

Lee, Yong Ki

Phone : 1-310-776-1235
Address: 221 S. Doheny Apt# 305, Beverly Hills, CA 90212

E-mail : jfirst@ee.ucla.edu
Web : www.ee.ucla.edu/~jfirst

Education

University of California, Los Angeles, Electrical Engineering, Sep. 2004 – Present

Ph.D. candidate, Advisor: Dr. Ingrid Verbauwhede (GPA: 3.714/4.0)

Major: Communications and Telecommunications

Katholieke Universiteit Leuven (K.U.Leuven), Belgium, Apr. 2007 – Mar. 2008, Jul. 2008 – Jun. 2009 (2 years)

Visiting Scholar, Computer Security and Industrial Cryptography Lab. (COSIC)

University of California, Los Angeles, Electrical Engineering, Dec. 2006

M.S., Major: Communications and Telecommunications, Advisor: Dr. Ingrid Verbauwhede (GPA: 3.746/4.0)

Hanyang University, Computer Science and Engineering, South Korea, Mar. 1997 – Feb. 1999

M.S., Advisor: Dr. Jongkyu Lee (GPA : 3.88/4.0)

Hanyang University, Computer Science and Engineering, South Korea, Mar. 1993 – Feb. 1997

B.S. (GPA : 3.93/4.5, Rank: 3 out of 84)

Research Interest

- Embedded Software/Hardware implementation for Security applications.
- Low Cost Authentication Protocol design and Implementation for RFID systems and sensor networks.

Experience

University of California, Los Angeles – Embedded Security Lab.

Research Assistant

Jun. 2005 – Present

- Hardware/Software co-design for security processing
- Privacy-friendly authentication and search protocols design for RFID systems. Security proof in a mathematical model.
- Security processor design project: Leading member in a security processor design team. RTL level architecture design. Simulation and Verification with GEZEL and ModelSim. Functional test and side channel analysis on a FPGA. Collaboration with custom circuit designers as well as crypto mathematicians. Taped-out with UMC 130nm tech.
- Cryptographic hash algorithm implementation in RTL level. Research on signal processing techniques to improve the performance, such as the iteration bound analysis, the retiming transformation, and the unfolding transformation.

Republic of Korea Air Force – Computer Department at the 9785th Unit

Department Chief & Staff officer of Information and Communication

Oct. 1999 – Jan. 2003

- Intranet Software development (implemented with PHP).
 - : Intranet document management system, logistics management, vehicles management.
- Network management and installation.
- Server and Database management: Operating logistics server.

Hanyang University, South Korea – Communication Lab.

Research Assistant

Mar. 1997 – Feb. 1999

- Research in wireless communication. Hand-off algorithm in cellular network.
- Research in secure key exchange protocol design and analysis.

Teaching Assistant

Mar. 1997 – Feb. 1999

- Teaching general computer skills to undergraduates

B.S. Graduation Project

- Application: 3D Lego System (implemented with C++).
- 3D graphic rendering with shutter (flickering) glasses.
- Rendering two images for each eye and synchronizing with shutter glasses.

Grants and Awards

- '98 **Information Security Thesis Prize** from Korea Information Security Agency, *Dec. 12, 1998*
- B.S. with honors** from Hanyang University, *Feb. 21, 1997*
- Scholarship** for studying abroad from Hanyang University, *Sep. 2004 – Aug. 2006* (for 2 years)
- Scholarship** awarded from The Rotary Club, *Dec. 1996, Mar. & Sep. 1995* (for 1.5 years)
- Scholarship** awarded from Hanyang University, *Sep. 1993 – Aug. 1995* (for 2 years)

Professional Activities

- Program committee member**, RFIDSec 2010: 6th Workshop on RFID Security, Istanbul, Turkey, 2010

Research Tools

- Programming Language:** C/C++, Visual C++, Assembly, HTML, PHP
- Synthesis:** Design Compiler, Xilinx (ISE)
- RTL Simulation:** Modelsim, GEZEL
- Modeling Tool:** Matlab, GEZEL

Publications and Presentation

<Security Protocols>

1. **Y. K. Lee**, L. Batina, and I. Verbauwhede, “**Secure Communication Protocols for RFID Systems**,” *submitted to Proceedings of the IEEE*, 2009.
2. **Y. K. Lee**, L. Batina, D. Singelee, and I. Verbauwhede, “**Low-Cost Untraceable Authentication Protocols for RFID**,” *submitted to Third ACM Conference on Wireless Network Security (WiSec’10)*, 2009.
3. **Y. K. Lee**, L. Batina, and I. Verbauwhede, “**Privacy challenges in RFID systems**,” 20th Tyrrhenian Workshop on Digital Communications (Invited), Springer, *to be published as a book chapter*, 2009.
4. **Y. K. Lee**, L. Batina, and I. Verbauwhede, “**Untraceable RFID Authentication Protocols: Revision of EC-RAC**,” In IEEE International Conference on RFID 2009, IEEE, pp. 178-185, 2009.
5. **Y. K. Lee**, L. Batina, and I. Verbauwhede, “**EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol**,” In IEEE International Conference on RFID 2008, IEEE, 8 pages, 2008.
6. Y. Lee, **Y. K. Lee**, Y. Chung, and K. Moon, “**One-Time Templates for Face Authentication**,” In Proceedings of the 2007 IEEE International Conference on Convergence Information Technology, pp. 1818-1823, 2007.
7. **Y. K. Lee**, L. Batina, and I. Verbauwhede, “**EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol**,” In 2nd Benelux Workshop on Information and System Security, September 20-21, 2007, Luxembourg city, Luxembourg.
8. **Y. K. Lee**, and I. Verbauwhede, “**Secure and Low-cost RFID Authentication Protocols**,” 2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN), November 28, 2005, St. Louis, Mo, USA.
9. **Y. K. Lee**, and J. K. Lee, “**Elliptic Curve Secure Remote Password Protocol**,” Korea Institute of Information Security & Cryptology, 9(1), pp 85-102, 1999.
10. **Y. K. Lee**, and J. K. Lee, “**EC-SRP Protocol; Elliptic Curve Secure Remote Password Protocol**,” Korea Information Security Agency, pp. 37-58, December 1998.

<System Design and Implementation for Security Processing>

11. **Y. K. Lee**, M. Knezevic, and I. Verbauwhede, “[Architecture Design of Hash Algorithms for Hardware](#),” In Secure Integrated Circuit Systems, Springer, *to be published*, November 2009.
12. **Y. K. Lee**, K. Sakiyama, L. Batina, and I. Verbauwhede, “[Elliptic Curve Based Security Processor for RFID](#),” IEEE Transactions on Computers 57(11), pp. 1514-1527, 2008.
13. **Y. K. Lee**, H. Chan, and I. Verbauwhede, “[Design Methodology for Throughput Optimum Architectures of Hash Algorithms of the MD4-class](#),” Journal of Signal Processing Systems, 53(1-2), Springer, pp. 89-102, 2008.
14. **Y. K. Lee**, L. Batina, J. Fan, D. Karaklajic, M. Knezevic, U. Kocabas, V. Rozic, and I. Verbauwhede, “[Tiny Public-Key Security Processor](#),” In IEEE ISSCC09 Student Forum, February 8, 2009, San Francisco, CA, USA.
15. M. Knezevic, K. Sakiyama, **Y. K. Lee**, and I. Verbauwhede, “[On the High-Throughput Implementation of RIPEMD-160 Hash Algorithm](#),” In IEEE 19th International Conference on Application-specific Systems, Architectures and Processors (ASAP), IEEE, pp. 85-90, 2008.
16. **Y. K. Lee**, K. Sakiyama, L. Batina, and I. Verbauwhede, “[A Compact ECC Processor for Pervasive Computing](#),” Secure Component and System Identification (SECSI), March 17-18, 2008, Berlin, Germany.
17. **Y. K. Lee**, and I. Verbauwhede, “[A Compact Architecture for Montgomery Elliptic Curve Scalar Multiplication Processor](#),” In Information Security Applications, 8th International Workshop, WISA 2007, Lecture Notes in Computer Science 4867, S. Kim, H. Lee, and M. Yung (eds.), Springer-Verlag, pp. 115-127, 2007.
18. **Y. K. Lee**, H. Chan, and I. Verbauwhede, “[Iteration Bound Analysis and Throughput Optimum Architecture of SHA-256 \(384,512\) for Hardware Implementations](#),” In Information Security Applications, 8th International Workshop, WISA 2007, Lecture Notes in Computer Science 4867, S. Kim, H. Lee, and M. Yung (eds.), Springer-Verlag, pp. 102-114, 2007.
19. **Y. K. Lee**, Herwin Chan, and I. Verbauwhede, “[Throughput Optimized SHA-1 Architecture Using Unfolding Transformation](#),” IEEE 17th International Conference on Application-specific Systems, Architectures and Processors (ASAP), pp. 354-359, September 2006.

<Algorithm and Etc>

20. **Y. K. Lee**, M. S. You, and J. K. Lee, “[SIR-Based Dynamic Code Allocation Method Prioritized for Handoff Call in DA-CDMA Cellular System](#),” The Journal of the Korean Institute of Communication Sciences, 23(9), pp. 2131-2140, September 1998.
21. **Y. K. Lee**, and J. K. Lee, “[The Efficiency of the Elliptic Curve Public Key Algorithm](#),” Journal of Engineering & Technology Hanyang University, 7(1), pp. 295-311, July 1998.

Technical Classes taken in UCLA

- This is much more than the Ph.D. requirement (which is 4 classes), and resulted in a MS degree during Ph.D. program.

1. EEM202A Embedded Systems
2. EE232A Stochastic Modeling with Applications to Telecommunication Systems
3. EE232B Telecommunication Switching and Queueing Systems
4. EE232D Telecommunication Networks and Multiple Access Communications
5. CS212A Queuing Systems Theory
6. CS118 Computer Network Fundamentals
7. EE238 Multimedia Communications and Processing
8. EEM208A Analytical Methods 1
9. EE231A Information Theory: Channel and Source Coding
10. EE231E Channel Coding Theory
11. EE230A Estimation and Detection in Communication and Radar Engineering
12. EE230B Digital Communication Systems
13. EE219A Special Topics in Circuits and Signal Processing