Post-Quantum Cryptography

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- C. Kaufman, R. Perlman, M. Speciner, R. Perlner, "*Network Security: Private Communication in a Public World*", Pearson Education, 3rd edition, 2023
- W. Stallings, "*Cryptography and Network Security*", 8th edition, Pearson Education, 2023

Quantum Computer

- Computer that exploits quantum mechanical phenomena
- A scalable quantum computer expected to be able to perform some calculations exponentially faster than classical computers, e.g.:
  - factoring large products of prime numbers,
  - unstructured search
- Common misconception:
  - quantum computer is faster than a classical computer,
  - since Moore's law is slowing down, eventually all classical computers will be replaced by quantum computers
- Above is not true:
  - there is only a narrow set of problems for which a quantum computer would be faster
- Property of a quantum computer that makes it excel at some tasks is that:
  - it can compute, with only storage size n, as if it were operating on 2^n values in parallel
- However, it also has serious limitations, e.g.:
  - if you read/ measure the state, you will see only one value and the others disappear
- A typical quantum program tries to ensure that:
  - the quantum computation it performs raises the probability that when you finally measure a result, it will be a useful value

Quantum Computer (contd.)

- Another common misconception:
  - quantum computer can solve NP-hard problems (e.g., traveling salesperson problem, set cover problem) in polynomial time
- Above is almost certainly not true:
  - although nobody has proved that it is impossible, no known quantum algorithm for solving such problems is that powerful
- Although, in principle, a quantum computer can do any calculation that a classical computer can do:
  - for most calculations, quantum computers would be no faster than conventional computers
- Also, in practice, quantum computers are likely to be much more expensive to build and operate
  - e.g., most designs would need to operate at temperatures very close to absolute zero
- So it is not likely that quantum computers will ever serve more than a small niche market
- Instead of bits, a quantum computer uses *qubits*, where a qubit’s state can be a mixture of a 0 and a 1
  - known as superposition

Quantum Algorithms Relevant to Cryptography

- Grover's algorithm:
  - Makes brute-force search faster
  - E.g., in encryption or hashes, a brute-force search can find a key or pre-image
  - Can do brute-force search in the square root of the time it would take on a classical computer, e.g.:
    - assume that we want to know which n-bit secret key k encrypts plaintext m to ciphertext c
    - on a classical computer, we could try all possible $(N = 2^n)$ keys, and in the average case (respectively, worst case), it would take $\frac{N}{2}$ (respectively, N) guesses to find the right key
    - on a quantum computer running Grover's algorithm, the number of iterations to get n qubits into a state where it is very probable that the state will be read as the key k is proportional to $\sqrt{N} = 2^{n/2}$
  - Squaring the size of the space being searched (e.g., using an encryption key twice as long) is adequate to protect against Grover's algorithm

Quantum Algorithms Relevant to Cryptography (contd.)

- Shor's algorithm:
  - ❑ Can efficiently factor numbers and calculate discrete logs
  - ❑ If run on a sufficiently large quantum computer, would break all our widely used public key algorithms (e.g., RSA, Diffie-Hellman)
  - ❑ Currently, no quantum computer large enough to break the currently deployed public keys has ever been publicly demonstrated
  - ❑ There are a number of difficult engineering challenges that remain, and it may never be economically viable to overcome them
  - ❑ But because such a computer might be possible, it is important to convert to quantum-safe public key algorithms well before a quantum computer of sufficient size might exist
  - ❑ The cryptographic community is actively developing and standardizing such algorithms

Post-Quantum Cryptography

- Replacement algorithms for existing public key algorithms are being developed, which not even a combination of classical and quantum computers will be able to break in reasonable time
- These algorithms known as:
  - ❑ Quantum-resistant,
  - ❑ Quantum-safe, or
  - ❑ Post-quantum cryptography
- It is important to start migrating away from the current public key algorithms well before a sufficiently large quantum computer might exist
- National Institute of Standards and Technology (NIST):
  - ❑ has played an important role in standardization of cryptography (e.g., AES and SHA),
  - ❑ and is playing an important role in the standardization of post-quantum algorithms
- In late 2017 (the deadline for submissions), NIST received about 80 proposed schemes
- Several rounds were conducted, where in each round, some algorithms are discarded and others are studied closely
- On August 13, 2024, the U.S. National Institute of Standards and Technology (NIST) released final versions of its first three Post Quantum Cryptographic Standards
- Four of the best-known families of schemes are:
  - ❑ Hash-based cryptography,
  - ❑ Lattice-based cryptography,
  - ❑ Code-based cryptography, and
  - ❑ Multivariate cryptography

Post-Quantum Cryptography (contd.)

- **Hash-based signatures**:
  - ❑These are digital signatures constructed using cryptographic hash functions
- **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 cryptography**:
  - ❑These schemes are based on the difficulty of solving systems of multivariate polynomials over finite fields

Post-Quantum Cryptography (contd.)

- Recall: quantum computing poses a threat to current public key algorithms
- In contrast, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure against attacks by quantum computers
- While Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively block these attacks
- Thus, post-quantum symmetric key cryptography does not need to differ significantly from current symmetric key cryptography