Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IEEE INDUSTRY APPLICATIONS SOCIETY Bangalore Chapter

6th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS

(PKIA 2025)

SEPTEMBER 3-4th, 2025

Extending Elliptic Curve Cryptography for Quantum Readiness (Paper ID 30)

Kunal Abhishek

C-DAC Patna

Organization of Paper

- Important Questions
- Key contributions of the paper
- Discussions
- Technical Trade-offs And Strategic Trade-offs
- ECC And Quantum Readiness
- Conclusion

Important Questions

1. *Should resources be directed toward scaling up legacy algorithms such as adoption to a higher-order elliptic curve for cryptography? Is it a good strategy to address immediate security concerns by using higher-order elliptic curves?*

2. *Is it better to focus exclusively on transitioning to quantum-resistant algorithms?*

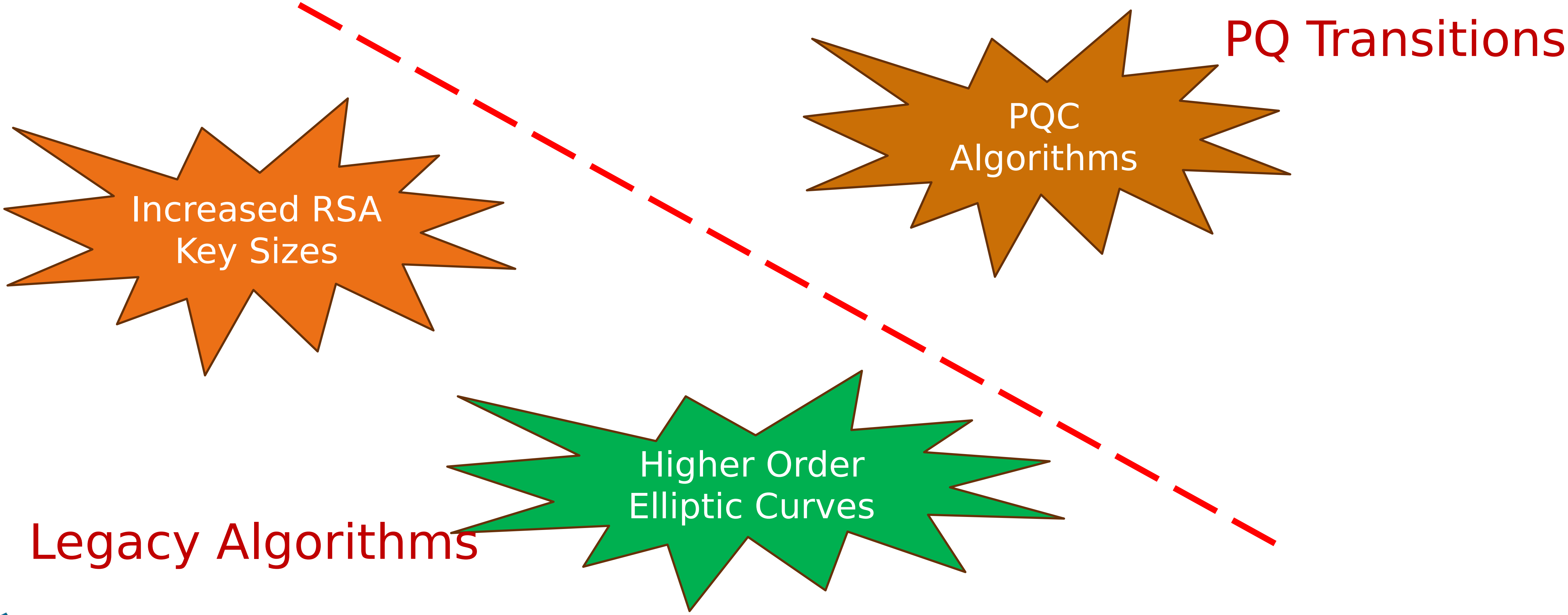
Key Contributions

- *Discussion on the current status of legacy and post-quantum algorithms along with the scalability challenges in generating higher-order elliptic curves.*
- *Technical and Strategic Trade-offs of ECC and PQC algorithms to argue that higher order elliptic curves can still be adapted to provide adequate quantum resilience for existing security infrastructures for a reasonably long duration.*
- *We present a strong basis for saving the immediate technology migration investments required for developing and adopting new*

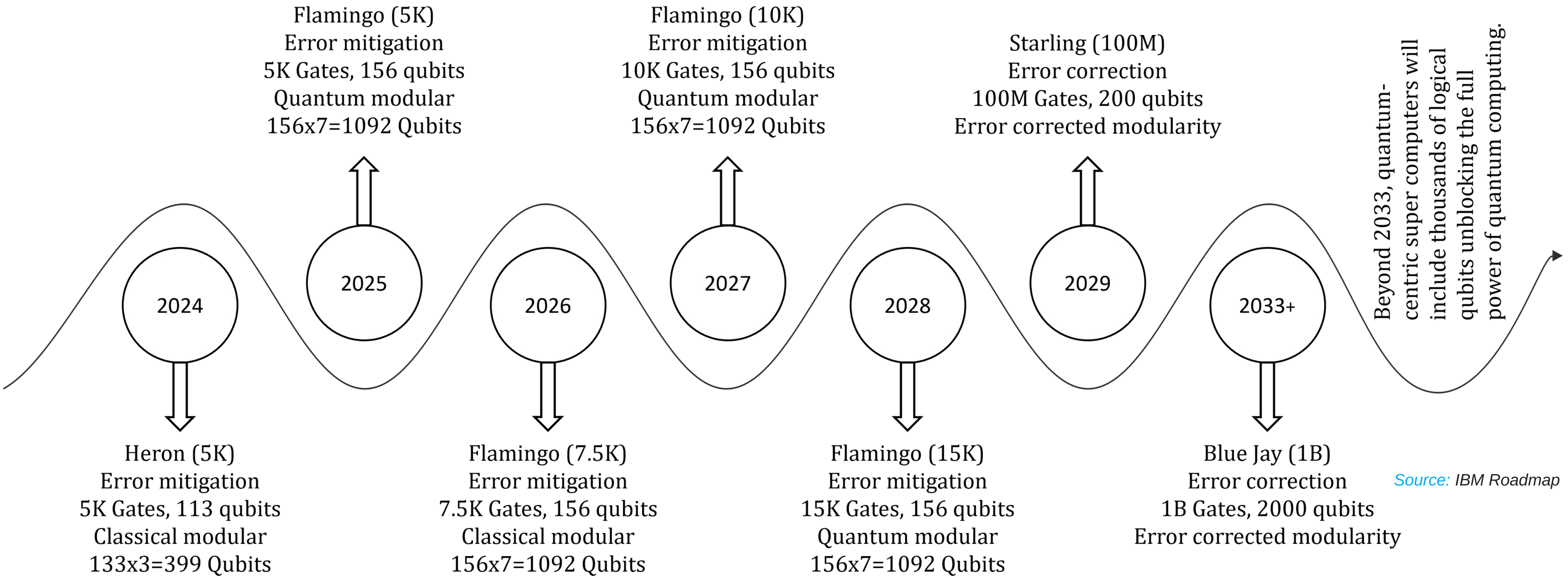
Our Arguments

- *We give arguments in favour of extending physical resources to be extended to ECC rather than in transition to the PQC which still needs thorough field evaluation and maturity.*
- *We deliberate on key factors essential for discussions on migrating cryptographic systems from ECC to PQC .*

Security Approaches in Post Quantum Era



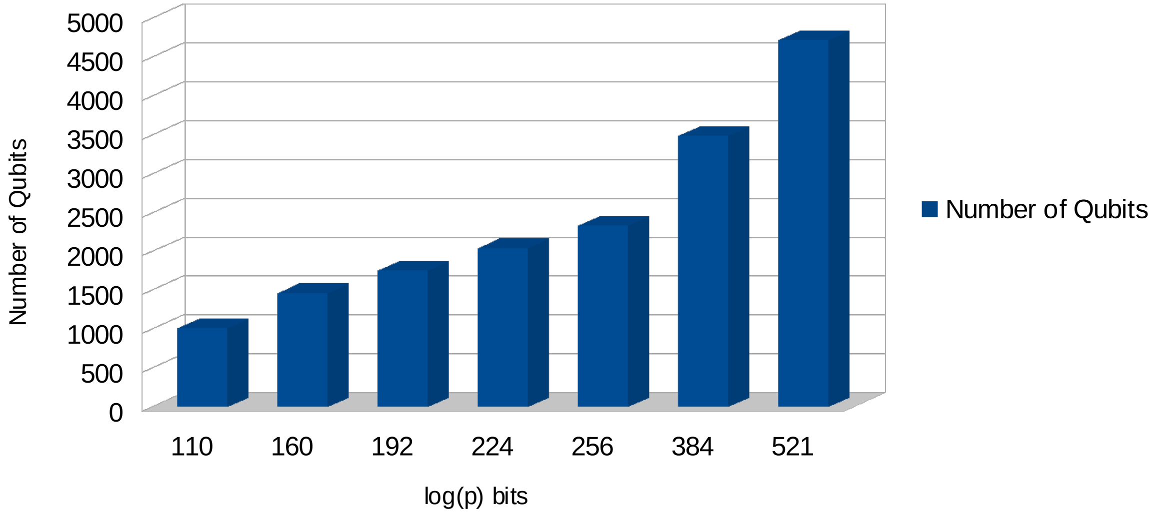
Realization of Logical Qubits



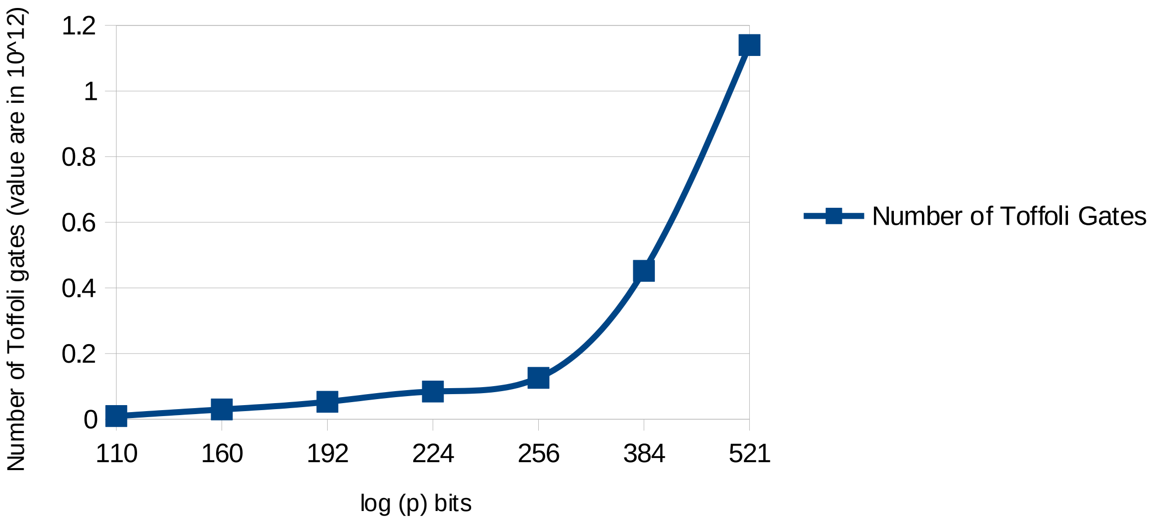
Source: IBM Roadmap

Quantum Resource Estimates for solving ECDLP

Resource estimates of Shor's algorithm for computing elliptic curve discrete logarithms



Required number Toffoli gates for the computation of elliptic curve discrete logarithms



Source: Roetteler, Martin, Kristin Lauter, and Krysta Svore. "Quantum resource estimates for computing elliptic curve discrete logarithms." U.S. Patent 10,430,162, issued October 1, 2019.

Certicom ECC Challenge Levels

Level 1 (Prime/Binary Field)	Level 2 (Prime/Binary Field)
109-bit challenge **SOLVED (2004)**	163-bit challenge
---	191-bit challenge
131-bit challenge	239-bit challenge
---	359-bit challenge

Scalability Challenges of Legacy Algorithms

Computational challenges in higher order curves

- Need of sufficient hardware resources
- Need of highly optimized software programs
- Cryptographic validations

Higher order *elliptic curves* such as one over *768-bit prime field size* are *still computationally feasible* to provide better quantum resilience!

Technical Trade-Off

Duration	Algorithms	Key Size (bits)	Security Level
2024–2029	RSA	2048 / 4096	$\geq$ 112-bit AES
	ECC	256 / 521	$\geq$ 128-bit AES
	PQC	As applicable	256-bit AES
	Quantum Computers	200 logical qubits	Experimental; limited fault tolerance
2029–2034	RSA	7680 / 15360	$>$ 128-bit AES
	ECC	384 / 521	$\geq$ 192-bit AES
	PQC	As applicable	Recommended for sensitive data
	Quantum Computers	2000 logical qubits (projected)	May threaten RSA/ECC
2034–2039	RSA	$\gg$ 15360	$>$ 256-bit AES
	ECC	$>$ 521	$>$ 256-bit AES
	PQC	As applicable	Strong post-quantum security
	Quantum Computers	Scalable fault-tolerant systems	Practical threat to RSA/ECC
2039–2044	PQC	As applicable	Post-quantum security established
	Quantum Computers	Millions of qubits	Advanced capabilities; real-world risks
Beyond 2044	PQC	As applicable	Fully resilient against quantum threats

Strategic Trade-Off

Strategic Trade-offs	RSA-2048	RSA-4096	ECC-256	PQC Algorithms (FIPS 203)
Bit (Symmetric) Security	112	128	128	256
Quantum-Safe	Yes [Resilient to 3000 qubits]	Yes [Resilient to 9000 qubits]	Yes [Resilient to 2330 qubits]	Yet to be evaluated (field trials)
Qubits to Break (Physical)	20M	>20M	317M	Yet to be evaluated (field trials)
Field Tested	Since 2000	Since 2000	Since 1985	Since 2017 (ongoing evaluation)
Transfer of Technology	Cryptographic libraries and hardware modules support legacy algorithms extensively.			Challenging—requires updates to protocols, authentication, and key handling
Training	IT/security teams are well-trained due to legacy maturity and wide adoption.			Requires new training programs to close skill gap in PQC

Comparison of ECC and PQC in the Post-Quantum Era

Factor	ECC	PQC
Maturity	Well-established and standardized, with decades of deployment and cryptanalysis	Recently standardized; NIST selected Kyber, Dilithium, and SPHINCS+ in 2024
Quantum Resistance	Not resistant; vulnerable to quantum attacks using Shor’s algorithm	Designed to resist quantum attacks (e.g., lattice-, code-, or hash-based schemes)
Key and Signature Size	Compact: ECC-256 public key ≈ 32 bytes; signature ≈ 64 bytes	Larger: Kyber public keys ≈ 800–1500 bytes; Dilithium signatures ≈ 2–3 KB
Efficiency	Highly efficient for embedded and resource-constrained systems; optimized libraries available	Generally slower and more resource-intensive; some schemes suitable for constrained use
Deployment	Widely supported across TLS, smartcards, TPMs, and mobile apps	Limited support; PQC integration into protocols (e.g., TLS 1.3) still under development
Security (Current)	Strong resistance to classical attacks; extensively analyzed	Strong post-quantum assumptions, but some schemes are still relatively new
Transition Risk	Low; well-understood operational practices and tooling	Medium–high; implementation and cryptanalysis are still evolving

Quantum Readiness with ECC

Once the order of the curves is finalized in light of their expected quantum resilience, following are subsequently needed for the realization of quantum-safe applications using ECC.

- *Computation of cryptographically secure elliptic curve needs to be computed over a desired prime field size and of desired order.*
- *Target applications need to be updated with the integration of the new higher-order elliptic curve.*
- *The new elliptic curve needs to be standardized for global acceptance and interoperability among applications.*

Conclusion

- *When quantum computers achieve their full potential, theoretically secure algorithms will only be resistant to quantum attacks!*
- *ECC is not secure against Shor's algorithm, but remains secure until a reliable quantum computer with millions of physical qubits becomes a reality to break the ECDLP.*
- *Using higher-order elliptic curves will enable strategy decision makers to save immediate technology migration investments for a reasonably long period until a practical quantum computer with millions of physical qubits is realized.*

Legacy algorithms can still be adapted to provide adequate quantum resilience for existing security infrastructures for a reasonably long duration

meanwhile let *PQC algorithms continue to evolve and mature through evaluation and field testing.*

Thank you.