PUFcc: An Essential Crypto Coprocessor for RISC-V.

PUFsecurity

White Paper

August 2021

Authors:
Sam Chung,
Sean H. Wu,
Evans Yang

Foreword

The number of connected IoT devices exceeded 46 billion in 2021 and is expected to reach a remarkable 125 billion by 2030. This will shift the semiconductor market significantly as each IoT device requires a processor core to effectively process the enormous amount of data and associated transactions. To make the most out of such market potential, RISC-V architecture has become a new alternative to x86 or ARM for SoC designers, thanks to its open instruction format and low cost.

However, as the IoT market continues to expand, so does the destructiveness of adversarial attacks. The security of connected applications is now an essential element of their design. Connected devices must be able to authenticate one another, ensure safe data transmission, and include secure storage. While the security guidelines of RISC-V are still under development, providing RISC-V users with an effective plug-and-play solution to strengthen the security of SoCs and beyond is critical.

What kind of designs are needed to secure IoT applications?

In most cases, there are six key SoC Security factors to consider…

- **Trusted Execution Environment (TEE):** Isolates codes, data, and memory that require a higher security level.
- **Root-of-Trust:** Safeguard crucial security parameters; comprises unique ID, certificates, secret keys, and secure storage.
- **Secure Boot:** Blocks unauthorized OS and applications from running.
- **Data-at-Rest Security:** Stores data in an encrypted/obfuscated form with solid access control to prevent leakage.
- **Data-in-Transit Security:** Utilizes keys to encrypt data before transmission to prevent interception.
- **Secure OTA Update:** Ensures that firmware or software updates in the field come as encrypted ciphertext and that no downgrading is allowed.

Having a CPU alone cannot attain these six security factors. A chip's design would need a key storage unit and a set of cryptographic algorithms to assist the CPU in performing security functions, including authentication, encryption, decryption, and integrity check to attain these features. In addition, an isolated and trusted secure execution environment is required for secure operations (separated from non-secure operations). Anti-tampering designs should also be implemented to protect a secure environment from being attacked.

With these risks in mind, an experienced designer would often use a Crypto Coprocessor that comes with a Hardware Root of Trust and anti-tampering designs, to support the CPU in executing all necessary security functions for applications and services.

The Crypto Coprocessor takes care of security-related affairs within a system and allows the CPU to perform its primary functions safely. When implemented, a hardware-accelerated Crypto Coprocessor will protect sensitive information and perform security functions far more efficiently than a CPU, without siphoning off its computational power. This not only simplifies the system design but also enhances the overall performance.

Remedying the Insufficiencies of Existing Coprocessors

Within their architecture, ARM offers the CryptoCell-312 integrated with its CPU as the Crypto Coprocessor to deal with security operations. In comparison, the RISC-V ecosystem is still maturing and does not yet have a fitting solution for Crypto coprocessors. RISC-V users will have to either develop by themselves or adopt IPs from partners to obtain the aforementioned security features. If they choose to develop in-house, several challenges may arise. Do they have a security development team capable enough? How will it affect the time to market? Can the self-developed security functions gain certification? How well can they deal with technical issues when they arise? And finally, what would be the cost? All of these challenges can be avoided by adopting integrated IPs from capable partners.

Existing solutions lack a comprehensive Hardware Root of Trust and don't provide a solid secure boundary, leaving them vulnerable to attack. Most Crypto coprocessors in the market may cover one to two of the key functions but come up short. For instance, some Coprocessors fail to support certain crypto algorithms, are prone to attacks, or haven't passed 3rd party certifications. Some do not come with secure storage for keys, resulting in the Coprocessor retrieving keys from outside the secure boundary (imagine leaving your key to the vault at the front door). Even options that include secure key storage have inevitable drawbacks, requiring key injection into the chip one by one during production, making it costly and difficult to fabricate or operate. Some Coprocessors have the same activation key for all products, endangering identity and application service management.

All these insufficiencies may end up being vulnerabilities in IoT devices, that will inevitably become targets for hackers looking to compromise a network. Consequently, even a tiny IoT device, that only transmits non-sensitive data, can cause massive harm if manipulated by hackers. There are countless incidents like this, a recent one being 2021 May, when Colonial Pipeline, the largest oil pipeline system, was under attack. Not only did they shut down the entire pipeline, but the government also even issued a regional emergency declaration. The loss in ransom paid alone was 4.2 million USD.

PUFcc enables Security on Chip for RISC-V Architectures

To address the absence of a complete Crypto Coprocessor from the RISC-V ecosystem, PUFcc, one of PUFsecurity's integrated IP solutions, is the ultimate answer. Protected by a multi-layered design, it utilizes a comprehensive suite of fully integrated hardware security IPs. Unlike purely software-based designs, PUFcc's secure boundary is based on physical separation of hardware, therefore establishing a sound Trusted Execution Environment (TEE).

Figure 1 demonstrates the design architecture of PUFcc. At the heart of PUFcc is an Analog Hardware Root of Trust design. The Hardware Root of Trust

encompasses eMemory's patented NeoPUF, providing each chip with a unique chip fingerprint (UID) and offers Riscure certified anti-tampering secure OTP for key storage, preventing physical/electrical attacks on crucial security parameters. The Hardware Root of Trust also comes with a True Random Number Generator (TRNG), a source of dynamic entropies to secure cryptographic engines and communications between systems.

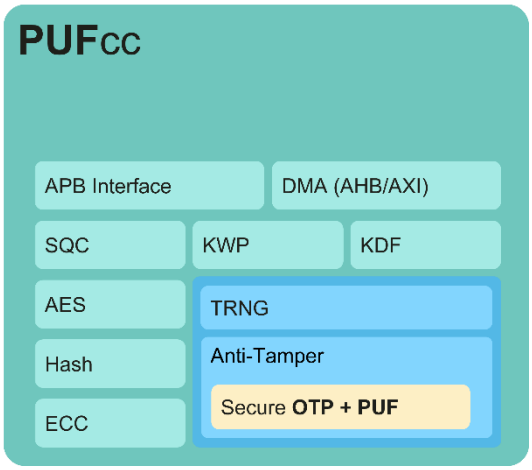

Fig.1: The design architecture of PUFcc

PUFcc supports a complete set of NIST CAVP-certified and 3rd Party certified Chinese OSCCA hardware cryptographic algorithms. Customization of PUFcc crypto algorithms remains flexible due to the modularized design. This means that the user's requirements, such as choosing between SM4 and AES, can be accommodated in a simple process. PUFcc can therefore meet the current and future security requirements of RISC-V. Besides the security functions, numerous digital and analog anti-tampering designs strengthen PUFcc further, making it a reliable crypto coprocessor. Similarly, to lower the complexity of the entire SoC system design, PUFcc supports a standard APB control interface used for register access control and a DMA with a standard AXI4 control interface to access larger amounts of data stored in system memory quickly. The accompanying Software Development Kit (SDK), including Linux bare-

metal firmware and high-level APIs, to help accelerate software development and deployment.

Along with NIST-standard Key Wrapping (KWP) and Key Derivation Function (KDF) to protect key usage and export, PUFcc can generate multiple keys on-demand for the RISC-V physical memory protection (PMP) to protect each application separately. Furthermore, the property of PUF serves well for Secure Boot and Secure OTA update, as the same software on different IoT devices each have its secret key. We can thus establish a firm foundation of security potentially for the many billions of new IoT devices set to enter the market. Figure 2 shows a RISC-V SoC design with PUFcc as its crypto coprocessor.

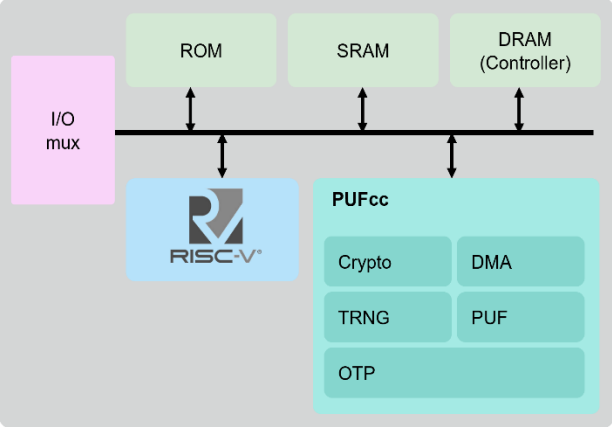

Figure 2: A RISC-V SoC design incorporating PUFcc

PUFcc has a free evaluation version available for users who would like to try the IP at https://www.pufsecurity.com/ip-go.

Conclusion

To secure IoT applications, PUFsecurity utilized chip fingerprint technology to fortify the Root of Trust and developed PUFcc, the Crypto Coprocessor with an extensive secure boundary that can easily incorporate into secure RISC-V systems. PUFcc enables Zero Touch Deployment needed in the world of IoT. With hardware-accelerated security functions and access controls, PUFcc also meets the requirements of Zero Trust Security in cloud applications. PUFcc as a security solution is, therefore, the perfect fit for IoT devices with RISC-V

PUFsecurity

8F, No. 5, Tai-Yuan 1st St.,
Jhubei City, Hsinchu County,
302082, Taiwan

Tel: +886-3-560-1
www.pufsecurity.com