Why Attorneys Should Care About Post-Quantum Cryptography

Second X.509 Day – Session 2

Hoyt L Kesterson II

Why attorneys care about encryption

- Attorneys in the US and many other countries have an ethical obligation to protect their communications with their clients.
  - Like most businesses they want their communications across the internet to be confidential and protected against unnoticed modification.
  - Like most businesses they want to similarly protect stored information.
- They need to “sign” electronic documents such as contracts.
  - Laws and regulations were amended to recognize such signatures.
  - Electronic notary—authorized notary’s digital signature binds that notary’s attestation that the notary verified the bona fides of the signer of an electronic document at a date and time to that signed document.

Effective quantum computing breaks digital signature

- Fortunately, NIST has given us CRYSTALS-Dilithium, FALCON, and SPHINCS+
- I suggest that although error-resistant quantum computing is not yet nigh, products should be cryptographically agile now.
  - Why? DES was standardized in 1977; its three-key variant prohibited at the end of this year; and yet still in use although AES arrived in 2001.
  - IOT devices using ECC rather than RSA because of smaller keys but key sizes of quantum-resistant algorithms are quite large.

The sky is not falling—at least, not yet. When it does…

- Either sign and time stamp aggregates of signed documents; or…
- Already be signing long-life documents with a classical digital signature and one (or two) quantum-resistant algorithms.
  - Implementations not supporting quantum resistance can still validate.
- Keeping attorneys informed but not nervous.
  - The American Bar Association Section of Science and Technology Law may take the lead on this.
  - I had an article, *What's Quantum Computing Got To Do With It?,* published in the Spring 2022 issue of The SciTech Lawyer.