Will Post Quantum Crypto make Constrained IoT Devices and Networks obsolete?

Hannes Tschofenig

<Hannes.Tschofenig@gmx.net>

Lots of Progress over the last 10+ years

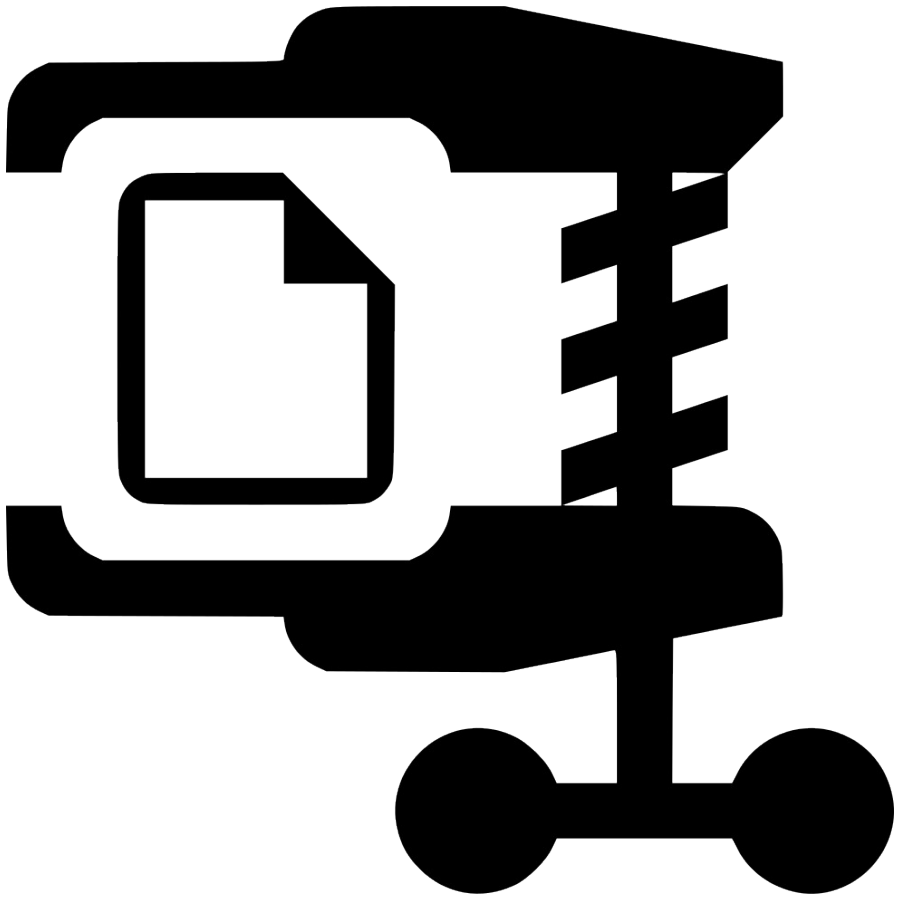
- Constrained IoT devices have traditionally not be blessed with great security capabilities.
- Work in the IETF and other bodies to tailor security and protocols to those devices.
- Today, they can run public key crypto well.

Picture References

Optimizations

- A lot of energy was spent with “compressing” protocols to reduce every byte of protocol exchanges for low-power networks like LoRaWAN.

Examples	Bytes
DTLS 1.3 - RPKs, ECDHE	880
cTLS-08 - X.509s by reference, ECDHE	405
EDHOC - Signature X.509s, x5t, ECDHE	242



Reference: https://datatracker.ietf.org/doc/draft-ietf-iotops-security-protocol-comparison/

Picture reference

… then PQC algorithms came along!

- Performance and key sizes not great.
- Uncertainty about
  - the timeframe for Cryptographically Relevant Quantum Computer
  - the security of the new algorithms
  - the transition
  - operational aspects
  - ….

What does this mean for constrained IoT devices and networks?

- Preconditions are not great: Long lifetime and limited resources
- Options:
  - Switch to general purpose hardware
  - Use symmetric key cryptography (with longer key sizes) / Kerberos
  - Invent new cryptographic algorithms
  - ???

I am interested in your view.

Reach out to me at Hannes.Tschofenig@gmx.net