진리 · 긍지 · 봉사

The sprit of Truth, Pride, and Service

Mobile Network Security Technology Research Center

Kyungpook National University

MSRC

June 2006

History

June, 2000	Applied for “the University Information and Telecommunication Research Center (ITRC) Promotion and Support Project” sponsored by the Ministry of Information and Communication.
August, 2000	Selected as an information and telecommunication research center (ITRC) in the network. Named to “Mobile Network Security Technology Research Center (MSRC)”
July, 2002	Presented the 2nd research report to KIPA (Korean IT Industry Promotion Agency) Evaluated and approved as a competitive ITRC
September, 2004	Selected as 2nd stage ITRC and extension of the period of project

Organization of this center

Director of the center (Prof. Moon)

Project part 1 (KNU : Prof. Moon)	Project part 2 (Postech : Prof. Lee)	Project part 3 (KNU : Prof. Kim)
Hybrid physical attack and countermeasures development for cryptographic algorithm	Development of cryptographic mechanism for ad-hoc network and sensor network	Development of security platform for interlocking with heterogeneous devices in ubiquitous network
Development of key management authentication protocol in ubiquitous network	Research for an ID based cryptosystem in small group	Study of SCTP and development of security technology for mobile terminals
Study of link cryptosystem with low-power and high-speed for sensor network	Development of security foundation in ubiquitous environment	Study of link cryptosystem with low-power and high-speed for sensor network

International, domestic and Industrial Collaboration

Research Facilities

- 9 rooms with 471.24m^2 in Kyungpook National University
- All rooms are equipped with 100Mbps LAN
- World-level environment for experiment

Participants

Participant		Number (per year)		
		2000.8 ~ 2003.7	2003.8 ~2004.7	2004.9 ~ now
Professor		11	12	11
Graduate student	MS	34	39	29
	Ph.D.	19	25	19
Total		64	76	59

Research Results

		2000. 8 ~ 2003. 7	2004. 9 ~ now
Paper	SCI	85	82
	Non SCI	66	33
	Domestic	336	59
Patent	Applied	19(4)	10
	Registered (international)	18(1)	8(2)
International Collaboration		4 nations	5 nations
Industrial Collaboration		14 company	11 company

International Research - 1

- **Side-Channel Attack**
  - **LCIS, NCU(National Central University), Taiwan**
    - “Differential Power Analysis on Block Cipher ARIA”, HPCC 2005
    - “Power analysis by expoliting chosen message and internal collisions”, Mycrypt 2005
    - “Improvement on Ha-Moon randomized Exponentiation Algorithm”, ICISC 2004
    - “RSA speedup with chinese remainder theorem immune against Hardware Fault Cryptanalysis”, IEEE, Trans. 2003

International Research - 2

- **Stream Cipher (LILI-II)**
  - **ISRI, QUT(Queensland University of Technology), Australia**
    - “Dragon : A Fast Word Based Stream Cipher”, ICISC 2004
    - “Efficient & secure word based ciphers for mobile application”, submitted to SAC 2004 through international collaboration

International Research - 3

- **Digital signature and its applications**
  - **ICSD, IIR (Institute for Infocomm Research), Singapore**
    - “An Improved Double Auction Protocol against Fase Bids”, TrustBus 2005
    - “A Robust Double Auction Protocol based on a Hybrid Trust Model”, ICISS 2005
    - “Security Analysis of Two Signcryption Schemes”, ICS 2004

International Research - 4

- **Security Analysis and Design of Ubiquitous Network Security Protocol**
  - **Xidian Univ. , China**
    - " On the Security of the Authentication Module of Chinese WLAN Standard Implementation Plan", ACNS 2006
    - "Security extension for the Canetti-Krawczyk moddel in identity-based systems", Science in China, Series F

Research Institute Collaboration

- ETRI (Electronics and Telecommunications Research Institute)
  - Analysis of RFID system
- KISA (Korea Information Security Agency)
  - Analysis of Side-channel attack
- NSRI (National Security Research Institute)
  - Hybrid Analysis Attacks
  - USB Interface

Industrial Collaboration

- **Samsung Electronics**
  - Side-channel attack
- **N-LINE SYSTEM**
  - Security solution through user certification (MaGer-PKI)
- **REDGATE**
  - Secure OS
- **CentaVision**
  - Intrusion Control System (FireWall + IPS +QOS)
- **JEMI InterMediaTech**
  - Java Engineering for Multimedia
- **NADSOFT**
  - Online-right protection solution
- **DigitalHomenet**
  - Home network & Java application

Main publications (Recent two years)

Project part 1

[Development of air-interface access security in ubiquitous network]

- **IEICE Trans. Fundamental (2006)**
  - "An Attack on the Identity based Key Agreement Protocols in Multiple PKG Environment"
- **MADNES 2005**
  - "How to Generate Universally Verifiable Signatures in Ad-Hoc Networks"
- **HPCC 2005**
  - "Differential Power Analysis on Block Cipher ARIA"
  - "A CRT-Based RSA Countermeasure against Physical Cryptanalysis"
- **ICISC 2004**
  - "Improvement on Ha-Moon Randomized Exponentiation Algorithm"
  - "Dragon : A Fast Word Based Stream Cipher"
- **ISC 2004**
  - "Security Analysis of Two Signcryption Schemes"

Main publications (Recent two years)

Project part 2
[Development network security technology for ubiquitous network]

- **ISPEC 2006**
  - "Efficient Public Key Broadcast Encryption using Identifier of Receivers"
- **Applied Mathematics and Computation (2005)**
  - "Supersingular hyperelliptic curves of genus 2 over finite fields"
  - "Efficient identity- based authenticated key agreement protocol from pairings"
- **ICISC 2004**
  - "Separable Implicit Certificate Revocation"
  - "New Power Analysis on the Ha-Moon Algorithm and the MIST algorithm"
- **ACISP 2004**
  - "Fast algorithms for securing elliptic scalar multiplication against side-channel attacks"
  - "Generic Construction of Certificateless Signature"
  - "TTS without Revocation Capability Secure against CCA2"

Main publications (Recent two years)

Project part 3
[Development of mobile terminal security management in ubiquitous network]

- **IEICE Trans. Communications (2006)**
  - "Cryptanalysis of Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks"
- **IEE Proceeding- Circuits, Devices and Systems (2005)**
  - "Low-power exponent architecture in finite fields"
  - "Digital-serial AB2 Systolic architecture in GF (2^M)"
- **EUC 2005**
  - "A Study on fast JCVM with new transaction mechanism and Caching-Buffer based on Java Card Objects with a high"
  - "The research on how to reduce the number of EEPROM writing to improve speed of Java Card"
- **ICIC 2005**
  - "Performance Comparison of SCTP and TCP over Linux Platform"
  - "Analysis of SCTP Handover by Movement Patterns"