# Quantum Cryptography

**Introduction to Computer Security**

Naercio Magaia and Imran Khan

# Quantum Cryptography

- Concerned with the development of cryptographic algorithms that are secure against the potential development of quantum computers
- Concerned with the security of asymmetric cryptographic algorithms

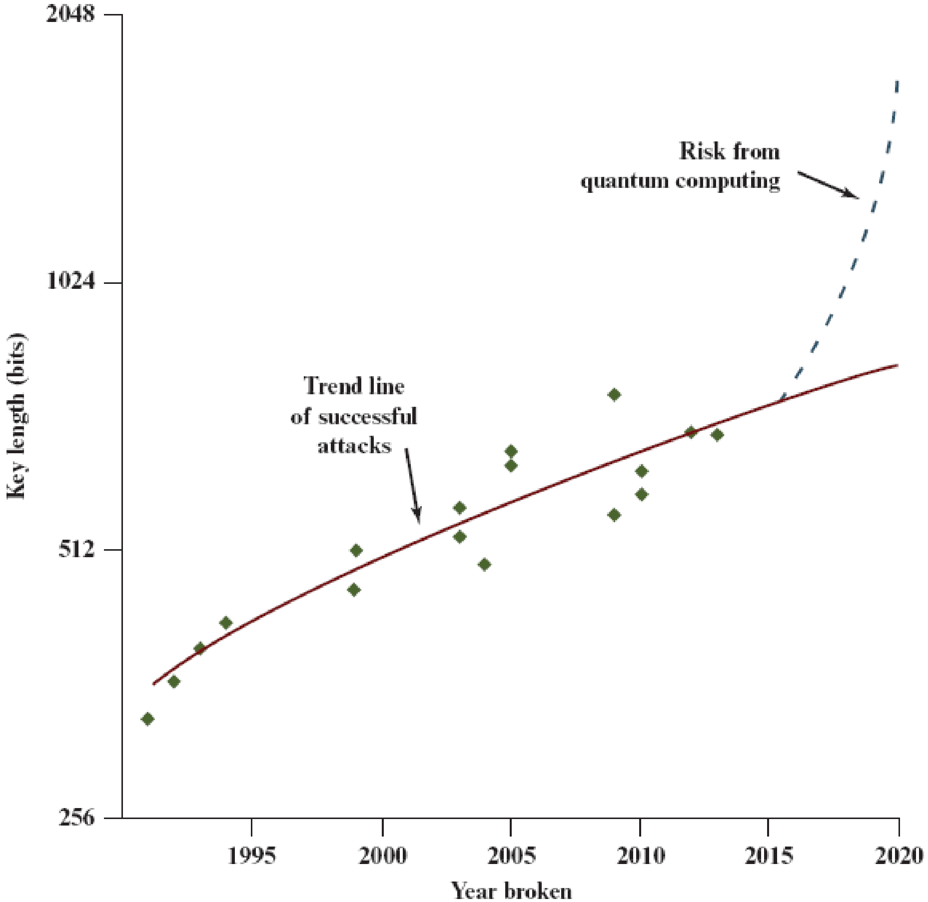
# Quantum Computing

- *Quantum computing* is based on the representation of information in a form analogous to the behavior of elementary particles in quantum physics
- A practical application of this representation requires producing a physical system that performs computation making use of quantum physical principles
- As yet, no such general-purpose computing system has been developed but in principle it is possible to do so

# Qubits

- Information in a quantum computer is represented as quantum bits, or *qubits*
  - A qubit can be viewed as a quantum analog of a classical bit, one that obeys the laws of quantum physics
- Qubits have two properties that are relevant to quantum computing:
  - ***Superposition:*** A qubit does not exist in a single state but in a superposition of different states. It is only when a measurement is taken that the qubit collapses into a unique state (binary 1 or 0). Prior to that it is only possible to express a probability that the qubit is a 1 or a 0. The qubit can be thought of a vector of unit magnitude in a two-dimensional vector space.
  - ***Entanglement:*** Qubits can be linked to each other over the course of operations reflecting the physical phenomenon known as quantum entanglement. The relevant implication of this is that state of a multiple-qubit system is not represented by a linear combination of the state vectors of each qubit but rather a tensor product.

# RSA Key Lengths Broken by Conventional Computing Architectures



# Grover's Algorithm

- Searches an unordered list in $O(\sqrt{n})$ time, while conventional algorithms require $O(n)$
- Can reduce the cost of attacking a symmetric cryptographic algorithm
- A 128-bit AES key is considered secure for the foreseeable future
  - To guard against a quantum attack using Grover's algorithm, the same level of security could be maintained by moving to a 256-bit key
- Similarly, Grover's algorithm can theoretically reduce the security of a cryptographic hash algorithm by a factor of two
  - This can be countered by doubling the hash length

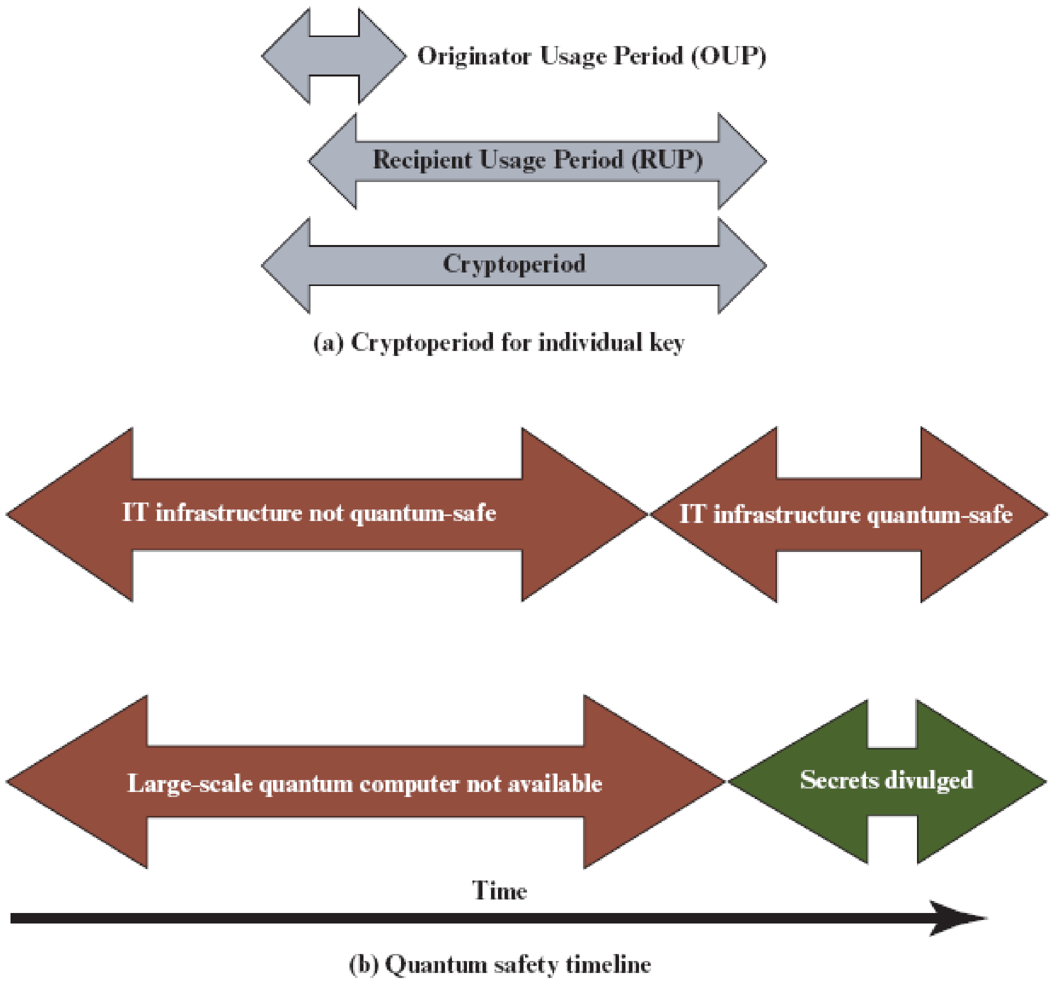
# Raising Awareness

- Although practical large-scale quantum computers are not likely for a number of years, there has been considerable interest and some urgency in developing cryptographic algorithms that are secure against such computers
- The following are examples:
  - In 2014, the ETSI Quantum Safe Cryptography (QSC) Industry Specification Group was formed to assess and make recommendations for quantum-safe cryptographic primitives and protocols
  - In 2015, the U.S. National Security Agency (NSA) released a major policy statement on the need for post-quantum cryptography
  - In 2016, NIST announced a request for submissions for public-key *post-quantum cryptographic algorithms*

# Cryptoperiod

- The cryptoperiod of a cryptographic key is the time span during which a specific cryptographic key is authorized for use for its defined purpose
- A number of potential security threats make it advisable that any key not be used for a prolonged period of time. These threats include:
  - Brute-force attacks
  - Cryptanalysis
  - Other security threats

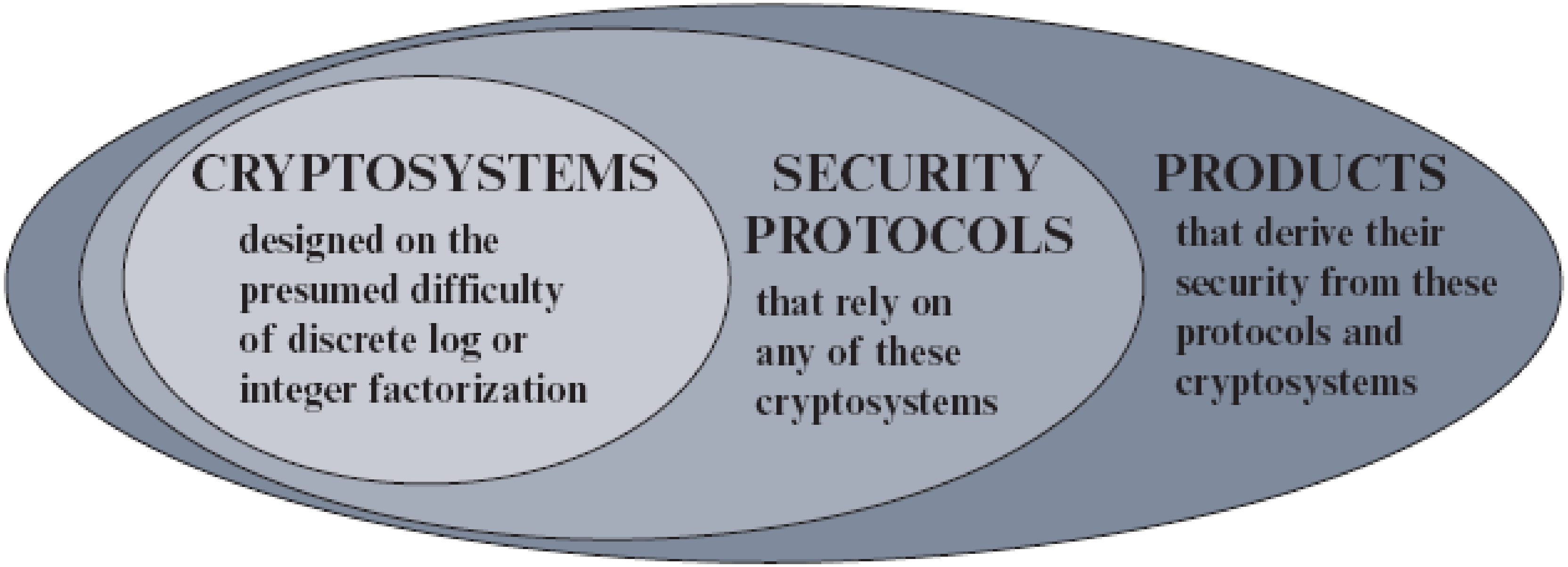
# Lead Time for Quantum Safety



# Suggested Cryptoperiods from SP 800-57

| Key Type | OUP | RUP |
|---|---|---|
| 1. Private Signature Key | 1 to 3 years | — |
| 2. Public Signature-Verification Key | Several years (depends on key size) | |
| 3. Symmetric Authentication Key | ≤ 2 years | ≤ OUP + 3 years |
| 4. Private Authentication Key | 1 to 2 years | |
| 5. Public Authentication Key | 1 to 2 years | |
| 6. Symmetric Data Encryption Keys | ≤ 2 years | ≤ OUP + 3 years |
| 7. Symmetric Key Wrapping Key | ≤ 2 years | ≤ OUP + 3 years |
| 8. Symmetric RBG Keys | See [SP800-90] | — |
| 9. Symmetric Master Key | About 1 year | — |
| 10. Private Key Transport Key | ≤ 2 years | |
| 11. Public Key Transport Key | 1 to 2 years | |
| 12. Symmetric Key Agreement Key | 1 to 2 years | |
| 13. Private Static Key Agreement Key | 1 to 2 years | |
| 14. Public Static Key Agreement Key | 1 to 2 years | |
| 15. Private Ephemeral Key Agreement Key | One key-agreement transaction | |
| 16. Public Ephemeral Key Agreement Key | One key-agreement transaction | |
| 17. Symmetric Authentication Key | ≤ 2 years | |
| 18. Private Authentication Key | ≤ 2 years | |
| 19. Public Authentication Key | ≤ 2 years | |

# Entities Vulnerable to Quantum Computing



# Impact of Quantum Computing on Common Cryptographic Algorithms

| Cryptographic Algorithm | Type | Purpose | Impact from Large-Scale Quantum Computer |
|---|---|---|---|
| AES | Symmetric key | Encryption | Larger key sizes needed |
| SHA-2, SHA-3 | Cryptographic hash | Hash function | Larger output needed |
| RSA | Asymmetric key | Signature, key establishment | No longer secure |
| ECDSA, ECDH (elliptic curve cryptography) | Asymmetric key | Signature, key exchange | No longer secure |
| DSA (finite field cryptography) | Asymmetric key | Signature, key exchange | No longer secure |

# Vulnerable Categories

- The types of asymmetric algorithms that are vulnerable to quantum computing are in the following categories:
  - Digital signatures
  - Encryption
  - Key-Establishment Mechanisms (KEMs)

# Alternatives

- There is no single widely accepted alternative to the existing algorithms based on integer factorization or discrete logarithms
- Of the approaches reported in the literature, four general types of algorithms predominate:
  - *Lattice-based cryptography:*
    - These schemes involve the construction of primitives that involve lattices
  - *Code-based cryptography:*
    - These schemes are based on error-correcting codes
  - *Multivariate polynomial cryptography:*
    - These schemes are based on the difficulty of solving systems of multivariate polynomials over finite fields
  - *Hash-based signatures:*
    - These are digital signatures constructed using hash functions

# Submissions to NIST Post-Quantum Cryptography Competition

| | Signatures | KEM/Encryption | Total |
|---|---|---|---|
| **Lattice-based** | 4 | 24 | 28 |
| **Code-based** | 5 | 19 | 24 |
| **Multivariate** | 7 | 6 | 13 |
| **Hash-based** | 4 | _ | 4 |
| **Other** | 3 | 10 | 13 |
| **Total** | 23 | 59 | 82 |

# Summary

- Explain the need for post-quantum cryptographic algorithms and which types of algorithms are affected