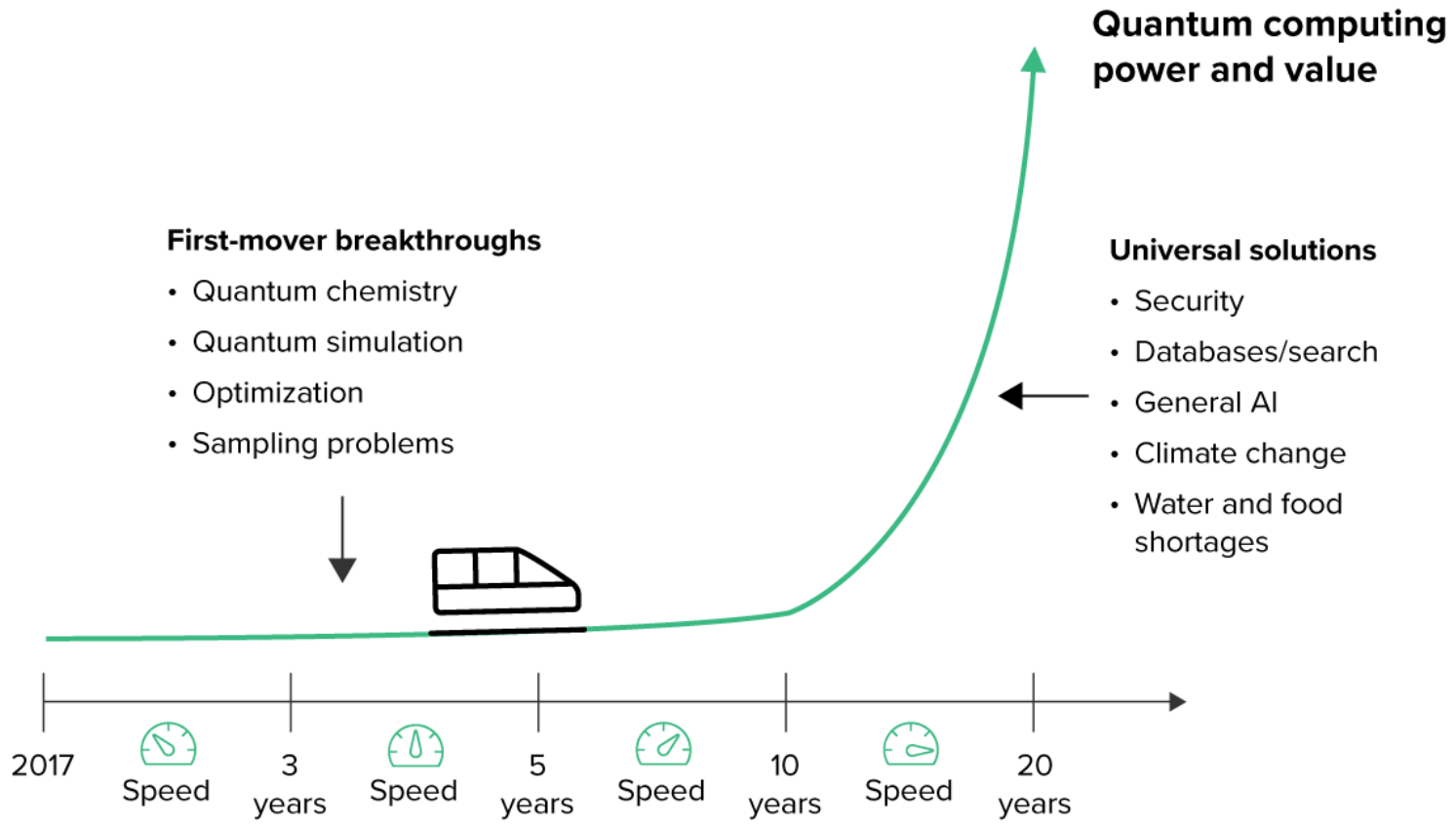
FORRESTER®

Planning For Post-Quantum Security

Heidi Shey

BOLD AT WORK

Where are we today with quantum computing?



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Source: Forrester report “Security Guide To Quantum Computing”

Types of vulnerabilities

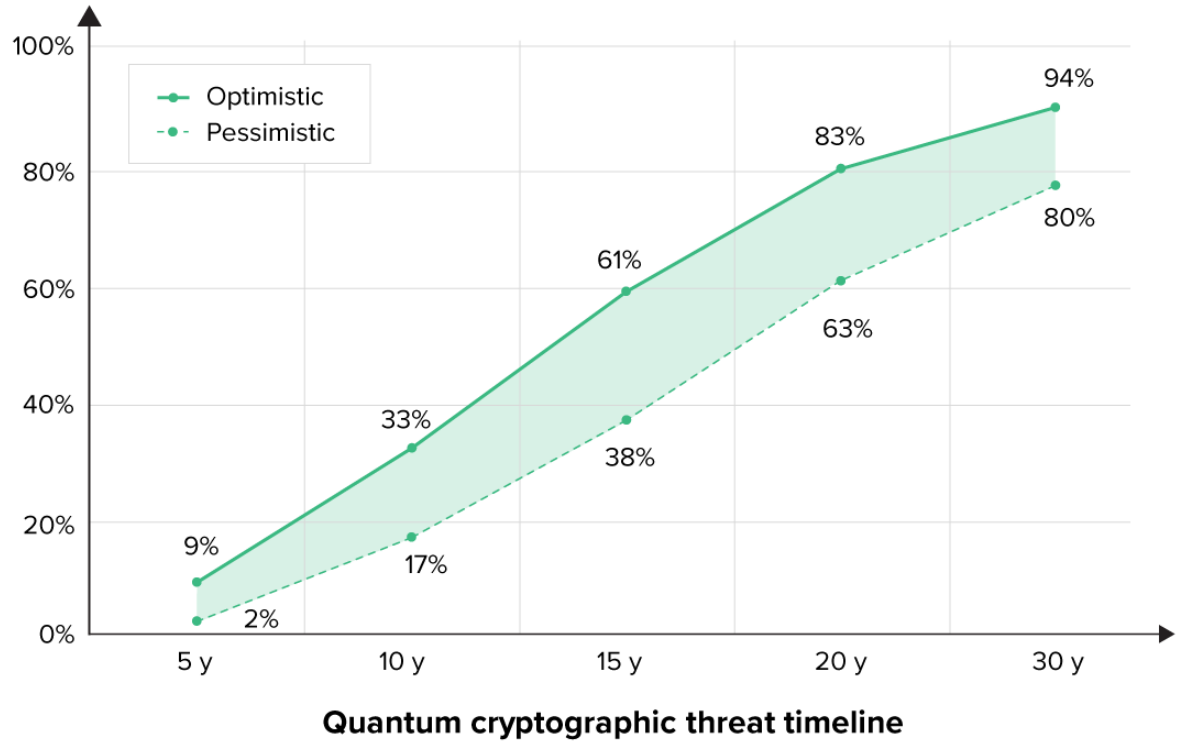
Use case	Vulnerability to quantum algorithms
Encryption	Symmetric key algorithms like AES will not be vulnerable to quantum computers. However, since key exchange algorithms will be vulnerable, assume that AES keys are not protected and that encrypted data can be decrypted (see key exchange below).
Key exchange	Asymmetric key algorithms like RSA and elliptic-curve (ECC) will be vulnerable to quantum computers. If a system uses RSA or ECC to exchange a symmetric key, an attacker could use a quantum computer to breach RSA or ECC and use that information to determine the symmetric key.
Digital signatures	Digital signature algorithms like RSA, ECSDA and DSA will be vulnerable to quantum computers.

Source: Forrester report “Security Guide To Quantum Computing”

How much time do we have?

See Dr. Michele Mosca's theorem of quantum risk against an optimistic vs. pessimistic probability analysis of when a real threat might be present

Opinion-based estimates of the cumulative probability of a digital quantum computer able to break RSA-2048 in 24 hours as function of time



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Source: Forrester report "Security Guide To Quantum Computing"

What is post-quantum cryptography?

Aka quantum-resistant cryptography

Goal

Cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks (NIST)

Where are we today?

PQC algorithms selected by NIST as of January 2023

Algorithm name	Algorithm type	Status
CRYSTALS-Kyber	Encryption/key exchange	Selected
CRYSTALS-Dilithium	Digital signature	Selected
FALCON	Digital signature	Selected
SPHINCS	Digital signature	Selected
BIKE	Encryption/key exchange	Moved to Round 4
Classic McEliece	Encryption/key exchange	Moved to Round 4
HQC	Encryption/key exchange	Moved to Round 4
SIKE	Encryption/key exchange	Moved to Round 4, but found to be insecure on August 5

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Source: Forrester report “Security Guide To Quantum Computing”

It’s time to prepare

The signs are here

- Standards development is in progress. National Institute of Standards and Technology (NIST) competition is key.
- Take cues from governments that have issued guidance and mandates.
- Remember that commercial viability is different from nation-state viability.
- Migration to post-quantum cryptography will take time.

What you can do while we wait on standards

- Form an internal task force for ongoing queries on commercial and open-source software suppliers.
- Map out the encryption of and assess the value of your sensitive data.
- Conduct a cryptographic discovery and inventory.
- (Re)design infrastructure for cryptographic agility.

Examples of technology providers

Established security tech providers and newer startups

- Arqit
- Crypto4A
- Cryptomathic
- DigiCert
- Entrust
- Envieta
- Fortanix
- IBM
- Infosec Global
- ISARA
- Keyfactor
- PQShield
- Qrypt
- Quantinuum
- QuantumXchange
- Quintessence Labs
- QuSecure
- SandboxAQ
- SSH Communications
- Thales
- Utimaco

Thank You.

Heidi Shey