GERMANY/HONG KONG JOINT RESEARCH SCHEME
THE PROJECT REPORT
(for Project Completion)

Project Number: G_HK015/11

Title

Side-Channel Resistance of Secure Processor Architecture 運用側信道攻擊和保護的安全處理器架構

Particulars

	Hong Kong team	German team
Name of Project Co-ordinator (with title)	Dr. Ray C.C. Cheung	Prof. Dr.-Ing. Sorin A. Huss
Name of Co-Investigator (if any)		
Institution or Institutional affiliation	√ CityU; ☐ CUHK; ☐ HKBU; ☐ HKIEd; ☐ HKU; ☐ HKUST; ☐ LU; ☐ PolyU	☐ University of _____ ☐ Others: Technische Universität Darmstadt, CASED
Other project team members (if any)		

Funding Period

	1st year	2nd year (if applicable)
Start Date	1/1/2012	1/1/2013
Completion Date	31/12/2012	31/12/2013

Objective(s) as per original application

1. Develop system models, analysis techniques, and algorithms to systematically verify the influence of different side-channel attacks on FPGA-based secure processor architecture.
2. Investigate timing attack and power monitoring attack techniques to analyze the internal data such as the cache, memory structure, and interconnect models on the secure processor.
3. Develop design and analysis techniques for modern memory technologies in secure processor platform, with the goal of improving the security level of those embedded platforms.

Details of Report [Please attach relevant document(s)]

i) Outline of proposed research and results obtained

Due to the natural parallelism and the speed enhancement, the Residue Number System (RNS) has been introduced as a foundation for the execution of the modular multiplications, which is the core computational component for the secure processor, in public-key cryptography. In this work, we examine the secure performance of RNS under side-channel attacks, expose the vulnerabilities, and propose efficient countermeasures. The presented methods improve the resistance against side-channel attacks without great area overhead or loss of speed performance, and are compatible to other countermeasures on both the logic level and the algorithm level. We prototype the elaborated methods on an FPGA and demonstrate that the implementation results confirm the efficiency of the advocated countermeasures. Specifically, the key contributions of this work are:

1) Side-Channel Attack (SCA) vulnerabilities are examined for the RNS-based modular multiplier and second order attacks are conceived for cryptographic design using Leakage Resistant Arithmetic (LRA).
2) Several low-overhead countermeasures are proposed against various power analysis attacks, which can also be embodied independently to satisfy different security requirements.
3) In-depth experiments on implemented multipliers are performed in order to demonstrate the efficiency of the proposed methods.

ii) Significance of research results

As security breaches escalate, secure processors have become increasingly important for trustworthy computing. Residue Number System (RNS) represents a large integer by a batch of small integers, and the computation in RNS is distributed into several independent rings with small sizes. Due to this nature, RNS is proposed to perform modular arithmetic, and parallel architectures are available to accelerate the computation, which is highly suitable for secure processor computation. In this project, we research and analyse the side-channel attack behaviour RNS modular arithmetic. We also implement the architectural design and provide the efficient countermeasures on FPGA platform for system validation. The experimental setup can be used to further research in this hot area.

iii) Research output

We have produced one research paper, Gavin Xiaoxu Yao, Marc Stottinger, Ray C.C. Cheung, Sorin A. Huss, "Side-Channel Attacks and Efficient Countermeasures on Residue Number System Multipliers", submitted to Journal of Cryptographic Engineering. Currently this paper is under its final review process.

iv) Potential for or impact on further research collaboration

We are currently extending this research work for covering wider side-channel attack behaviour, such as using the Electromagnetic (EM) trace. Among side-channel attacks some exploit the timing behavior of IC, while others exploit the power consumption or the EM emissions. EM side channel efficiency is due to the inner properties of EM emissions. Their ability to propagate through different materials is the most striking one. Indeed, it allows attackers targeting the bounded hardware area integrating the crypto-module under attack or part of it. For this part, we are currently starting a new research project with a collaborator in France.