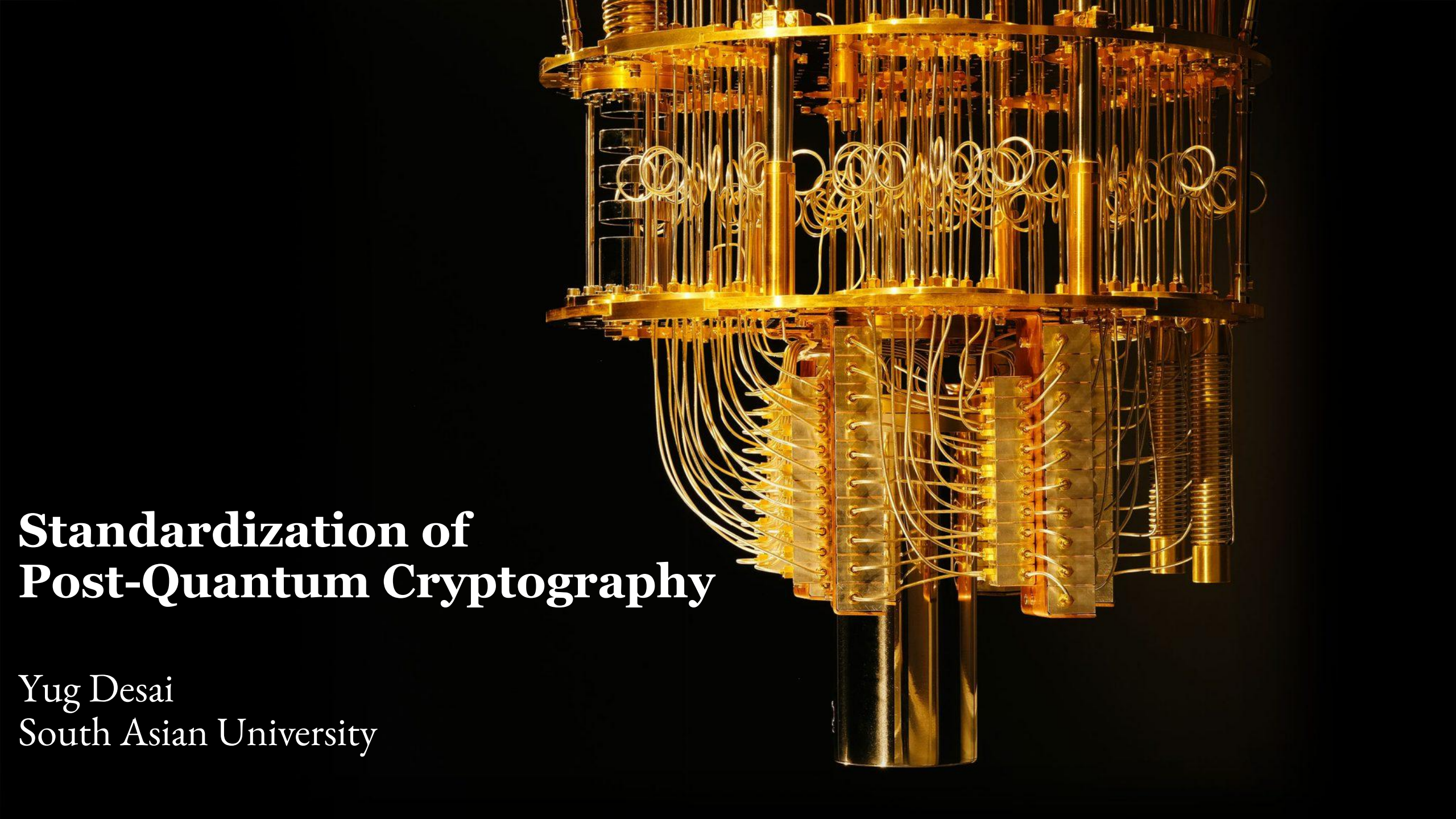


Standardization of Post-Quantum Cryptography

Yug Desai
South Asian University

Project Title: Role of Epistemic Communities in Standardization of (Post)Quantum Technologies.

- Interested in understanding the nature of networks involved in standardization of emerging early-stage technologies and their philosophies.
- This started as my M. Phil Project about 2 years ago but I have continued working on it after that.
- Started off as an International Relations project with the goal of understanding how technological competition and geopolitics bleeds into standardization.

Scope

- This presentation focuses on the threat from Quantum Computers and Standardization work related to Post-Quantum Cryptography (PQC).
- Centred around the National Institute for Technology and Standards (NIST) PQC Standardization Process.
- A Brief Note on relevance to Domain Name System
- Word of caution: Standardization ecosystem is acronym heavy.

KPMG Our Insights What we do About KPMG Careers

Our Insights > AI and Technology > Quantum is coming — and bringing new cybersecurity threats with it

Quantum is coming — and bringing new cybersecurity threats with it

Quantum computing changing the security infrastructure of the digital economy

NEWS 2 NOV 2023

UK Banks Warn Quantum Will Imperil Entire Payment System

Phil Muncaster
UK / EMEA News Reporter, Infosecurity Magazine
Email Phil Follow @philmuncaster

You may also like

NEWS 20 SEP 2024

MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HTSI

Time to get serious about the dangers of quantum computing

CryptoSlate

Alpha

Search

Top

NEWS hi Nakamoto reveal • Bitwise shifts Bitcoin, Ethereum futures ETFs to dynamic crypto and treasuries strategy • VanEck optimistic on Bitcoin's

News > CBDCs

WEF raises concerns over quantum computing risks to CBDCs, cryptographic encryption

According to the WEF, quantum computing poses significant risks to current encryption techniques.

Assad Jafri
May. 22, 2024 at 7:26 pm UTC

2 min read
Updated: May. 22, 2024 at 7:26 pm UTC

Fintech Events Community Jobs APIs

retail wholesale wealth regulation crime crypto sustainable startups devops

cyber and physical threats to banks and fintechs worldwide.

Singapore warns banks to prepare...

Singapore warns banks to prepare for quantum computing cyber threat

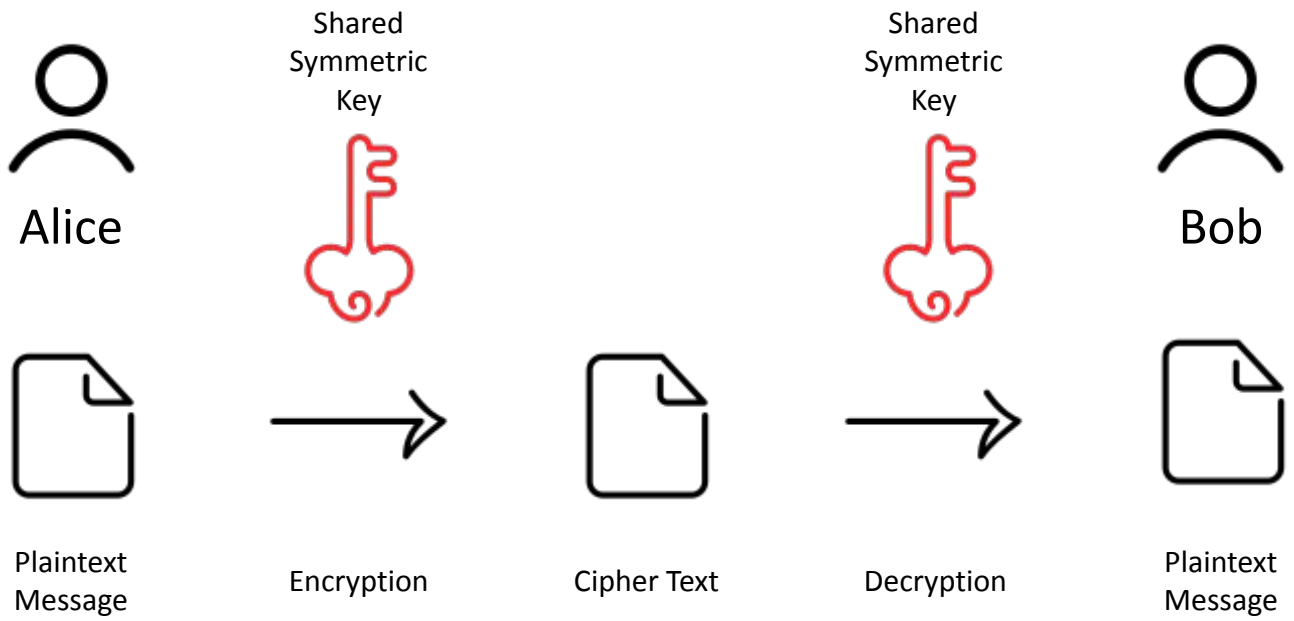
The Monetary Authority of Singapore has told the country's financial institutions to make sure they are prepared for the rising cybersecurity risks posed by quantum computing.

22 February 2024 Be the first to comment

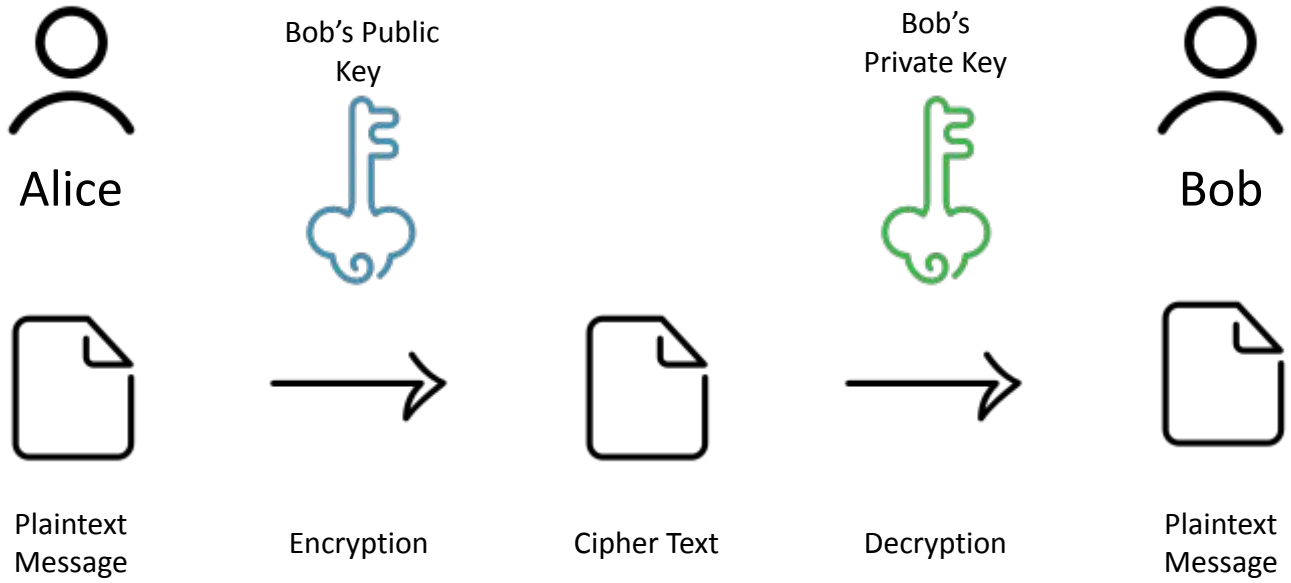
Understanding Encryption

A Short Detour

Symmetric Cryptography (Confidentiality)



Public-Key/Asymmetric Cryptography



ASYMMETRIC ENCRYPTION

Uses of Asymmetric Encryption

Source: https://www.collidu.com/presentation-asymmetric-encryption

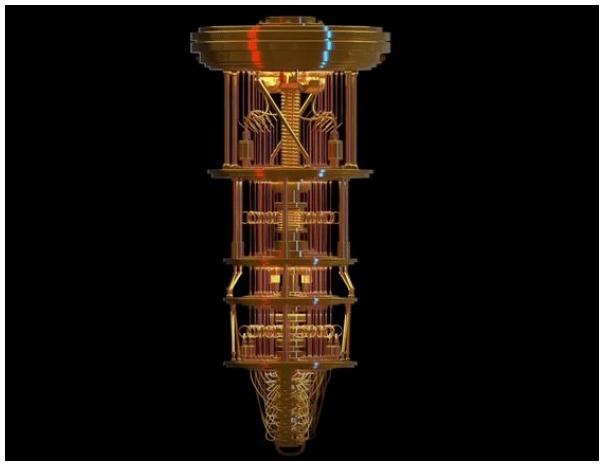
Common Cryptographic Approaches

Feature / Algorithm	Hash	Symmetric	Asymmetric
No. of Keys	0	1	2
NIST recommended Key length	256 bits	128 bits	2048 bits
Commonly used	SHA	AES	RSA
Key Management/Sharing	N/A	Difficult	Easy & Secure
Effect of Key compromise	N/A	Loss of both sender & receiver	Only loss for owner of Asymmetric key
Speed	Fast	Fast	Relatively slow
Complexity	Medium	Medium	High
Examples	SHA-224, SHA-256, SHA-384 or SHA-512	AES, Blowfish, Serpent, Twofish, 3DES, and RC4	RSA, DSA, ECC, Diffie-Hellman

Source: www.cryptomathic.com

The Threat

Shor's Algorithm



Public Key

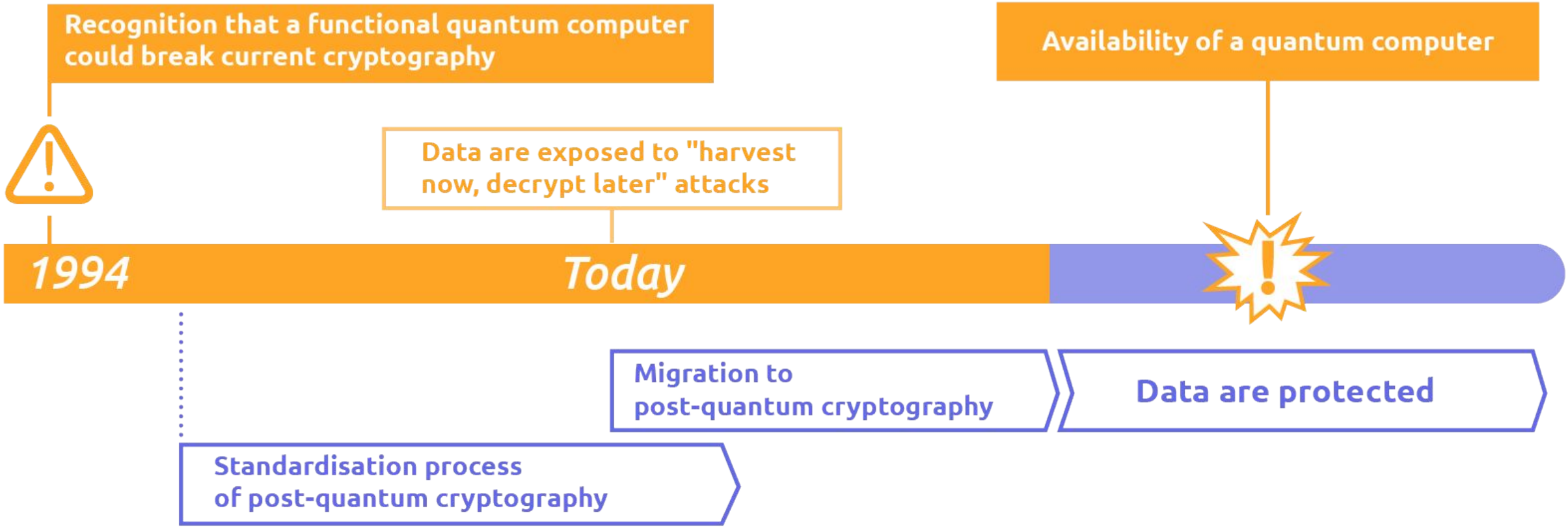
Private Key

Cipher Text

Message

Attacker

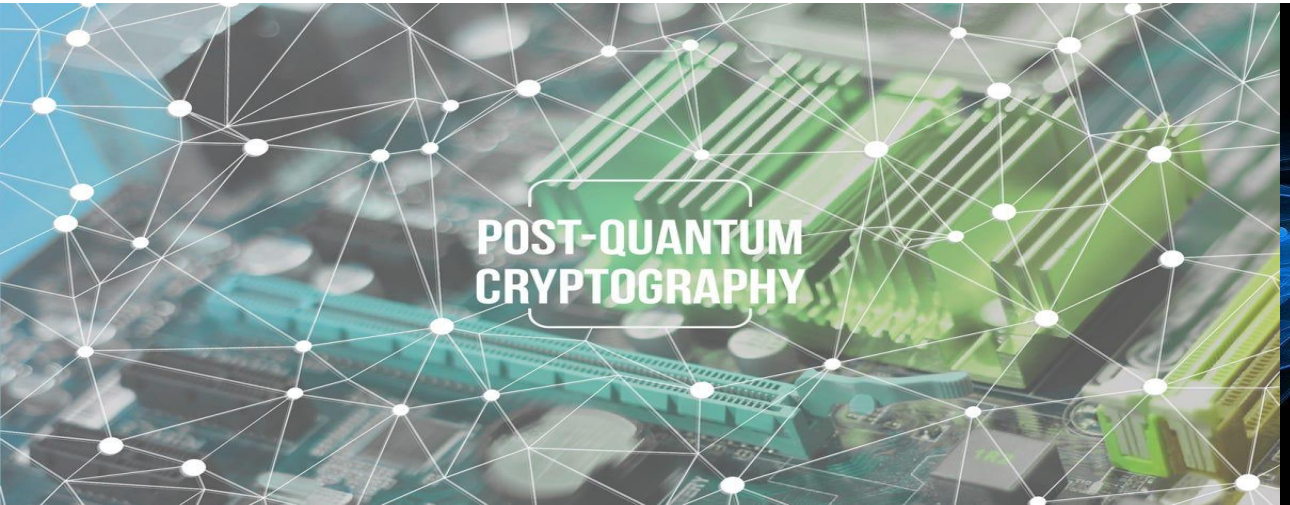
The Solution

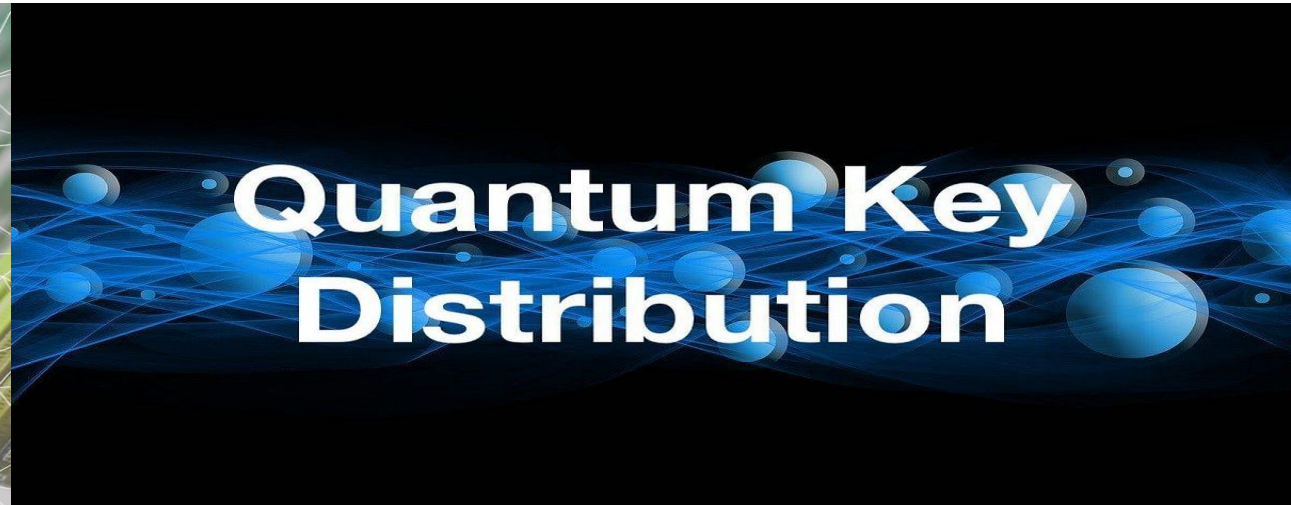


Source: https://www.bis.org/about/bisih/topics/cyber_security/leap.htm

Post Quantum Cryptography

- Two primary means of securing communications from the threat of quantum computers.
  - Post-quantum cryptography, which relies on a different class of mathematical problems to develop algorithms that can secure our data and communication from cryptanalysis by large-scale quantum computers.
  - Quantum cryptography refers to the exploitation of quantum phenomena to perform cryptographic functions.
- PQC involves the creation of new encryption methods that are resistant to cryptanalysis by quantum computers.





Background

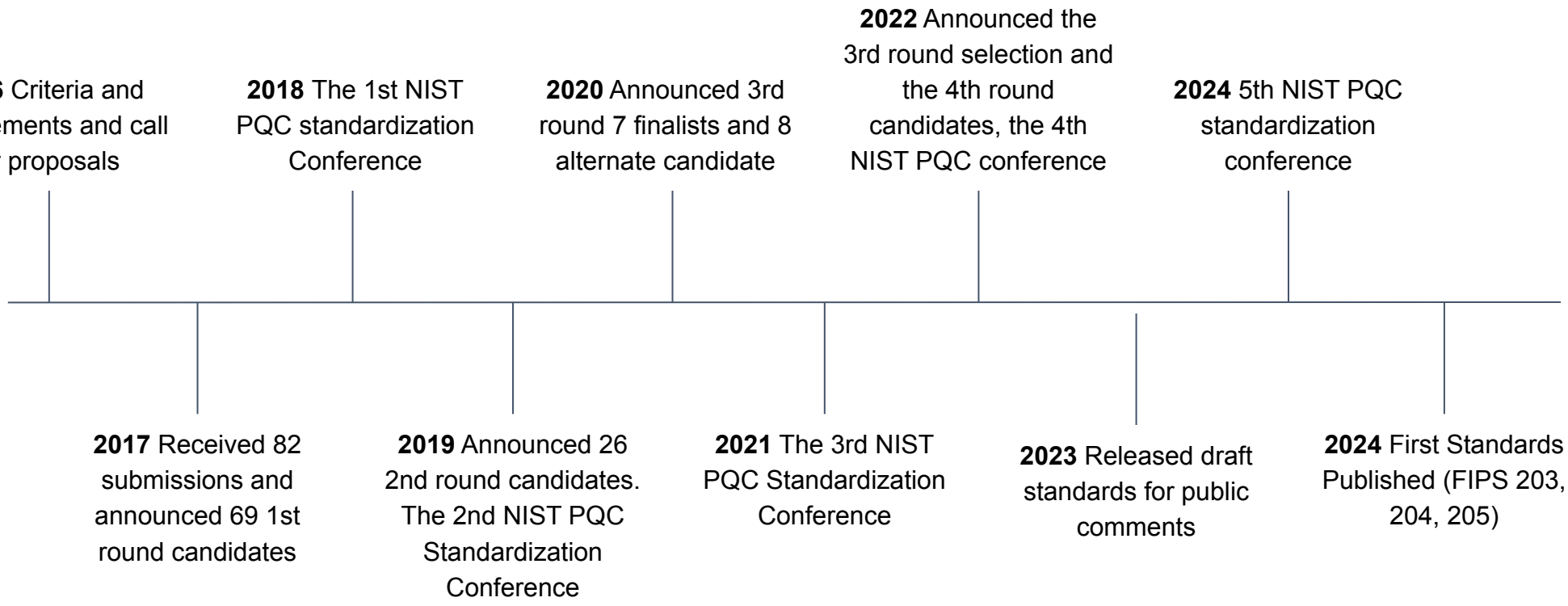
- Current encryption algorithms rely on the mathematical complexity of problems such as integer factorization and discrete logarithms that require prohibitively high computational effort to solve. Quantum computers operate differently from classical computers.
- However, Cryptographically Relevant Quantum Computers (CRQCs) could break these crypto-systems, rendering much of our public key cryptography vulnerable to cryptanalysis or breaking by quantum computers
- Quantum computing poses a considerable risk to secure communications
- Technologies such as post-quantum cryptography (PQC) and quantum key distribution (QKD) will play an important role in ensuring secure communication in the quantum age.
- Key standards development organizations SDOs in relation to PQC: the National Institute of Standards and Technology (NIST), and the Internet Engineering Task Force (IETF).

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST

- Standardization coordination is one of the key tasks of NIST in addition to conformity assessment to ensure adherence to standards, and education and training of members of governments and industry on issues related to standards
- Areas like Artificial Intelligence, Cybersecurity, the Internet of Things, and Future Computing are priorities for Information Technology Lab (ITL). The U.S. Government National Standards Strategy for Critical and Emerging Technologies identifies several emerging technologies that are relevant to ITL
- NIST standardized the Data Encryption Standard (DES), a symmetric key block cipher encryption algorithm, in 1977. Eventually, it became the de facto standard for cryptographic products in the U.S.
- To ensure that the standard has widespread acceptability, it was decided that the global cryptographic community should be involved in the development of the new Advanced Encryption Standard (AES) from the beginning
- The PQC project at NIST set out to select at least one public-key cryptographic algorithm through a process akin to AES and SHA. The process would yield new public-key cryptographic standards specifying at least one digital signature, public key encryption, and key-establishment algorithms. NIST published a call for proposals in December 2016. This call received an overwhelming response from the global cryptographic community, and NIST received 82 submissions
- The most important evaluation criterion for the NIST algorithms is security, followed by cost and performance. Furthermore, criteria like perfect forward secrecy, protection against side-channel attack, diverse hardness assumptions also feature after the initial criteria are met.

NIST Standardization Timeline



NIST - Coordination and Collaboration

- Engaging with the wider community is important for NIST for its cryptographic standards to be endorsed by other the industry and other SDOs around the world (Chen et al., 2016). The development of standards for PQC will require considerable resource investment to properly analyze candidate algorithms. Public engagement is critical to ensuring trust in the process and the resultant standards. The PQC standardization process also serves as an opportunity to engage the wider community
- The public feedback process was critical for the selection of algorithms in the second and third rounds. External feedback and performance estimates of various algorithms were provided by the cryptographic community engaged in the PQC standardization process
- NIST also uses a public mailing list to allow for the free flow of information and discussions among members of the cryptographic community engaged in the standardization of PQC. The community-wide effort was sustained over time, with greater interest generated as the the draft standards were released, as evidenced by the peak in the mailing list activity, which is open to all stakeholders.
- Another method for coordination and collaboration comes in the form of an annual PQC standardization conference organized by NIST, specifically focusing on the candidate algorithms and important cryptanalysis developments relevant to the standardization process at NIST.
- Migration Challenges: Integrating these into the existing applications, systems, and legacy infrastructure is also a significant challenge. These challenges have to do with issues related to performance, compatibility with existing infrastructure, and other practical implications of the transition from classical to quantum or quantum-resistant crypto-systems

Concerns

- All for nothing? What if quantum computers never materialise. What then is the point of all this effort?
- Or are we already late? What if we get quantum computers in the next five years and the migration is not complete?
- How does this affect the DNS ecosystem?

Relevance to the DNS

- Current Vulnerability: DNSSEC uses RSA and elliptic curve cryptography, vulnerable to future cryptographically relevant quantum computers (CRQCs). These could compromise DNSSEC's integrity by determining private keys and signing malicious records. Post-Quantum Cryptography (PQC) algorithms are necessary to protect DNSSEC from quantum attacks.
- Transition Timeline: The DNSSEC community should implement PQC algorithms years before CRQCs become feasible, ensuring sufficient time for widespread adoption and infrastructure updates.
- Encrypted DNS Protocols: DNS protocols using TLS or QUIC (e.g., DNS-over-TLS, DNS-over-HTTPS) should align their PQC adoption with broader web standards.
- ICANN's Office of CTO Position: PQC implementation for DNSSEC is unnecessary, as CRQCs are unlikely to be a near-term threat. Waiting allows observation of quantum computing advancements, benefits from ongoing PQC algorithm research, enables informed choice of suitable algorithms for DNSSEC. But community inputs are lacking in this matter.
- Economic Considerations: Early CRQCs will be extremely expensive. While DNSSEC impersonation could be valuable as adoption increases, its priority for attackers compared to other targets remains unclear.

Conclusion

- Timing for standardization of PQC is critical because of the amount of infrastructure that relies on traditional cryptographic methods. We cannot take the risk even if large scale quantum computers are not yet a reality.
- Hence, NIST standards come at a good time as we can begin the migration work which will still take a lot of time - close to a decade.
- It also brings more attention to the problem of quantum computers breaking encryption and will draw more resources and effort in understanding the available algorithms in the future.

Thank You!

Please Reach Out!

Email: yugdesai508@gmail.com
Website: yugdesai.com

Resources:

- **NIST PQC Project: https://csrc.nist.gov/projects/post-quantum-cryptography**
- **ICANN's Position: Hoffman, Paul (2024) 'Quantum Computing and the DNS', Office of the Chief Technology Officer**