Preparing for Post-Quantum: Securing Internet Infrastructure for the Long Term

Dr. Burt Kaliski, Sr. Vice President and CTO

Post-Quantum Cryptographic Algorithms Are Coming

Quantum Computing Is on the Long-Term Technology Horizon

Bit → Qubit

State → Superposition & Entanglement

Boolean Gate → Unitary Operator

Certainty → Measurement Probability

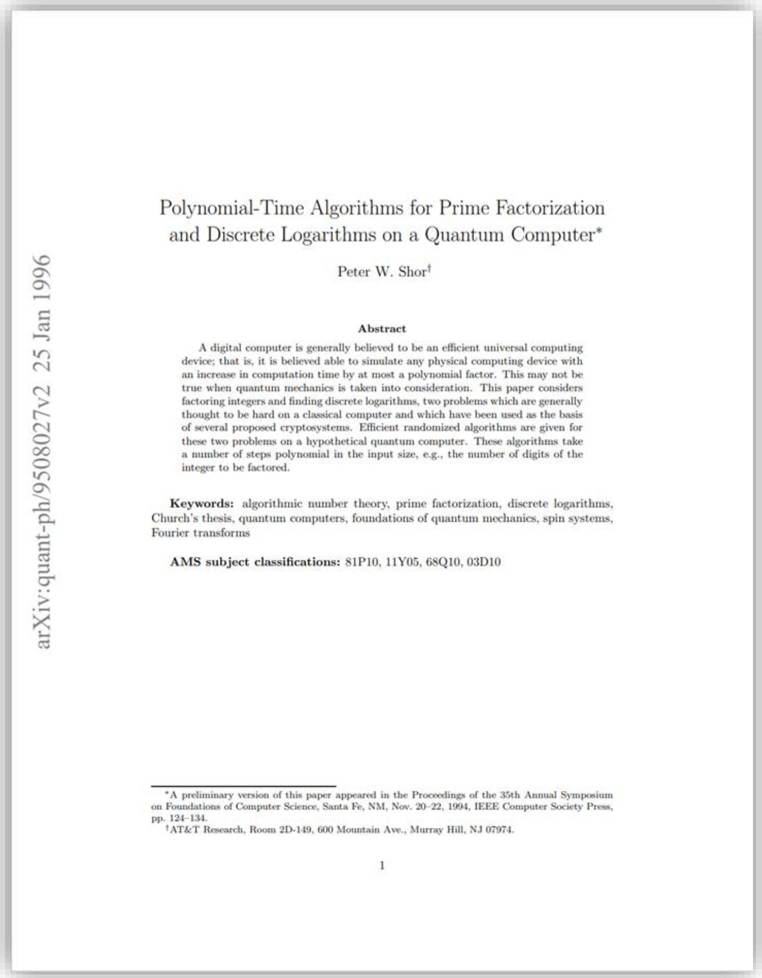
Classical → Quantum Algorithms

"Computation based on quantum mechanical effects, such as superposition and entanglement, in addition to classical digital manipulations."

Paul E. Black, Dictionary of Algorithms and Data Structures[1]

A Cryptanalytically Relevant Quantum Computer Could Break Today’s Public-Key Cryptography

- **Shor’s 1994 breakthrough:**[2] Quantum computers can break all three current public-key families: **RSA, DH/DSA, elliptic curve**
- Symmetric-key encryption, hash functions impacted by other quantum algorithms including Grover’s quantum search, but less significantly
- **Threat timeline:** Expert opinions range from 15 to 50 years[3]



arXiv:quant-ph/9508027v2 25 Jan 1996

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church’s thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

*A preliminary version of this paper appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20–22, 1994, IEEE Computer Society Press, pp. 124–134.

†AT&T Research, Room 2D-149, 600 Mountain Ave., Murray Hill, NJ 07974.

1

New Post-Quantum Algorithms are Being Developed, Evaluated and Standardized

Examples from US NIST	**Public-Key Encryption/KEMs**	**Digital Signatures**	*Family*	
PQC Standardization Process (July 2022)[4]	CRYSTALS-KYBER	CRYSTALS-Dilithium	Lattice-Based	
		FALCON		
		SPHINCS^{+}	Stateless	Hash-Based
SP 800-208 (Oct. 2020)[5]		XMSS^MT	Stateful	
		HSS/LMS		

Other families considered: Code-Based, Multivariate-Based

New Algorithms Bring New Design Considerations

Style

Key Encapsulation Mechanisms (KEMs) have different “interface” than public-key encryption (vs. RSA), key agreement (vs. DH)

Size

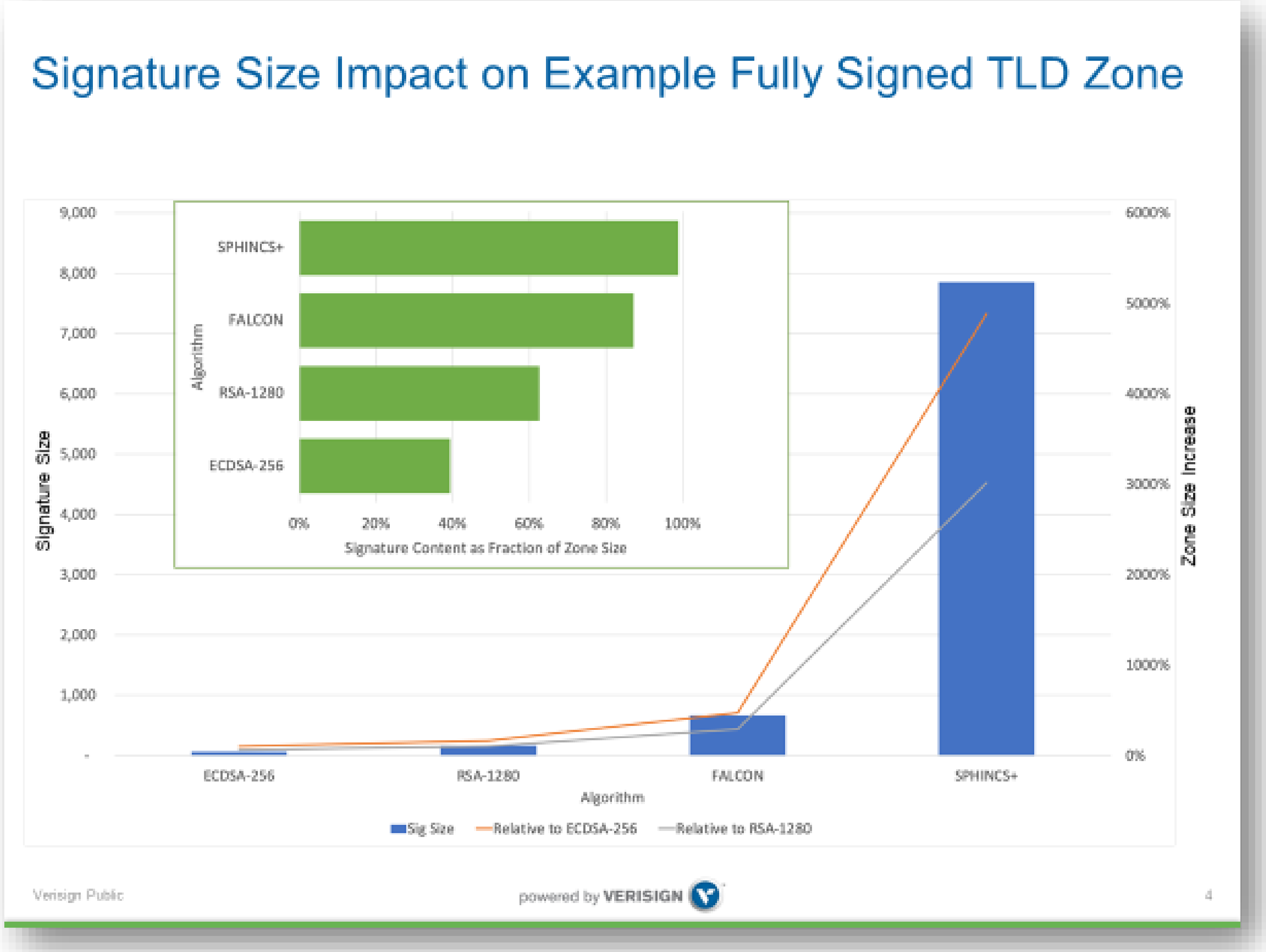
New ciphertext, signature and (sometimes) key sizes can be 10-100x larger (or more) than pre-quantum algorithms

State

Private key is continually updated in current stateful hash-based signature schemes — same state must not be used twice

Use Case Example: DNSSEC

(From A. Fregly, OARC 40, Feb. 2023)[6]



Signature Size Impact on Example Fully Signed TLD Zone

Verisign Public

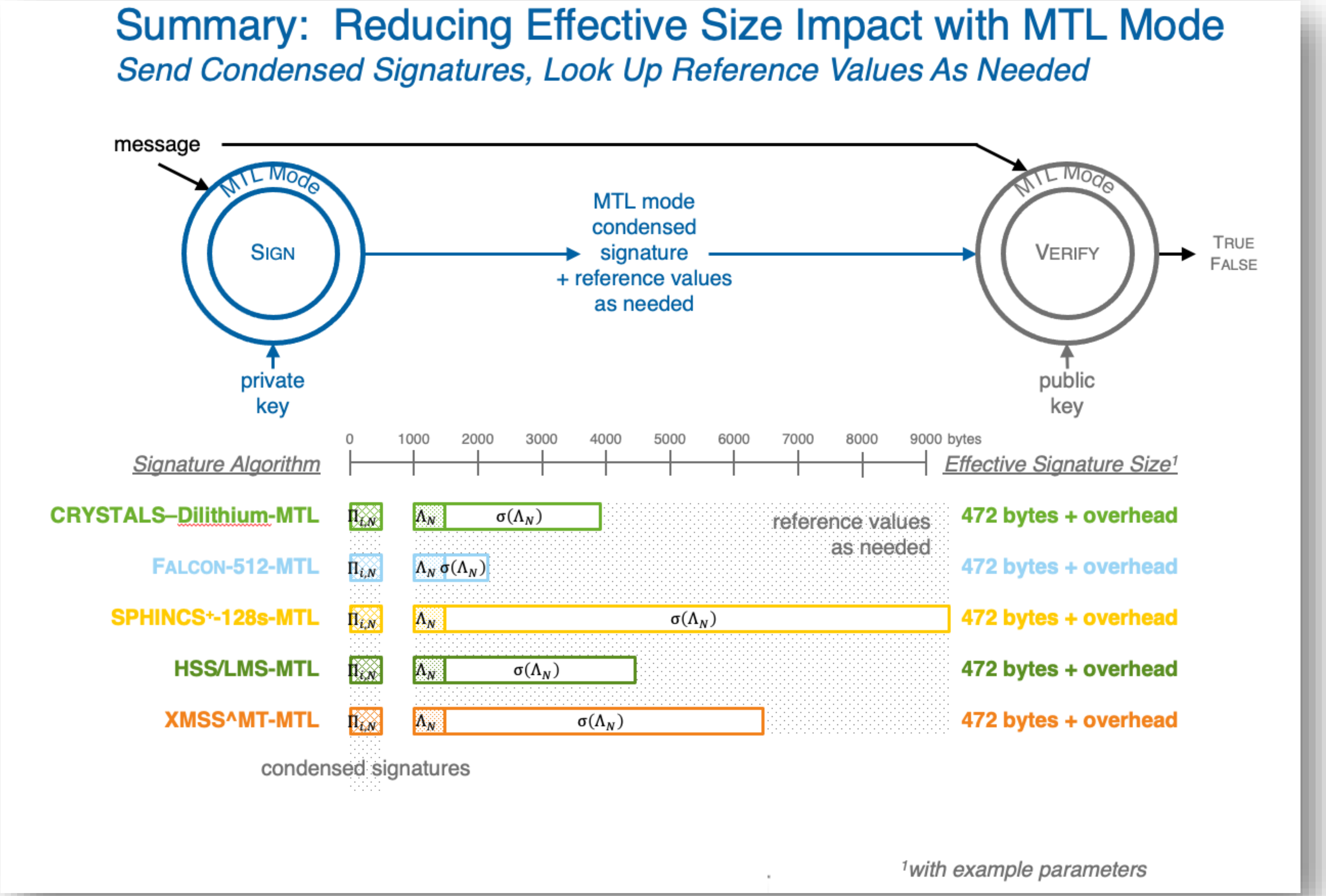
powered by VERISIGN

4

With stateless hash-based algorithm, DNS zone files would consist almost entirely of signatures

Example Redesign Proposal: Signature "Condensation" with Merkle Tree Ladder Mode

(From B. Kaliski, NIST Fourth PQC Standardization Conference, Dec. 2022)[7]



Summary: Reducing Effective Size Impact with MTL Mode

Send Condensed Signatures, Look Up Reference Values As Needed

message

MTL Mode

SIGN

private key

MTL mode condensed signature + reference values as needed

MTL Mode

VERIFY

public key

TRUE
FALSE

Signature Algorithm	Effective Signature Size[1]
CRYSTALS–Dilithium-MTL	472 bytes + overhead
FALCON-512-MTL	472 bytes + overhead
SPHINCS+-128s-MTL	472 bytes + overhead
HSS/LMS-MTL	472 bytes + overhead
XMSS^MT-MTL	472 bytes + overhead

reference values as needed

condensed signatures

[1] *with example parameters*

472-byte condensed signature size for NIST Level V security. Only **248 bytes** for Level I

(10,000-message series)

Migration Planning Is Already Underway in Anticipation of the New Algorithms

Mosca’s Model:[3]

Threat Exposure Time =

(Migration Time + Shelf Time) - Threat Timeline

Threat Timeline	Expert opinions range from 15 to 50 years[3]
Migration Time	Experience indicates 10 to 15 years
Shelf Time	For encryption, potentially decades. For signatures, minimal to years

Key Questions for Internet Infrastructure Providers: Where, When, How to Prepare for Post-Quantum?

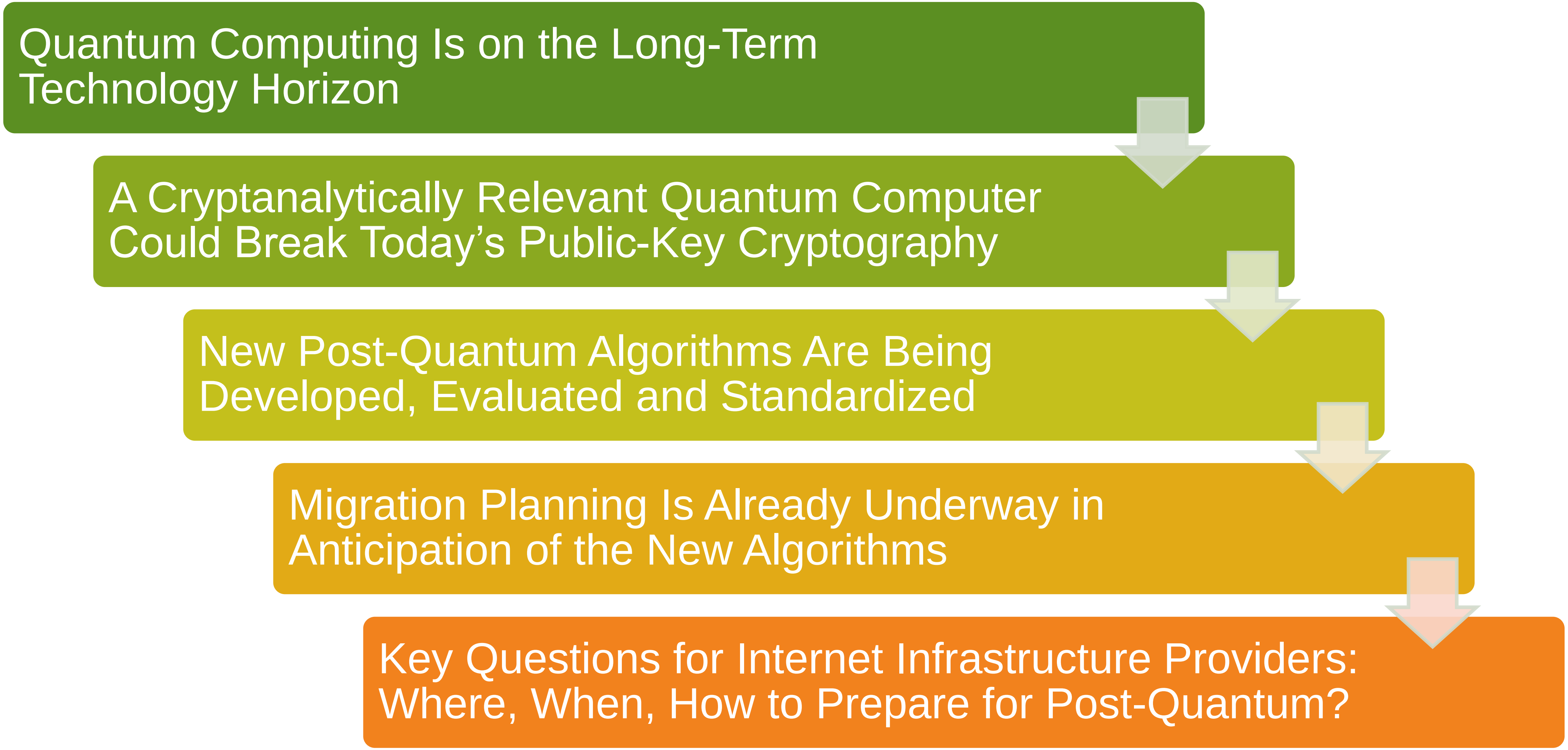
Identify

Prioritize

Migrate

See: NIST, “Migration to Post-Quantum Cryptography,” May 2016[8]

Summary: Post-Quantum Algorithms Are Coming



Quantum Computing Is on the Long-Term Technology Horizon

A Cryptanalytically Relevant Quantum Computer Could Break Today's Public-Key Cryptography

New Post-Quantum Algorithms Are Being Developed, Evaluated and Standardized

Migration Planning Is Already Underway in Anticipation of the New Algorithms

Key Questions for Internet Infrastructure Providers: Where, When, How to Prepare for Post-Quantum?

References

1. Paul E. Black, “Quantum Computation,” in Paul E. Black (ed.), *Dictionary of Algorithms and Data Structures*, Dec. 17, 2007, https://www.nist.gov/dads/HTML/quantumComputation.html, last accessed Feb. 16, 2023.
2. P.W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Review* 41.2 (1999): 303-332.
3. M. Mosca, M. Piani, “Quantum Threat Timeline Report 2020,” https://globalriskinstitute.org/download/quantum-threat-timeline-report-2020/
4. “PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates,” NIST, July 5, 2022, https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4
5. “Recommendation for Stateful Hash-Based Signature Schemes,” NIST SP 800-208, Oct. 2020, https://csrc.nist.gov/publications/detail/sp/800-208/final
6. A. Fregly, “Research Agenda for a Post-Quantum DNSSEC,” OARC 40, Feb. 16-17, 2023, https://indico.dns-oarc.net/event/46/
7. B. Kaliski, “Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms,” NIST Fourth PQC Standardization Conference, Nov. 29-Dec. 1, 2022, https://csrc.nist.gov/Events/2022/fourth-pqc-standardization-conference
8. “Migration to Post-Quantum Cryptography,” NIST NCCoE, https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms, last accessed Feb. 16, 2023

VERISIGN®