2. Enhancing the security of SCU chip and Enhancing the system security with SCU

A
Creation & Confirmation

SCU : Secure Cryptographic Unit

AFFILIATION: Electronic Commerce Security Technology Research Association (ECSEC TRA), Yokohama National University (YNU), Tokyo University, Kobe University, Tohoku University, Nara Institute of Science and Technology (NAIST)

This technology detects hardware Trojans mounted on PCB during the manufacturing process of the device and after it is shipped. It then ensures the hardware security as the root of trust.

Technical Features

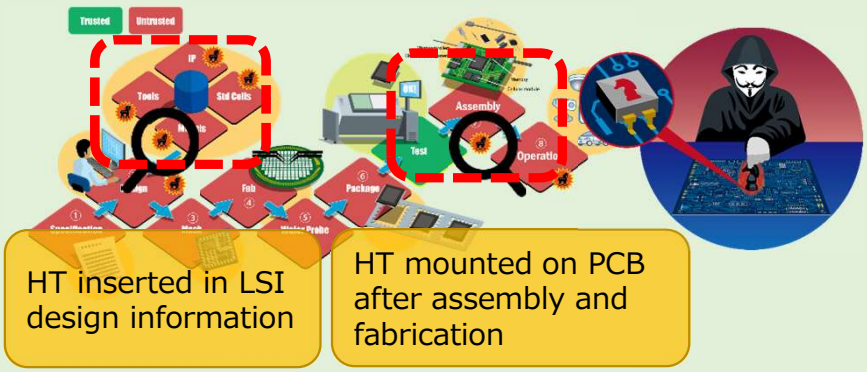
Hardware Trojan detection methods

We are developing detection methods of hardware Trojan mounted on the PCB board after the manufacturing process and fabrication. Based on this, we will secure hardware security as the root of trust.

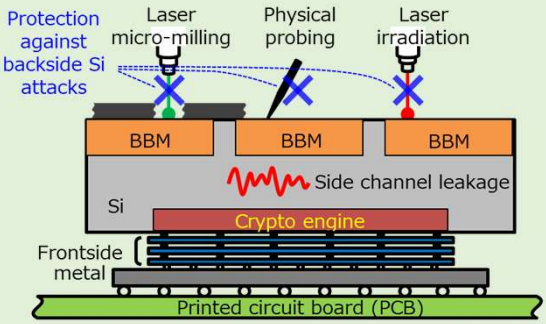
Formal verification methods for hardware Trojan-free IC design

We are integrating hardware logical description verification methods for IP cores and formal verification used for software security. Based on this, we will build fundamental theories that guarantee hardware Trojan-free IC design.

Hardware Trojan (HT) threats in supply chains



Secure packaging technologies



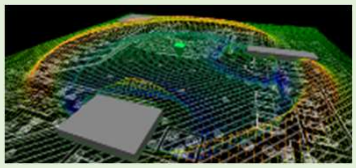
Backside buried metal (BBM) packaging technology for advanced attack protections and supply chain trusts

Formal verification methods

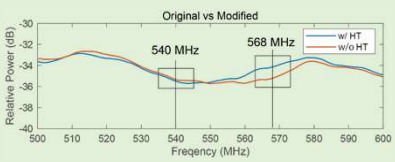
Assuming that HT is installed in IP purchased from a third party when designing a semiconductor chip, we are developing a theory to detect HT inserted into IP using formal verification methods.

Electrical detection methods

Time-domain detection



Frequency-domain detection



We are developing methods of measuring the electrical variations in the ICs and PCBs using the active sensor inside the SCU and detecting the mounted position of HTs based on the measurement information.

November 2020