Security Technologies for SoCs

Yasuura, Hiroto
System LSI Research Center Kyushu University

Security Technologies for SoCs

Hiroto Yasuura
System LSI Research Center
Kyushu University
Fukuoka, Japan
yasuura@slrc.kyushu-u.ac.jp

Abstract - *Application area of SoC has been spread to various social infrastructures handling "Trust" and "Value" as systems for e-commerce and e-government. New technologies on security are required in design of SoC, for examples, implementations of security cores for cryptography and hash functions, protection of programs and data on SoC from attacking, and secure design/fabrication/test flow for SoC. In this talk, new problems and solutions for secure SoC design are presented. As an example of the security technologies, implementation of QUPID system (Kyushu University Personal ID System) developed by System LSI Research Center of Kyushu University is introduced.*

Keywords: SoC design, security, social infrastructure, authentication, e-money.

1 Introduction

In the last four decades of the 20th century, many information and communication technologies have been developed and also introduced in several social infrastructures, which are supporting our daily lives. Since the information technologies have progressed very rapidly, the basic structure of each social infrastructure, which was mostly designed in the 19th or the beginning of 20th centuries with few information technology, should be redesigned under the assumption of the existence of the advanced information technologies. Based on the high-performance SoCs (System-on-a-Chip) connected by wide-band networks, we can design next generation of social systems, which are directly related with quality of our society including individual rights and national security.

In the design of semiconductor devices, the following technical challenges are discussed and attacked:

(1) Challenges to Physical Barriers: Deep submicron process technology brings out new physical phenomina to be managed, such as PVT variations, reliability, energy consumption and signal integrity. New design methodology and techniques handling these physical difficulties are big challenges.

(2) Challenges to Logical Complexity: Since the complexity of a system on a chip increases exponentially, sophysticated design and verification techniques for the large and complicated systems are required. System design methodologies, new design platforms and new design criteria are proposed and developed.

(3) Challenges to Social Problems: Since SoC becomes a basic component of the social infrastructure systems such as economic systems, governmental services, and transportation and communication systems, new requirements for SoC in the domain of reliability, dependability, and seculity becomes important. New design and fabrication techniques are requested.

In this paper, the third challenge will be the major topic esspecially security issue of SoC. Since application area of SoC has been spread to various social infrastructures handling "Trust" and "Value" as e-commerce and e-government services, new technologies on security are required in design of SoC, e,g. implementation of security cores for cryptography and hash functions, protection of programs and data on SoC from attacking, and secure design/fabrication/test flow for SoC. New problems and solutions for secure SoC design require development of new technologies. As an example of the security technologies, an implementation of PID system (Personal ID System) developed by System LSI Research Center of Kyushu University is introduced

2 Security and SoC Design

2.1 SoC and Social Information Infrastructure

In the 20th century, many information and communication technologies were developed and introduced in various social infrastructures such as governmental services, economic systems, energy supply systems, transportation systems, and communication systems. SoC technology is now one of the most fundamental information technologies for the social infrastructure as well as network technology and embedded software technology. Since the rapid progress of these information technologies causes the drastic reduction of time and space of information transfer, processing and storage, new scheme of social infrastructure are redesigned under the assumption of the utilization of these information technologies.

The social infrastructure is directly related with human life, properties and privacy. The new social infrastructure requests dependable information technologies with high reliability, high quality and great security. SoC is a physical component of the social infrastructure, which is embedded in personal devices and backborn systems. Since security of the infrastructure is physically supported by SoC, security of SoC directly affects dependability of the infrastructure.

2.2 Trust and Value on SoC

Consider LSI chips in smart cards (IC cards) or advanced cellular phones, various valuable information on "Trust" and "Value" are stored on the LSI chips. Your personal information, biological information for authentication, electric money, information on your credit and/or ATM cards, and your signature are stored in a chip, cost of which is less than only 30US dollars (Figure 1).

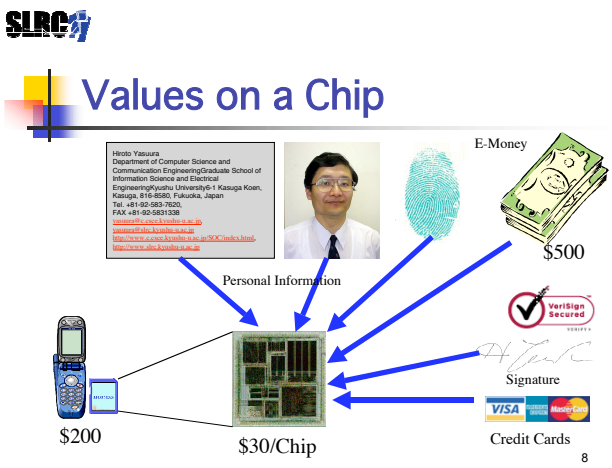

Figure 1. Values and Trusts on a Chip

A user of the device cannot directly see the information of the value and the trust on the chip. Security of the privacy and properties of the user should be protected by security technology of LSI chip and software.

2.3 Social Problems

Several new social problems are leaded by the introduction of SoC in the social systems. Various private moneys like mileage of airlines, points of credit cared and e-cache of transportation systems have been used in our daily lives. Some of them are already kind of money and problems on tax collection and seigniorage (the right of issuing money) become critical. One of the simplest questions is "Is an SoC chip handling e-money a purse or money itself?" If the chip is a purse, we can avoid troublesome of counterfeit and copy of the chip. But, if the chip is a part of money system, we have to consider a new technology to prevent copy of design data, illegal fabrication and illegal issueing.

Similar problems also exist in SoCs for carrying "Trust". Some LSIs have been introduced in credit cards, ATM cards, personal ID cards, driver's licenses, and passports. Technologies for preventing counterfeit are very important as well as protection techniques of the contents (data and programs) on the chips from various attacking.

3 Technical Challenges

3.1 Researches of Security on SoC

Various discussions and researches have been done on the security on SoCs. Many international conferences and symposium on SoC design started new sessions on security issue in these few years. Most of them are concerning with implementation of new functions for security on chips like cryptography and anti-tampering. New algorithms and circuits for cryptographic computation are developed. Protection from side-channel attacks is the hottest topic for anti-tampering.

Other important field on security of SoC is how to design and fabricate the secure SoC. There is various possibility of attacking in the design and fabrication stages of SoC. But, unfortunately, there are very few discussions and researches in this field. In the design stage, protection of the design data is an important problem. Since design environment of SoC includes many tools and computers connected by a network, design data can be stolen through the tools and the network. Designers use automated tools for logic synthesis, scan chain insertion and physical design optimization, but they can't control details of their design. If tool developers try to get design information or to set up traps, it is not difficult to cheat on the SoC designers. In fabrication and test stages, we also have many security holes. Foundry and test engineers can get various design information, which are useful for attack of the chips. They also have opportunity to put chips to black market by extra production or cheating in test process. It may be required a new special design and fabrication flow for SoC handling "Value" and "Trust" in the social information infrastructure.

3.2 Security Core

It is not economically feasible to design and fabricate a whole system using the special flow for security. The reasonable solution is that most part of the system is implemented by ordinal flow and process and a core part for the security is designed and/or processed by the secure flow. The core, called a security core, can be supplied by several ways. The easiest way is that the core is

implemented as pure software. No hardware technique is required but security is not so high. If the core is supplied as an IP block designed by secure design flow and embedded into the system designed by the ordinary flow, security problem of design phase will be partly resolved. Some practical chips for IC cards are adopted this method, but it is not a perfect solution for the threats in the fabrication stage. Another solution is that the security core is designed and fabricated by the secure flow and pasted on the master chip using SiP technology.

New technologies and flows for the secure SoC should be discussed and a standard should be proposed.

3.3 Countermeasure s for Counterfeit

It is important to establish a technology for protection and detection of counterfeit of the secure SoCs. In design and fabrication stages, implementation of particularity is key technology. Special functions and characteristics will be useful for distinction of counterfeit chips. New materials, devices and circuits will be useful for the implementation of the particularity. Development of materials, devices, process technologies, circuits, algorithms and design tools are required (See figure 2). In some sense, we have to make a similar effort to Mint Bureau who has fought against bogus bills.

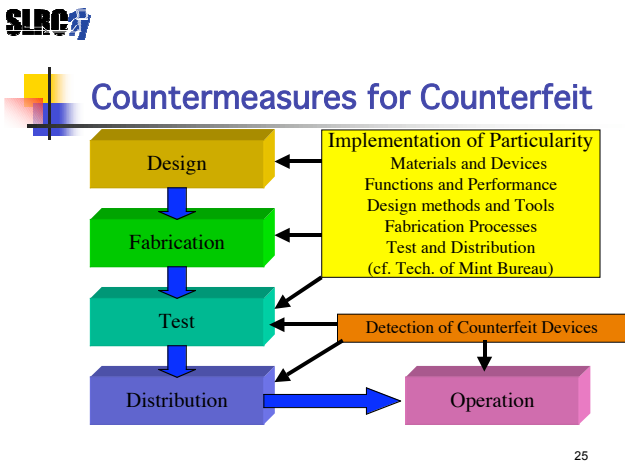

Figure 2. Countermeasures for Counterfeit

In the operation of the systems in the social infrastructures, we need methods to detect counterfeit chips without costly test operations. Figure 4 shows an idea of a detection mechanism. In the deep submicron processes under 90nm, process variation can't be avoidable. According to the process variation, we can implement devices with different characteristics (e.g. delay time, power consumption etc.), which are randomly distributed. If the characteristics can be measured easily, we can use the characteristics as a fingerprint of the chip. Public key cryptosystem is applicable for the detection system. The measured data (fingerprint) in the fabrication stage are encrypted using secret key and stored in the chip. In the operation phase, the characteristics are measured and compared with decrypted data using public key.

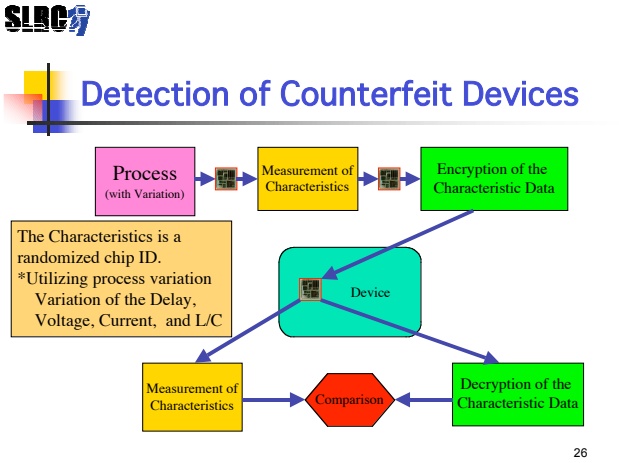

Figure 3. An Example of Detection

4 QUPID

In the realization of e-commerce and e-government, mutual authentication between partners communicating each other through a network is fundamental technology. The authentication system must be bidirectional and have a mechanism that takes the protection of individual privacy into consideration. The system should be easy to understand its fundamental concept and structure. It should have high reliability and ability to recover from damages by attacks and accidents. It is also important that the system reflects the trust and credit relationships among individuals and organizations.

We proposed PID system, which can be implemented in IC cards and mobile phones, for authentication of various social infrastructures [1][2]. The PID system has an extremely simple mechanism and is based on the existing social trust relationship. Individual authentication using PID consists of three kinds of participants– PID Issuers, Users, and Service providers (See Figure 4). Issuers are various kinds of organizations that individuals belong to (Communities, Companies, Schools, Credit card service companies, etc). Issuers are basically assumed to have a resposibility to protect their individual participants. This social trust relationship is the basis for the PID system.

Assume a person A is a member of an organization B, which is the PID issuer in this context. The issuer B examines A's personal identity, and decides if A is deserved to be authenticated or not. When B determines to give the authentication to A with B's responsibility, the

issuer B gives A “a Personal Identifier”, called PID, that is a long bit sequence (ex. one million bits). This sequence is stored in storage media like an LSI on IC card and mobile phone, and issued to A.

When a service provider C, who deal with services to users, want to make an e-commerce service to the members of the organization B, the provider C applies to the issuer B for permission of usage of the PID system issued by B. The issuer B investigates confidence of the provider C whether the services provided by C are beneficial and harmless for the members of B. When B determines that it is beneficial for the members, B provides a part of PID of each member (ex. 256 bits, we call it a sub-PID) to the service provider C. B also notifies the members that the sub-PID of each PID have been given to C. The person A is now a user of the services provided by C. The user A and service provider C mutually authenticate using this sub-PID each other using a technique of 0-knoeleage proof.

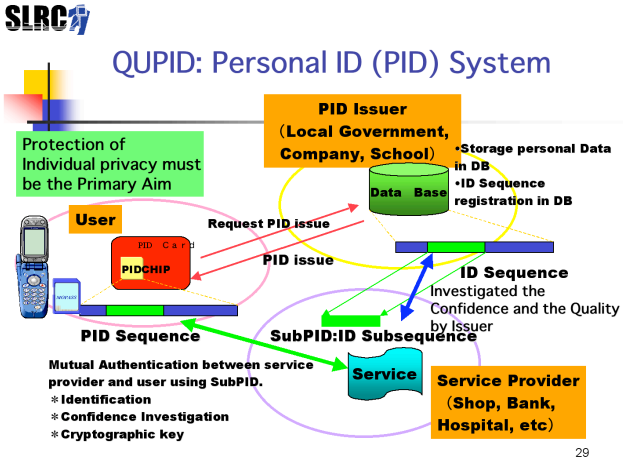

Figure 4. Structure of PID System

It is the most primitive mutual authentication. Distinct secret information, a sub-PID, is assigned to each link of communication between a user and a service provider. If the sub-PID is leaked, the damages are limited only the corresponding link between them. All other links connecting different services to the user and other users to the service are safe (See Figure 5). Users can understand the concept of the mutual authentication easily and intuitively without knowledge of complicated algorithms of authentication protocols.

Kyushu University is now developing a new IT campus with QUPID (Kyu(Q)shu University Personal ID) system based on the PID system. IC cards with QUPID system will be distributed to all students and employee by 2007. Various services on/off campus will be provided through authentication by QUPID. Through the experiments, we will get new problems and solutions for the SoC implementation handling “Value” and “Trust”.

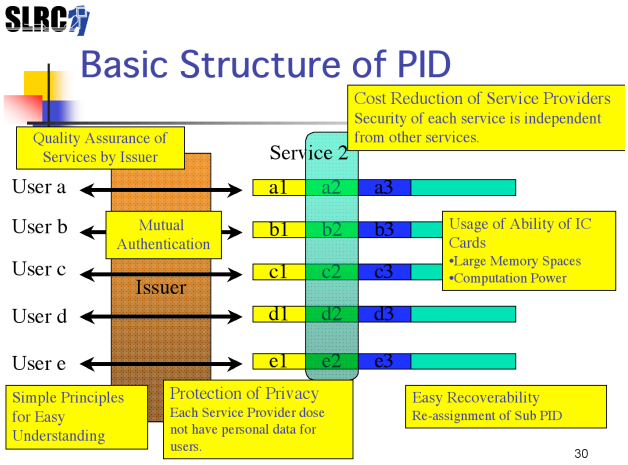

Figure 5. PID and Mutual Authentication

5 Conclusion

Social infrastructure will be a new primary application domain of SoCs. Security technology on silicon chips will play an important role in this field. Comprehensive discussions on social system, software, network, and SoC are requested. The technology will be directly related with safety and stability of our society and national security.

Acknowledgement

This work has been partly supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 and 21 Centuary COE Program of the Ministry of Education, Science, Sports and Culture(MEXT) from 2002 to 2006. We are grateful for their support.

References

[1] H. Yasuura, ``Towards the Digitally Named World - Challenges for New Social Infrastructures based on Information Technologies-", Proc. of Euromicro Symposium on Digital System Design -Architectures, Methods and Tools-(DSD2003), pp.17-22, Sep. 2003.

[2] H. Yasuura, “[Plenary Speech 2p.1]Digitally Named World: Challenges for New Social Infrastructures”, 5th International Symposium on Quality Electronic Design(ISQED 2004), pp.323, March. 2004.

[3] Y. Nohara, S. Inoue, and H. Yasuura, ``Toward unlinkable ID Management for Multi-service Environments", Proc. 3rd Int'l Conf. Pervasive Computing and Communications(PerCom) Workshops, pp.115-119, March 2005.