Cryptographic Hash Workshop
October 31 – November 1, 2005

Xiaoyun Wang, *Center for Advanced Study in Tsinghua University*
xywang@sdu.edu.cn

BIOGRAPHY:

Xiaoyun Wang received the M.S. and Ph.D. degrees in Mathematics from Shandong University in 1990 and 1993 respectively. She is now a C.N.Yang Professor at the Center for Advanced Study in Tsinghua University, and a professor at the School of Mathematics & System Sciences of Shandong University. Her research fields focus on hash functions, block ciphers and public-key cryptography. Especially, Xiaoyun Wang gave a kind of collision attack on a series hash functions including MD4, HAVAL-128, RIPEMD, SHA-0 and SHA-1. Two papers “How to break MD5 and other Hash functions ” and “Cryptanalysis for Hash functions MD4 and RIPEMD” shared “best paper award” in Eurocrypt 05, and the paper "Finding collisions in the full SHA-1" gained the "best paper award" in Crypto 05.