Why Hardware Root of Trust Needs Anti-Tampering Design

How to strengthen the anti-tampering design in
Hardware Root of Trust to resistant attacks

PUFsecurity

Whitepaper

Mar. 2022

Dr. Meng-Yi Wu
吳孟益博士

Foreword

As the development of AIoT advanced in more diversified applications, such as artificial intelligence, image recognition, intelligent sensing, or smart healthcare, endpoint devices are exposed to more information security risks than ever. The technology boom also brings more security needs, so ensuring that devices are secure and trusted is critical. All layers of the system need corresponding security designs, from the application, operating system, and firmware to the hardware, to ensure the entire system's security level. The most important design in the overall security network is the root of trust in the hardware layer, which is the foundation of trust in the entire chip.

The hardware root of trust (HRoT) provides the trust base (root key), hardware identifier (UID), hardware unique key (HUK), and entropy required for the secure operation of the entire chip and therefore is often the focus of hacker attacks. If the design can't effectively resist attacks, hackers can easily obtain the secrets of the entire chip. Attackers can use the secrets to crack identity authentication and data encryption and steal product design know-how, causing application security problems.

Common Methods of Chip Attack

There are three main chip attack methods: invasive, semi-invasive, and non-invasive attacks. Invasive and semi-invasive attacks use physical methods to peel off the chip layer by layer. Then, the attack uses TEM, SEM, or nanoprobe to directly obtain and analyze the design and operation information of the physical circuit layer. Non-intrusive attacks usually refer to software and firmware attacks that exploit bugs in the system to understand or obtain secrets of secure operations. For example, Fault Injection uses illegal command or fatal logic control to cause a system crash. The system will reset due to a lack of resources, thus, creating a security window and vulnerability. Power Attacks can lead to unstable chip operations and result in information leaks or missing security checks. For further information on-chip attack techniques, please refer to Tamper Resistance.

How to strengthen the HRoT design to resist attacks

The HRoT protects the most important confidential information on the chip, such as hardware identification numbers (UIDs), hardware unique keys (HUKs), shared keys for external communication, public keys for related secure service certificates, and so on. However, simply using Non-Volatile Memory (NVM) such as eFuse, OTP and Flash Memory to store confidential data is not secure enough. To fully enhance the defensive power of the HRoT in the chip, the three following aspects must be considered from early design phase:

1. **Secure Storage:** The storage unit used to store important security information on the chip must have function designs that include: 1) access control and privilege management; 2) obfuscation and encryption of data read and stored to prevent electrical or physical reverse engineering during power-up and power-down operations.

2. **Trusted Environment:** The chip design must include the dedicated register, the logic circuit design for secure operation, and additional auxiliary circuits for detecting abnormal behavior. This avoids loopholes in the circuit design that could allow a hacker to steal confidential data through power analysis.

3. **Authorized Secured Operation with Detection and Privilege Control:** The overall design must have operational privilege control to monitor the legality of the confidential information read. This also prevents hackers from using fault injection to crash the system to control or obtain important information during operation.

Therefore, a qualified HRoT requires a comprehensive anti-tampering design and a complete security policy to protect the entire system. For more information on anti-tampering designs, see tamper-proofing.

Having a credible third-party certification laboratory to evaluate the anti-tampering design's effectiveness is also important. The evaluations will determine the anti-tampering design’s ability to reduce hacking risks and enhance the operational security of the chip. These audits are typically conducted using a white-box setup and physical chip to crack and evaluate risks for the overall design and confidential data protection from component, circuit, and functional design perspectives. After passing the security risk assessment, a security certification lab will issue a security report or certificate. For more information on third-party certification laboratories, please see PSA.

PUFrt enhances the design protecting HRoT by adopting chip fingerprint

PUFrt is PUFsecurity's new hardware root of trust IP, which integrates native chip fingerprint and true random number generator with secure OTP. PUFrt also combines the static random number from the PUF with the dynamic random number from TRNG to protect the whole design. The digital circuit function (soft macro) and the analog circuit design (hard macro) enable the anti-attack design to perform against invasive, non-invasive, and semi-invasive attacks. PUFrt's anti-tampering design has passed the white-box analysis conducted by Riscure and is adopted by FPGA, AIOT, Vertical and Military customers. The relevant anti-tampering technology features are categorized according to the three protection aspects mentioned in the previous section.

Protective design for secure data storage: Secure storage requires both digital design and analog storage blocks to resist attacks. In addition to the NVM components’ inherited security, a circuit design with cryptographic obfuscation and a circuit layout that resists reverse engineering is required.

1. **Secure Storage Components and Layout:** Anti-Fuse OTP is inherently resistant to SEM and TEM probes.
2. **Runtime data encryption and obfuscation:** Using the unique static random number of each chip's built-in fingerprint to XIP (Execution-In- Place) encrypt data in real-time stored into OTP.
3. **Secure layout and top metal shielding:** Multi-level security deployment and top metal shielding effectively prevent any possibility of invasive and non-invasive probes.

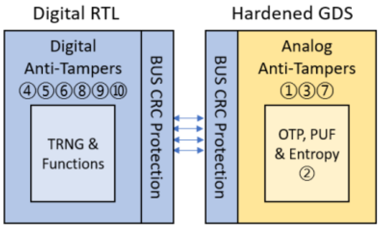
Providing a trusted and secure operating environment: The HRoT design requires a separate security circuit design and other designs to build a complete security environment.

1. **Post-Masking Design:** Helps avoid a Replay Attack by limiting the number of times the hardware reads the action.
2. **Security Privilege Management:** Realizes complete privilege settings by using the word lock, NA or zeroization implemented by the security OTP and combining them with the security field settings (secure/non-secure) in APB.
3. **Health Check:** Performs self-check circuit and algorithm to confirm whether the entire operating environment, including the circuit, static or dynamic random number generation circuit or output quality is normal.

Provide secure operation with attack detection and privilege control: Additional auxiliary detection circuits can monitor and protect the normal operation of the entire module.

1. **Resistance to Voltage and Power Detection:** Analog voltage regulator circuits and comparators detect abnormal voltage behavior and increase the power analysis difficulty.
2. **Dynamic random readout:** Dynamic random numbers randomizes the operation to prevent Addressing and Fault Injection attacks.
3. **BUS protection:** HRoT operation mode and addressing uses CRC (Cyclic Redundancy Check) to prevent hackers from arbitrarily changing input values.
4. **Resistance to Fault Injection:** CRC protects analog read path and register from malicious attacks such as entering incorrect values for output.

Figure 1 shows the security design architecture of PUFrt, including the digital (blue block) and the analog (yellow block) anti-tampering design. The table on the right lists each anti-tampering design for different types of attacks (invasive, semi-invasive and non-invasive).



Types	PUFrt Security Design Features	
Invasive	Analog	Intrinsically Physical Security ①
	Digital	Real time encryption using PUF ②
Semi-invasive	Analog	Secure-oriented Layout ③
	Digital	Output Data Fault Detection ⑧⑨⑩
Non-invasive	Analog	Power Detection, Unified Read/Write Power ⑦
	Digital	Access Privilege, Post-masking, Zeroization, BUS protection, Register protection ④⑤⑥⑨⑩

Figure 1. PUFrt architecture and anti-tampering designs for different attack types

Conclusions

The hardware root of trust is the cornerstone of secure operation for the entire chip. In addition to providing the identity, keys, and entropy source required for secure operation, it must also be designed to resist various invasion attacks to protect the chip's trust base from theft and ensure the security of chip operation. PUFrt with built-in anti-tampering design effectively meets the protection requirements of a HRoT for secure storage, secure environment, and secure operation and further ensures the security of chip operation and system application services.

PUFsecurity

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

Tel: +886-3-560-1010
www.pufsecurity.com