Dr. Xiaoyun Wang

Institute for Advanced Study
Tsinghua University
China

Xiaoyun Wang is currently the C. N. Yang Professorship of Institute for Advanced Study at Tsinghua University, the Academician of Chinese Academy of Sciences and the IACR fellow. She developed the collision attack theory on cryptographic hash functions, namely, the modular bit differential cryptanalysis, and broke five globally used hash functions, including MD5 and SHA-1. She was in charge of the design of the Chinese hash function standard SM3, which has currently been deployed widely in financial, transportation, state grid and other important economic fields. In October 2018, SM3 officially became the ISO/IEC international standard.

Xiaoyun Wang has published more than fifty academic papers, and three of them were given the best paper awards at CRYPTO 2005 and EUROCRYPT 2005. Due to her contribution on Cryptology, Xiaoyun Wang was awarded the special prize for cryptographic innovation of the Chinese Association for Cryptologic Research in 2014, the CSIAM Su Buchin Prize in 2010, the 2nd Class Prize of China's National Natural Science Award in 2008, the Tan Kah Kee Science Award and the Qiushi Outstanding Scientist Award in 2006, etc.