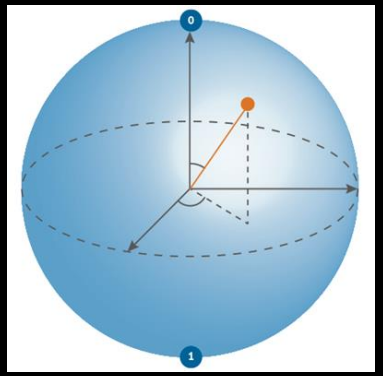


Security in a Quantum World

Dr. Michael A. Enright

Quantum Dimension, Inc.

WHAT WE DO

- *Quantum Dimension, Inc.*
  - Engineering Technology firm located in *Huntington Beach, "Southern" California, USA*
  - Focused on advanced technology development and consulting in *RF Communication, Cybersecurity, and Quantum Security and Computing* since 2016
- *Dr. Michael A. Enright*
  - CEO and President of *Quantum Dimension, Inc*. with over 30 years of experience in *RF Communication, Computing, Navigation* research and development
  - Member of IEEE standards groups – *Post-* and *Quantum Security and Computing, Zero Trust Security* – and others
  - Earned a Ph.D. Electrical Engineering from the *University of Southern California (USC*), in Los Angeles, California
  - Former Adjunct Professor in EE at USC teaching *Signal Processing, RF Communication, Linear Algebra and more*

MOTIVATION

Due to the existence of the Quantum Computer, specifically concerning information security by utilizing Shor's algorithm for the factorization of prime numbers, there has been significant interest in developing encryption techniques that will be secure, even in the presence of quantum computers. These techniques take different forms:

- Post-Quantum Cryptography (PQC) – Augmentation of classical techniques, such as lattice, etc.
- Quantum Cryptography/QKD – Using the properties of quantum mechanics and qubits
- Hybrid Cryptography – Hybrid of post-quantum, classical, quantum, e.g. Muckle and Muckle+

WHAT IS CRYPTOSECURITY?

- Types of cryptosystems
  - *Symmetric Key* – both sides, Alice and Bob, share the same key
    - Advanced Encryption Standard AES – AES128, AES256 – Data Encryption Standard (DES) in 2003 for US gov.
  - *Asymmetric Key* – each side a shared-secret
    - Diffie-Hellman Key Exchange is one example
    - Faster used for encryption
  - *Public-Private Key* – known public, unknown private
    - Used for authentication due to being slow
    - RSA algorithm
  - *Hash algorithms* – use cryptosystems for digital signatures

POST-QUANTUM CRYPTOGRAPHY

- "Classical" cryptosystems are based on prime factorization >> g^a mod p
- "Modern" cryptosystems use Lattice-based, Code-based and Multivariate cryptography
- New NIST standards, beginning in 2017, for *Key Encapsulation Mechanism (KEM) and Digital Signatures*
  - Draft FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard – CRYSTALS-Kyber*
  - Draft FIPS 204, *Module-Lattice-Based Digital Signature Standard – CRYSTALS-Dilithium*
  - Draft FIPS 205, *Stateless Hash-Based Digital Signature Standard – SPHINCS+*
- *New round "on-ramp" began on July 5, 2022*
- *For details see https://csrc.nist.gov/Projects/post-quantum-cryptography*

QUANTUM SECURITY

- Two important Quantum properties
  - No-cloning
  - Collapse of the Wave Function
- Quantum Security algorithms require Classical and Quantum components
- There have been many others over the decades that use properties of photons and information theoretic techniques
  - Earliest algorithm is BB84 in 1984
  - Many other since then include BBP2, SSP, DPS, SARG04, COW, S13 and others
- Background in physics and communication is good

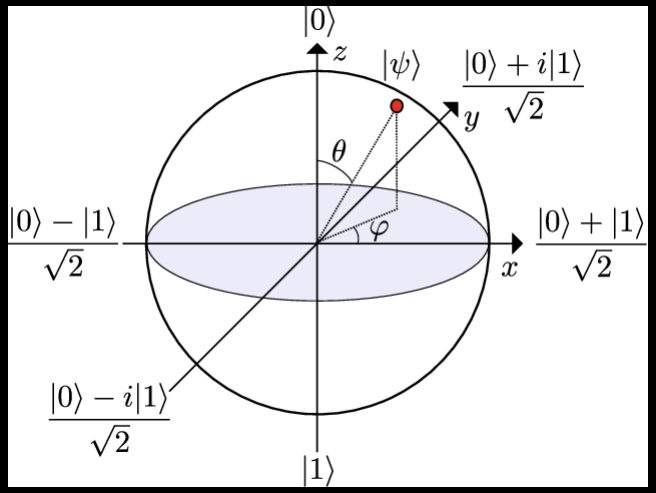
QUANTUM COMPUTING AND INFORMATION

- Quantum Comput-er
  - Superconducting – the most popular type of quantum computer hardware
  - Others include Photonic, Neutral Atoms, Trapped Ions, Quantum Dots ...
- Quantum Comput-ing
  - Quantum Annealing – solves an *optimization problem* via a cost function such as in Neural Networks

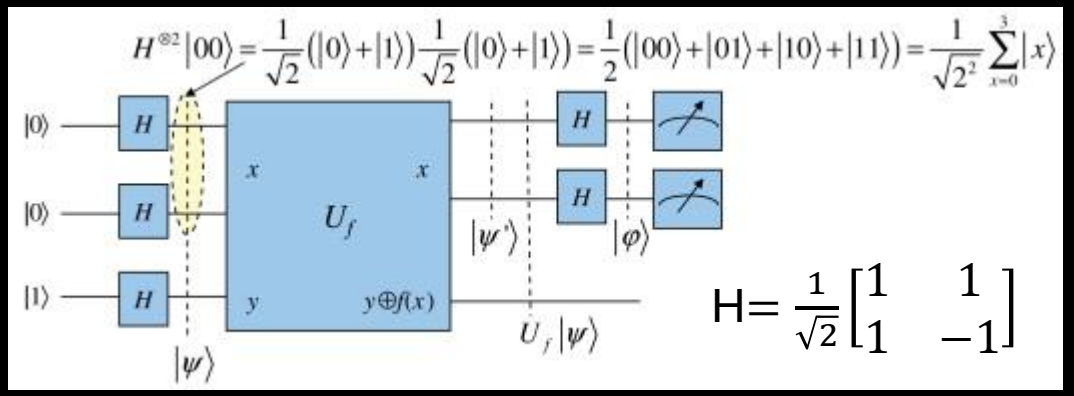
$$J(x_1, x_2, \cdots x_N) = f(x_1, x_2, \cdots x_N) + \lambda * g(x_1, x_2, \cdots x_N)$$

  - Universal Gate – Implement quantum functions via *gate-based logic operations*
    - Linear Algebra and Information-Theoretic based

QUBIT – THE BASIC UNIT OF QUANTUM INFORMATION



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longleftrightarrow P(|0\rangle) = \alpha^2, P(|1\rangle) = \beta^2$$



- The QuBit has a state, ψ, and probabilities α^2 and β^2
- *Linear Algebra and Change of Basis* – Changes of state are functions that are implemented by Unitary operations
  - Pauli gates, Hadamard gate, NOT, CNOT, etc.
- Quantum Crytopraphy BB84 requires that bases are known

IS QUANTUM SECURITY WORTH IT?

From U.S. NSA - https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Technical limitations

1.Quantum key distribution is only a partial solution. QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile.

2.Quantum key distribution requires special purpose equipment. QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches.

3.Quantum key distribution increases infrastructure costs and insider threat risks. QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration.

4.Securing and validating quantum key distribution is a significant challenge. The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs. The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than in most physical engineering scenarios making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems.[2]

5.Quantum key distribution increases the risk of denial of service. The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

Conclusion

In summary, NSA views quantum-resistant (or post-quantum) cryptography as a more cost effective and easily maintained solution than quantum key distribution. For all of these reasons, NSA does not support the usage of QKD or QC to protect communications in National Security Systems and does not anticipate certifying or approving any QKD or QC security products for usage by NSS customers unless these limitations are overcome.

ETSI SECURITY CONFERENCE

https://www.etsi.org/events/2155-etsi-security-conference-2023

ON-GOING ACTIVITIES

- IEEE Standards Association (SA) Working Group (WG) and FNTC Activities
  - Post- and Quantum Security, Quantum Computing, Zero Trust (Zero Trust) Security
  - Sign-up: https://development.standards.ieee.org
  - FNTC Security & Privacy WG
- Cybersecurity
  - IEEE SA Post-Quantum Network Security – P1943
  - IEEE SA Quantum Security WG – P3172
  - IEEE SA ZT Security WG – P2887 and P3409
- Quantum Computing
  - IEEE SA Quantum Computing Architecture WG – P3120
  - IEEE SA Hybrid Quantum-Classical Computing WG – P3185

IEEE SA P1943

Scope of proposed standard: This standard defines a method to implement optimized post-quantum version of existing network security protocols [1]. It is based on a multi-layer protocols approach and allows data packets and/or data encapsulated to be quantum resistant to future cryptographically relevant quantum computers (CRQCs). This standard includes hybrid modes for key exchange and authentication and specifies mechanisms for handling the larger public key sizes of post-quantum algorithms. This standard excludes any definition of a new post-quantum cryptography (PQC) algorithm.

Need for the Project: Quantum technologies are challenging today's network security: data packets are already vulnerable to future fault-tolerant quantum computing (FTQC) attacks. The current public key standards (e.g., Rivest-Shamir-Adleman known as RSA, Diffie-Hellman, Elliptic Curve Digital Signature Algorithm known as ECDSA) are not strong enough to withstand attacks using future cryptographically relevant quantum computers (CRQCs). The encrypted data with long life cycle (cf. Mosca's theorem) are at risk since they can be intercepted (data traffic) today, stored and decrypted latter once CRQCs are available. Following international recommendations [2], all network security protocols (e.g., Transport Layer Security known as TLS, Internet Protocol Security known as IPsec) should be upgraded to quantum-safe cryptography as soon as possible.

IEEE SA P3172

Scope of proposed standard: This recommended practice describes multi-step processes that can be used to implement hybrid mechanisms (combinations of classical quantum-vulnerable and quantum-resistant public key algorithms). Existing post-quantum cryptography (PQC) systems are described. Desired characteristics of the hybrid mechanisms, such as crypto agility are also described.

Need for the Project: The identified cyber threat is based on the future existence of cryptographically relevant quantum computers (CRQCs) and concerns all PKC systems today that encrypt sensitive data with a long life cycle (cf. Mosca's theorem). In order to preserve the confidentiality of the data from a future CRQC attack, the classical public-key cryptographic (PKC) algorithms (e.g., Rivest-Shamir-Adleman known as RSA, Diffie-Hellman, Elliptic Curve Digital Signature Algorithm known as ECDSA) must be replaced by PQC algorithms.

INTERESTING PLACES

- *https://csrc.nist.gov/Projects/post-quantum-cryptography*
- https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
- https://www.pqcrypto.org/
- https://2023.qcrypt.net/
- https://www.youtube.com/@qcryptconference239
- https://qce.quantum.ieee.org/2023/
- https://www.etsi.org/events/2155-etsi-security-conference-2023
- https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
- https://development.standards.ieee.org
- Satellite-to-Ground QKD 2017 Paper: https://arxiv.org/ftp/arxiv/papers/1707/1707.00542.pdf

CONTACT INFORMATION

Dr. Michael A. Enright
Quantum Dimension, Inc.
menright@qdimension.com
(714) 893-6004 x 606

Ms. Julie Isenberger
Quantum Dimension, Inc.
jisenberger@qdimension.com
(714) 893-6004 x 600

THANK YOU