清华大学高等研究院
Institute for Advanced Study, Tsinghua University
密码学学术报告
Cryptology Seminars

Title: Key Recovery Attack on HMAC/NMAC based on Reduced Whirlpool

Speaker: Jian Guo
Institute for Infocomm Research (I2R), Singapore

Time: 9:30am, Wednesday, Nov 28, 2012
(9:00~9:30am, Tea, Coffee, and Cookie)

Venue: Conference Hall 322, Science Building, Tsinghua University

Abstract: In recent years, significant progress has been made in cryptanalysis of hash functions, e.g.,collision attacks breaking MD5 and SHA-1. However, progress in analysis on hash based MAC, one of themost important applications of hash functions, is rather limited, i.e., mainly distinguishing attacks. In this paper, we present key recovery attacks on the most popular hash-based MAC constructions, e.g., HMACand NMAC, instantiated with AES-like hash function Whirlpool. These attacks work with Whirlpool reduced to 5 out of 10 rounds in single-key setting, and 6 rounds in related-key setting. Moreover,we consider other hash based MAC constructions, and Whirlpool variants in some PGV modes, similar results are obtained. To the best of our knowledge, this is the first original key recovery on HMAC.Interestingly, the number of attacked round is comparable with that for collision and preimage attacks on Whirlpool hash function itself. This is joint work with Lei Wang, and Shuang Wu from Nanyang Technological University, Singapore.

Biblio: Jian Guo is a research scientist with the Institute for Infocomm Research (I2R) in Singapore since 2010. He obtained his bachelor degree in Computer Engineering and PhD in Mathematical Sciences from Nanyang Technological University in 2007 and 2011, respectively. His research focuses on design and analysis of symmetric key cryptography such as hash functions, and block ciphers.