PQ Secure

Hardware Deployment of Hybrid PQC: **SIKE+ECC**

Reza Azarderakhsh, Ph.D.

Founder and CEO
PQSecure Technologies, LLC

Quantum Timeline

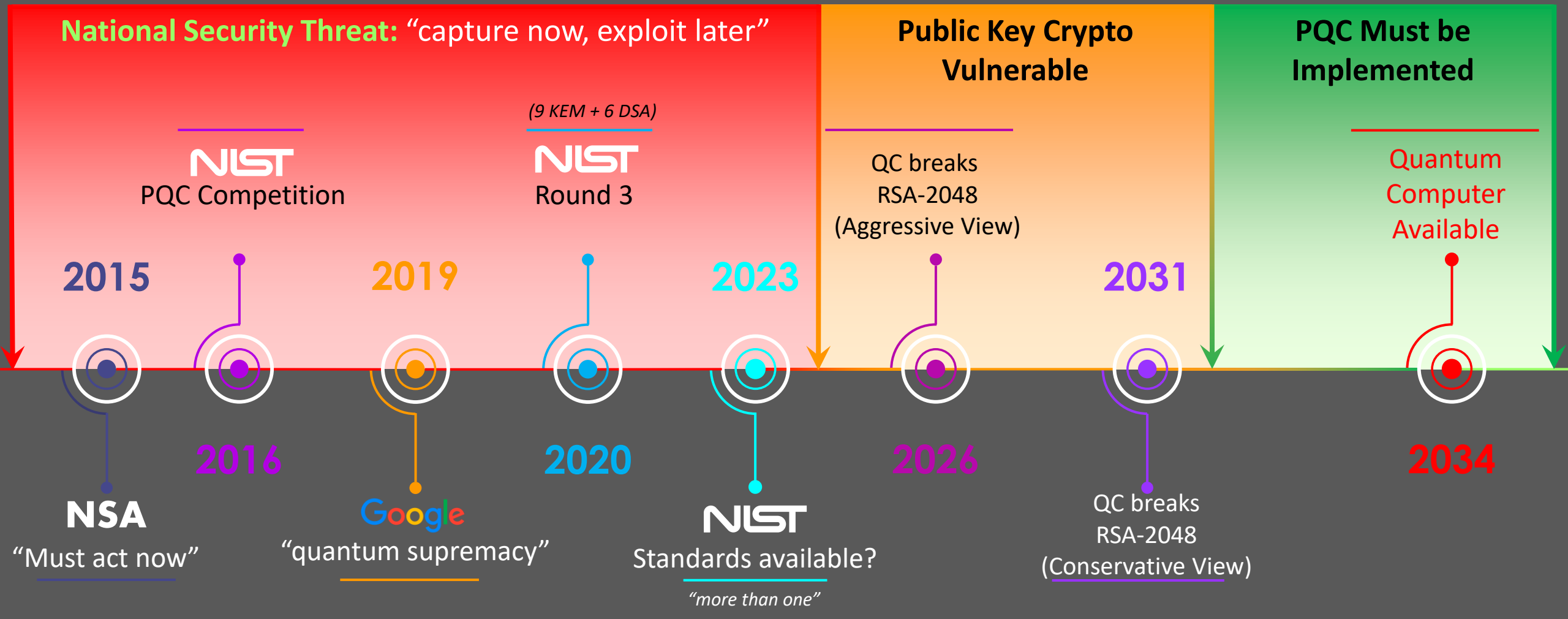
PQ Secure

3 - 8 years to transition…

National Security Threat: "capture now, exploit later"

Public Key Crypto Vulnerable

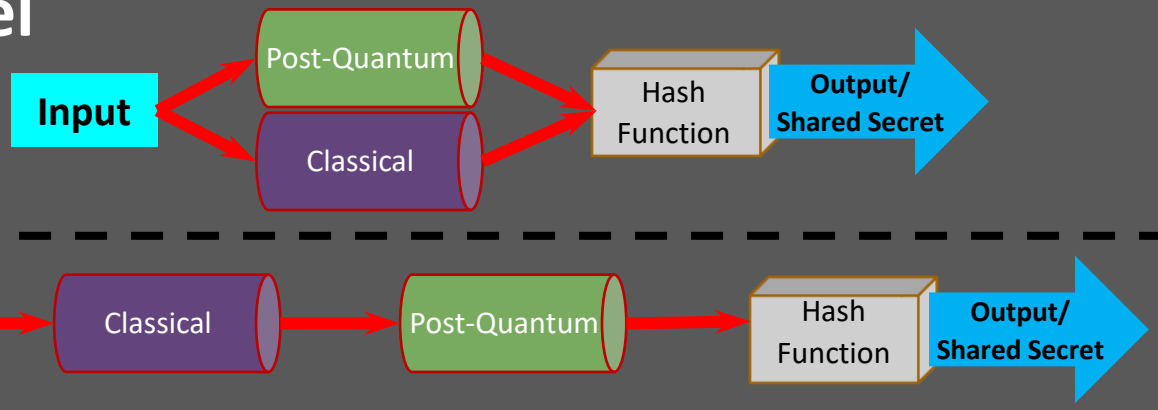
PQC Must be Implemented



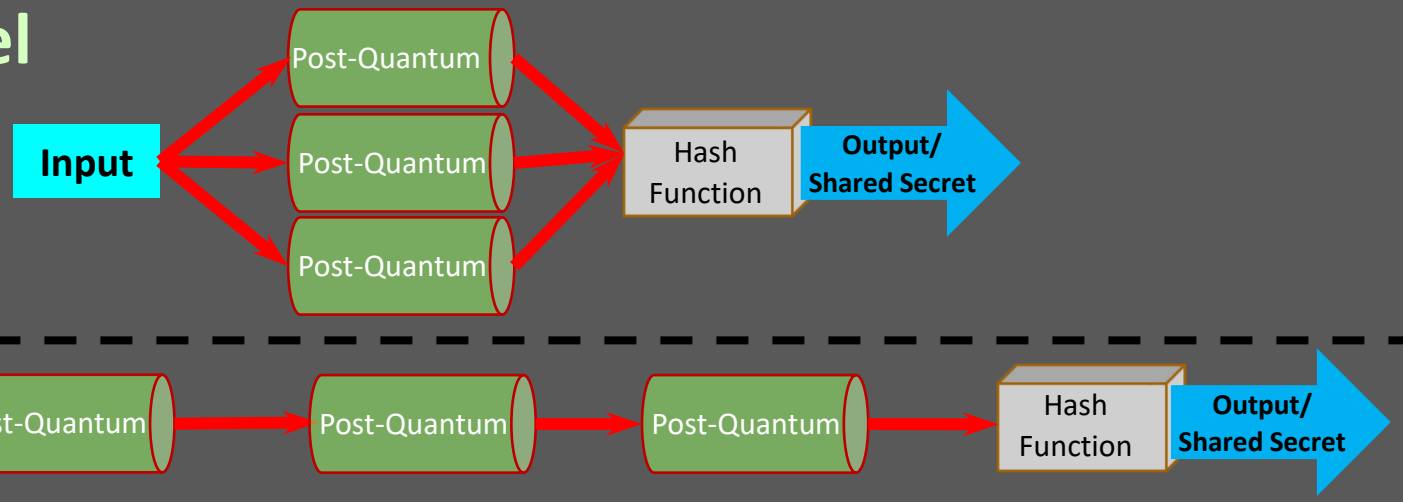
Possible Models

PQ Secure

Hybrid Model

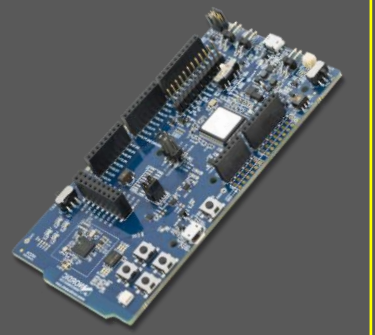


Composite Model



IoTs + Crypto HW Accelerators

PQ Secure

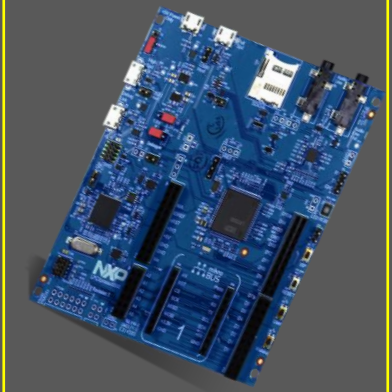


nRF5280
Arm® Cortex™-M4
@ 64 MHz
Arm CryptoCell CC310
HW Crypto Engine:
AES, Hash, RSA/ ECC, etc.

STM32L5xx
Arm® Cortex®-M33
TrustZone®
@ 110 MHz
HW Crypto Engine:
AES/ DES3, MD5/
SHA/SHA2. RNG etc.

CC2642R
ARM® Cortex® -M4F
@ 48 MHz
HW Crypto Engine:
AES/ DES/ DES3, SHA2,
RNG, RSA/ ECC, etc.

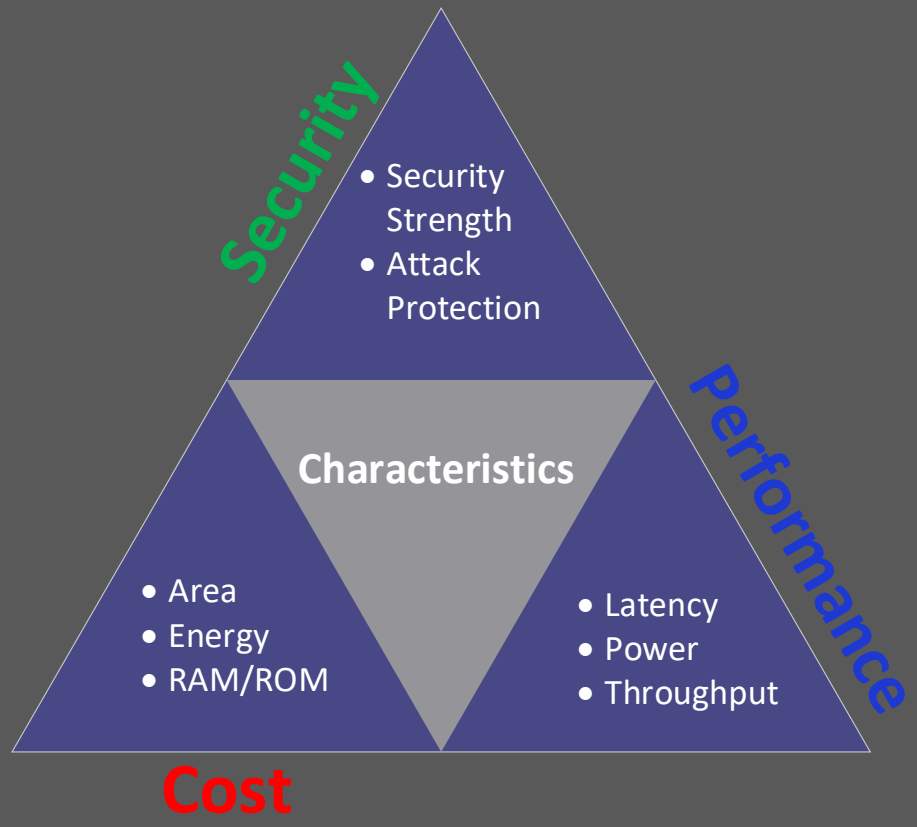
EFM32
ARM Cortex-M4
@ 40MHz
HW Crypto Engine:
AES, Hash, ECC, etc.

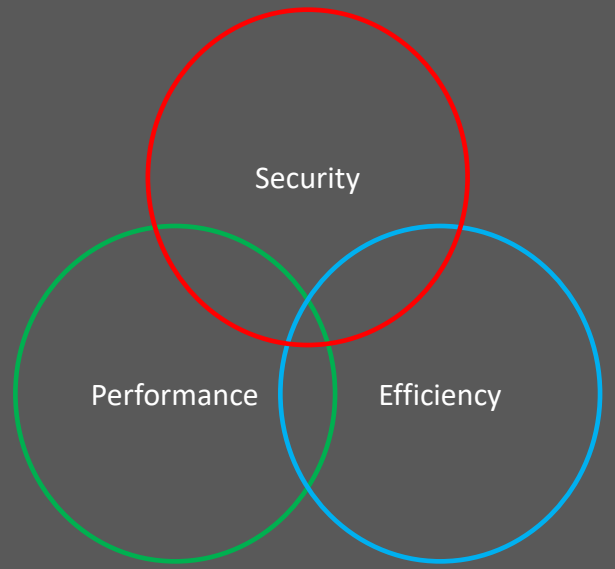


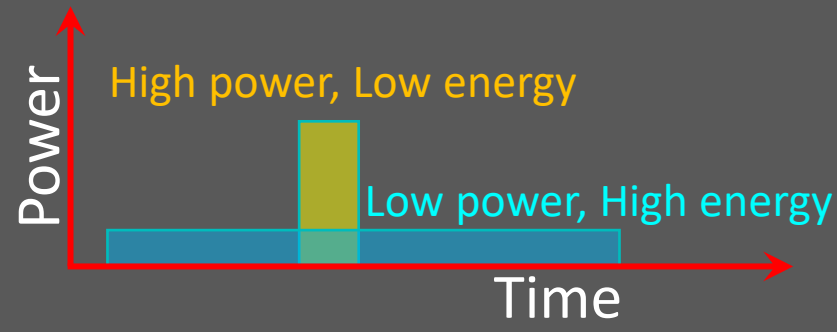
LPC55S6x
Arm® Cortex®-M33
TrustZone®
@ 150 MHz
HW Crypto Engine:
AES, SHA2, RNG, etc.

ATECC608A
Crypto Co-Processor
HWCrypto Engine:
AES, SHA2, ECDH,
ECDSA etc.
SCA protection

Why Crypto HW Accelerators?

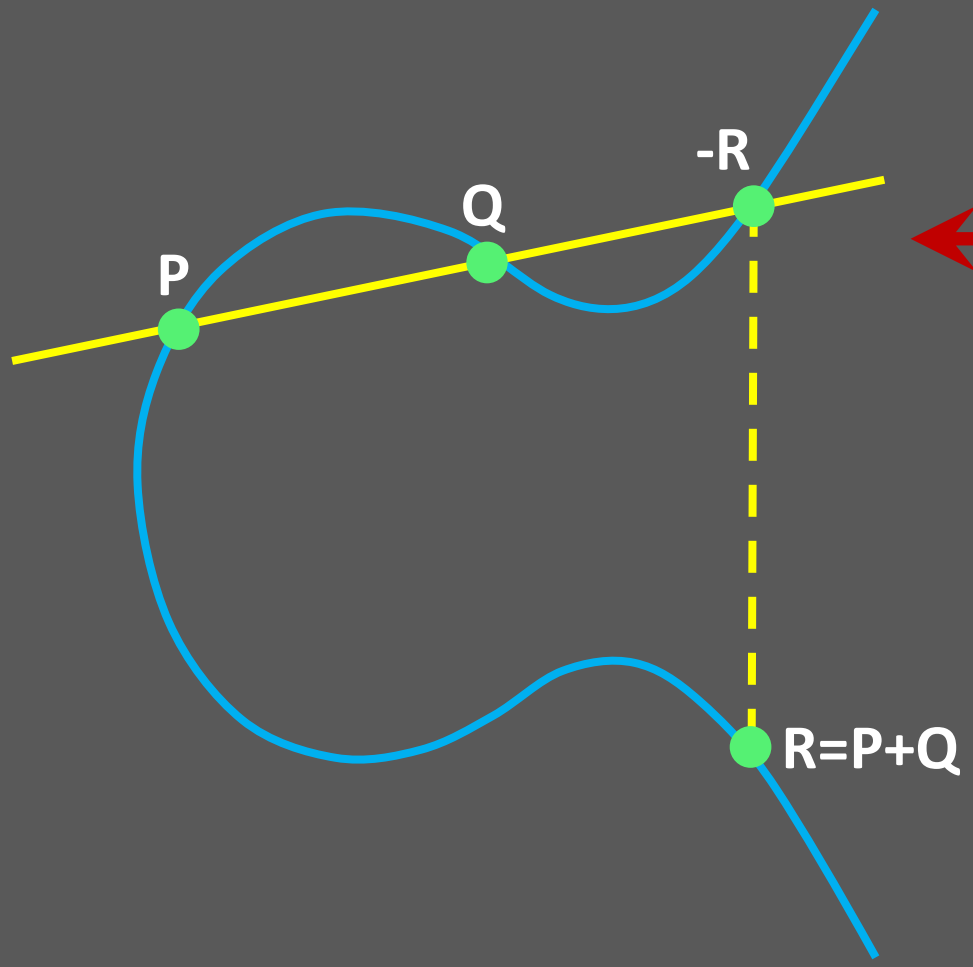






SIKE+ECC

PQ Secure

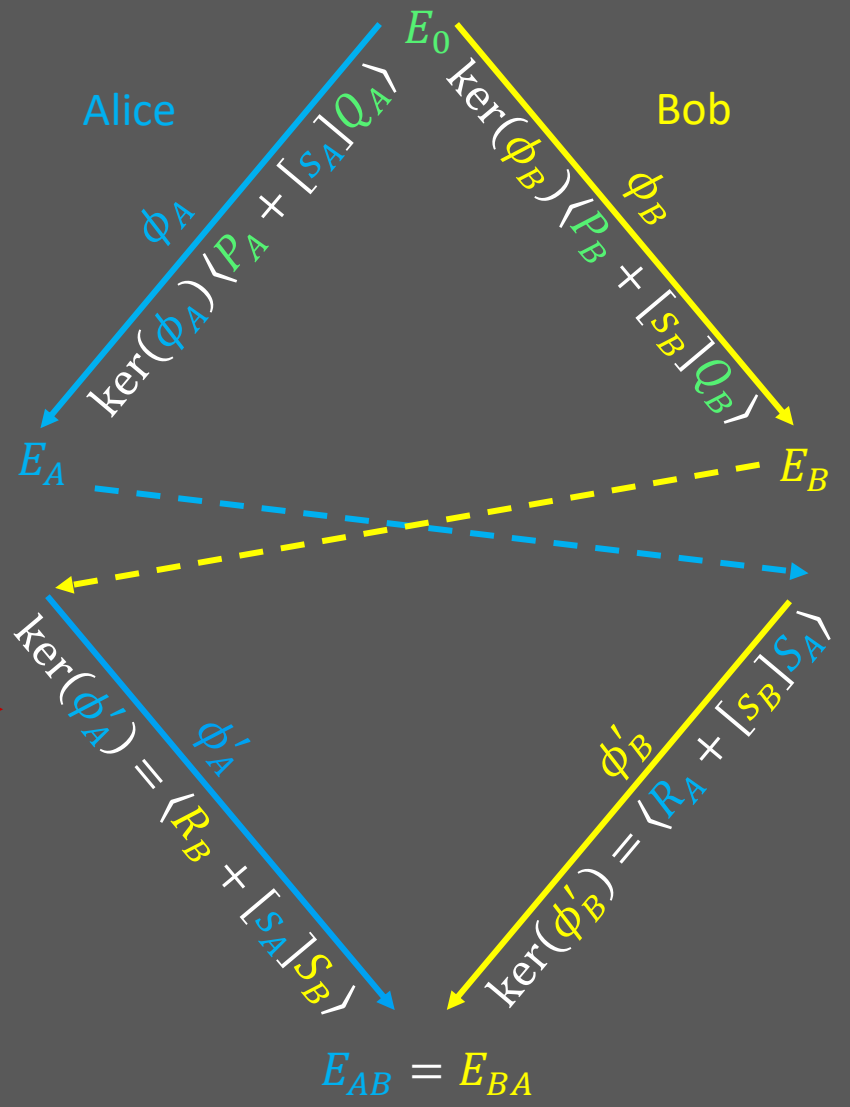


ECDH

+

SIKE

Hybrid



SIKE curves for ECC?

PQ Secure

$$E/\mathbb{F}_{p^2} : y^2 = x^3 + 6x^2 + x$$

- ✓ Used for all SIKE primes ($p = 434, 503, 610, 751$)
- ✓ **Supersingular:** Good for isogeny-based crypto but weak for classical ECC

New/Better curves:

ECHD: X434, X503, X610, X751* and **EdDSA: Ed434, Ed503, Ed610, Ed751**

- ✓ Share SIKE primes (Same NIST security Level)
- ✓ Adapted from RFC 7748 (X25519, X448) and RFC 8032 (Ed25519, Ed448)
- ✓ Satisfy Safecurves criteria (safecurves.cr.yp.to)
- ✓ Public Keys are 55 – 94 bytes

(* X751: CLN-2016)

Choices for ECDH

PQ Secure

Similar Curves for all SIKE primes (sizes in bytes)

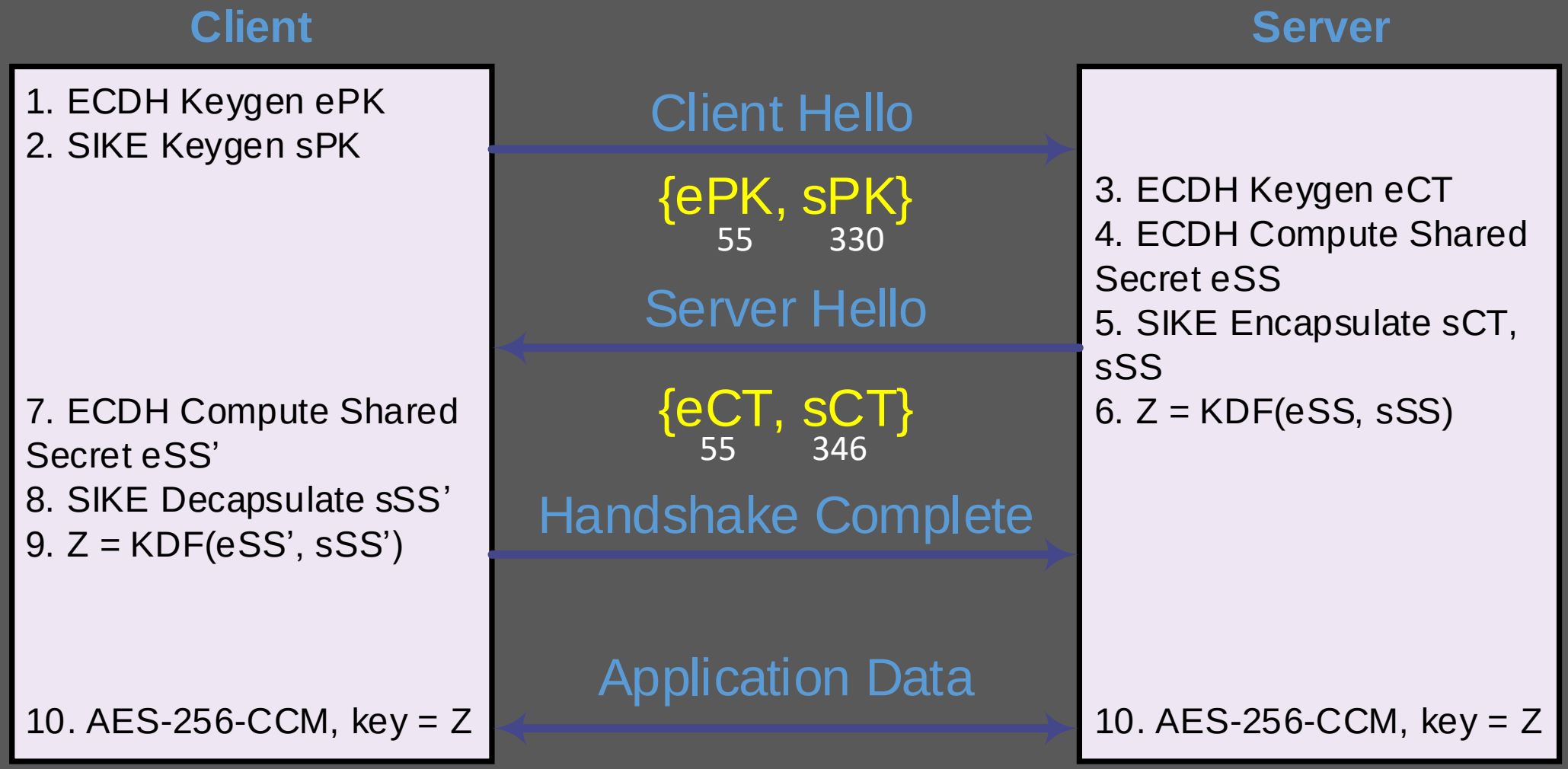
SIKE				ECDH				SIKEX	
Scheme	NIST Level	Public Key	Ciphertext	a coef	Base x-coord.	Pollard Rho Attack (ops)	Public Key	Public Key	Ciphertext
p434	1	330	346	439,322	4	$2^{215.4}$	55	385	401
p503	2	378	402	308,290	2	$2^{249.8}$	63	441	465
p610	3	462	386	1,135,802	2	$2^{303.5}$	77	539	563
*p751	5	564	596	624,450	3	$2^{374.2}$	94	658	690

Montgomery form: $E/\mathbb{F}_q : by^2 = x^3 + ax^2 + x$ s. t. $a, b, x, y \in \mathbb{F}_q$

* X751: CLN-2016

SIKEp434 + X434 = SIKEX434

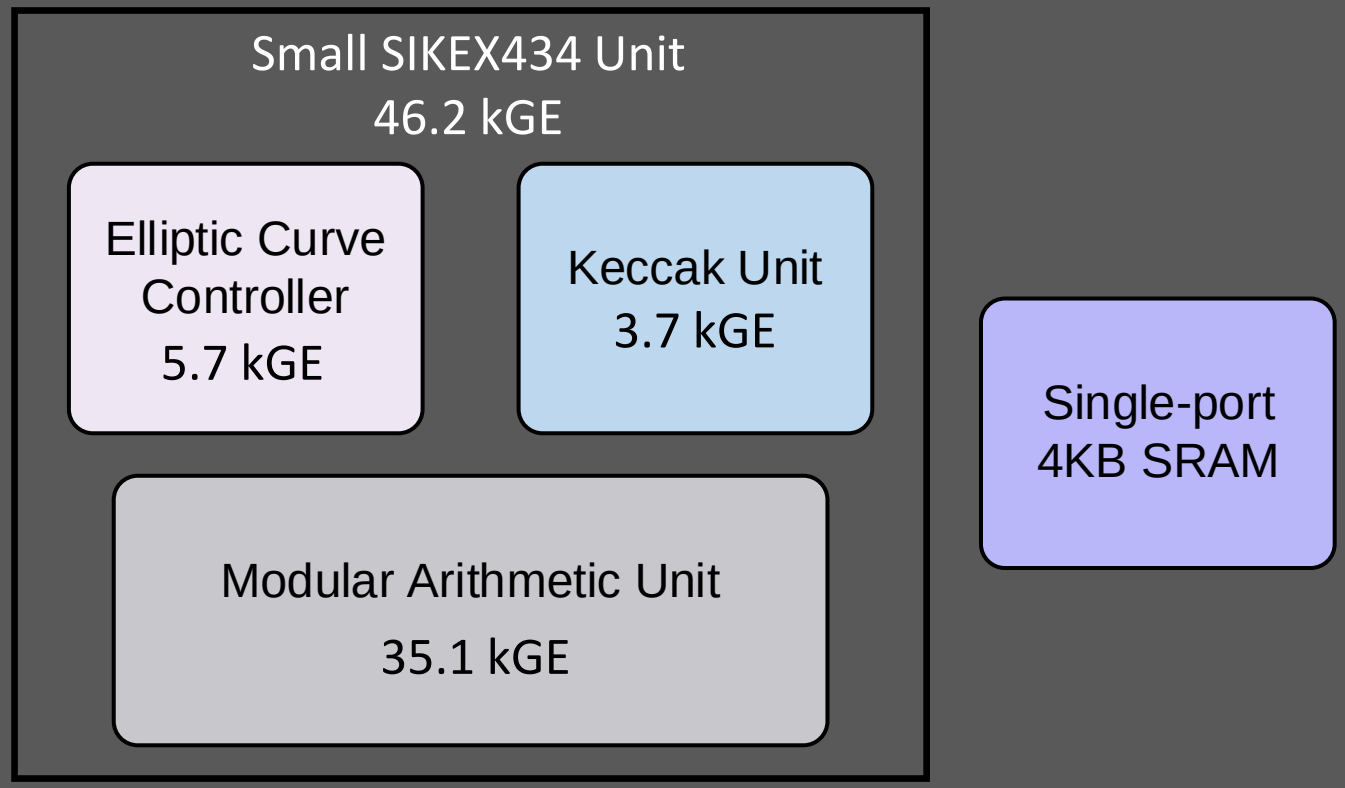
PQSecure



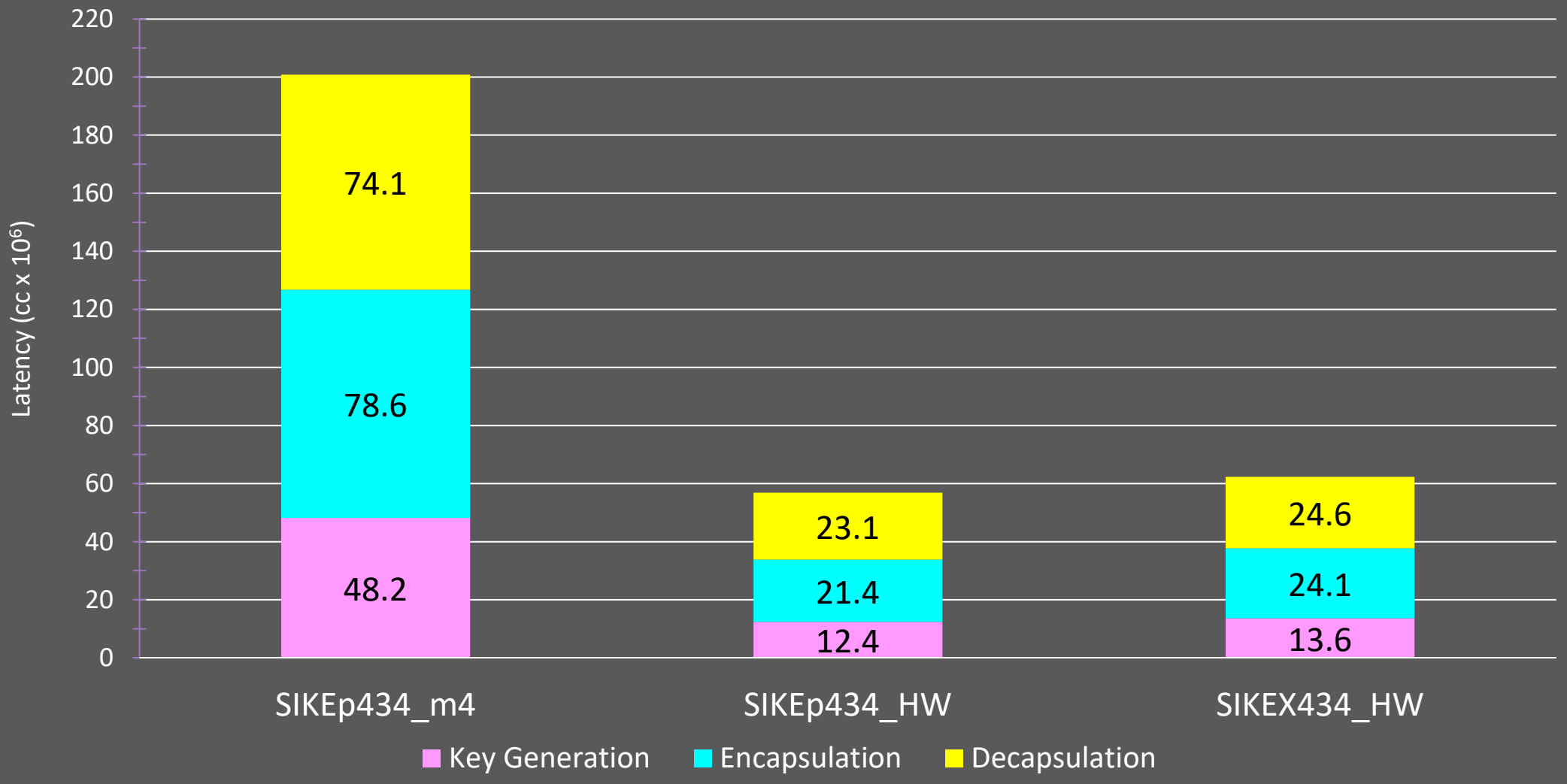
SIKEX434 Hybrid Key Exchange

PQSecure

SIKEp434 + X434 = SIKEX434

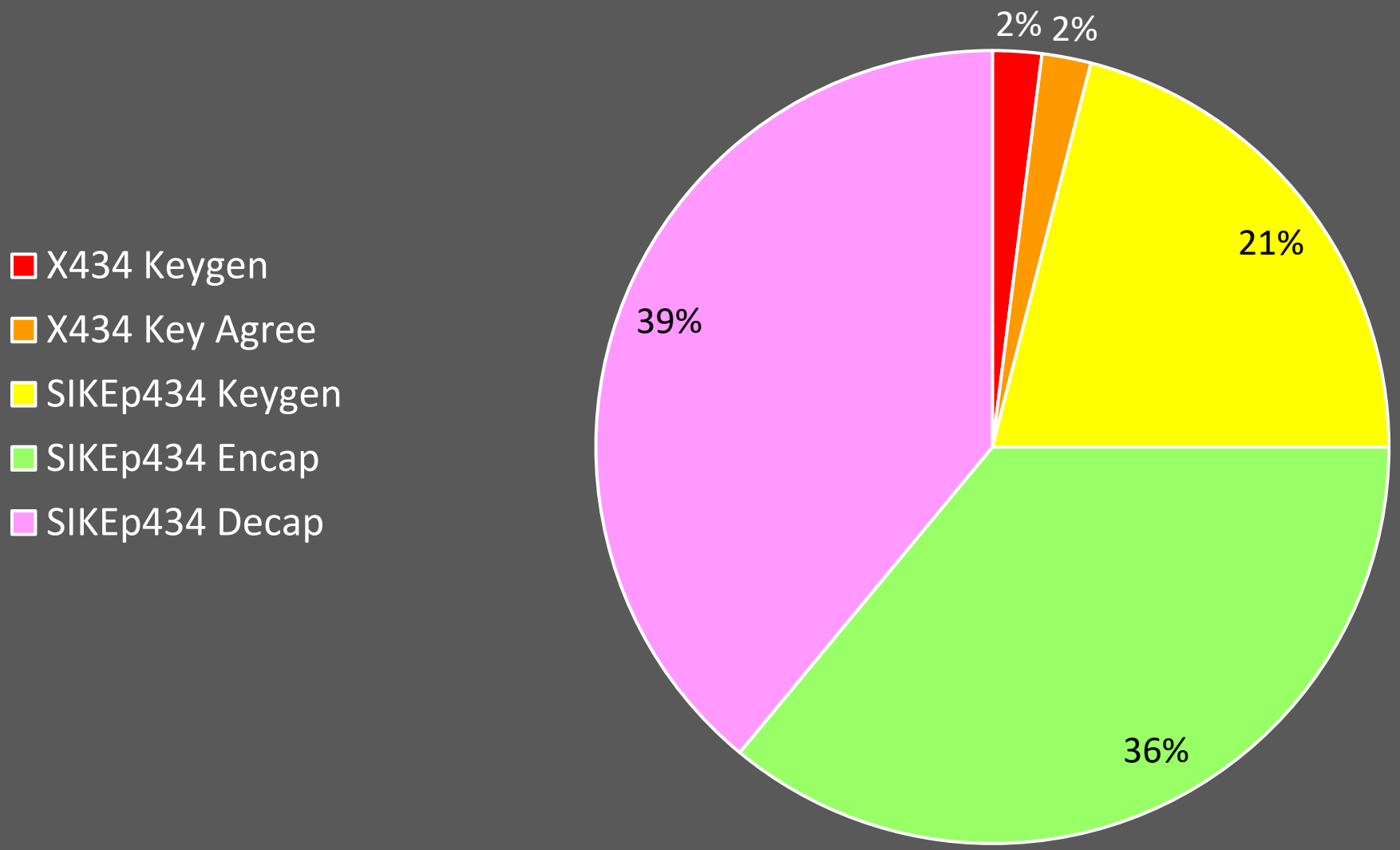


SIKE: Software vs. Hardware



SIKEX434 Timing Breakdown

PQ Secure



Note: X434 operations are performed twice in full SIKEX434 operation

Happy Hybrid: SIKE+ECC

PQ Secure

- Our focus was on small implementations
  - Faster implementations are possible with a bit increase in area
- Why not X25519 or X448?
  - SIKE limited (performance) to smooth isogeny-friendly primes
  - Can’t take advantages of X25519 or X448
  - Would need additional registers/control logic to switch between
- Similarly, for Ed25519 and Ed448
- These primes save area/hardware = **smaller**
- Under development: prototype with 3x performance for small area increase