POST-QUANTUM CRYPTOGRAPHY EXPLAINED

for security professionals

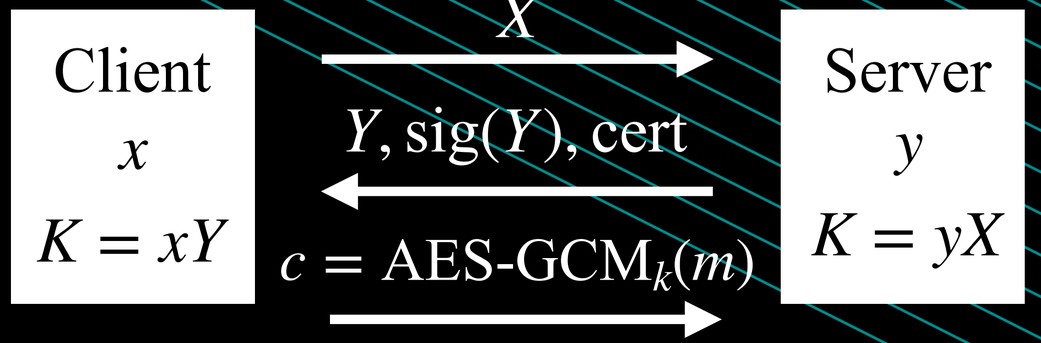
THE QUANTUM THREAT: PROTOCOLS

ALFRED MENEZES

SECURE CHANNELS

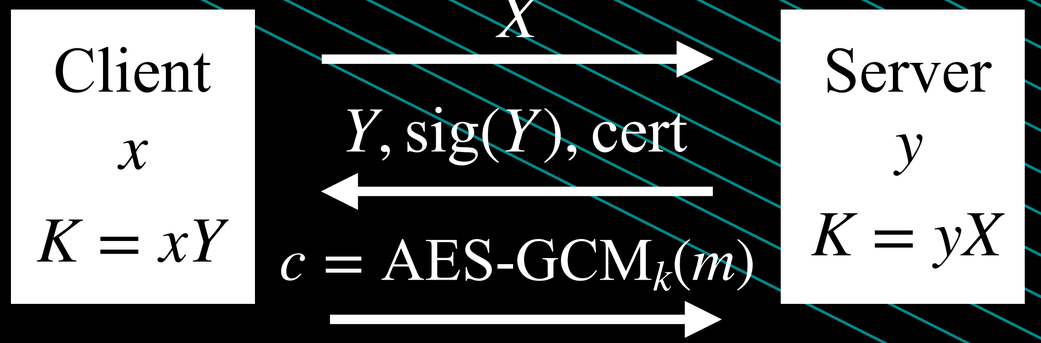
- Large-scale cryptographic deployments typically rely on a combination of symmetric-key and public-key primitives to establish a secure channel.
- An example is TLS, the cryptographic protocol that secures communication between a client (a web browser) and a server (a website).
- TLS uses RSA signatures for authentication, elliptic-curve Diffie-Hellman (ECDH) for key agreement, and AES-GCM for authenticated encryption.

TLS 1.3 DESCRIPTION



1. The client selects secret x and sends $X = xP$.
2. The server selects secret y, and computes $Y = yP$.
   It sends Y, its RSA signature on Y, and its digital certificate.
   - The certificate contains the server's identifier and RSA public verification key. This data is signed by a Certification Authority (CA) using the CA's own RSA private key.
3. The client verifies the CA's signature on the certificate. It then uses the server's RSA public key to verify the server's signature on Y.
4. Both client and server compute the ECDH shared secret $K = xY = yX$.
5. From K, they derive a session key k, which is used with AES-GCM to encrypt and authenticated all data exchanged for the rest of the session.

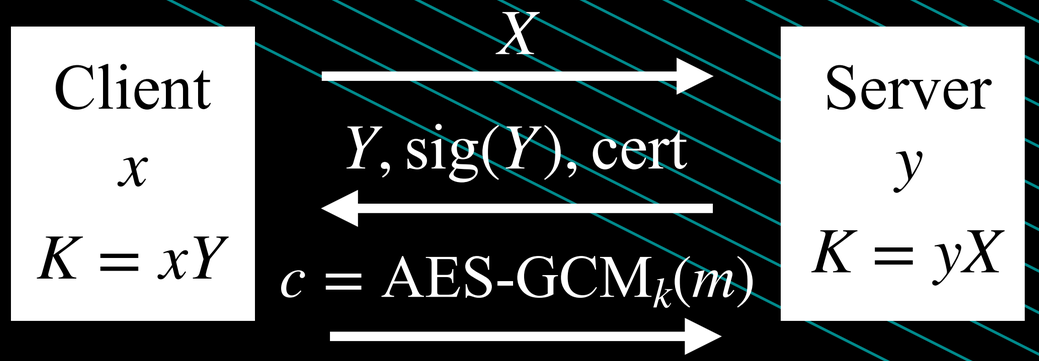
TLS VULNERABILITIES



Quantum computers threaten several TLS components including AES-GCM, RSA signatures, and ECDH.

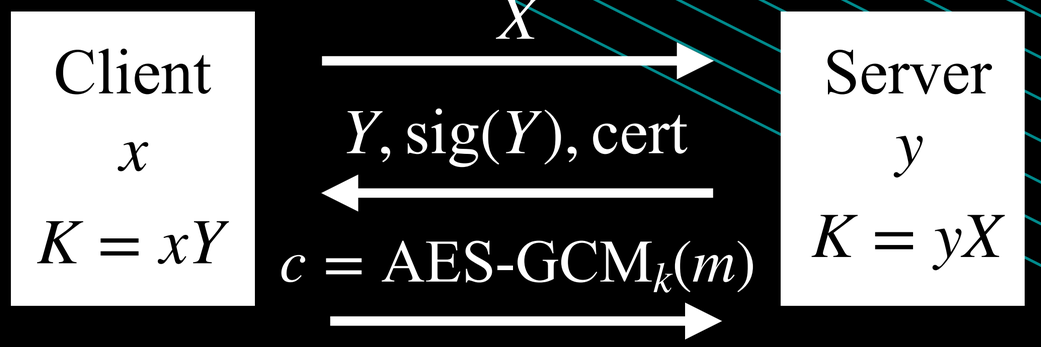
1. AES-GCM is easy to protect against quantum attacks:
    - Increase key sizes from 128 bits to 256 bits.
2. Shor's algorithm completely breaks RSA.
    - An attacker can recover a CA's RSA private key and use it to create fraudulent certificates. They could also recover a server's RSA private key and use it to impersonate that server.
3. Shor's algorithm completely break ECDH.
    - By efficiently recovering the secret value x from the public point X, an attacker can compute the session key k. This allows them to decrypt all recorded TLS traffic.

COUNTERMEASURES



- Replace RSA and ECDH with quantum-safe alternatives:
  - Replace RSA with Dilithium.
  - Replace ECDH with Kyber.
- Question: When do we need to make these replacements?

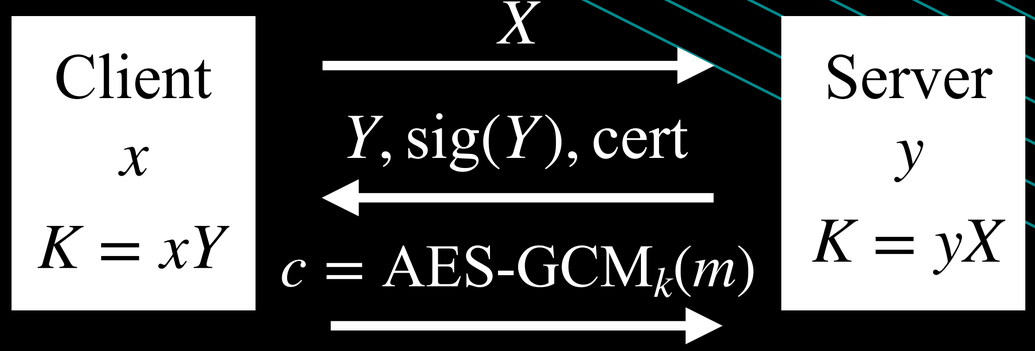
MIGRATION TIMELINE: SIGNATURES



- Quantum-safe digital signatures do *not* need to be deployed immediately.
  - Signatures are typically verified only at the time they are created, or shortly afterwards.
- Nevertheless, replacing a signature scheme in large-scale systems takes time.
  - This deployment timeline should be considered when deciding when to begin the transition.

MIGRATION TIMELINE: KEY AGREEMENT

- There is a stronger case for replacing ECDH with a quantum-safe alternative *today*.
  - To protect against Harvest-Now Decrypt-Later (HNDL) attacks.
  - Some data must remain confidential for many years, including government secrets and medical records.
- Governments or regulators may mandate the use of quantum-safe cryptography.
- Market forces also matter.



CLOSING

- Quantum computing poses challenges to today's cryptographic infrastructure.
- By understanding where the risks lie, and by carefully planning migrations to quantum-safe cryptography, you can ensure that communication remains secure well into the future.
- Next: Quantum-safe cryptography.