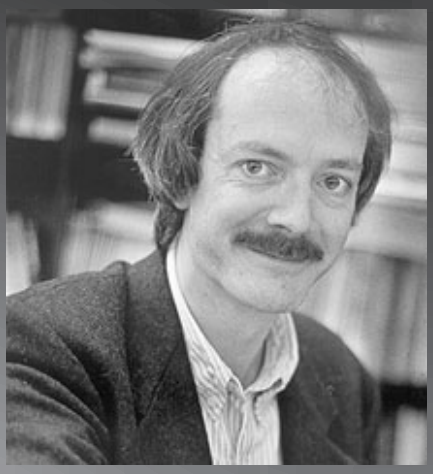
中央研究院 資訊科學研究所
Institute of Information Science, Academia Sinica

Distinguished Lecture Series

Cryptographic Hash Functions and the SHA-3 competition



Wednesday, December 1st, 2010 10:00am
Auditorium 106 at New IIS Building

Bart Preneel

Professor, in the research group COSIC of the Electrical Engineering Department of the Katholieke Universiteit Leuven in Belgium

Abstract

Cryptographic hash functions are an essential building block for security applications. In 2004, Microsoft Windows software used about 800 instances of the hash function MD5 and HMAC-MD5 was widely deployed for securing web transactions and VPNs. In spite of this central role in applications, the amount of theoretical research and cryptanalysis invested in cryptographic hash functions was rather limited. Moreover, designing a secure hash function turns out to be rather hard: from the hundred designs published before 2004, about 80% have been shown to be weak. In 2004, Wang et al. made a cryptanalytic breakthrough for the widely used hash functions MD4, MD5 and the US government standard SHA-1. In addition, serious shortcomings have been identified in the theoretical foundations of existing designs. In response to this hash function "crisis", a large number of papers has been published with theoretical results and novel designs. In November 2007, NIST (National Institute for Standards and Technology, NIST) has announced the start of the SHA-3 competition, with as goal to select a new hash function family by 2012. About half of the 64 submissions were broken within 6 months. In July 2009, 14 submissions were selected for the second round. In this talk, we present a brief outline of the state of the art of hash functions half-way the SHA-3 competition.

For more infomation: http://www.iis.sinica.edu.tw/