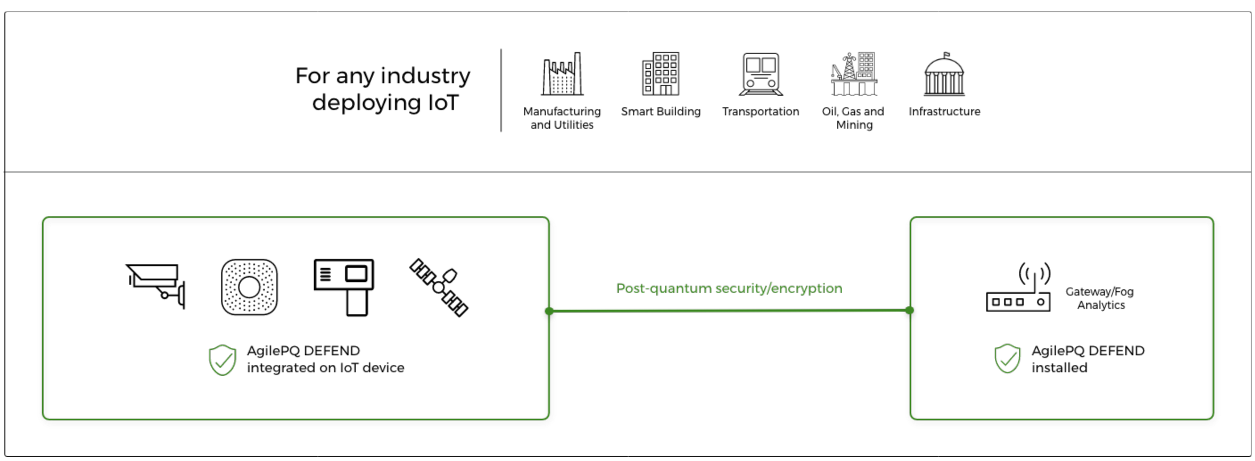
AgilePQ DEFEND IoT Device Security

AgilePQ DEFEND IoT Device Security is a C-code based library and API solution designed specifically for small footprint IoT devices, providing post-quantum resistant data protection with minimal overhead, minimal latency and minimal power-draw.



What is AgilePQ DEFEND IoT Device Security?

AgilePQ defines IoT Device Security as the ability to:

- Quickly and easily Provision, Deploy, Identify, Authenticate, and Authorize all IoT devices - no matter how small.
- Encrypt initial and on-going communications with post-quantum resistant security and be able to tailor implementations to requirements in terms of speed, efficiency and power.
- Seamlessly integrate with an organization's existing network and cloud infrastructure.

Concepts

- There is now an IoT device security solution for securing small footprint devices today and into the future.
- Small footprint devices are defined as devices that utilize microprocessors with limited availability of RAM, Flash, or CPU processing power.
- New code theory algorithms enable post-quantum encryption for data in transit that is faster and more efficient than other block cipher algorithms.
- Until now, the concept in security was that one must increase compute capacity/power to achieve higher levels of data obfuscation (or a larger key size and search-space). This because traditional cryptographic solutions were largely based on numbers theory or a number-crunching approach. To achieve a higher level of security, more compute power was required.
- Data in transit encryption can be provided for any data-packet size (and is not constrained to 16 or 32 byte blocks) saving network bandwidth and power.

Background

When AES was introduced as a world-standard in 2001 – the expectation was that increasing compute-power would readily be available as we encountered requirements for larger key sizes (AES64, AES128, AES256, etc.). AES was designed before the advent of billions of 'connected' devices, the majority of which operate with bare-minimum compute resources. As such, AES code does not fit easily on small footprint IoT devices, and when added dramatically impacts performance. Furthermore, AES was designed prior to the development of quantum computing.

The Invention, and how AgilePQ DEFEND IoT Device Security is different

AgilePQ's optimized code-table methodology is rooted in the world of RF signaling. Bruce Conway, AgilePQ co-founder and inventor, was working on a solution for improving communication links with Unmanned Aerial Vehicles (UAV's) specifically in high-noise environments.

His discovery in solving this problem led to a method for extremely high levels of data security through very fast and efficient algorithms, which was further refined to optimize as well as obfuscate the algorithms themselves. The result is a software solution we call AgilePQ DEFEND IoT Device Security.

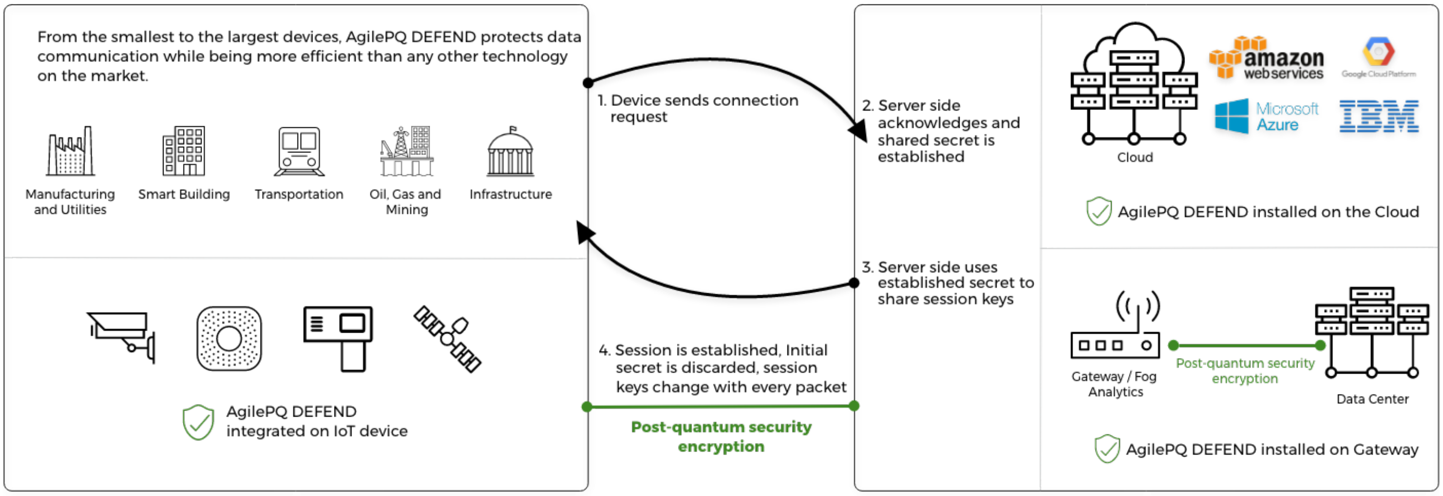
Using the core cryptographic requirements of confusion and diffusion as AgilePQ's metric for the quality of our algorithms as a cryptographic solution – we injected large quantities of digital data and observed the output. The result was a Gaussian distribution on the randomness of the obfuscated data. Of particular note – this same distribution is observed whether input is static (repeatedly sending the same data) or dynamic. AES, for example, without re-initializing, will output the same data given same data in (AgilePQ Cryptographic Strength paper).

AgilePQ DEFEND IoT Device Security – How it Works

AgilePQ's code is implemented at the transport layer, providing a secure socket connection in IP environments. As such, any application layer protocol can easily ride on top of an AgilePQ secured socket. For a device-to-cloud implementation, AgilePQ has a streamlined version of MQTT, now tailored to work directly on constrained devices.

For any broadly used cryptographic implementation, it is expected the general public will know the algorithms themselves. The challenge then becomes protection of the keys.
AgilePQ DEFEND was designed to work with and has been implemented with a variety of initial key exchange algorithms. While a good number of these are commonly in use today (Public Key / Private Key, Diffie-Hellman, ECDH), they are not ideally suited to constrained devices both due to the code footprint as well as the computational requirements.

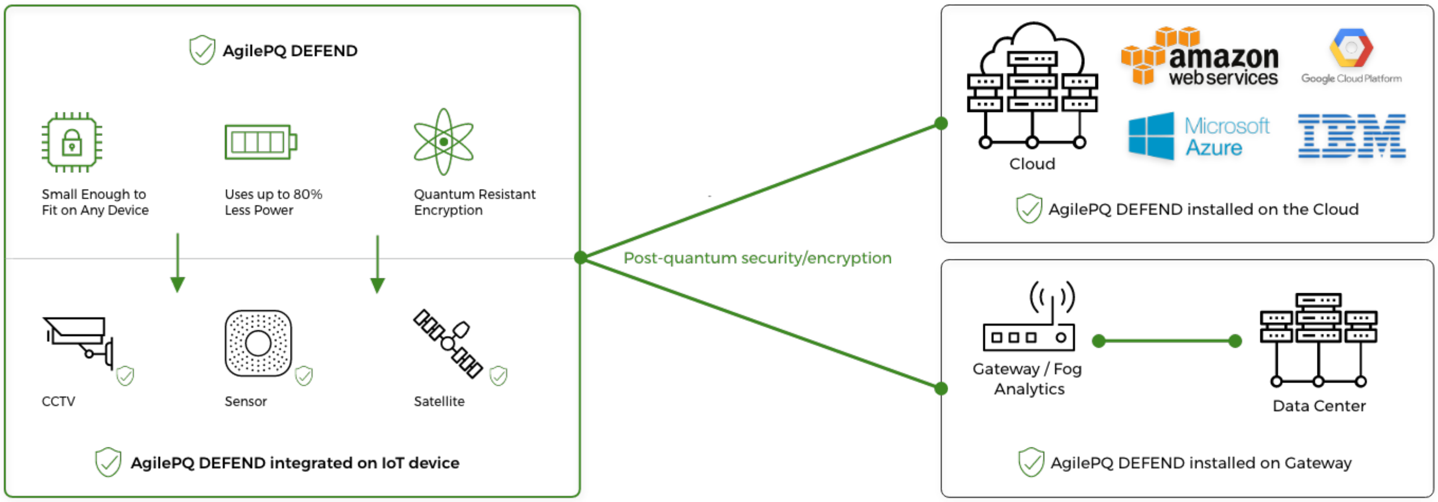
As such, AgilePQ has implemented two solutions for quantum secure initial key exchange that are designed for constrained devices: a tailored a version of the publicly available algorithm called "The New Hope" that works well with Class 2 devices, and an AgilePQ developed Key Distribution Server for Class 0/1 devices.



Why it is Better?

AgilePQ DEFEND was developed with the design-goal of protecting data transmissions on constrained devices, which are expected to become the broadest base of IoT device deployments. This requires the code to have an extremely small dynamic memory footprint, a commensurately small static footprint, be efficient and fast in operation, and be flexible enough to protect data while adding minimal overhead.

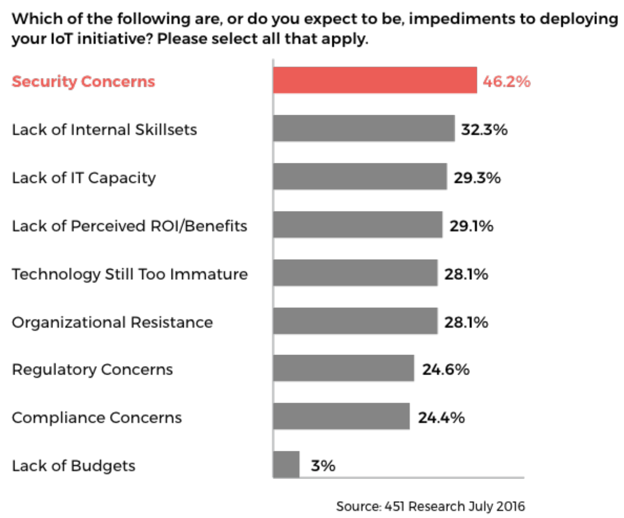
AgilePQ's DEFEND C-code will fit on any microcontroller regardless of size. AgilePQ DEFEND is extremely efficient, consuming 50% - 80% less energy than legacy encryption, and introduces minimal overhead with an agile key size. The solution is fast; up to 30 times faster than AES application to application, while delivering a key search space 429 orders of magnitude greater than AES 256.



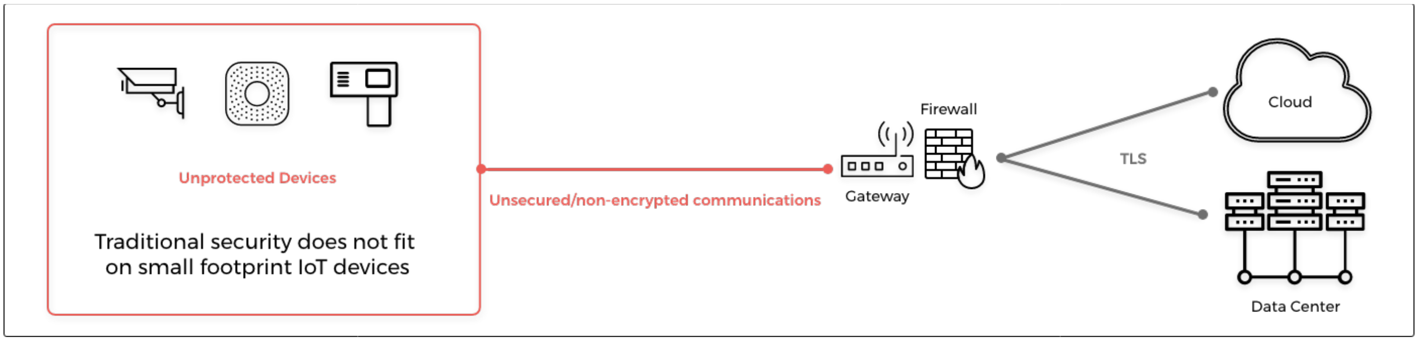
Why Now

Today IoT represents over a $20B market (IHS) with many billions more devices scheduled to be connected to the Internet in the next four years. A large portion of these new devices will not have the capacity to run legacy cryptographic solutions.

NIST, recognizing the shortcoming of legacy encryption standards, is actively engaged in "developing a strategy for standardization of new lightweight cryptographic algorithms" (NIST.IR. 8114). AgilePQ's DEFEND was designed with these requirements in mind.



Simultaneous to the advent of billions of newly connected constrained devices, we also see the advent of quantum computing posing a real threat-vector on data communications.
As such, any deployment of connected devices, constrained or otherwise, needs to build-in protection from the ever-increasing compute capacity available to adversaries. Traditional perimeter security is not a sufficient answer going forward. Security needs to be truly end-to-end, which includes all devices connected to the network regardless of size. AgilePQ DEFEND provides a solution where there previously has been none.



Conclusion

AgilePQ DEFEND for IoT Device Security is a series of algorithms that highly randomize and scramble data streams using a code-theory approach. The C libraries, designed specifically for constrained devices, can be implemented on any device or sensor that supports a traditional compute stack down to the smallest Class 0 devices. The system implementation encompasses initialization, device identification, authorization and authentication, and has been hardened against attack, including eventually expected attacks from quantum computers.

Patents & Standards

AgilePQ has 6 U.S. patents, and 9 U.S applications pending, with numbers foreign filings. AgilePQ is actively engaged with the NIST process for identifying new “lightweight cryptography” standards. Global Network and Lab Validation Completed by:

- **Innovation Lab** for which AgilePQ demonstrated its functionalities, security, and the improved DCM Performance when compared to AES256.
- **University of New South Wales** (World Leader for Red-Team Attack Competitions) inserted 32 million packets with no collisions.
- AgilePQ architecture and integration document were reviewed and approved by **Advanced Services Labs.**
- **UCSD Cryptography Professors Evaluated for Mathematical Proof**: “No Known Attack Surface.”
- **University of Nebraska-Omaha Cryptography**: Three Years of Red Team Assaults – No Breaks.
- **Ponemon Institute**: Nuclear Physicist Red Team Assault – No Breaks.

If you would like to receive a more in-depth version of this paper under NDA, or any further information, please contact:

Greg Ward (VP Product Strategy)
Email: gward@AgilePQ.com

