

# **Cryptographic Hash Workshop**

## ***October 31 – November 1, 2005***

---

**Donghoon Chang, Korea University**  
**dhchang@cist.korea.ac.kr**

### **BIOGRAPHY:**

Company: Center for Information Security Technologies, Korea University

Position: Doctor-course student

Tel: +82-10-8978-1815

### Education:

1997.3 – 2001.2: Korea University, Mathematics (Bachelor)

2001.3 – 2003.2: Korea University, Cryptology (Master)

2003.3 – present: Korea University, Cryptography (Doctor-course)

### Career:

2002.12: The honor prize of the 5<sup>th</sup> public announcement of paper on Information Security, Korea Information Security Agency. The title is "Multi-Dimensional Construction of UOWHF".

2003.8.1 – 2003.8.31: Co-work with Professor Palash Sarkar about 'Theory of Hash Functions' at Applied Statistics Unit of Indian Statistical Institute. (on leave from the CIST, Seoul)

2002.9 - 2004.8: Teaching Assistant, Linear Algebra and Abstract Algebra and Calculus at Korea University.

2005.3 – present: CIST, Korea University (Researcher)

### Selected Publications:

- Full-Round Differential Attack on the Original Version of the Hash Function Proposed at PKC'98, SAC2002

- New Parallel Domain Extenders for UOWHF, Asiacrypt2003

- Differential attacks on TEA and XTEA, ICISC2003

- A Generalized of PGV-Hash Functions and Security Analysis in Black-box Model, ACISP2004

- Impossible of Construction of OWHF and UOWHF from PGV model based on Block Cipher secure against ACPCA, Indocrypt2004

Research Area: Design and Analysis of Cryptographic Primitives