公益財団法人 セコム科学技術振興財団
研究成果報告書

研究課題名

高安全・高信頼な情報通信のためのトロイフリーLSI システム設計・検証技術の開発

Development of Trojan-free LSI system design and verification technology for highly secure and reliable information communication

研究期間

平成 30 年 10 月 ～ 令和 4 年 9 月

報告年月

令和 4 年 12 月

研究代表者
東北大学　電気通信研究所　教授
本間　尚文

Professor, Research Institute of Electrical Communication, Tohoku University
Naofumi Homma

Abstract

This research aimed to establish a systematic LSI system design methodology that can detect and eliminate advanced and diverse Hardware Trojans (HTs), whose threat has been pointed out in recent years. More concretely, assuming that the possibility of HT contamination in LSI manufacturing is low, we promoted research and development of fundamental technologies against the following three threats: (1) HT insertion via software IP cores in Front-End (FE) design, where the basic design of circuit functions is performed from the design specification, (2) HT insertion via hardware IP cores in Back-End (BE) design, where the circuit layout design is performed from the circuit description in HDL code, and (3) HT insertion into printed circuit boards during and after system implementation.

As the HT detection technology in FE design, we have developed an HT detection method based on a formal description based on ZDD (Zero-suppressed Binary Decision Diagram) that can represent circuit specifications and circuit descriptions (HDL codes), and its effectiveness was demonstrated by applying it to the international standard cipher AES (Advanced Encryption Standard) hardware core. In this method, the (simultaneous) algebraic equations obtained from the design specifications and the target hardware HDL code are converted into the formal description, their equivalence is verified by checking between them. We showed that all HTs that involve functional modifications such as changing variables and extra functions in practical hardware could be detected in a realistic time.

As the HT detection technology during BE design, we have targeted the HT inserted into the transistor-level physical layout (GDS) generated by the logic cell library of the foundry and the hardware IP core of the third party, and developed a technology that electrically guarantees HT-free in BE design by integrating pre-manufacturing verification by simulation and post-manufacturing verification by wafer level test. In the developed method, we first correlate the physical features of circuits in HDL and GDS, which have different levels of abstraction, by simulation under a multi-test scenario, and obtain their sensitivities to design falsification. Then, we perform post-manufacturing verification by matching evaluation with measurement data from wafer-level testing.

As the HT detection technology in system implementation, we have developed a technology that makes it difficult to insert HT during system design by detecting wiring layouts that may contain HT and element layouts that may be used for HT. In particular, we classified the HTs inserted at the system level according to their functions, and clarified the circuit configuration for realizing each HT. With this knowledge, we then extracted layout patterns for substrates and peripheral elements that make it easy to install HT, and determined the possibility that HT could be implemented based on system configuration data such as LSI layout data and input/output pin assignments. We showed the layout and element placement that could potentially behave as HT, and the suppression method.

The above technologies developed in this research eliminate and/or suppress the possibility of HT contamination significantly. Appropriate combination of these technologies can serve as a foundation for preventing incidents caused by HT. In addition, the developed technology can also be a core technology to prevent malfunctions by HT in embedded systems equipped with AI in the future.