QDID: quantum-driven hardware root of trust

Version 1.0

CRYPTO QUANTIQUE

Table of Contents

1 Introduction

A Physical Unclonable Function, or PUF, provides a physically defined “digital fingerprint” that serves as a unique identifier, most frequently for semiconductor chips such as microcontrollers and microprocessors. PUFs are usually based on unique physical variations which occur naturally during semiconductor manufacturing.

This document provides an overview of the state of PUF technology, along with analysis of benefits and shortcomings when compared with the Crypto Quantique Quantum Driven Identity (QDID).

Please note that this document exclusively focuses on the QDID (and PUF) as root of trust. It does not address the critical issue of secure provisioning, onboarding and monitoring. Fully integrated software is necessary for seamless end to end management of IOT devices and scalable deployment. **This is provided by the Crypto Quantique Quark solution, which is not discussed further in this document.**

2 Why are PUFs important?

Because we are now in a connected era where billions of connected devices all need to communicate securely, it is of paramount importance that we have silicon derived identities. All of these connected devices require a persona in order for the services to be able to take advantage of those devices and the data that they are producing. Currently the most widespread way of creating these personas is by injecting a secret key into each device which is a process fraught with risks: programming facilities need to be trusted or secure, increasing the cost; keys need to be generated and stored on potentially unsafe media; and there is also the risk that secret keys are leaked either through human error or intentionally via a bad actor.

3 Crypto Quantique's solution

Crypto Quantique invented a new approach to Physical Unclonable Functions that harnesses quantum effects on silicon to generate unique and unclonable identities. The radical quantum tunnelling based chip design enables connected devices to originate multiple tamper-proof, unforgeable cryptographic keys on demand, that can never be compromised during the lifetime of the device.

They were the first to lay claim to quantum tunnelling PUFs (see patent: Unique identifiers based on quantum effects – GB2567642B). The technology is based on the ability to measure the nano-differences in the gate oxide thickness variability of the MOSFET due to manufacturing process variations in the foundry. They refer to the root-of-trust IP as Quantum Driven IDentity (QDID). Figure 1 shows a schematic representation of the interface roughness between the SiO_2 layer (oxide) and the silicon layer of MOSFET. The quantum tunnelling current that is the source of our randomness is an exponential function of the thickness of this oxide layer, which means that even a variation of one atomic layer is sufficient to give rise to a detectable change in the tunnelling current.

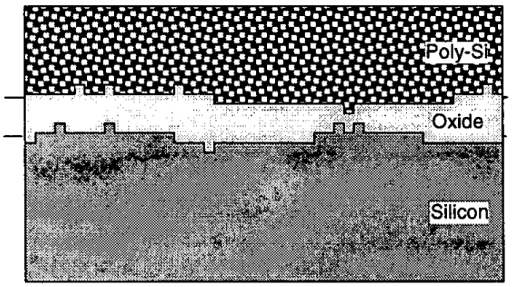

Figure 1 – Schematic illustration of gate oxide variation with an average thickness of 12 Å. The step height is approximately 3 Å. [1]

The ability to measure these tiny differences in gate tunnelling currents is achieved by a state-of-the-art differential measuring system that was developed in-house. The system is able to detect and measure pico- and femto-amp current levels of accuracy. Figure 2 is a schematic diagram of how the difference in tunnelling currents between two devices is measured. Essentially it is an extremely accurate source-measure circuit that is insensitive to changes in process, voltage, and temperature.

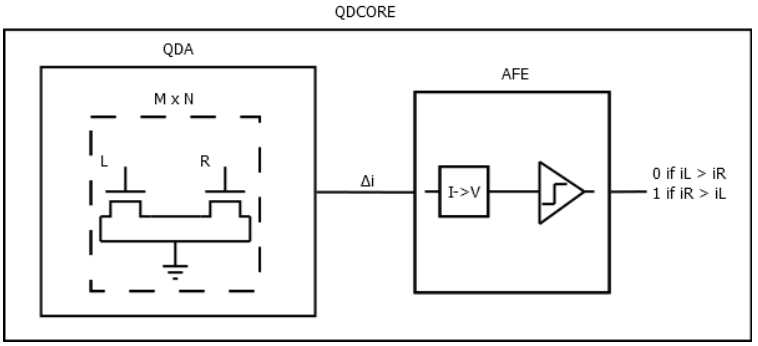

Figure 2 – Schematic representation of how gate leakage variability is measured, and a unique value extracted.

Figure 3 – A unique, unclonable, and tamper-evident ID. Each or a combination of Quantum Driven Arrays can be used as a key.

Figure 3 is a representation of the QDID 4096-bit array output where the light and dark coloured 'pixels', represent 0 and 1, respectively.
One might ask the question why were quantum tunnelling currents chosen as the source from which randomness is extracted, given that the absolute values are so small and so hard to measure? The simple answer is that firstly they are largely insensitive to environmental temperature variations and secondly established side-channel attacks would be rendered largely ineffective.

Rather than trying to repurpose something like SRAM to behave as a PUF, Crypto Quantique designed the circuit from the ground up to be able to control and mitigate threats from side-channel attacks, produce random bits that are stable in a wide range of environmental conditions and have a high level of entropy.

In addition to the array of tunnelling current devices and the accurate read-out circuitry the IP has the necessary building blocks to be able to interface with standard bus protocols on systems-on-chip for seamless integration – see Figure 4.

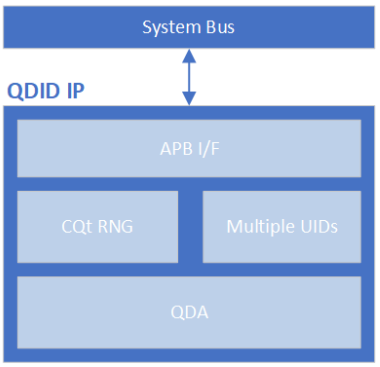

Figure 4 – QDID architecture

4 How is Crypto Quantique better?

PUF technology has been around for over 10 years, but they all suffer from some major drawbacks. SRAM PUFs, for example, require a lot of post-processing to correct for the errors that arise from environmental conditions such as temperature variations. This results in powerful error correction algorithms which take up a lot of silicon area as well as require a fair amount of processing power to correct. Aging is yet another factor that affects the stability of SRAM PUFs.

Other PUF technologies such as arbiter PUFs and ring oscillator PUFs suffer from side-channel attacks related to power consumption and electro-magnetic emissions given by their architectures.

Another PUF is based on oxide rupture, or gate oxide breakdown. Even though this technology is currently being marketed as being quantum in nature, the technology is based on applying a high voltage across the oxide of the MOSFET to damage it and cause oxide breakdown. This effectively creates a contiguous path between the gate layer and the silicon substrate creating a short circuit making the process a classical rather than a quantum process. Figure 5 shows different stages of the oxide breakdown starting from temporary soft breakdown all the way to hard breakdown which is permanent.

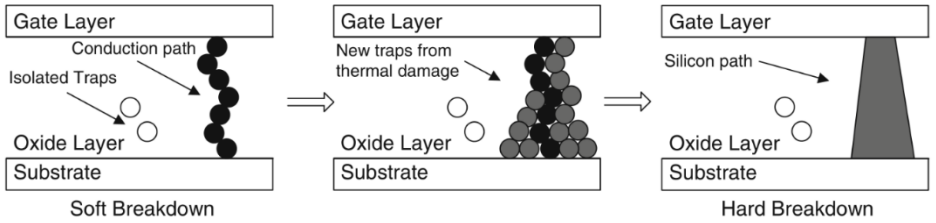

Figure 5 – Evolution of the gate-oxide breakdown, hard and soft breakdown through the creation [2]

The principle relies on dopant mismatch between two adjacent transistors where only one transistor randomly breaks-down upon the application of a high voltage to both gates. In order to ensure that the process generates good randomness one needs to assume identical matching in the geometrical aspect, otherwise the claimed randomness may end up being biased. Since the technology requires a high voltage to induce the gate oxide rupture, this requires additional silicon overheads making it costly. In contrast, Crypto Quantique's technology does not suffer from any of these disadvantages because mismatch only increases as technology nodes get smaller and no high-voltage generation circuitry is required.

Yet another PUF is based on quantum confinement and the characteristics of resonant tunnelling diodes. This technology also has some major pitfalls, the biggest of which being that it requires III-V semiconductor materials making it incompatible with standard CMOS

processes. Reliability over process, voltage and temperature has also not been verified and the technology has only been demonstrated in a laboratory setting which clearly limits its usefulness. In contrast, Crypto Quantique has optimised its quantum PUF technology using standard CMOS and is certified to work over a wide range of temperatures, process and voltages to ensure seamless integration with all sorts of MCUs and systems-on-chip.

5 Status of technology

The technology is currently available and Crypto Quantique is already in partnership with the leading semiconductor manufacturers to implement its IP in their upcoming state-of-the-art security chips.

6 Contact us

For more information on the QDID root of trust and the Quark universal security platform please see https://www.cryptoquantique.com/ or contact info@cryptoquantique.com.

7 References

[1] A. Asenov, S. Kaya, and I. Ieee, “Effect of oxide interface roughness on the threshold voltage fluctuations in decanano MOSFETs with ultrathin gate oxides,” *2000 Int. Conf. Simul. Semicond. Process. Devices*, no. 2, pp. 135–138, 2000, doi: 10.1109/sispad.2000.871226.

[2] H. Solar Ruiz, R. Berenguer Pérez, H. Solar Ruiz, and R. Berenguer Pérez, *Linear CMOS RF Power Amplifiers*. 2014.