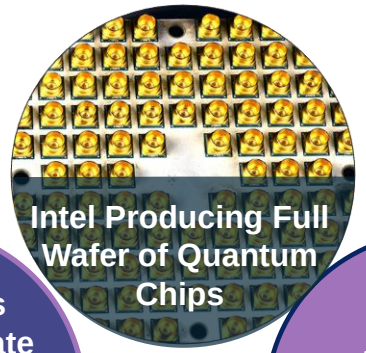

# Post-Quantum Suite-Q™ For Embedded Devices

Presenter: Brett Kim – Senior Embedded Solutions Engineer



MICROCHIP

# A New Quantum Age




The Race is on to Dominate Quantum Computing - The Economist

'At Last America Is Moving On Quantum' – Forbes

China Wants to win Computing Arms Race - Bloomberg







MICROCHIP

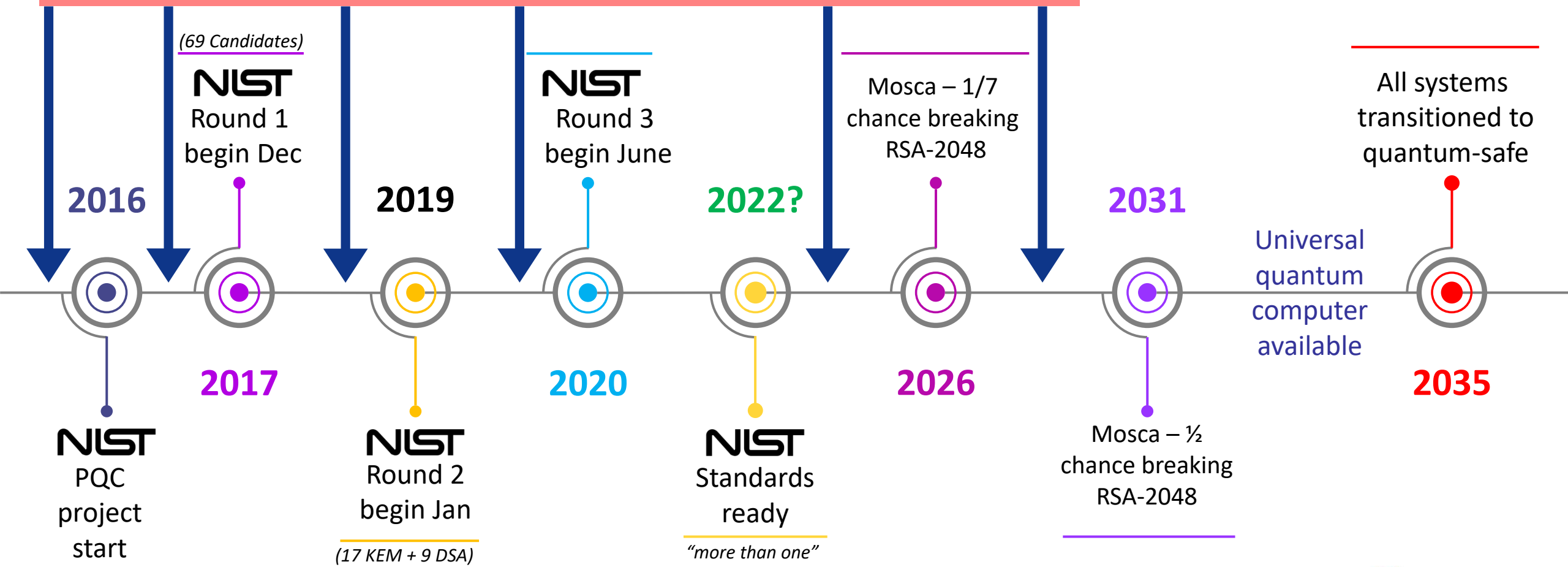
# Quantum Threat to Information Security

- IoT is the future of computing
- Quantum is the future of computing performance
- IoT represents major security vulnerabilities
- Quantum represents a major security threat
- Must design security specific for IoT
- Must transition to quantum-safe security
- Question: When should we start?

- Better question: How long does the transition take?
- Best question: When will we be at risk?

# Quantum Threat Timeline

Retroactive Decryption:
Record encrypted communication now,
Decrypt once quantum computers are available






MICROCHIP

# Post-Quantum Key-Exchange Mechanism

## Code-based

Key size: 100’s of Kilobytes

## Lattice-based

Key size: Kilobytes

## Isogeny-based

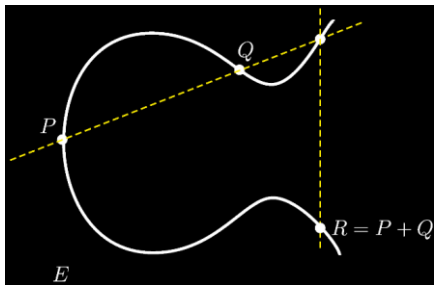
Key size: 100’s of bytes

# Suite-Q™ for IoT

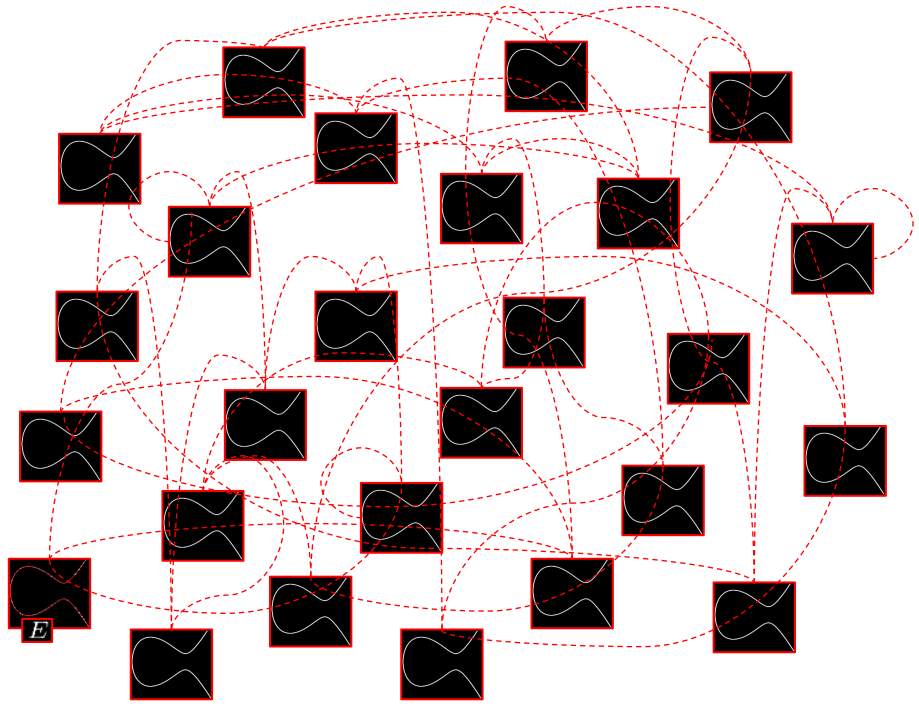
- **What is Suite-Q?**
  - An all inclusive, quantum-safe security IPs designed for the IoT environment
- **Why Suite-Q?**
  - IoT and quantum-safe security are increasingly important. Incorporate tomorrows security, today
- **When is it needed?**
  - Quantum-safe products need to be available before quantum computers as transitions take years

# From ECC to SIKE

- Elliptic Curve Cryptography is the current standard and used widely
- ECC (like RSA and Diffie-Hellman) is not quantum safe
- SIKE Supersingular Isogeny Key Encapsulation
- SIKE is quantum-safe and works on maps, called isogenies, between elliptic curves



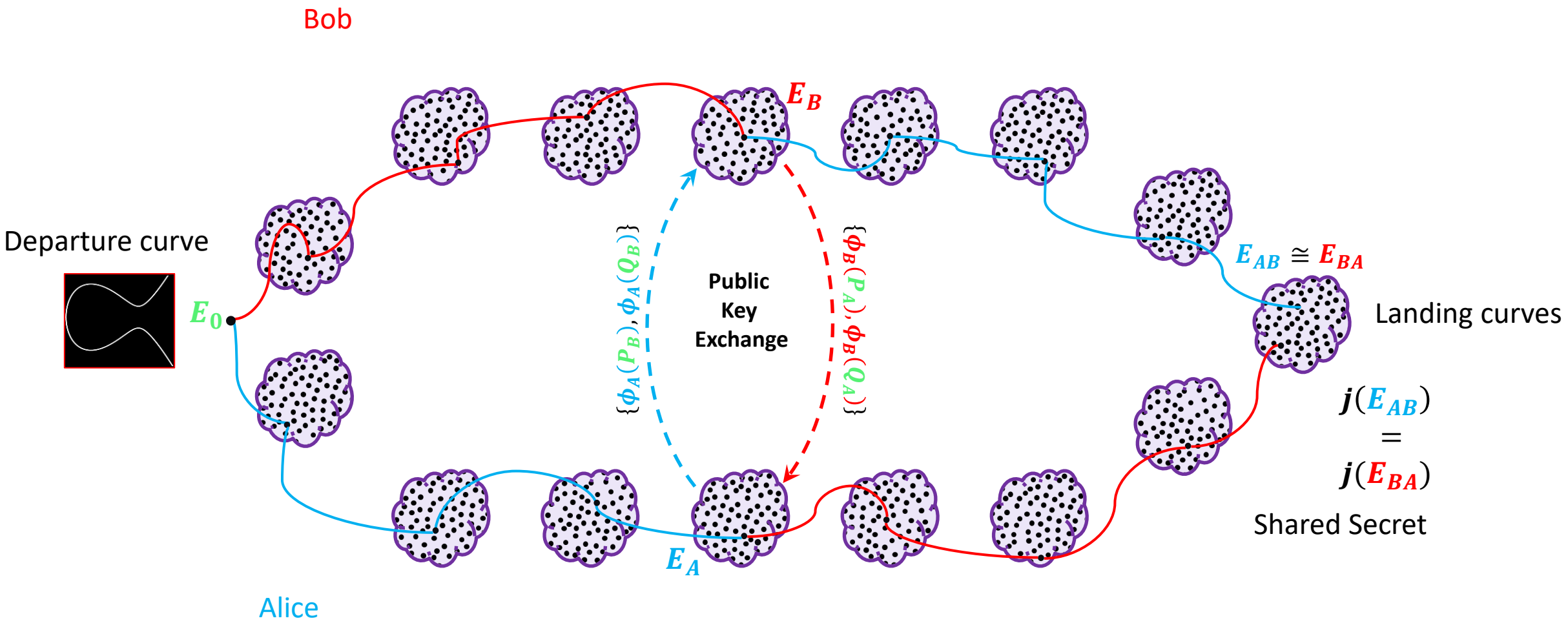

ECC vs SIKE






MICROCHIP

# SIDH/SIKE Protocol






MICROCHIP

# SIKE Key Sizes

| NIST Level | Prime Size (bits) | Prime | Public Key Size (bytes) | Compressed Public Key Size (bytes) |
|---|---|---|---|---|
| 1 | 434 | $2^{216}3^{137} - 1$ | 330 | 196 |
| 2 | 503 | $2^{250}3^{159} - 1$ | 378 | 224 |
| 3 | 610 | $2^{305}3^{192} - 1$ | 462 | 273 |
| 5 | 751 | $2^{372}3^{239} - 1$ | 564 | 331 |

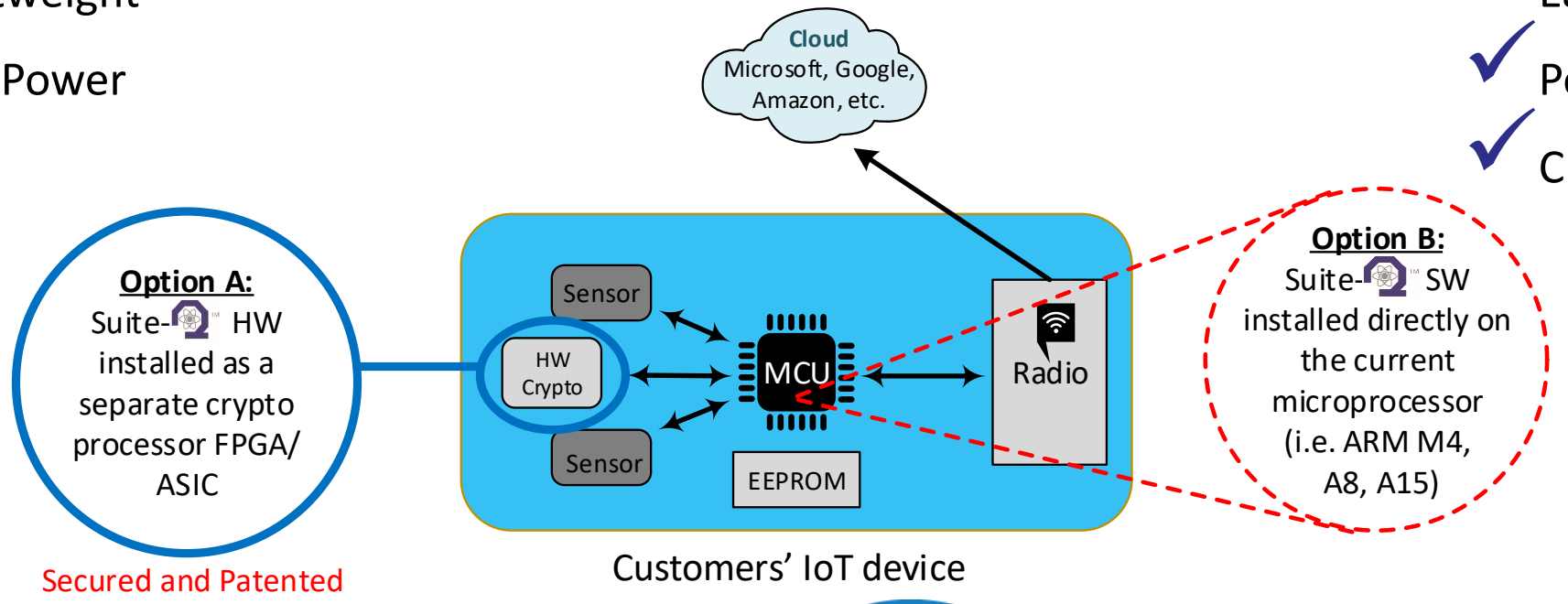
# Product: Suite-Q™

Suite-Q Hardware License

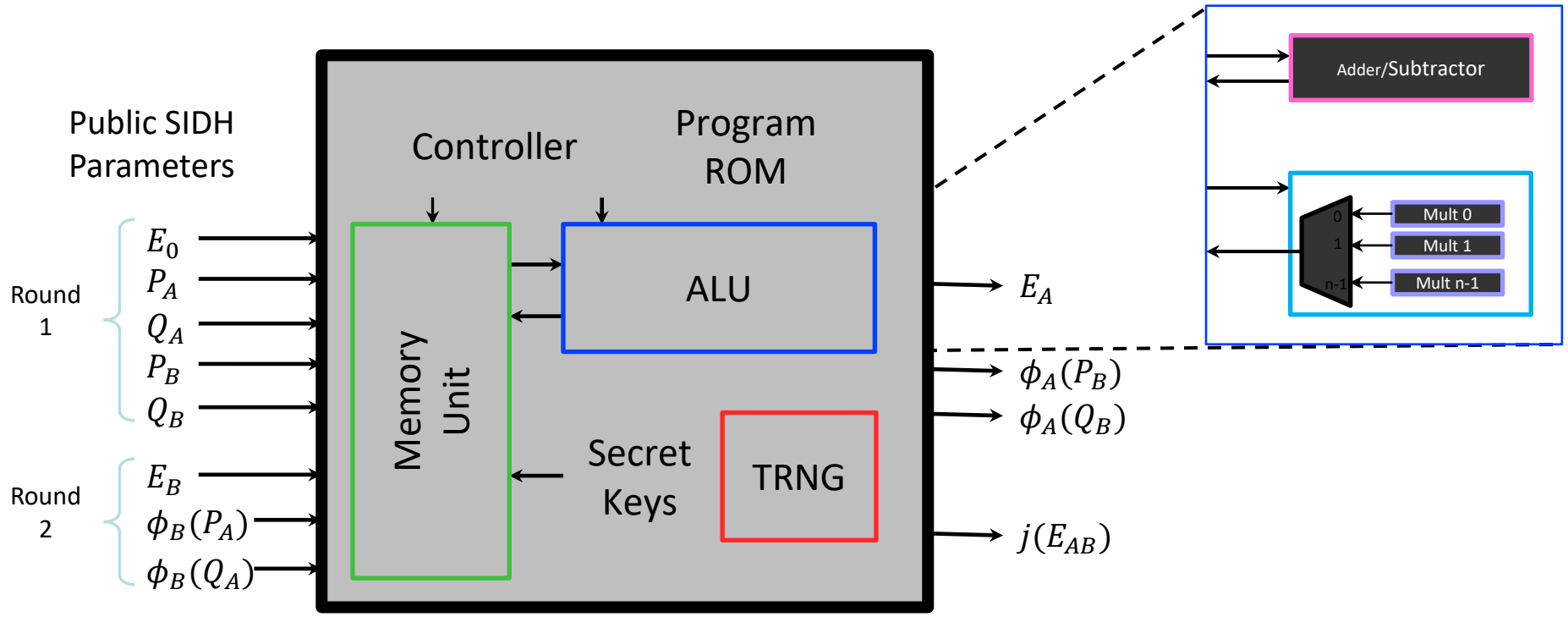
- ✓ Lightweight
- ✓ Low Power
- ✓ Fast

Suite-Q Software License

- ✓ Easy to install
- ✓ Portable
- ✓ Cheaper



# Suite-Q™: Scalable from Small IoT Devices to High Performance Applications






MICROCHIP

# Microchip PolarFire® FPGA Area Results


**Area results on PolarFire Splash Kit, MPF300TS-1FCG484E for NIST Level I**

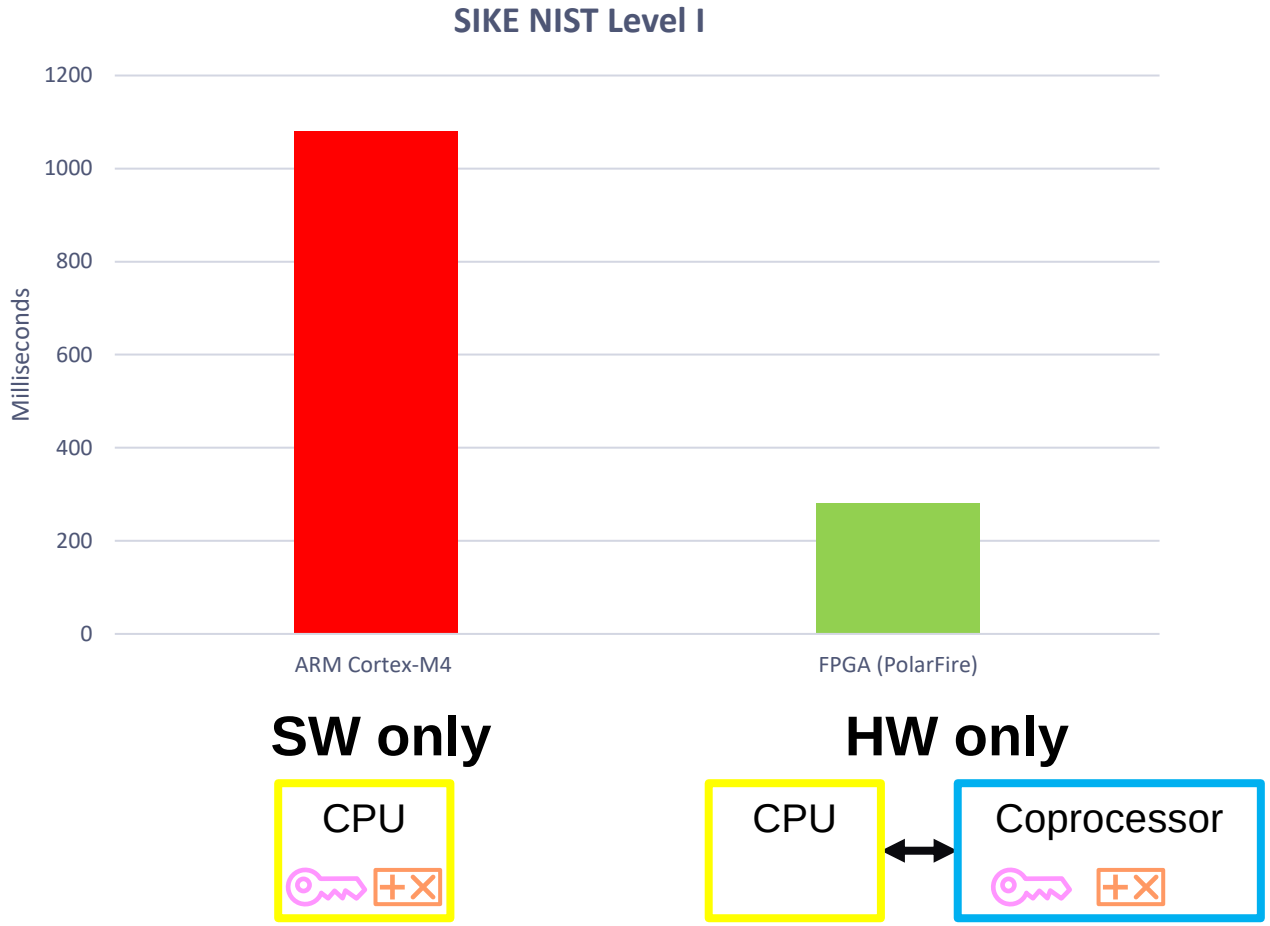
| Area | #4LUT | #DFF | #Logic Elements | #1K µSRAM | #DSP |
|---|---|---|---|---|---|
| SIKE Core | 20,536 | 5,803 | 20,844 | 49 | 3 |
| Total Resources | 299,544 | 299,544 | 299,544 | 2,772 | 924 |
| KeyDecap | 6.86% | 1.94% | 6.96% | 1.77% | 0.32% |

# Microchip PolarFire® FPGA Timing Results


**Timing results on PolarFire Splash Kit, MPF300TS-1FCG484E @145.6 MHz for NIST Level I**

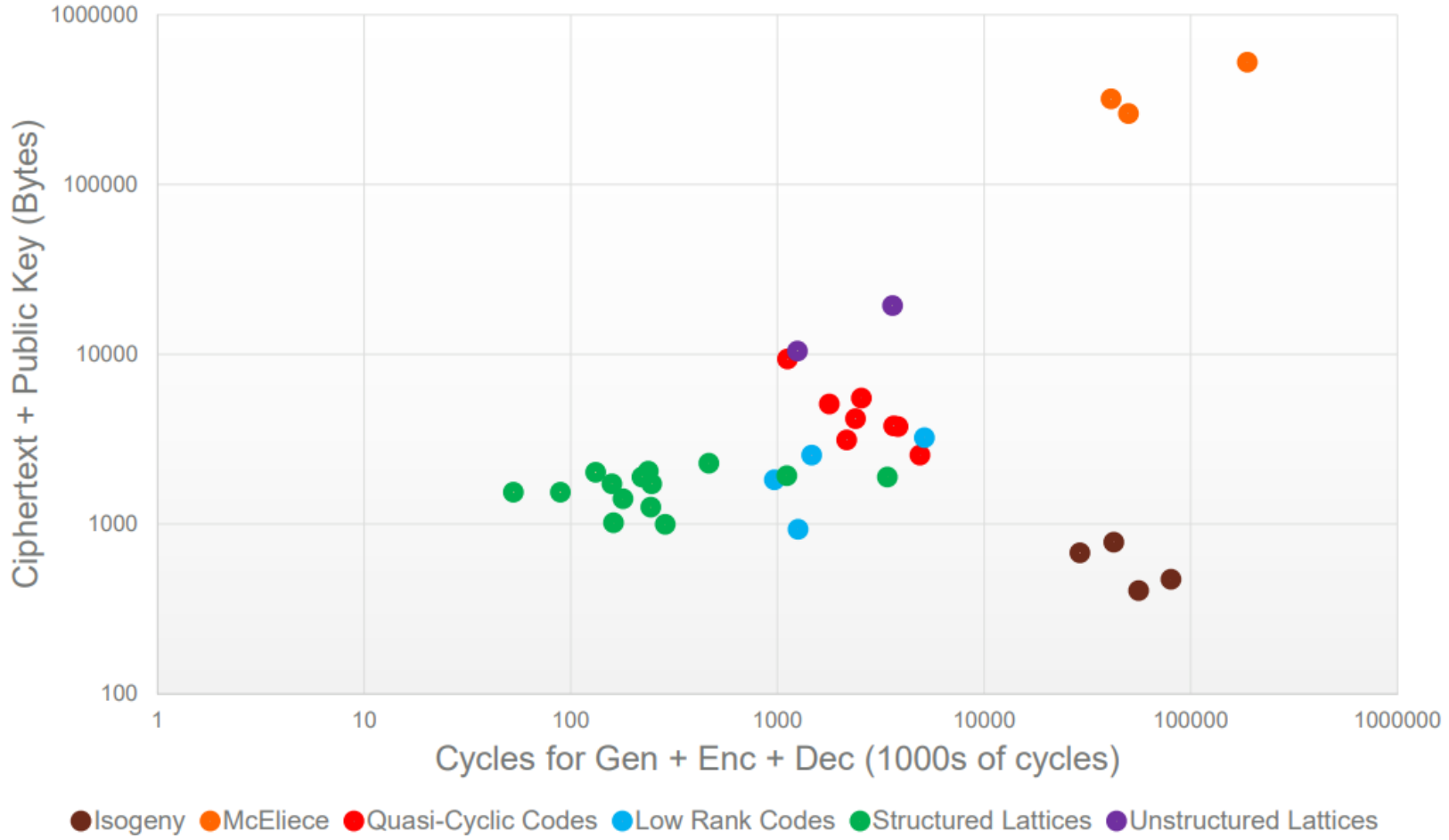
| **SIKE Operations** | **Clock Cycles** [10^6 cc] | **Time** [ms] |
|---|---|---|
| KeyGen | 1,241 | 85.22 |
| KeyEncap | 1,981 | 136.04 |
| KeyDecap | 2,151 | 147.70 |

# SIKE: Software Results for NIST Level 1



# Comparisons (NIST Workshop by D. Moody)

## Speed vs Size (PC implementations)






MICROCHIP

# SIKE Team


UNIVERSITY OF
WATERLOO


FAU
FLORIDA ATLANTIC
UNIVERSITY


IN·DEI·NOMINE·FELICITER
Radboud
Universiteit


UNIVERSITY OF
TORONTO


IBM Research | Zurich


Microsoft Research


amazon


Linked in


Texas
Instruments


INFOSEC
GLOBAL


PQSecure


evolution

# The Future of SIKE: Computational/Communication Costs

- **Hardware and software get faster over time**
- **As hardware and software gets faster, attacks get faster**
- **Faster attacks require larger keys to counteract**
  - RSA 1024, 2048, 3072, 7680, 15360
  - ECC 192, 224, 256, 384, 448, 521
- **An across-the-board key size increase enlarges the communication cost benefits of SIKE (in absolute terms)**
- **Variance in communication channels is much higher than variance in cycle counts. SIKE already wins today on desktop browsers when including variance.**

# Summary

- **Suite-Q™ IP is a post-quantum key exchange accelerator**
- **Scalable architectures for optimal performance/resource usage**
- **Available in both SW and HW**
- **Available in all NIST PQC security levels**
- **Optional side-channel countermeasures**
  - PolarFire® FPGAs also come with a CRI DPA countermeasure pass through license
- **Can be optimized to your application**
- **Can run on Microchip FPGAs, Microcontrollers or Microprocessors**

# Get Started Today

- **MCUs and MPUs**
  - https://www.microchip.com/design-centers/microcontrollers
- **PolarFire® and PolarFire SoC FPGAs**
  - https://www.microsemi.com/product-directory/fpgas/3854-polarfire-fpgas
- **Suite-Q**
  - http://www.pqsecurity.com/

# Thank You