Joo Yeon Cho
Researcher

Email: joo.cho@tkk.fi
Office: (+358) 9 451 3379
Fax: (+358) 9 451 3369
Mobile: (+358) 40 877 8789
http://www.tcs.hut.fi/~jcho/

Education

2003–2007	Ph.D. Macquarie University, Sydney, Australia
1991–1992	Master of Science, POSTECH, South Korea
1987–1990	Bachelor of Electric Engineering, Seoul National University, South Korea

Ph.D Thesis

Project Title	New Results on Cryptanalysis of Stream Ciphers
Supervisor	Josef Pieprzyk and Huaxiong Wang

Professional experience

Jan 2008–Dec 2009	Researcher, Helsinki University of Technology, Finland
Sep 2008–May 2009	Teaching Assistant, Helsinki University of Technology, Finland
Jan 2000–Dec 2002	Senior Hardware and Software Engineer, Venture companies, South Korea
Mar 1993–Dec 1998	Senior Hardware and Firmware Engineer, LG Electronics, South Korea

Technical skills

Programming	C, C++, x86 assembly, Matlab
Hardware	Embedded System Design using 8-bit, 16-bit and 32-bit CPU (Intel x86, IBM PowerPC, Geode, etc.)
System	Smartcard ISO Interface, Automatic Banking System, Surveillance System

Projects Experience

Automatic Teller Machine	Automatic banking system, smart card application
Network Video Streamer	Web based video streaming system
Digital Video Recorder	MPEG based video and audio recording for surveillance system
Virtual Private Network	Secure telecommunications through public network

Research Interests

Cryptanalysis of symmetric key cryptosystem

Design and analysis of lightweight cryptographic algorithms

Algorithm implementation and hardware embedded system design

List of publications

FSE 2004	Algebraic attacks on SOBER-t32 and SOBER-t16 without stuttering, with Josef Pieprzyk, LNCS Vol. 3017, pp. 49-64, New Delhi, India
SASC 2006	Linear distinguishing attack on NLS, with Josef Pieprzyk, Leuven, Belgium
ACISP 2006	Distinguishing attack on SOBER-128 with linear masking, with Josef Pieprzyk, LNCS Vol. 4058, pp. 29-39, Melbourne, Australia
SAC 2006	Crossword puzzle attack on NLS, with Josef Pieprzyk, LNCS Vol. 4356, pp. 249-265, Montreal, Canada
ISC 2007	Multiple modular additions and crossword puzzle attack on NLSv2, with Josef Pieprzyk, LNCS Vol. 4779, pp. 230-248, Valparaiso, Chile
IWCC 2007	An improved distinguisher for Dragon, with Josef Pieprzyk, Series on Coding Theory and Cryptology, Vol. 4, China
SASC 2008	An improved estimate of the correlation of distinguisher for Dragon, Lausanne, Switzerland
ACISP 2008	Multidimensional linear cryptanalysis of reduced round Serpent, with Miia Hermelin and Kaisa Nyberg, LNCS Vol. 5107, pp. 203-215, Wollongong, Australia
ICISC 2008	A new technique for multidimensional linear cryptanalysis with applications on reduced round Serpent, with Miia Hermelin and Kaisa Nyberg, LNCS Vol. 5461, pp. 383-398, Seoul, Korea
FSE 2009	Multidimensional extension of Matsui's algorithm 2, with Miia Hermelin and Kaisa Nyberg, LNCS Vol. 5665, pp. 209-227, Leuven, Belgium
EUROCRYPT 2009 poster	Statistical tests for key recovery using multidimensional extension of Matsui's algorithm 1, with Miia Hermelin and Kaisa Nyberg, Germany
ICISC 2009	Improved linear cryptanalysis of SOSEMANUK, with Miia Hermelin, accepted
CT-RSA 2010	Linear cryptanalysis of reduced-round PRESENT, submitted