Yong Ho Hwang

Department of Computer Science
Johns Hopkins University
3400 N. Charles Street
Baltimore, MD, 21218

yhhwang@cs.jhu.edu
http://www.cs.jhu.edu/~yhhwang
Phone: +1 443 564 9375
Fax: +1 410 516 8457

Education

POSTECH Pohang, Republic of Korea. Mar. 2001 - Feb. 2006
Ph.D. in Electronic and Electrical Engineering
- Thesis title: Multi-User Oriented Cryptosystems
- Advisor: Pil Joong Lee (The president of KIISC in 2004)
  * KIISC: Korea Institute of Information Security and Cryptology.

HongIk University Seoul, Republic of Korea. Mar. 1995 - Feb. 2001
B.S. in Electronic Engineering, February 2001. GPA 4.06/4.50 (99 %)
* Military Service, ROK army (Jul. 1996 - Sep. 1998)

Career

Post-doctoral Researcher Jul. 2006 - Present
Department of Computer Science, The Johns Hopkins University.
Advisor: Prof. Giuseppe Ateniese (Security and Privacy Applied Research Lab.)

Post-doctoral Researcher Mar. 2006 - May. 2006
Department of Electronic and Electrical Engineering, POSTECH.
Advisor: Prof. Pil Joong Lee (Information Security Lab.)

Research Assistant Mar. 2001 - Feb. 2006
Information Security Lab., POSTECH.

Teaching Assistant Fall of 2001
Electronic and Electrical Engineering, POSTECH.

Honors and Awards

Best paper award at the 2005 Conference on Information Security and Cryptology (CISC'05)
Paper title: Security analysis of group key exchange protocols against insider adversaries

National scholarship for an engineering researcher by Korea Research Foundation Fall of 2005

Research Interests

My research interests are in the categories of network security and applied cryptography. I am particularly interested in design and analysis of efficient and provably secure cryptographic algorithms for the purpose of building secure systems. Current research topics include:

- Broadcast Encryption and Traitor Tracing Scheme
  - Revocation scheme for stateless receivers
  - Public key traitor tracing scheme secure against CCA2

- Authentication and Key Exchange Protocol
  - Protocols for authentication and for the generation of cryptographically-strong keys among a set of parties in insecure network
- Pairing-based Cryptosystems and Protocols
  - ID-based cryptosystems and protocols
  - Certificate-based and certificateless public key encryptions
  - Public key systems with special properties by the bilinear map
- Network Security Applications
  - Fair exchange protocols (certified e-mail system, non-repudiation protocol, etc)
  - Keyword search on encrypted data
- Design of Secure Protocols for Ubiquitous Computing
  - Security and privacy in Radio-Frequency Identification Devices
  - Protocols for distributive or collaborative environments as ad-hoc network

Publications

International Journals or Proceedings (in English)

1. Yong Ho Hwang and Pil Joong Lee
   "Efficient Broadcast Encryption Scheme with Log-Key Storage"
   Financial Cryptography and Data Security - FC 2006, LNCS Vol. 4107, pp.281-295, 2006.

2. Jung Wook Lee, Yong Ho Hwang, and Pil Joong Lee
   "Efficient Public Key Broadcast Encryption using Identifier of Receivers"
   Information Security Practice and Experience Conference - ISPEC 2006, LNCS Vol. 3903, pp.153-164, 2006.

3. Yong Ho Hwang, Dae Hyun Yum, and Pil Joong Lee
   "Timed-Release Encryption with Pre-open Capability and Its application to Certified E-mail System" *Information Security - ISC 2005*, LNCS Vol. 3650, pp.344-358, 2005.

4. Chong Hee Kim, Yong Ho Hwang, and Pil Joong Lee
   "Practical Pay-TV Scheme using Traitor Tracing Scheme for Multiple Channels"
   Information Security Applications - WISA 2004, LNCS Vol. 3325, pp.265-279, 2004.

5. Sung Ho Yoo, Yong Ho Hwang, and Pil Joong Lee
   "System for Preventing Counterfeiting of Retail Items using RFID tags"
   The pre-proceeding of WISA 2004, pp.593-604, 2004.

6. Chong Hee Kim, Yong Ho Hwang, and Pil Joong Lee
   "TTS without Revocation Capability Secure against CCA2"
   Information Security and Privacy - ACISP 2004, LNCS Vol. 3108, pp.36-49, 2004.

7. Yong Ho Hwang, Chong Hee Kim, and Pil Joong Lee
   "An Efficient Revocation Scheme for Stateless Receivers"
   Public Key Infrastructure - EuroPKI 2004, LNCS Vol. 3093, pp.322-334, 2004.

8. Yong Ho Hwang, Sang Gyoo Sim, and Pil Joong Lee
   "Bit-Serial Multipliers for Exponentiation and Division in $GF(2^m)$ using Irreducible AOP"
   Computational Science and Its Applications - ICCSA 2004, LNCS Vol. 3043, pp.442-450, 2004.

9. Chong Hee Kim, Yong Ho Hwang, and Pil Joong Lee
"An Efficient Public Key Trace and Revoke Scheme Secure against Adaptive Chosen Ciphertext Attack" *Advances in Cryptology - ASIACRYPT 2003*, LNCS Vol. 2894, pp.359-373, 2003.

10. Yong Ho Hwang, Dae Hyun Yum, and Pil Joong Lee
"EPA: An Efficient Password-based Protocol for Authenticated key exchange"
Information Security and Privacy - ACISP 2003, LNCS Vol. 2727, pp.452-463, 2003.

11. Yong Ho Hwang, Chong Hee Kim, and Pil Joong Lee
"An Efficient Revocation Scheme with Minimal Message Length for Stateless Receivers"
Information Security and Privacy - ACISP 2003, LNCS Vol. 2727, pp.377-386, 2003.

Domestic Journals or Proceedings (in Korean)

- 16 papers written in Korean were presented at Korean domestic conferences or published in Korean journal.

Projects Performed

- Server-Aided Signatures for Low-Power Device — Feb. 2007 - Present
  - Collaborative work with Johns Hopkins Applied Physics Laboratory
- A Study of Ubiquitous Network Security Technology — Aug. 2004 - Jul. 2005
  - Sponsored by Ministry of Information and Communication (of Korea.)
- Research on Suitable Public Key Cryptosystems to Mobile Environment — May. 2004 - Jan. 2005
  - Sponsored by NSRI (National Security Research Institute of Korea.)
- A Study of Mobile Network Security Technology — Aug. 2001 - Jul. 2004
  - Sponsored by Ministry of Information and Communication (of Korea.)
- Research on Group Key Management System — Dec. 2002 - Nov. 2003
  - Sponsored by PIRL (POSTECH Information Research Laboratories)
- Implementation of Elliptic Curve Cryptosystem in ARM7TDMI chips — Jan. 2002 - Jan. 2003
  - Collaborative work with Samsung Electronics Co., Ltd.
- Research on Password-based Key Exchange Protocol — Jul. 2001 - Jun. 2002
  - Sponsored by POSCO
- Fingerprint Identification — Jan. 2001 - Apr. 2001
  - Collaborative work with High-Q Tech

Professional Activities

IACR International Cryptology Conference - ASIACRYPT 2004 Jeju island, Korea.
Secretariat for Program Committee
Chair: Pil Joong Lee
Organized by IACR (International Association for Cryptologic Research)

International Conference on Information Security and Cryptology 2002 Seoul, Korea.
Secretariat for Program Committee
Co-Chairs: Pil Joong Lee and Chae Hoon Lim
Organized by KIISC

Conference on Information Security and Cryptology - CISC 2003 Seoul, Korea.
Secretariat for Program Committee
Co-Chairs: Pil Joong Lee and Heung-Youl Youm
Organized by KIISC

Invited Paper Reviewer
IEEE Communication Letters
Information Processing Letters.

External Paper Reviewer
IEEE Transaction on Information Theory
IACR International Cryptology Conference - Crypto 2005, 2004
IACR International Cryptology Conference - Eurocrypt 2006, 2002
IACR International Cryptology Conference - Asiacrypt 2005, 2003-2001
Workshop on Cryptographic Hardware and Embedded System (CHES) 2003
RSA Conference - Cryptographers Track (CT-RSA) 2006, 2002
International Conference on Cryptology and Network Security 2005
International Conference on Applied Cryptography and Network Security (ACNS 2004);
Australian Conference on Information Security and Privacy (ACISP 2003)
Workshop on Information Security and Applications (WISA 2003)

Conference Talks

International Conference on Information Security Practice and Experience Conference 2006
Hangzhou, China. (Apr. 2006)
"Efficient Public Key Broadcast Encryption using Identifier of Receivers"

Financial Cryptography and Data Security 2006, *Anguilla, British West Indies.* (Mar. 2006)
"Efficient Broadcast Encryption Scheme with Log-Key Storage"

Information Security Conference 2005, *Singapore.* (Sep. 2005)
"Timed-Release Encryption with Pre-open Capability and Its application to Certified E-mail System"

Workshop on Information Security and Applications 2004, *Jeju Island, Korea.* (Aug. 2004)
"TTS without Revocation Capability Secure against CCA2"

European PKI Workshop: Research and Applications 2004, *Samos Island, Greece.* (Jul. 2004)
"An Efficient Revocation Scheme for Stateless Receivers"

International Conference on Computational Science and Its Applications 2004,
Assisi, Italy. (Jun. 2004)
"Bit-Serial Multipliers for Exponentiation and Division in $GF(2^m)$ using Irreducible AOP"

Australian Conference on Information Security and Privacy 2003, *Wollongong, Australia.* (Jul. 2003)
"EPA: An Efficient Password-based Protocol for Authenticated key exchange"

References

Available upon request.