POST-QUANTUM CRYPTOGRAPHY EXPLAINED

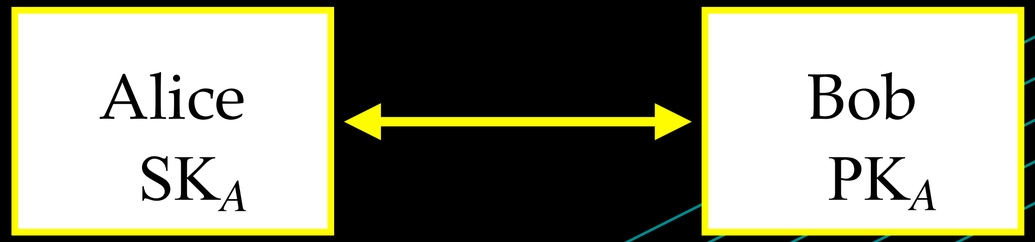
for security professionals

THE QUANTUM THREAT: PRIMITIVES

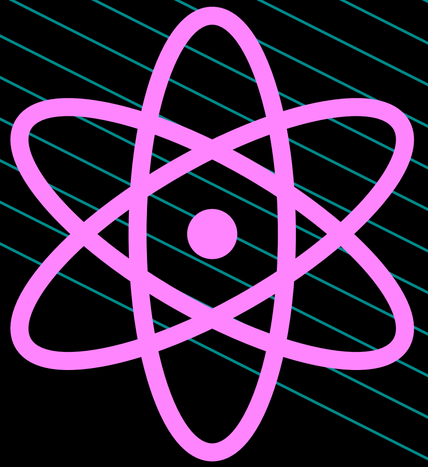
ALFRED MENEZES

SYMMETRIC-KEY vs. PUBLIC-KEY

- Symmetric-key cryptography
  - Encryption: AES
  - Message authentication: HMAC
  - Authenticated encryption: AES-GCM
  - Hash functions: SHA256
- Public-key cryptography
  - Public-key encryption: ECC, RSA
  - Key agreement: ECDH
  - Digital signatures: ECDSA, RSA



QUANTUM ALGORITHMS



- Quantum algorithms most relevant to cryptography:
  - Shor's algorithm: breaks some families of public-key schemes
  - Grover's algorithm: limited effect on some symmetric-key primitives.

SHOR'S ALGORITHM

- The public-key systems in use today rely on hard mathematical problems.
  - RSA: integer factorization
  - Discrete-log (DL): discrete logarithm problem
  - Elliptic curve cryptography (ECC): elliptic curve discrete logarithm problem.
- In 1994, Peter Shor discovered a quantum algorithm that can solve all of these problems efficiently. As a result, quantum computers are able to completely break RSA, discrete log, and elliptic curve cryptography.

GROVER'S ALGORITHM (1)

- Grover's algorithm, discovered in 1996, speeds up brute-force attacks against some symmetric-key schemes.
- It can find an n-bit secret key in $\sqrt{2^n}$ steps, instead of the 2^n steps required by classical brute force.
  - Brute force key search on AES-128, AES-192, AES-256 using classical computers: 2^{128}, 2^{192}, 2^{256} steps.
  - Brute force key search on AES-128, AES-192, AES-256 using Grover's algorithm: 2^{64}, 2^{96}, 2^{128} steps
  - Security level of AES-128, AES-192, AES-256, drops from 128, 192, 256 bits, to 64, 96, 128 bits.

GROVER'S ALGORITHM (2)

- 2^{128} operations is considered infeasible, even for quantum computers.
- So, Grover's attack can be effectively countered by using AES-256 instead of AES-128.
  - Modest increase in key size, and about 40% increase in encryption/decryption time.
- Grover's algorithm does *not* threaten the security of hash functions.
  - A common claim is that a certain quantum attack can find collisions faster than the fastest known classical attacks. However, this is misleading — the quantum attack is more expensive, so is less cost effective.

CLOSING

- Quantum computers completely break all RSA, discrete-log, and elliptic curve cryptosytems.
- Quantum computers have a limited effect on symmetric-key encryption schemes, and this effect can be easily mitigated by doubling key sizes.
- Quantum computers do *not* threaten the security of hash functions.