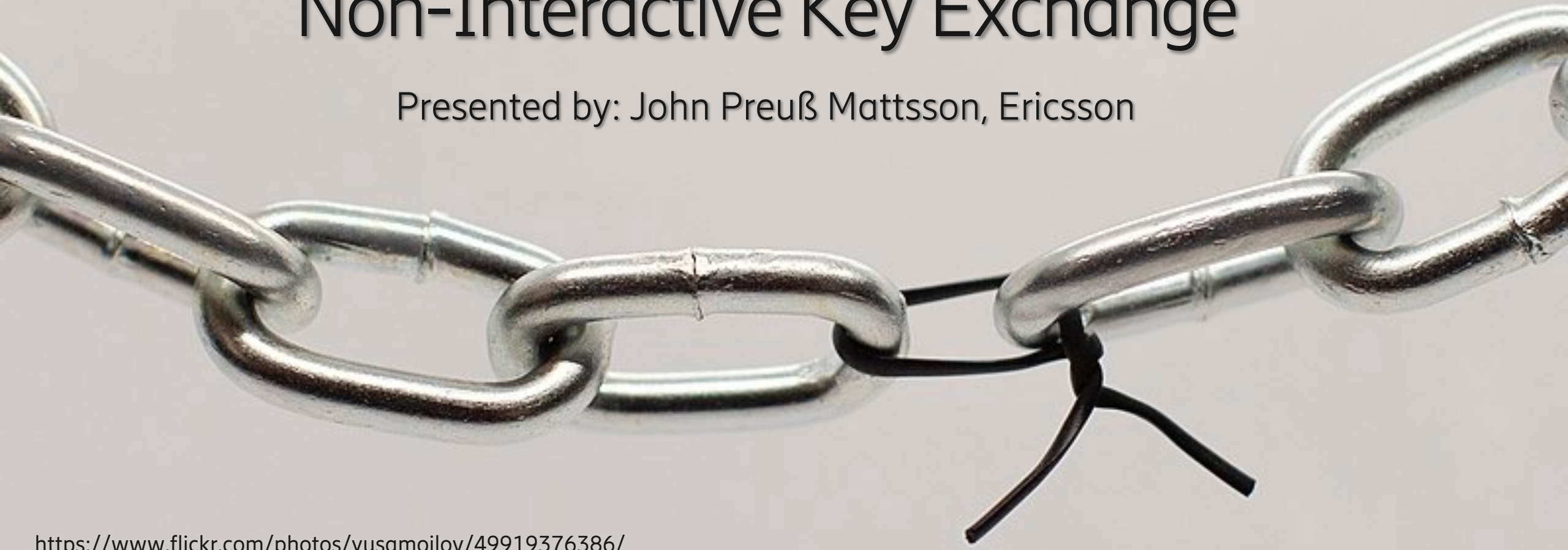
Constrained Radio Networks, Small Ciphertexts, Signatures, and Non-Interactive Key Exchange

Presented by: John Preuß Mattsson, Ericsson



https://www.flickr.com/photos/yusamoilov/49919376386/

Constrained Radio Networks

- Sustainable digitalization in many areas of society (agriculture, environment/climate, etc.) depend on the deployment of low-power technologies that makes use of constrained radio networks
- There are several types of constrained radio networks, and the market is growing rapidly.
  - Constrained radio networks can have a reach of a few centimeters, a few meters, or several kilometers.
  - Market size estimate for Bluetooth: 27 billion USD by 2028; for LPWAN: 1000 billion USD by 2027.
- Bandwidth in radio networks can be very limited. Transmitting, receiving, and listening use relatively much energy. Radio is often a more limiting factor than CPU power due to bandwidth, latency, and energy.
  - **LoRaWAN** is often used with **51 bytes frames** in Europe and **11 bytes frames** in the US. LoRaWAN is often used with duty cycles less than 1%. A 1% duty cycle means that a device has a 36 second period where it can transmit information and then the device **must pause transmission for an hour.**
  - **6TiSCH** is a multi-hop mesh network. The frames are at most 127 bytes but drops for each hop. The actual payload size in a typical 5-hop network can be about **45 bytes**.
  - **NB-IoT** is operating in licensed spectrum that is not characterized by fixed sized frames. The effects of larger messages are not as extreme as in LoRaWAN and 6TiSCH but byte count has a significant impact on time and energy consumption.

Increased Use of Non-KEM Diffie-Hellman Features

- Noise IK pattern used in WireGuard; Noise XX pattern used in EDHOC method 3
- Encapsulations are ephemeral public keys and can be reused in different ECDH functions.
- Ephemeral-Static ECDH gives implicit authentication by the ability to compute the shared secret.
- Static-static ECDH is used.

```
XX:
  -> e
  <- e, ee, s, es
  -> s, se
```

```
IK:
 <- s
 ...
 -> e, es, s, ss
 <- e, ee, se
```

Increased Use of Non-KEM Diffie-Hellman Features

- Signal DH Ratchet uses that encapsulations are public keys.
- Group OSCORE pairwise mode uses Static-Static ECDH (NIKE) for very constrained networks.

```
Signal DH Ratchet:
   -> e
   <- e, ee
   -> e, ee
   <- e, ee
   ...
```

```
NIKE:
   -> s
   <- s
   ...
   -> ss
```

Standardization for for Constrained Radio Networks

- To reduce overhead and processing in constrained radio networks, the IETF has created several technologies and even dedicated working groups targeting constrained networks, e.g.: 6lo, 6LoWPAN, 6TiSCH, ACE, CBOR, CoRE (CoAP, OSCORE), COSE, LAKE (EDHOC) ROLL (RPL), LPWAN (SCHC), TLS (cTLS).
  - (Technologies in parenthesis when the name is different from the working group.)

- Examples:
  - **EDHOC**: Designed by the IETF Lightweight Authenticated Key Exchange (LAKE) working group. Its main design goal it to standardize an AKE with as small messages as possible. The message sizes in EDHOC method 3 (similar to Noise XX) are in a typical use case 37, 45, and 19 bytes long for a total of 101 bytes.

  - **Group OSCORE**: Addition to CoAP enabling group requests with a signature or pairwise communication between any nodes in the group with Static-Static ECDH (i.e., NIKE). A group request in OSCORE consists of a few bytes of header in addition to the payload and a 64 byte signature. A pairwise unicast message consists of a few bytes of header, the payload, and an 8 bytes AEAD tag.

Implications of NIST PQC Candidates Level 1-2

- Using the NIST KEMs or signatures leads to much larger messages and/or more flights.
  - Might be acceptable for non-constrained use cases where WireGuard is typically used.
  - Completely unacceptable performance degradation in many constrained use cases.

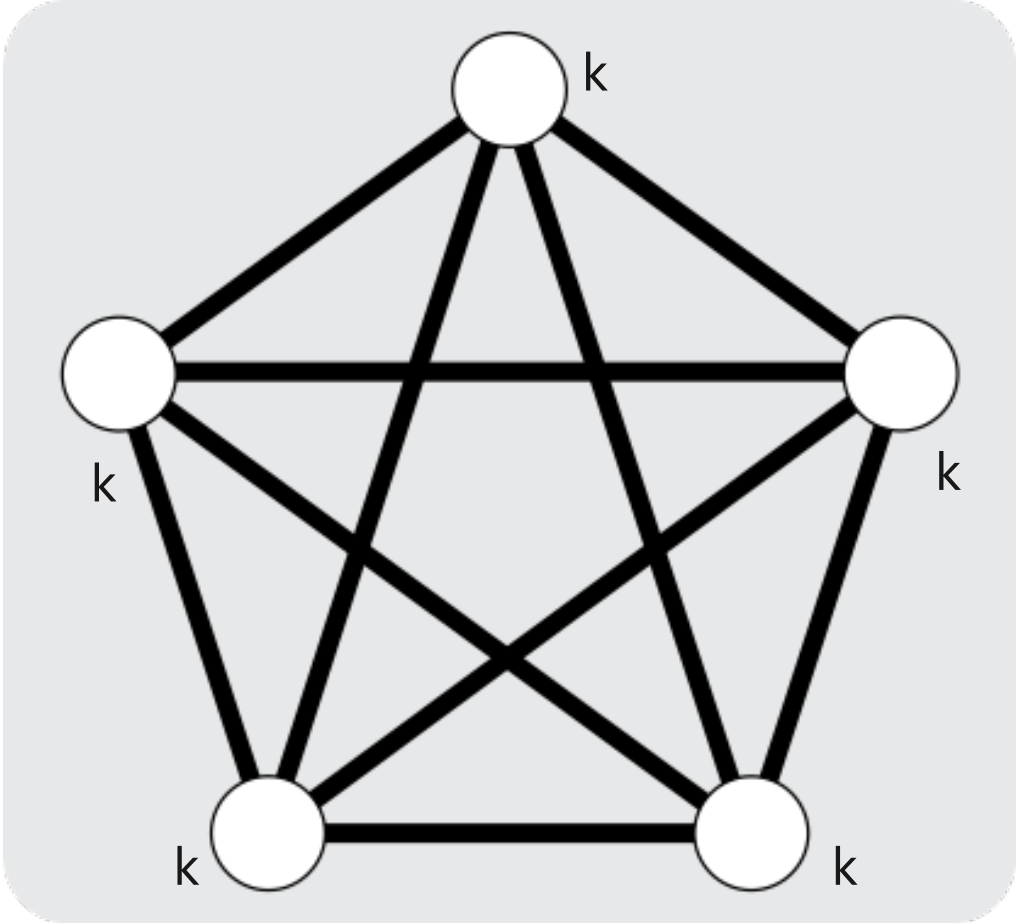
- Using Kyber and Falcon in EDHOC, the number of bytes increases from 101 to 2896 bytes or **28 times**
  - Using only Kyber would increase the number of bytes more than using Kyber and Falcon, and also require more flights, which would further increase latency.
  - As stated by NIST, Falcon may be infeasible to implement on constrained devices
- Using Falcon in Group OSCORE increases the overhead **9 times**
- Using Dilithium increases the overhead **9 times** and using Kyber instead of NIKE increases the overhead with **90 times**

Candidate	Public key	Ciphertext	Signature
Kyber512	800	768	
Dilithium	1312		2420
Falcon-512	897		666
SPHINCS+-128s	32		7856

Public key, ciphertext, and signature sizes in bytes

Implications of NIST PQC Candidates Level 1-2

- Unless ECC is allowed, constrained IoT will likely use (group) PSK authentication and (group) PSK key exchange.
  - PSK authentication has major weaknesses, e.g.
    - it typically uses permanent key identifiers enables attackers to identify and track endpoints.
    - PSK supply chain vulnerability
  - PSK key exchange does not offer forward secrecy
    - a PSK disclosure leads to that all derived keys and protected messages are compromised.
  - Symmetric group keys are even worse
    - misbehaving group members can passively read messages between other members of the group or impersonate and actively inject messages between other members of the group.
- These kind of systems offer very weak security and privacy and should instead be phased out.



Conclusions

— **The current NIST PQC candidates are not usable in many constrained radio networks** due to bandwidth, time to completion, power consumption, and battery lifetime. NIST and academia must work together to-standardize algorithms with smaller ciphertexts, smaller signatures, and with additional Diffie-Hellman features such as NIKE. CSIDH seems like an extremely promising algorithm for constrained radio networks.

— **NIST should publicly acknowledge that post-quantum algorithms for constrained radio networks is a major unsolved problem** and that NIST might have a fifth round in the PQC project or a separate Lightweight Post-Quantum Cryptography Project. This would encourage academia and funding institutions to prioritize this important area.

— **NIST should publicly acknowledge that use of elliptic curve cryptography will be allowed** until the risk of Cryptographically Relevant Quantum Computers (CRQCs) is imminent. It is still uncertain if a CRQC will ever be built. Unless NIST allows use of ECC, constrained radio networks will likely use (group) PSK authentication and (group) PSK key exchange with its bad privacy and failure to adhere to NIST zero trust principles.