Security Technologies for SoCs

Yasuura, Hiroto
Faculty of Information Science and Electrical Engineering, Kyushu University | System LSI Research Center

http://hdl.handle.net/2324/9121
Security Technologies for SoCs

Hiroto Yasuura
System LSI Research Center
Kyushu University
yasuura@slrc.kyushu-u.ac.jp
Kasuga Koen 6-1, Kasuga, Fukuoka 816-8580, Japan
http://www.slrc.kyushu-u.ac.jp/index.html
Challenges of SoC

- Challenges to Physical Barriers
  - PTV variability, Reliability, High-Performance, Power Consumption, Interconnect, Clock Distribution, Modeling, Simulation⋯

- Challenges to Logical Complexity

- Challenges to Social Problems
  - Security, Smart Card, Quality, Reliability⋯
IT as a Basis of Social Infrastructure

- In the 20th century, many information and communication technologies were developed and introduced in various social infrastructures.
- Governmental services, economical activities, energy supplies, transportation services and communication services are provided based on the information technology.
Rapid Progress of IT Changed Time Constants

- Time of information transfer and processing has been shortened drastically by IT. ($10^{-6}$-10^{-9}$)
- Basic design of social systems was not supposed the speed-up of information spreading. Time constants of the systems are completely changed and the stability of the systems is not guaranteed.
  - Stock and foreign exchange markets
  - e-commerce, e-government, e-education, ...
Major Problem?

- How to handle Credit, Value and Property on SoC.
- 1,000$ on a 10$ chip.

2,000 years  
Metal Coins  
(before BC 10th C)  
- Value: Metal  
- Conservation: Metal  
the law of the indestructibility of matter

1,000 years  
Paper Bill (10th C)  
- Value: Printed information guaranteed by governments and/or banks.  
- Conservation: Paper

Electric Money  
(21st C)  
- Value: Digital Information.  
- Conservation: Digital Information?
Social Problems

- Diversification of Issuers of Money
  - Private Money
    - Mileage of Airlines, Points of Credit Cards, etc.
  - Foreign currency (US $, Euro, Yen, etc.)

- Influences upon National Fiscal System
  - Tax Collection
    - Tax for Electric Commerce
    - Tax for Trade of Private Money
    - How to Trap and Verify Them

- New Social Systems and Technologies for Them
  - Information Technology for Value and Credit
  - Private Property Management
  - New Systems for Value Circulation

- Security and Trustworthiness Technologies
  - Crime Prevention
  - Copy Management of the Value and Credit
Technological Challenges

- What are the basic Technologies for treating “Credit, Value and Property”? 
  - Authentication
    - How to authenticate your business partner
    - How to authenticate yourself
  - Value Assurance
    - How to assure the value trading
    - How to believe security of your property on IT
Researched on Security in SoC

- Cryptography
  - Public key system (RSA, Elliptic Curve etc.)
  - Design and Analysis
  - Applications and Standardization
- Secure Information System
  - Protection from attacks (Fire walls, Network structure)
- Security in Communication
  - Secure Protocols
- Security for Software
  - Protections from virus and warms
- Security for Hardware
  - Anti-tampering
  - Side Channel Attack
Possible Attacks for LSIs

- **What is attacked?**
  - Information on LSIs
  - Circuit and system in LSIs
  - Social systems and/or personal properties

- **When LSIs are attacked?**
  - In design and fabrication stages
  - In test stage
  - During operation

- **Why are LSIs attacked?**
  - Get some benefit (Silent and invisible attack)
  - Destroy systems (Terrorism)
Technical Problems in SoC

- New functions in LSIs for security
  - Cryptography, Authentication, Watermark
  - Security Core IP
  - Resistance to attacking and tampering
- Design, verification and test techniques
  - Secure Design and Test scheme
  - Performance, cost and power consumption for security
- Fabrication
  - Secure Fabrication
  - New devices and/or materials
  - Embedded security core
- Operation and Distribution
  - Prevention and detection
  - Recovery
  - Wireless communication
  - Human and social factors
Security Cores

- Core for Security Functions
  - Authentication and Value Assurance
  - Cryptography: Algorithms and Key information
  - Anti-tampering
- How to implement
  - Software: processors and memories
  - IP: Secure design flow
  - Chip: SiP (System in Package)
- How to design and fabricate
  - Design tools
  - Fabrication lines
  - Test methods
- Interfaces and Protocols to the security cores
Design Problems of SoC

- Power and Performance
  - Extra computation for security
- Test
  - DFT introduces some risks
  - Special test methods
- Anti-Tampering technology
  - Prevent from side channel attacks
- Anti-Counterfeit technology
  - Unique ID for a chip
Threat of Counterfeit

Examples

- Counterfeit note (e-money)
- Illegal ROM for Pachinco
- Counterfeit of certifications (passports, drivers licenses and credit cards)

Is the SoC a purse or money?
Countermeasures for Counterfeit

Implementation of Particularity
- Materials and Devices
- Functions and Performance
- Design methods and Tools
- Fabrication Processes
- Test and Distribution
  (cf. Tech. of Mint Bureau)

Detection of Counterfeit Devices

Operation
Detection of Counterfeit Devices

Process (with Variation) → Measurement of Characteristics → Encryption of the Characteristic Data

The Characteristics is a randomized chip ID. *Utilizing process variation Variation of the Delay, Voltage, Current, and L/C

Device

Measurement of Characteristics → Comparison → Decryption of the Characteristic Data
Experiments for **New Social Information Infrastructures** in moderately unrestricted society

- Campus Card with QuPID
  - IDs for students, staff with multiple usage
  - Keys to buildings, facilities, and parking
  - Access control to campus information
  - E-money
  - E-administration
  - Services to Students
  - NTT, Panasonic etc.
- RFID Tags to Equipments
  - Library
  - Equipments management
  - Hazard identification
  - Moving to the new campus

New campus of Kyushu University
Open in 2005.
QUPID: Personal ID (PID) System

Protection of Individual privacy must be the Primary Aim

User

PID Card

PID Issue
(Local Government, Company, School)

Data Base

• Storage personal Data in DB
• ID Sequence registration in DB

PID Issue

PID sequence

SubPID:ID Subsequence

Service Provider
(Shop, Bank, Hospital, etc)

Service

PID Sequence

Request PID issue

Mutual Authentication between service provider and user using SubPID.
* Identification
* Confidence Investigation
* Cryptographic key

ID Sequence

Investigated the Confidence and the Quality by Issuer
Basic Structure of PID

User a
User b
User c
User d
User e

Quality Assurance of Services by Issuer

Mutual Authentication

Issuer

Service 2

a1 a3
b1 b3
c1 c3
d1 d3
e1 e3

Cost Reduction of Service Providers
Security of each service is independent from other services.

Usage of Ability of IC Cards
• Large Memory Spaces
• Computation Power

Protection of Privacy
Each Service Provider does not have personal data for users.

Easy Recoverability
Re-assignment of Sub PID

Simple Principles for Easy Understanding

Simple Principles for Easy Understanding
Technical Challenges

- Mutual authentication for multiple services
- Multiple application system
  - Services on campus using PID system
  - Trial of e-money and e-commerce
  - PID on IC Cards, Mobile Phones and Back-end Systems
- LSI Architecture for Security and Privacy Protection
  - Resistance to tampering
  - Anti-counterfeit technology
  - Test and verification techniques
- Low Power RF and Cryptographic Computation
  - Hash and Cryptographic functions
  - Secure RF communications
- New Business Models
  - Fukuoka-Card (Local money and new services)
Conclusion

- New Application Area of LSI Technologies
  - Requirement of Standard Technologies
  - Collaboration with Communication and Software
  - Big Chance of New Business
  - Authentication, e-money and e-commerce

- New Social Infrastructure
  - Infrastructure of New Economic Systems
  - Basic Technology for Ubiquitous Computing Society

- National Security
  - Money System and Tax Collection
  - Secure and Safe Society
  - New Social Fabrics
