David Gotrik
AgilePQ
dgotrik@agilepq.com

## Constrained IoT Devices

Internet of Things device manufacturers often target microcontrollers which optimize for form factor, power consumption, and most importantly cost. This can lead to extreme constraints on processing speed and memory availability. The terminology for these constrained nodes is defined in IETF RFC 7228 *Terminology for Constrained-Node Networks [1]*. This review looks at the proposed PAKEs in the context of constrained node IoT devices.

The following table, defined in [1], names Class 0, Class 1, and Class 2 devices in terms of their memory availability.

| CONSTRAINED IoT DEVICE CHARACTERISTICS | | |
|---|---|---|
| **NAME** | **DATA SIZE (e.g., RAM)** | **CODE SIZE (e.g., FLASH)** |
| **Class 0** | < 10 KB | < 100 KB |
| **Class 1** | ~ 10 KB | ~ 100 KB |
| **Class 2** | ~ 50 KB | ~ 250 KB |

These constrained devices may also operate in “challenged networks”, which do not support IP connectivity directly. Examples of challenged networks are the Industrial, Scientific, Medical (ISM) radio band networks as well as Licensed radio bands: Bluetooth, Bluetooth Low Energy, Sigfox, Zigbee, LoRaWAN, NB-IoT, satellite uplink, and other proprietary RF technologies.

These challenged networks range in their capabilities, but in extreme cases they are purely one-way simplex links able to send fewer than 200 bytes per transmission. In other cases, they are duplex links with constraints on the allowable communication traffic. For example, in Sigfox, the device is limited to 144 uplink messages of only 12 bytes, and 4 downlink messages at 8 bytes. Bluetooth Low Energy can have packet sizes up to 251 bytes [2].

Furthermore, these challenged networks do not typically guarantee packet arrival, packet uniqueness, or any sort of imposed packet ordering. This “blind communication” can have great impacts on the efficiencies of various security protocols, and it can cause some protocols to be not viable, such as TLS 1.2, TLS 1.3. Even DTLS requires two-way communication between client and server during the handshake, so in certain challenged networks it cannot be used efficiently or at all [3].

## On PAKEs for constrained IoT

A number of the PAKE proposals target performance metrics on ARM Cortex M4 as well as the more limited ARM Cortex M0.

AuCPace defines the following table with metrics on memory footprints. In Class 0 and Class 1 devices, the total RAM is typically in the range of 8 – 32KB, with available ROM typically at 64-128KB. With these constraints, AuCPace/CPace seem to be good contenders for constrained node authentication.

| Target<br>Target | RAM<br>ACE | ROM<br>ACE | RAM<br>X25519 | ROM<br>X25519 | |
|---|---|---|---|---|---|
| Cortex-M0 | 264 (396) | 11252 | 0 (572) | 6108 | this work |
| Cortex-M4 | 264 (268) | 8896 | 0 (444) | 3324 | this work |
| Cortex-M4 | | | | 4152 | [FA17] |
| Cortex-M4 | | | | 3786 | [DSS16] |

## On Round Efficiencies

In terms of round efficiency, or the number of message flows, the following table describes the PAKE candidates. Due to the limitations outlined above in challenged networks, many of the PAKE options would have difficulty due to the two-way communication bandwidth needed. However, for many widely used protocols like Bluetooth and standard TCP/IP over WiFi, these proposals would work fine.

| Proposal Name | Number of Rounds |
|---|---|
| AuCPace | 4 |
| BSPAKE | 2-3 (start) , 3-4 (for verification) |
| CPace | 4 |
| J-PAKE | 2-3 |
| OPAQUE | 2-3 |
| SPAKE2 | 1 |
| SPEKE | 3-4 |
| VTBEKE | 3 |

A password-based authenticated key exchange capable for challenged networks would be interesting and appealing for certain use cases, but the round efficiency of the proposals is adequate for Class 2 and above devices. To note is that a number of Class 0 and Class 1 devices use Pre-Shared Keys (PSK) installed by the manufacturer in addition to PSK methods and protocols, but a PAKE alternative would be appealing for using devices in the absence of a trusted-third party key server.

## On Quantum-Resistance

As of late, an effort across the cryptographic community has focused on the “next generation” of encryption to counter the threat of quantum computers. It is widely believed that computers capable of efficiently implementing Shor’s, Grover’s, Simon’s, and other algorithms will be available in the next 15 years, with a possibility that these machines will come later or sooner depending on technological hurdles or advancements.

In the proposals thus far, each of them rely on some hardness problem relating to the Discrete Logarithm Problem (DLP), Computational Diffie-Hellman (CDH), Simultaneous Diffie-Hellman (SDH), Decisional Linear (DLin), or some implementation of elliptic curves. The discrete logarithm problem has been shown to be threatened by Shor’s algorithm [5].

My recommendation would be for the proposers and IETF to investigate post-quantum PAKE options that can be implemented in the near future, as a number of IoT devices are expected to be deployed

and last between 10 and 15 years, plus design and manufacture time. A “PAKE for the Post-Quantum World” has been proposed in [4].

## References


[1] *Terminology for Constrained-Node Networks*, IETF RFC 7228 https://tools.ietf.org/html/rfc7228
[2] *BLE v4.2*, https://www.electronicdesign.com/communications/ble-v42-creating-faster-more-secure-power-efficient-designs-part-1
[3] *Datagram Transport Layer Security Version 1.2*, https://tools.ietf.org/html/rfc6347#page-14
[4] Ding et al., “Provably Secure Password Authenticated Key Exchange Based on RLWE for the Post-QuantumWorld.”
[5] Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.”