【Grant-in-Aid for Scientific Research (S)】

Development Framework of VLSI Circuits and Systems Free from Hardware Trojans

Principal Investigator	Kobe University, Graduate School of Science, Technology and Innovation, Professor NAGATA Makoto　　Researcher Number:40274138
Project Information	Project Number : 22H04999　　Project Period (FY) : 2022-2026 Keywords : Semiconductor, Supply chain, Hardware security, Cryptography

Purpose and Background of the Research

●Outline of the Research

"Counterfeit electronic components" become widely concerned as a security problem of authenticity under threats. The deception of semiconductor integrated circuit (IC) chips could specially compromise the functionality and performance of information and communication technology (ICT) equipment. The detection of fake IC chips, and the prevention of fake IC chips to be assembled, are necessary techniques toward the security and safety of trustworthy electronics, and their technology developments will be a key challenge to mitigate such threats.

In this research, the detection, elimination and verification techniques will be pursued on Hardware Trojan (HT) that will bring about undesired behaviors to compromise the security of an IC chip. The goal is universal VLSI design methodologies to logically and electronically prove the absence of HTs.

Our challenges will not stay simply in the protection of HTs in VLSI manufacturing, while pursue HT-free design and development frameworks of VLSI circuits and systems with mathematical and electrical approaches. A design platform for HT-free VLSI circuits and systems (Fig. 1) will be established through the four exploration items that are defined in the figure.

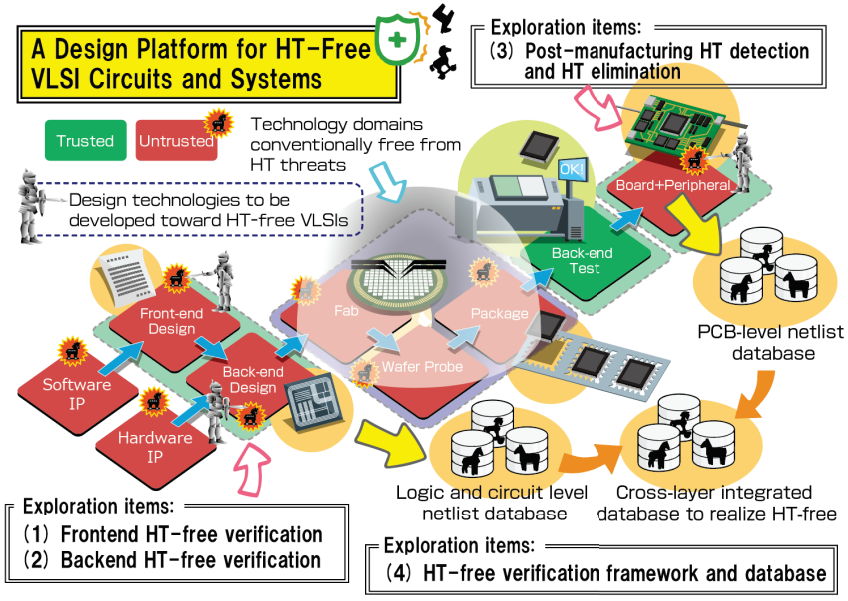

Figure 1. Research concepts of the design platform for HT-free VLSI circuits and systems

●Features of the Research

Hardware Trojans have been so far primarily discussed in the manufacturing phase of an IC chip. In contrast, our research envisions the whole process of VLSI developments, constructs HT-free design methodologies and detection schemes, and produces pseudo HT verification data as a public reference. The scheme includes the detection and prevention of malicious HT insertions in the frontend VLSI design, in the backend VLSI design, and throughout post manufacturing VLSI systems assembly. It will also be challenged not to postulate the use of so called golden wafers as the base reference in HT-free verification.

●Construction of the Research Team

To accomplish the systematic developments of this research toward cross-layer HT-free technologies, our research team involves the experts in semiconductor devices and integrated circuits[1], security and cryptography[2], and electromagnetics and electromagnetic compatibility[3]. (PI: [1]Kobe University, Co-PI: [2]Tohoku University, Co-PI: [3]NAIST.)

Expected Research Achievements

●Goals of the Research

"Hardware Trojans that bring about unwanted and untrustworthy behaviors" will be theoretically elucidated and prevented through the systematic approaches with HT detection schemes and HT-free design methodologies. Our research outcomes will contribute to the exclusion and deterrence of HTs and to evolve the security and safety for a smarter society. The items will be integrated in the design platform of HT-free VLSI circuits and systems (Fig. 2) and publicly shared through academic societies and industrial partnerships. The research impacts can be conceived as follows.

1. HT-based incidents will be proactively suppressed.
2. AI based Intelligent systems will be protected from misoperation led by HTs.
3. VLSI systems will be extremely reinforced for their reliability and safety in design, manufacturing and applications, which also promote further deployments.

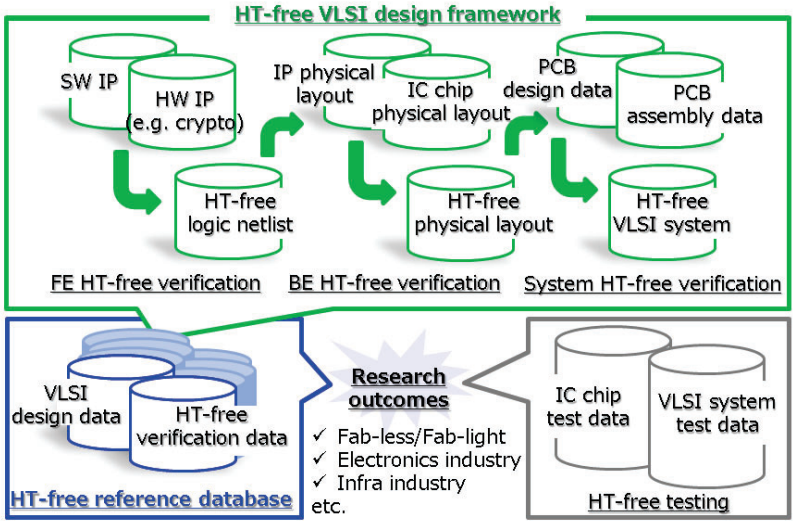

Figure 2. Conceptual image of HT-free VLSI design platform to be developed.

Homepage Address, etc.	Homepage of PI : https://www.edu.kobe-u.ac.jp/stin-secafy/en