

On Randomizing Hash Functions to Strengthen the Security of Digital Signatures

Dr. Praveen Gauravaram
Research Fellow
Department of Mathematics
Technical University of Denmark



Date : 20 March 2009 (Friday)
Time : 4.30pm – 5.30pm
Venue: SPMS-Executive Classroom 1, MAS-03-06
School of Physical and Mathematical Sciences

Halevi and Krawczyk proposed a message randomization algorithm called RMX as a front-end tool to the hash-then-sign digital signature schemes such as DSS and RSA in order to free their reliance on the collision resistance property of the hash functions. They have shown that to forge a RMX-hash-then-sign signature scheme, one has to solve a cryptanalytical task which is related to finding second preimages for the hash function. In this article, we will show how to use Dean's method of finding expandable messages for finding a second preimage in the Merkle-Damgard hash function to existentially forge a signature scheme based on a t -bit RMX-hash function which uses the Davies-Meyer compression functions (e.g., MD4, MD5, SHA family) in $2^{\lfloor t/2 \rfloor}$ chosen messages plus $2^{\lfloor t/2 + 1 \rfloor}$ off-line operations of the compression function and similar amount of memory. This forgery attack also works on the signature schemes that use Davies-Meyer schemes and a variant of RMX published by NIST in its Draft Special Publication (SP) 800-106. We discuss some important applications of our attack.

(Paper will appear in Eurocrypt2009)

Speaker Biography:

Dr. Praveen Gauravaram is currently a research fellow with Department of Mathematics, Technical University of Denmark. Before that, he had this PhD from Queensland University of Technology, Australia in 2007. More information on the speaker is available at <http://www2.mat.dtu.dk/people/P.Gauravaram/>.

Host: Coding and Cryptography Research Group, Division of Mathematical Sciences, School of Physical and Mathematical Sciences

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

NANYANG TECHNOLOGICAL UNIVERSITY
SPMS-MAS-03-01, 21 NANYANG LINK, SINGAPORE 637371
FAX: +65 6515 8213 TEL: +65 6513 7423