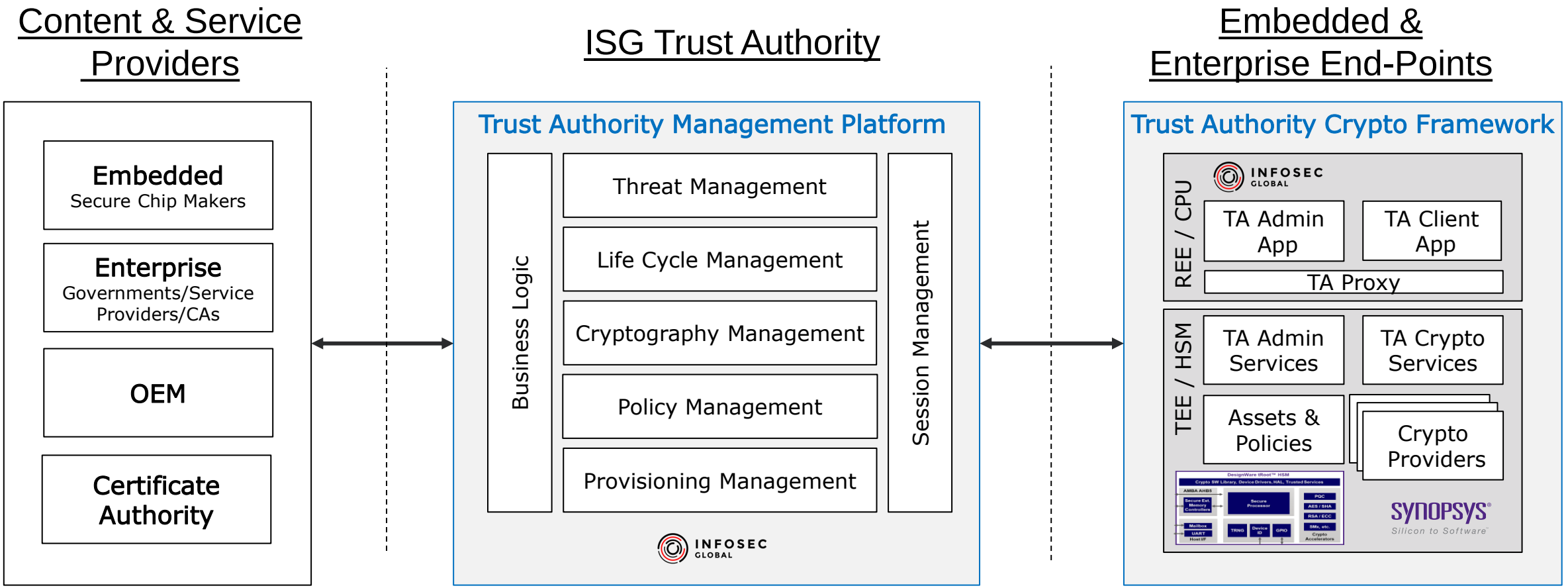
- Secure processor
- Crypto accelerator
- Trusted Execution Environment

SYNOPSYS® Silicon to Software™

Crypto Services Delivered to Application

Crypto Agility Management Platform and Crypto Agility Programming Framework INFOSEC GLOBAL

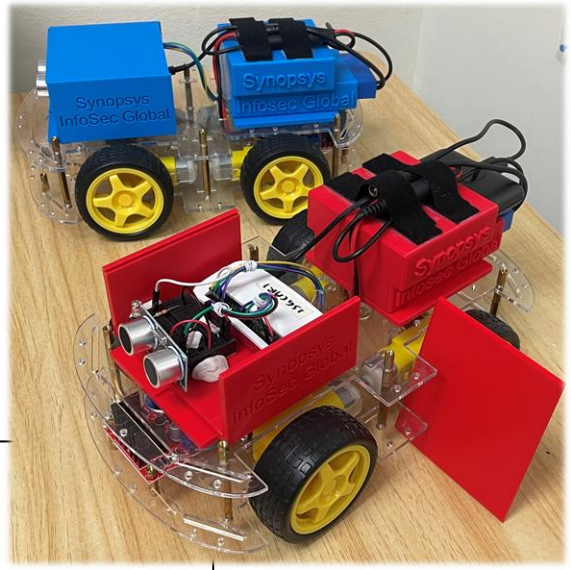
# Trust Authority I Architecture

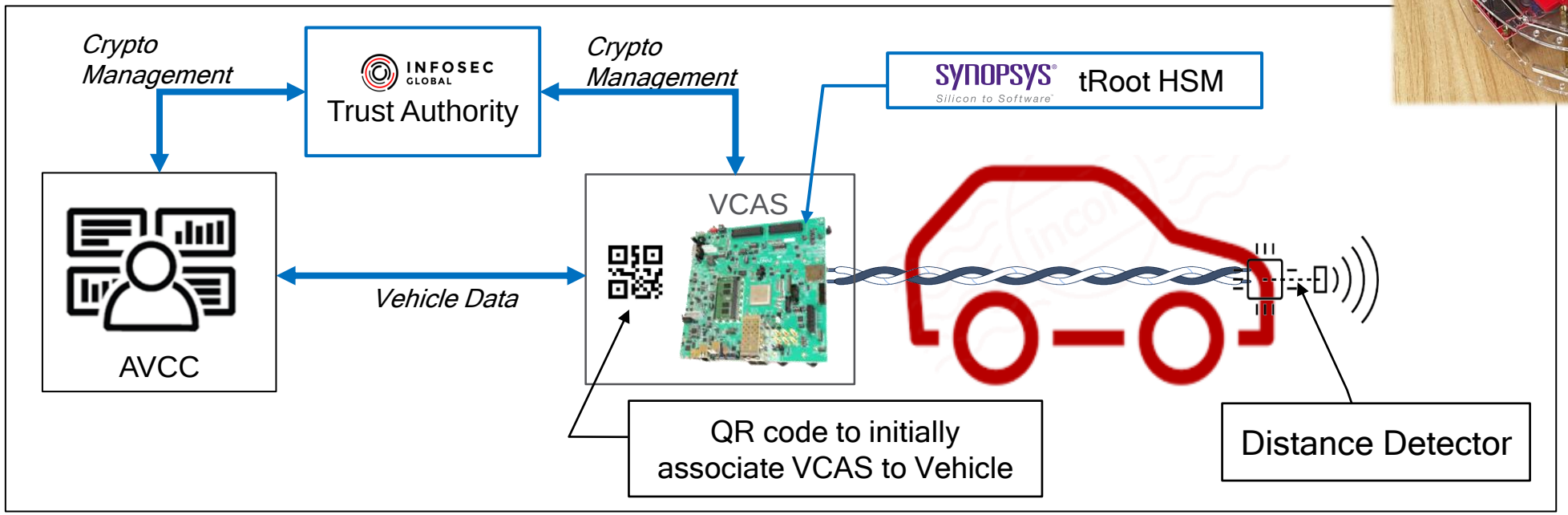



**End-to-End Management of Devices with Crypto Assets**

# Demonstration of Agile Cryptography & TA in Action

- Autonomous Vehicle with Vehicle Collision Avoidance System to constantly detect the distance between AV and obstacle, then display distance on AV Control Centre monitoring screen
- When Trust Authority detected crypto vulnerability, Trust Authority recommends AVCC to initiate crypto algorithm update in VCAS
- Crypto algorithm is then changed on the fly and AVCC is auto-synchronized with new crypto algorithm to continue displaying the readings



# Agenda

- Introduction
- PQC Overview
- Implementation & Acceleration
- End-to-End: Trust Authority for Agile Crypto Management
- **Conclusions**

# Conclusions

- Advance in Quantum Computing poses a threat to traditional public key cryptography
- Even though Quantum Computers won't be there tomorrow, the transition starts today
- NIST and others are investigating & standardizing new PQC security algorithms
- First standards expected in 2023-2024
- PQC crypto standards use different algorithms, requiring different hardware acceleration

  ✓ Synopsys & Infosec are ready to help with your next SoC

- What to do today?
  - Adopt Crypto Agility: minimize dependency on specific algorithms
  - Hybrid solutions combining traditional and PQC are a safe bet
  - Visit the Infosec & Synopsys demonstrator and learn more!

# Thank You

# Want to Learn More?
# Post-Quantum and Agility Government Initiatives

- USA
  - **NIST PQC Algorithms**
    - https://csrc.nist.gov/projects/post-quantum-cryptography
  - **NCCoE Participation**
    - https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
  - **CCC (Computing Community Consortium) Contribution**
    - https://cra.org/ccc/events/identifying-research-challenges-in-pqc-migration-and-cryptographic-agility/
- International
- Similar initiatives around the world are being launched