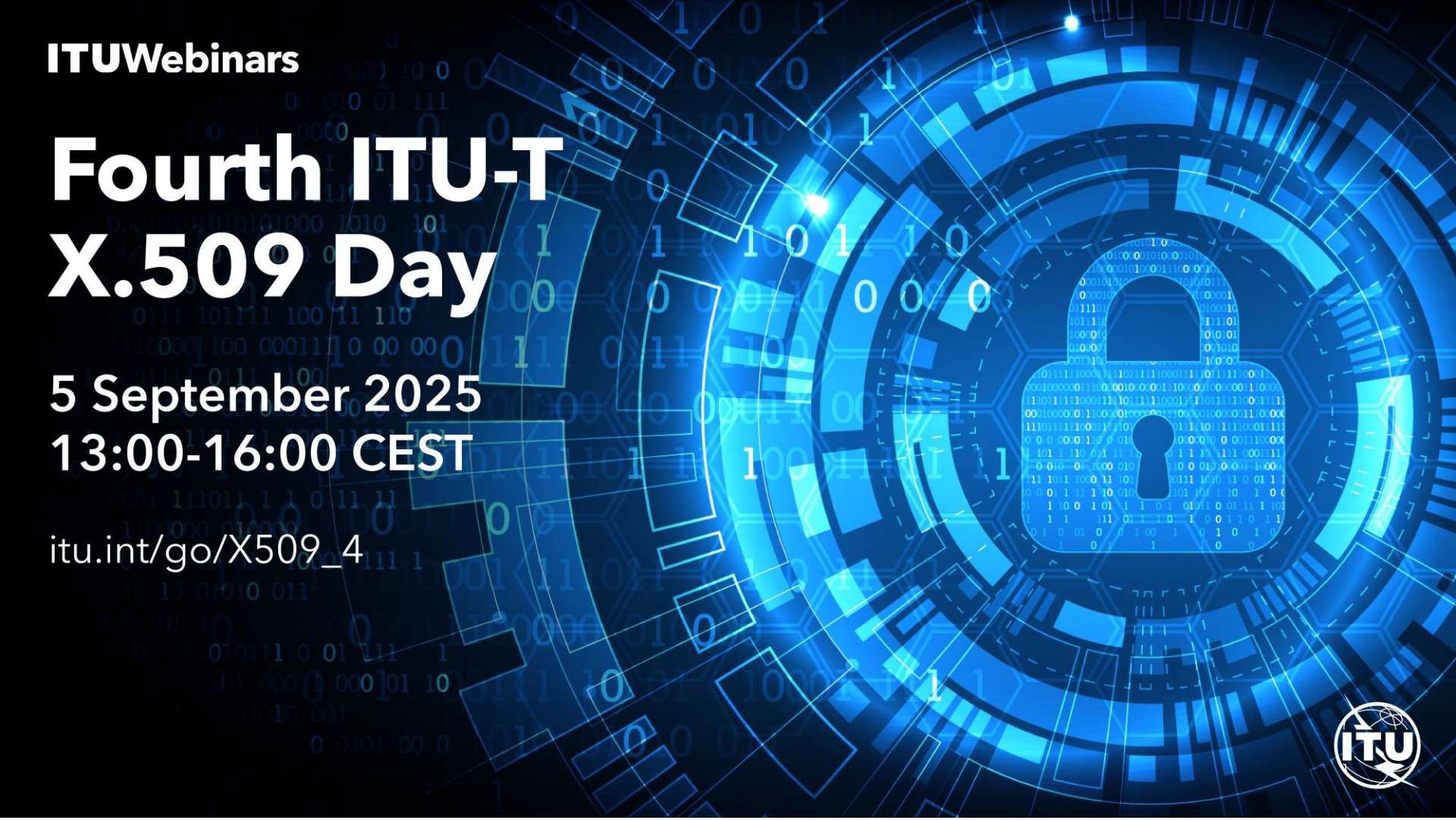


Protecting Legal Documents with Digital Signatures in the Quantum Computing Age

Hoyt Kesterson

Michael Lightowler

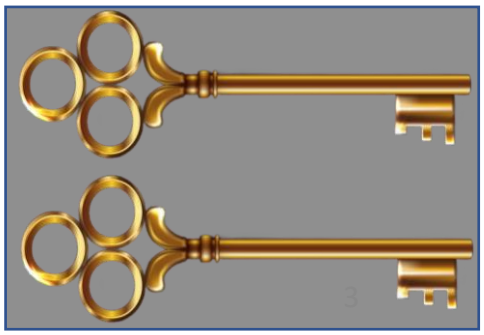
Stephen Mason

One day quantum computers will break digital signatures

We will lose the ability to state that we can assert that a presented document was signed by a specific entity and has not been altered since it was signed.

Asymmetric encryption

- A pair of keys
- The key used to encrypt cannot decrypt.
- Knowing a key does not give a hint of the other.
- Jane's key is kept *private*.
- Bob's et al keys are declared *public* and are given to one or more entities.
- Anything Bob locks in box can only be seen by Jane.
- Everyone knows when Jane locked box.



How digital signature works

- Asymmetric encryption is based on mathematical problems that are difficult to solve without some additional information.
- These are called trap door functions; there are several including RSA.
- RSA is based on the difficulty of factoring a number, X, i.e. determining which integers divide into X with no remainder. E.g. 15 can be evenly divided by 15, 5, 3, and 1.
- Can you factor 153? 1, 3, 9, 17, 51, and 153
- A prime number can only be divided by itself and 1.
- RSA's strength is based on the difficulty of factoring the product of two large prime numbers.

701,111 = 907 x 773

Can a classical computer factor such a product?

- In 1991the RSA Factoring Challenge provided a list of numbers that were the product of two prime numbers.
  - 155 decimal digits (512 bits) factored in 1991.
  - 250 decimal digits (829 bits) factored in 2020.
  - Challenge ended in 2007.
- NIST SP 800-131A, *Transitioning the Use of Cryptographic Algorithms and Key Lengths* recommends algorithms and key sizes.
- The standard is revised as processors become more powerful.
- It recommends an RSA minimum key size of 2048 bits as adequate until 2030; then 128-bit strength with < 3072.
- A predictable race between key size and processing power but quantum computing is a game changer.

Quantum computing effect on asymmetric encryption

- In 1994 Peter Shor published an algorithm that would quickly determine the prime numbers that went into the large product used to create a public and private key.
- It will also defeat other trap door functions that support other asymmetric encryption algorithms. In 2001 IBM implemented Shor's Algorithm to factor 15 using seven qubits.
- Don't just monitor the growth in qubits; quantum computers are noisy and require error correction; qubits are not yet persistent enough to support significant computation.
- A recent draft of SP 800-131A describes the quantum resistant algorithms but does not yet propose a transition schedule.

We have to have a plan

- Deploy the quantum-resistant algorithms recently standardized by NIST as quickly as we can.
- It's a risk decision as to when one starts using the new stuff.
- Effective quantum computing may take awhile but attorneys and notaries who digitally sign long-lived documents should consider signing those with the new algorithms as soon as they have been deployed.
- When it does arrive, it will be necessary to protect the integrity of documents already signed.
- Do we need to protect the original signing ceremony?

Let's ask some legal folk