SCTE® CABLE-TEC EXPO® FAST FORWARD 2021

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs®

UNLEASH THE POWER OF LIMITLESS CONNECTIVITY

2021 Fall Technical Forum
SCTE® • NCTA • CABLELABS®

Security & Privacy

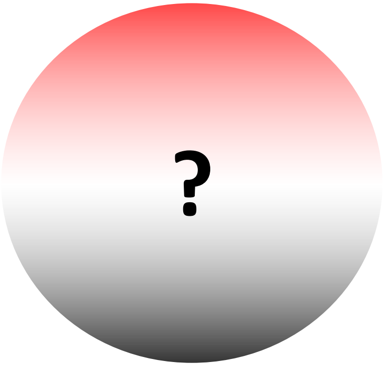
Navigating the Transition to a Post-Quantum World

Chujiao Ma

Senior Security R&D Engineer
Comcast

Qubits

$O(e^n)$



$O(n)$

Impact

Transition can be slow and costly

- SHA-1 to SHA-2 transition took over 10 yrs and cost organizations $5M on average
- PQCs are very different from classical algorithms and are subjected to change

Post-Quantum Algorithm Foundations

SCTE. CABLE-TEC EXPO
ATLANTA, GA > OCTOBER 11-14

Lattice
- Simple, efficient, parallelizable
- Large public key sizes

Code
- Better for encryption than signatures
- Large key sizes

Hash
- Well studied security-wise
- Limitation on scalability

Multivariate
- Short signatures
- Inefficient due to large public key and long decryption time

Isogeny
- One of the smallest key sizes
- Most recent and less studied

Post-Quantum Algorithms - NIST

SCTE CABLE-TEC EXPO
FAST FORWARD 2021
ATLANTA, GA > OCTOBER 11-14

	Name	Type	Public Key (bytes)	Private Key (bytes)	Ciphertext Size (bytes)
Key establishment	Classic McEliece	Code-based	261120 - 1357824	6492 - 14120	128 - 240
	Crystals-Kyber	Lattice	800 - 1568	1632 - 3168	768 - 1568
	NTRU	Lattice	699 - 1230	935 - 1590	699 - 1230
	Saber	Lattice	672 - 1312	1568 - 3040	736 - 1472
	*BIKE	Code-based	2542 - 6206	3110 - 13236	2542 - 6206
	*FrodoKEM	Lattice	9616 - 21520	19888 - 43088	9729 - 21632
	*HQC	Code-based	2249 - 7245	2289 - 7285	4481 - 14469
	*NTRU Prime	Lattice	897 - 1322	1125 - 1999	1025 - 1184
	*SIKE	Isogeny	197 - 564	28 - 644	197 - 596

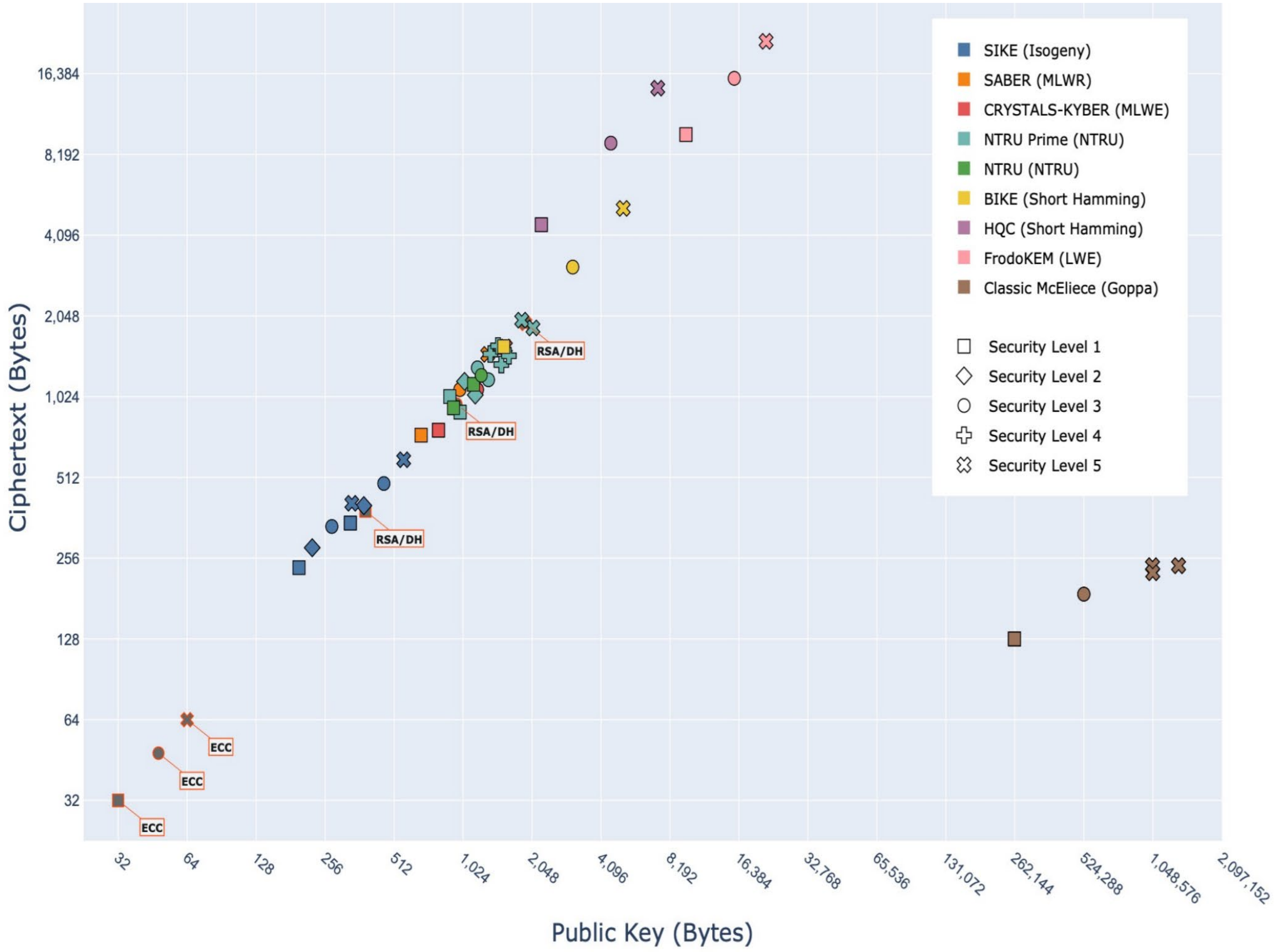
	Name	Type	Public Key	Private Key	Signature
Digital signature	Crystals-Dilithium	Lattice	1312 - 2592	2544 - 4880	2420 - 4595
	Falcon	Lattice	897 - 1793	1281 - 2305	690 - 1330
	Rainbow	Multivariate	60192 - 1930600	64 - 1408736	66 - 212
	*GeMSS	Multivariate	352000 - 10400000	13100 - 12300	240000 - 600000
	*Picnic	ZKP	33 - 65	49 - 97	14612 - 209510
	*SPHINCS+	Hash based	32-64	64-128	8080 - 49216

Post-Quantum Algorithms - NIST

PQC generally has larger key sizes, but some algorithms at lower security levels have a comparable size to classical algorithms at a higher security level.

The five security levels are denoted as:

- Level 1: At least as hard to break as AES-128
- Level 2: At least as hard to break as SHA-256
- Level 3: At least as hard to break as AES-192
- Level 4: At least as hard to break as SHA-384
- Level 5: At least as hard to break as AES-256

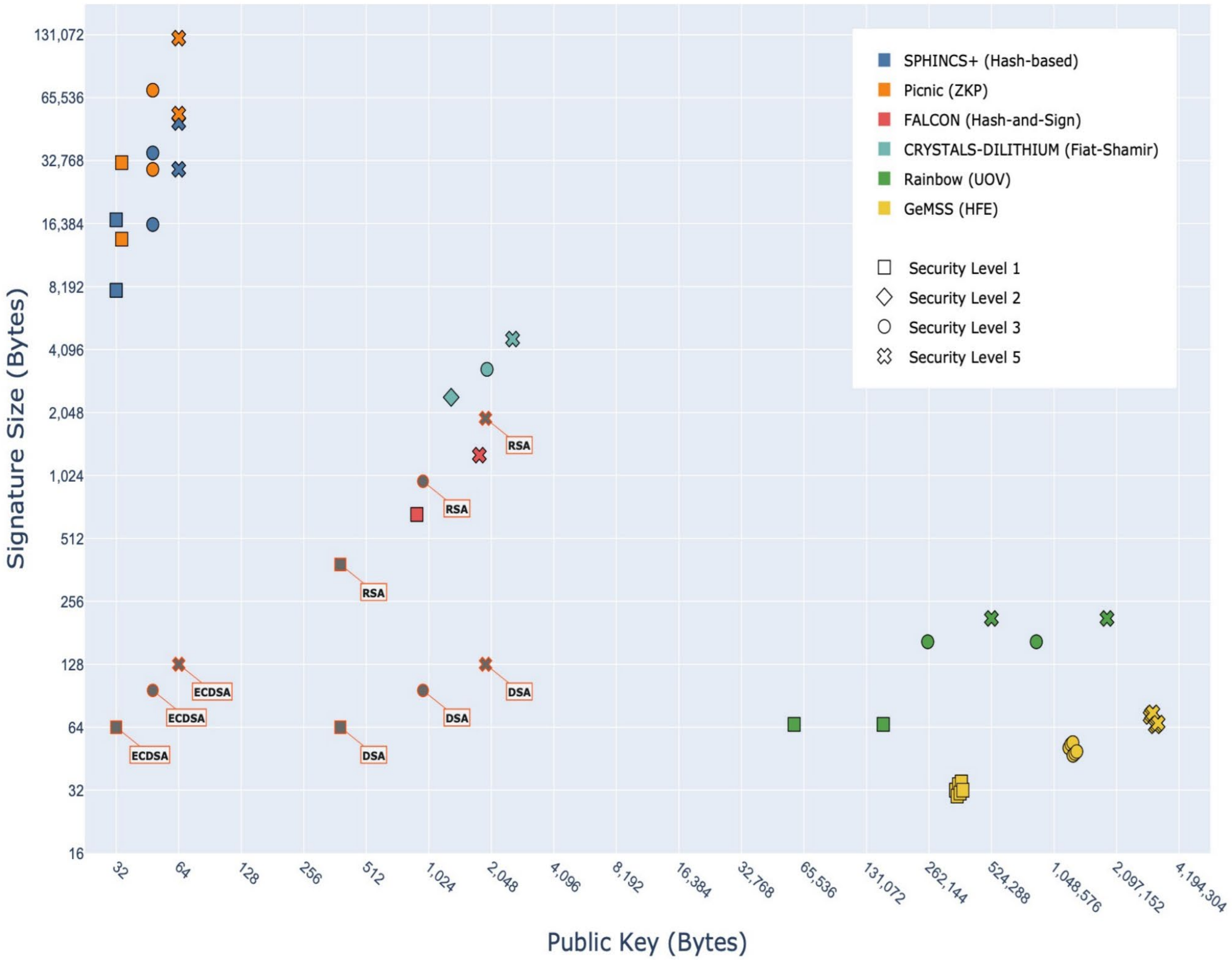


Post-Quantum Algorithms - NIST

PQC generally has larger key sizes, but some algorithms at lower security levels have a comparable size to classical algorithms at a higher security level.

The five security levels are denoted as:

- Level 1: At least as hard to break as AES-128
- Level 2: At least as hard to break as SHA-256
- Level 3: At least as hard to break as AES-192
- Level 4: At least as hard to break as SHA-384
- Level 5: At least as hard to break as AES-256



Post-Quantum Algorithms - China

CACR competition:

- 3 tracks (digital signature, public-key cryptography and key exchange)
- One round
- Started in Aug 2018, concluded in Dec 2019
- 14 finalists

Rank	Name	Category	Type
1st place	Aigis-sig	Signatures	Lattice
1st place	LAC.PKE	KEM	Lattice
1st place	Aigis-enc	KEM	Lattice
2nd place	LAC.KEX	KEX	Lattice
2nd place	SIAKE	KEX	Isogeny
2nd place	SCloud	KEM	Lattice
2nd place	AKCN	KEM	Lattice
3rd place	OKCN (SKCN-MLWE)	KEX	Lattice
3rd place	Fatseal	Signature	Lattice
3rd place	Mulan	Signatures	Lattice
3rd place	AKCN-E8	KEM	Lattice
3rd place	TALE	KEM	Lattice
3rd place	PKP-DSS	Signature	PKP
3rd place	Piglet-1	KEM	Code-based

Implementations - Libraries

libpqcrypto
- OpenSSH, OpenIKED
- Research oriented and not for production

liboqs
- TLS, SSH, x.509, CMS and S/MIME (via OpenSSL and OpenSSH)
- Some algorithms may cause failures when run on threads or in constrained env

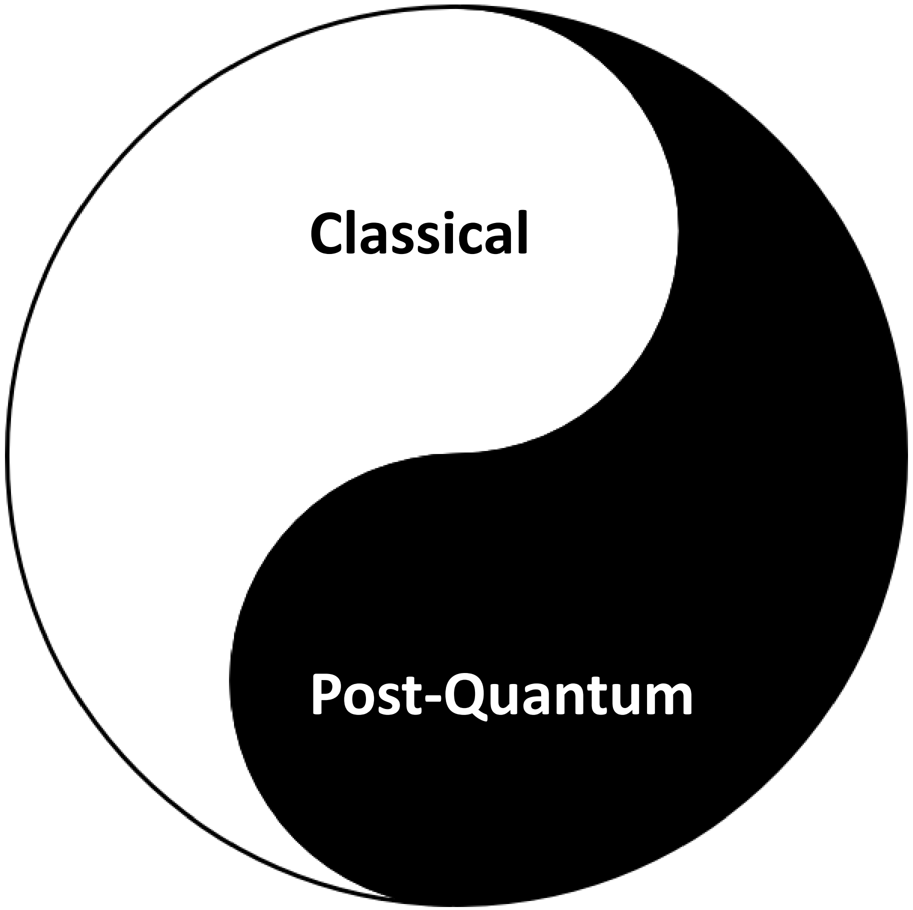
CIRCL
- TLS 1.3
- Currently only have hybrid of Diffie-Hellman and SIKE

Commercial
- ISARA Radiate Quantum Safe Toolkit for Android, iOS, Linux, MacOS, and Windows 10
- Pqshield for embedded devices, mobile and server

X.509

Considerations:

- Transmission overhead
- IP fragmentation
- Wasted bandwidth for connections
- New algorithm identifiers
- Size limit on x.509 fields by some app



Infrastructure - Protocols

IKEv2	• Derives a common key using Diffie-Hellman, authenticate it using digital signature or authentication key, then new keys are generated for IP packet • Rigid standard and algorithms need to be replaced in all three exchanges
TLS	• Authenticates server and client with a handshake protocol, then establishes shared secret keys for transmission of application data • The algorithm for handshake needs to be replaced, larger key size is enough for transmission
S/MIME	• Uses digital signatures for authentication/integrity, encrypt data with symmetric ciphers • Support extended key size and encryption method, only the digital signature needs to be replaced
SSH	• Transport protocol to create secure channel, authentication protocol for client/server, and connection protocol that multiplexes it into several channels for different usage • High level of crypto agility and should not require significant changes

Infrastructure - Cloud

Google is incorporating lattice-based algorithms into Chrome browser
Additional overhead will only decrease server throughput by less than a factor of two

IBM is integrating Kyber as part of IBM Key Protect for IBM Cloud
Algorithm performance may be affected by network profile, CPU speed and API call rates.

Amazon now supports BIKE and SIKE hybrid in AWS KMS.
ECDHE/BIKE have a larger size than ECDHE/SIKE but is faster.

Microsoft is now working on SIKE, Picnic and qTESLA for crypto systems.
They are also developing post-quantum branch of TLS and SSH with OQS as well on integrating PQC into a fork of Open VPN

Crypto Agility

Without proper planning, it may take decades to replace most of the vulnerable public-key systems currently in use. Thus, it is important to develop a playbook for crypto agility.

1. **Identify threat**
2. **Inventory of assets**
3. **Estimate risk**
4. **Secure assets**
5. **Create roadmap**

How to transition?

It is a big undertaking since different algorithms have different key lengths, performance and operational constraints.

What we can do now:

- Benchmarking of the algorithm
- Focus on hybrid cryptography
- Support a quantum-based crypto environment
- Crypto agility assessment of target assets

SCTE® CABLE-TEC EXPO® FAST FORWARD 2021

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs®

Thank You!

Chujiao Ma

Senior Security R&D Engineer
Comcast
Chujiao_ma@comcast.com