Geneva, August 31st 2021

ICTK partners with ID Quantique to secure IoT devices with Quantum PUF technology paired with QRNG

ICTK Holdings is a PUF[1] chip, module and security solution provider selling new-generation security solutions for smart devices, cloud computing, smart grid and intelligent automobiles.

It has developed a quantum security chip with "Physically Unclonable Functions", introducing thus a unique "Q-PUF" security solution to the market, paired with IDQ's Quantum Random Number Generator (QRNG) chip. Quantum random number generators (QRNGs) offer a greater degree of randomness used for encryption of data while also being invulnerable to environmental perturbations and allowing live status verification.

This innovative Q-PUF solution is designed to counter any currently existing security breaches in the most simple and cost-effective way.
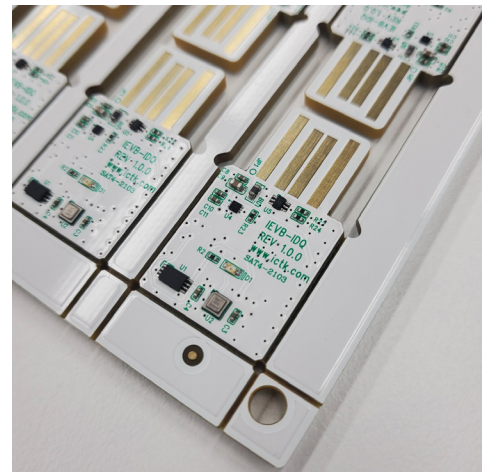
PUF is simply a 'digital DNA' created during the semiconductor process that cannot be copied or altered. This provides unclonable ID to various devices where authentication, firmware protection and upgrades are much safer.

In today's connected world, it is vital that devices, along with the data stored on and transmitted by them, can be trusted. Security must be built into solutions at the chip level — delivering a secure Root of Trust. Securing technology infrastructure at the chip level guarantees the highest levels of protection for the applications that deliver value to customers. **PUF-derived unique IDs are virtually impossible to duplicate, clone or predict, making them ideal for:**

✅ Secure key generation and storage	✅ Flexible key provisioning	✅ Device authentication	✅ Chip asset management	✅ Secure boot and update

Key applications are: IoT end point security including PKI authentication, secure boot and update, data integrity and security, anti-counterfeit, storing secure data.

---

[1] What is PUF? Physical Unclonable Function is a physical property that is based on random variations in the molecular structure of a chip. These variations are created during the manufacturing process. A unique binary code is generated for each chip based on these variations and that code becomes the Root of Trust — unclonable, tamper-proof and secure.

Focus industries targeted are the telecom industry, small appliances (Homes, cities), IP cameras, CCTV, mobile payments.

ICTK has been providing various authentication solutions between devices and networks to Korea's major companies including Mobile Network Operators, automotive and robotics companies.

QRNG offers strengthened security to IoT devices

ID Quantique's true QRNG chip offers the highest achievable robustness and security for the creation of random bits used to generate keys to encrypt data securely. Quantum Random Number Generators offer a greater degree of randomness while also being invulnerable to environmental perturbations and allowing live status verification. The chip's compact size and resistance to external environmental perturbations make it ideal for use in IoT, mobile phones, V2X automotive, computing, critical infrastructure and security applications. Three models of IDQ's QRNG chip are available, offering a range of size, performance, power consumption and certifications designed to meet various industry-specific needs.

> "
> *It is a milestone in IoT security to have the two leading security companies in PUF and quantum technology to come together to deliver the most secure solution for IoT security.*
>
> Justin J. Lee, CEO of ICTK Holdings

> "
> We are proud of partnering with ICTK. Our joint solution strengthens the security of IoT devices and brings a new level of security to the market more and more conscious of cyberthreats and of the new security challenges.
>
> Axel Foery, EVP Quantum-Safe Security at ID Quantique

For more information, please contact:

Catherine Simondi – VP Marketing & Communications

catherine.simondi@idquantique.com or +41 (0) 22 301 83 71