NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

CS SEMINAR

Title: Leakage resilient masking schemes

Speaker: Assistant Professor Sebastian Faust
Workgroup for Applied Cryptography
Department of Mathematics
Ruhr-University Bochum

Date/Time: 13 March 2017, Monday, 10:00 AM to 11:30 AM

Venue: SR8, COM1-02-08

Chaired by: Dr Aggarwal, Divesh, Assistant Professor, School of Computing
(divesh@comp.nus.edu.sg)

Abstract:

Masking schemes are widely used in practice to defeat side-channel attacks, which exploit the power consumption of devices. At the same time a large body of recent theoretical works study feasibility of computation in the presence of leakage and attempts to provide a formal security analysis of the masking countermeasure. In this talk, we will review some recent advances in the formal security analysis of masking schemes and present efficient ways how to apply the masking countermeasure at smart card level.

Biodata:

Sebastian Faust is an Assistant Professor at Ruhr University Bochum, where he is leading the research group on Applied Cryptography funded by the Emmy Noether Program of the German Science Foundation (DFG).

Before this, he has been a Marie Curie IEF fellow at EPFL, Switzerland in the group of Serge Vaudenay, and a Postdoc at Aarhus University in the group of Ivan Damgaard. In 2010, he received his Ph.D. in the COSIC group at KU Leuven. His research was funded through a Microsoft Research Ph.D. scholarship. He obtained a Master in Business Informatics from the University of Mannheim.