Reviving the Dragon

Dr. Matt Henricksen
Institute for Infocomm Research (I2R)

Date : 27 March 2009 (Friday)
Time : 4.30 pm – 5.30 pm
Venue: SPMS-Seminar Room, MAS-03-08
School of Physical and Mathematical Sciences

The recent eSTREAM competition recommended eight stream ciphers out of a submitted set of 34 candidates, based on various criteria. Four were chosen because they yield extremely high throughput in software. The Dragon cipher, while it was one of the finalists in the competition, did not make the final cut because of some speed and security issues. This talk is a case study of the issues with the Dragon cipher, from many perspectives, including implementation on the Intel platform, linear cryptanalysis and cache timing attacks, all of which are pivotal in stream cipher design today.

Speaker Biography

Matt Henricksen manages a small team of symmetric cipher analysts at I2R. Previously, he worked in the broader area of information security at Information Security Institute, Queensland, from which he obtained his PhD in 2005. Prior to this, he was a software engineer for companies such as Hewlett Packard and RSA Security.

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