Smart Card Vulnerability due to LSI Test Design and Its Countermeasures

Nozomu Togawa
Professor, Faculty of Science and Engineering
Waseda University

Summary

This research focuses on a scan-path test, one of the design-for-test techniques for LSI design and practically demonstrates that we can retrieve a “secret key” by using it from a public-key cryptosystem as well as from a symmetric-key cryptosystem. After that, we develop its countermeasure techniques against them.

Firstly, we demonstrate that AES cryptosystem has real scan vulnerability when it is implemented on an FPGA prototype system. In addition, we pick up a public-key cryptosystem, RSA cryptosystem (Rivest-Sharmir-Adelman cryptosystem) and demonstrate that it also has scan vulnerability theoretically. After that, we demonstrate that RSA cryptosystem has real scan vulnerability when it is implemented on an FPGA prototype system. Overall, our first goal is that we reveal that both a symmetric-key cryptosystem and a public-key cryptosystem have real scan vulnerability on FPGA platforms due to LSI test design.

Secondly, we fabricate an IC chip on a symmetric-key cryptosystem and demonstrate that the real IC chip also has scan vulnerability due to LSI test design. Based on this result, we theoretically propose a countermeasure against scan vulnerability on a symmetric-key cryptosystem and demonstrate it on an FPGA prototype system. Overall, our second goal is that we reveal that a symmetric-key cryptosystem fabricated on a real chip also has scan vulnerability and propose an efficient counter measure against it.

Thirdly, we fabricate an IC chip on a public-key cryptosystem and demonstrate that the real IC chip also has scan vulnerability due to LSI test design. Based on this result, we theoretically propose a countermeasure against scan vulnerability on a public-key cryptosystem and demonstrate it on an FPGA prototype system. Overall, our third goal is that we reveal that a public-key cryptosystem fabricated on a real chip also has scan vulnerability and propose an efficient counter measure against it.

Finally, we fabricate IC chips which realize a symmetric-key cryptosystem and a public-key cryptosystem against scan vulnerability and demonstrate that these fabricated chips no longer have scan vulnerability. Our fourth goal is that we implement countermeasures against scan vulnerability for both a symmetric-key cryptosystem and a public-key cryptosystem and demonstrate that we no longer face scan vulnerability using the proposed counter measure techniques.

In summary, we develop effective countermeasures against scan-vulnerable smart cards and realize secure and safe smart cards.