Cryptographic Hash Workshop
October 31 – November 1, 2005

Jaechul Sung, *University of Seoul*
jcsung@uos.ac.kr

BIOGRAPHY:
Company: Dep. of Mathematics, University of Seoul
Position: Full-time Instructor
Tel: +82-17-2210-5663

Education:

1992.3 – 1997.8: Korea University, Mathematics (Bachelor)
1997.9 – 1999.8: Korea University, Algebra (Master)
1999.9 – 2002.8: Korea University, Cryptography (Doctor)

Career:

1997.9 – 2002.7: CIST, Korea University (Researcher)
2002.8. – 2004.1: Korea Information Security Agency (Senior researcher)
2004.2. – Present: University of Seoul (Full-time Instructor)

Selected Publications:

- Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis, ASIACRYPT2000
- Provable Security against Differential and Linear Cryptanalysis for the SPN Structure, FSE2000
- Known-IV Attacks of Tripe Modes of Operation of Block Ciphers, ASIACRYPT 2001
- Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation, ICISC 2001
- Impossible Differential Cryptanalysis of Zodiac, IEICE 2002
- Full-Round Differential Attack on the Original Version of the Hash Function Proposed at PKC'98, SAC 2002
- Key Recovery Attacks on the RMAC, TMAC, and IACBC, ACISP 2003
- Impossible Differential Cryptanalysis of Block Cipher Structures, IINDOCRYPT 2003
- Padding Oracle Attacks on Multiple Modes of Operations, ICISC 2004
- Related-Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b, MyCrypt2005

Research Area: Design and Analysis of Cryptographic Primitives