Quantum Driven Hardware Root of Trust

Patrick Camilleri

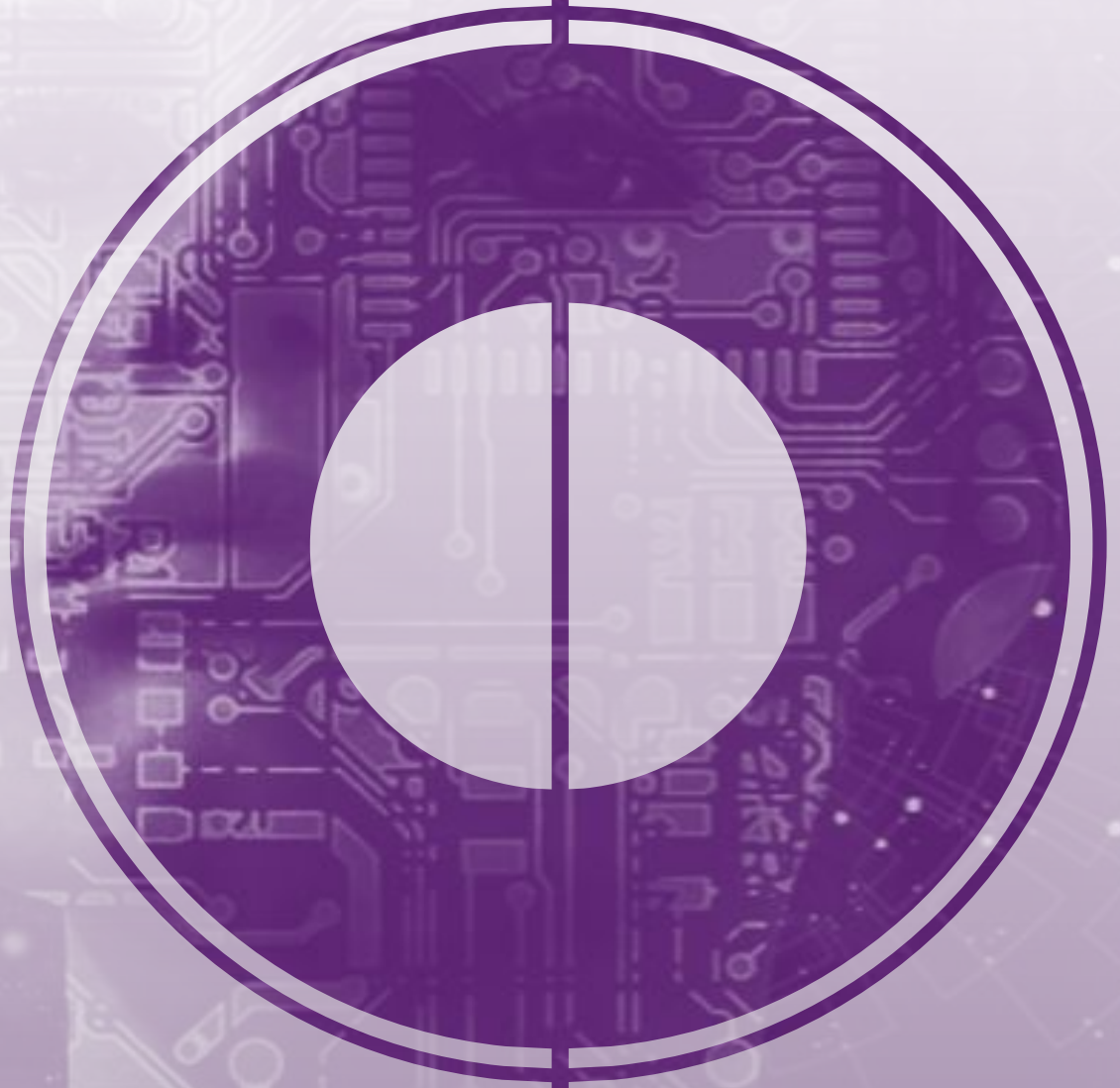
17 March 2022

OUR

VISION & MISSION

Securing the connected world with zero-trust

To ensure seamless end-to-end security for the IoT by providing unforgeable hardware Root of Trust and full life cycle security management over the cloud



Company Timeline

2016

Entrepreneur First cohort graduate

2017

$500k Angel round by AceCap

World class team of quantum physicists, electrical engineers and cryptographers **harness quantum effects of Silicon for unique identifiers**

2018

World first Quantum Driven Secure Chip delivered

55 nm CMOS process

NIST Tests prove best of breed entropy

Invited to **Thales Station F** accelerator programme

Airbus and several UK and Global defence organisations engaged

2019

$8m ADV Led seed extension

Awarded €1.7m EIC grant & €400k Eurostars grant

Cloud Key Mgmt. + chip provisioning system **complete**

LORCA 2nd Cohort Best UK Cyber talent

EIC R&D Grant from Horizon 2020 Research & Innovation framework

Eureka Eurostars Grant in collab with ETH Zurich

2020

Market Launch

3rd test chip bring up and tested (hard macro based)

Selected Partner engagements

Enterprise IoT PoCs

Support Organisation

Integration best practices

2021

IP integration

22 nm CMOS process

IP ready for integration by major MCU manufacturer

Paid Quarklink PoC

Won 3 Elektra awards and IET E&T Innovation award

Grew to 30 people

© Crypto Quantique 2022

Crypto Quantique has developed a **100% secure solution** combining HW and SW that is faster and **easier to deploy** at scale

Our products build on a strong and clear need

Highly secure unique unforgeable ID for each IoT device

We enable manufacturers to embed it in their processes and **create this 100% secure ID upon device awakening with no need of external involvement**

Enables the most secure and fastest provisioning, onboarding and security monitoring in the world

We build the software to manage all these devices securely and easily. Today connecting 10,000 devices to AWS takes 2 person years *, **Our solution can do it in 2 minutes.**

* McKinsey & Company

© Crypto Quantique 2022

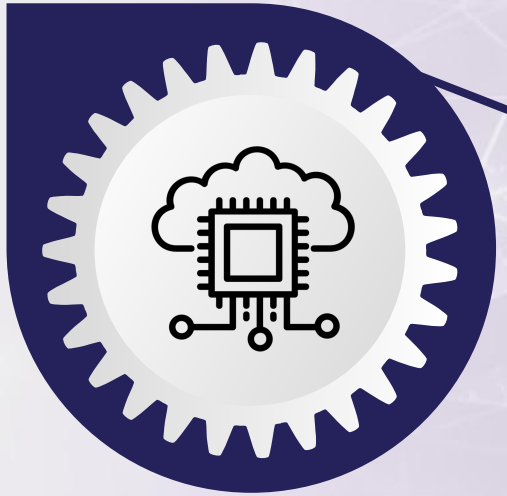
QuarkLink and QDID in combination

QDID – Quantum Driven Identity

Hardware root of trust

- Unforgeable, tamper proof, impossible to counterfeit
- Extremely easy to test
- Does not require key injection
- Multiple uncorrelated keys

More secure
Easier to use
Cheaper to manufacture
than any other solution



QuarkLink

Security life-cycle and certificate management

- Security from chip to application
- Data encrypted through the cloud
- OEM can be own Certificate Authority
- Supports third-party Roots of Trust

© Crypto Quantique 2022

QDID – detailed function

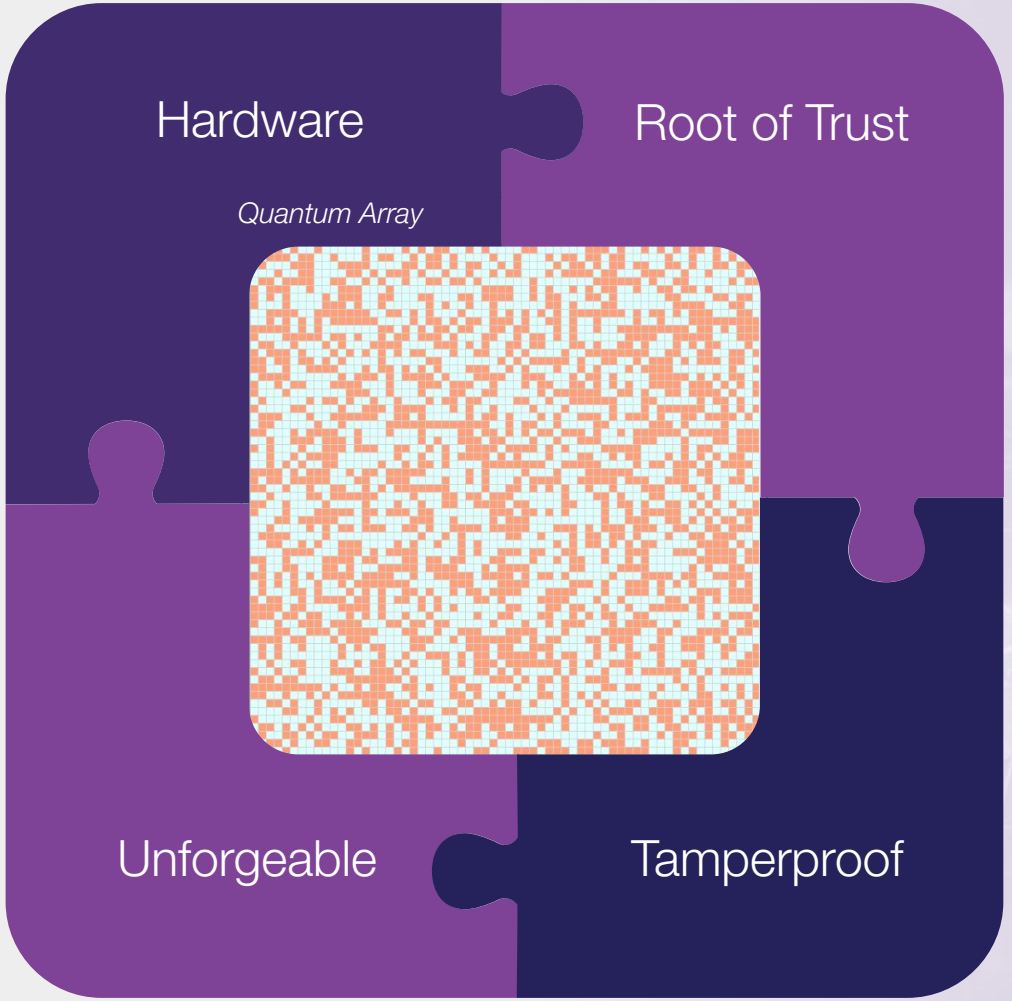
Plug and Play

- Hardware and MCU independent
- Self contained black box with AMBA interface
- Immune to side-channel attacks

Cost Effective

- Less silicon
- In-built error correction
- Simple on-boarding
- HWaaS model
- Easy to test it is working during wafer testing

Device ID using quantum tunneling (QDID)



Very High Entropy

- Multiple 128-bit keys
- Keys on demand
- TRNG not required
- Scalable > 128 bits
- Unforgeable
- No key injection required

Zero Touch security

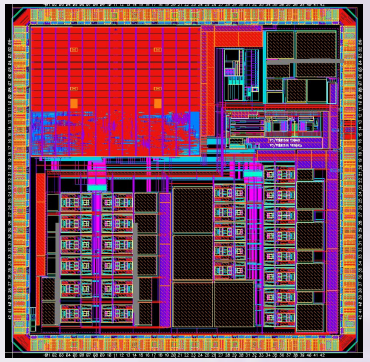
- Used with QuarkLink to deliver…
- Frictionless enrolment, provisioning, on-boarding and lifecycle management.
- Encryption from device to application (in a cloud or on-prem) - only encrypted data visible to the cloud

© Crypto Quantique 2022

Prototypes and chips to date

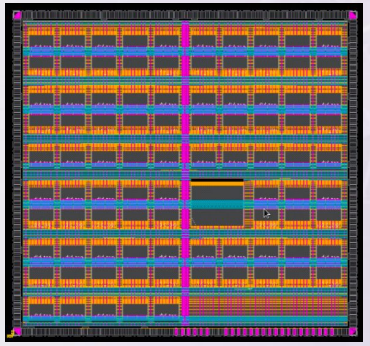
- **TC01, TC02 and QDID Microcontroller (TC03)**
  - 55 nm (Global Foundries)
  - 24 QDID 64x64 arrays
  - RISC-V MCU

9 mm^2 (24 QDIDs + MCU)



- **TC04**
  - 22 nm (TSMC)
  - 90 QDID 64x64 arrays

30 mm^2 (90 QDIDs)



16/03/2022
© Crypto Quantique 2022

Quantum Tunnelling

- Quantum tunneling is the process by which a tiny particle can pass through a solid barrier given certain conditions.

- At Crypto Quantique we use this property of quantum tunneling that takes place through the thin insulation layer of a pair of transistors.

- Quantum tunnelling is extremely sensitive to the nanostructure of the atomic layers that make up the SiO_2 oxide
    - Makes for a very good source from which to extract randomness

- Even though manufacturing processes are very tightly controlled (see Figure 1), it is still impossible to control the thickness of the oxide down to the atomic level

- Due to the inherently random nature of the atomic positions and imperfections of these nanostructures (see Figure 2) it would take vast amounts of computing power to simulate and predict

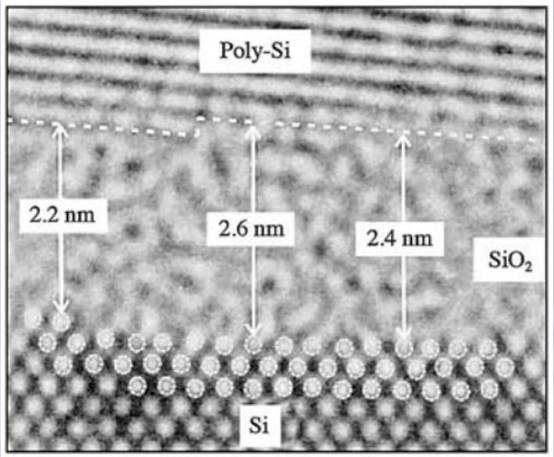


Figure 1 - SiO_2 interface roughness cross-section (IBM) [3]

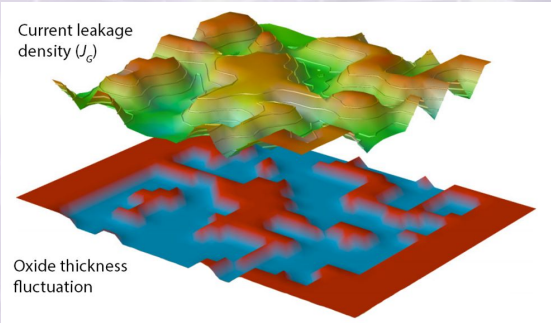
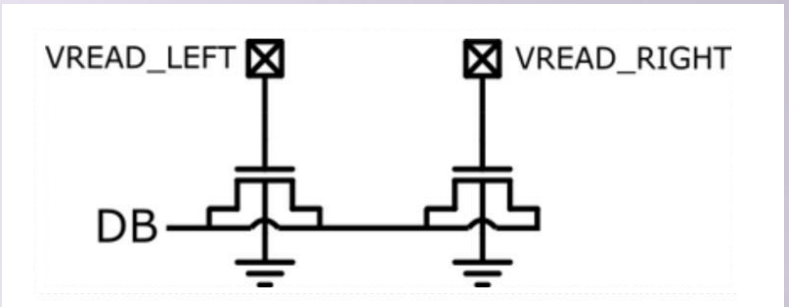


Figure 2 - Direct tunnelling current density, Si/SiO_2 interface roughness features (blue identifies regions of SiO_2 protrusions into the substrate, i.e. thicker oxide while red corresponds to thinner oxide) [4]

© Crypto Quantique 2022

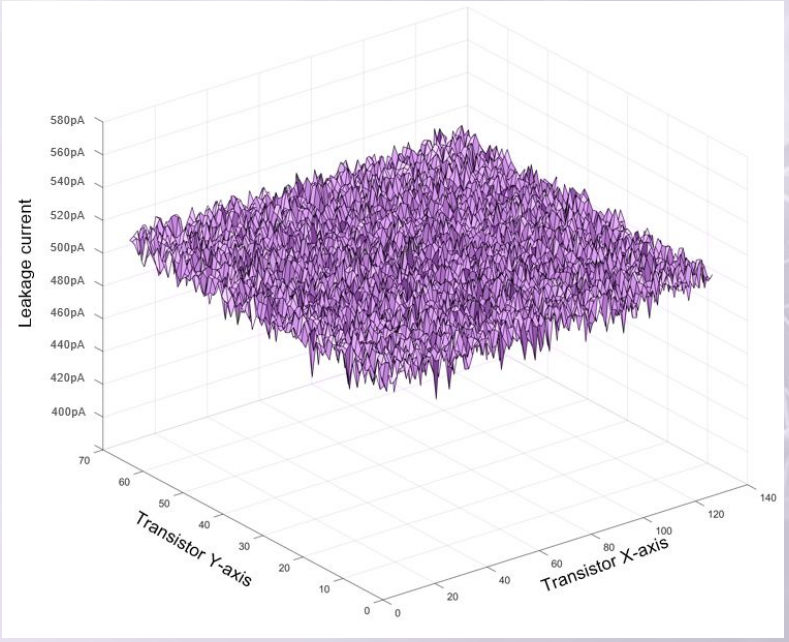
Quantum Tunnelling (cont.)

- A Quantum Array consist of transistor pairs. The random difference between the insulation layers for each transistor causes two different currents (≈400pA ±7pA) which we measure with our AFE.



1 bit (NOT qubit)

Representation of fingerprint output

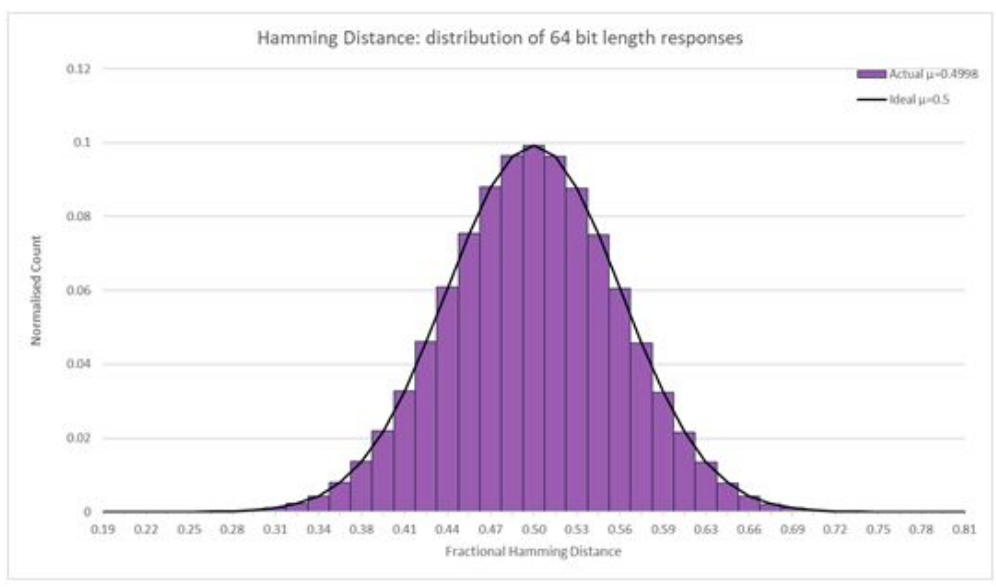


© Crypto Quantique 2022

Testing – Randomness

- Inter-chip Fractional Hamming Distance distribution of 64-bit length responses from **768 arrays**
- Over Process, Voltage & Temperature
  - Close match to the ideal binomial distribution (with n=64, p=0.5) shown as the black line
  - Test was run on pair-wise comparison of 768 arrays leading to **294,528 comparisons**
- Passed NIST SP800-22, NIST SP800-90B, and In-house specialised tests

Condition	Mean	Min	Max	STD
Ideal	0.5	-	-	0.0078
-40°C	0.4998	0.4658	0.5381	0.0078
25°C	0.4998	0.4651	0.5354	0.0078
125°C	0.4998	0.4639	0.5359	0.0079



© Crypto Quantique 2022

Security

- Crypto Quantique has architected a purpose-built full-custom analog PUF (3 patents granted, 4 patents pending).
- Obtained EAL4+ certification
- The core of our design is a differential approach that is inherently immune to:
  - Common mode inputs such as Process, Voltage and Temperature
  - Invasive attacks
  - Side-Channel attacks

Side-channel attacks	QDID
Glitch attacks	Design is fully differential and insensitive to such attacks
Photon emission attacks	Difference in current between transistors is only a few pA making photon emission attacks irrelevant
Remanence decay attack	Unlike SRAM cells, QDID cells are not affected by remanence decay because no information is stored
Very-low temperature attack	QDID cells not based on a bistable circuit and not affected by this attack
Aging attack	Experimental evidence that array not affected by aging
Tamper evident	Sensitive to invasive attacks due to sensitivity of the oxide layer

© Crypto Quantique 2022

Crypto Quantique Partners

STMicroelectronics

STMicroelectronics, a global semiconductor leader serving customers across the spectrum of electronics applications, including IoT and device security.

BT Labs

BT Labs is a global leader in the research, development and deployment of novel methods for device identity and on-device cryptography in IoT.

Renesas RA Ecosystem

Renesas is the world's largest auto semiconductor and MCU manufacturer providing technology solutions for consumer electronics, automotive, IIoT, and smart homes and cities.

Macronix

A leading integrated device manufacturer in the non-volatile memory (NVM) market, provides a full range of NOR Flash, NAND Flash, and ROM products.

Silex Insight

Silex Insight is a recognized market-leading independent supplier of Security IP solutions for embedded systems and custom OEM solutions.

EPS Global

EPS Global provides programming as a service to Tier 1 automotive electronic suppliers, OEMs and contract manufacturers. It owns and operates 18 programming centers around the world.

© Crypto Quantique 2022

THANK YOU

How bad is it really?

The **$200m** attack

On October 12, 2016, a massive distributed denial of service (DDoS) attack left much of the internet inaccessible on the U.S. east coast. The attack, which authorities initially feared was the work of a hostile nation-state, was in fact the work of the Mirai Botnet.

The **$400m per year** smart meter vulnerability

Smart meters that are being installed across the globe are easily hacked. Costing utility companies across the world millions.

40% of all devices lack basic encryption

Mirai Botnet DDoS

Smart Meters easily hacked

© Crypto Quantique 2022

Differentiators – QDID vs Other PUFs

CRYPTO QUANTIQUE

Truly random (Quantum-based)

QDID relies on measuring transistor gate currents due to quantum-tunnelling, a quantum phenomenon that cannot be predicted or copied regardless of computing power. Other technologies based on classical physics can be ultimately simulated, especially with the advent of quantum computers.

Small and cost-effective

QDID is efficient in terms of die area, especially considering the number of seeds available per area. At present it is in the range of 0.2 mm^2 at 55nm to generate 8 x 128-bits of raw material. Besides, the array can be scaled up and down according to how many seeds are needed.

Future-proof

Due to the flexibility in the use of the array of bits, QDID can be used as a key source for future post-quantum cryptography algorithms, making it a future-proof PUF.

No Key Injection or Secure Memory required

Most PUFs still require key injection of some sort, due to the limited number of keys for multiple purposes or the lack of integration with a software provisioning platform. With a large number of keys and full integration with QuarkLink, QDID devices do not need any type of key injection, being able to generate and provision keys without the need of costly HSMs or secure memory.

Side-channel resistance

Other PUFs use easily detectable electrical phenomena, such as ring-oscillators and arbiter PUFs, require non-standard designs, such as exotic materials or high-voltage, or use repurposed tech, such as SRAM, which makes them highly susceptible to side-channel attacks. Using standard CMOS, no exotic requirements, and fully differential circuitry, QDID is naturally resistant to side-channel and fault-injection attacks.

Other PUFs

SRAM PUFs require a large amount of raw data to generate each seed bit, demand a large setup time and require a lot of code for post-processing.

Arbiter and ring-oscillator PUFs are susceptible to side-channel attacks due to power consumption and EM emissions.

Resonant tunneling diode PUFs require III-V materials, not compatible with standard CMOS.

Gate oxide breakdown PUFs rely on a classical rather than a quantum process, the difference in transistor geometries, for the randomness. They also depend on a deterministic setup (breakdown) process that can input biases. On top of that, they require a costly high-voltage circuitry in the chip.

Confidential

© Crypto Quantique 2022

QuarkLink: Seamless end-to-end Security

An Enterprise Security Platform for managing:

1. Secure Provisioning

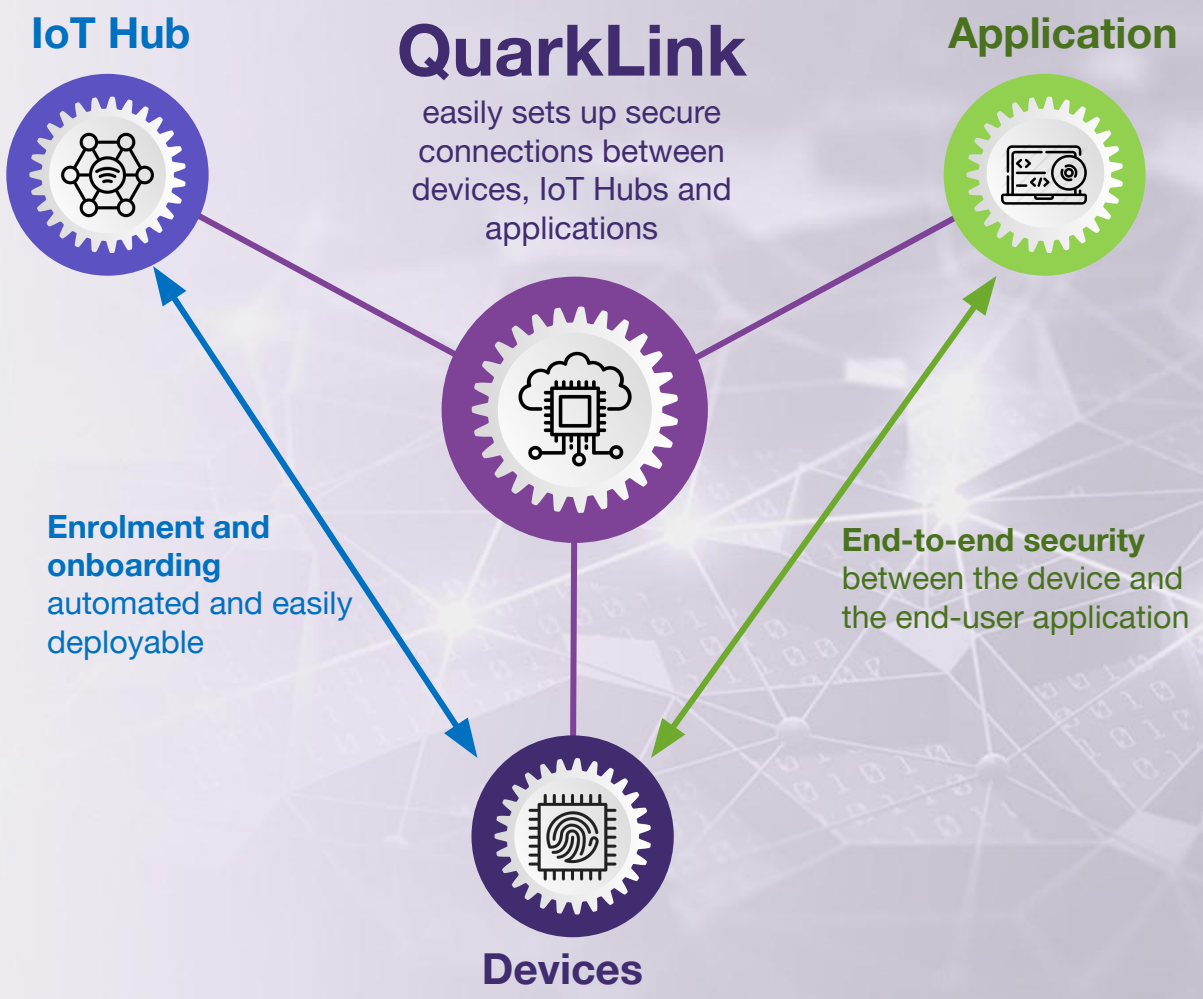
- No secret key injection
- No HSM

2. Automated Secure Onboarding

- Security policies
- Multiple IoT Hub support
- End-to-end security

3. Identity and Key Management

- Firmware updates - encryption and signing
- Certificate renewal and revocation



© Crypto Quantique 2022