VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series, 2012

National Capital Region

Evaluating Implementations of SHA-3 Candidates

Speaker: Prof. Jens-Peter Kaps
Dept. of Electrical and Computer Engineering
George Mason University

Friday, April 13, 2012
1:00PM- 2:00PM, NVC 325

Abstract

The National Institute of Standards and Technology (NIST) started a public competition to develop a new Secure Hash Algorithm (SHA-3) in November 2007. NIST is expected to announce the winner later in 2012. From the submitted 64 entries only 5 algorithms made it to the final round. Last month was the 3rd and final SHA-3 candidate conference in which research groups from all over the world presented their latest security analysis and implementation results. The Cryptographic Engineering Research Group (CERG) from GMU contributed to the state of the art of SHA-3 candidate implementations through 4 research papers presented at this conference. In this seminar I will summarize implementation results from our and other research groups. Comparing implementations of several functionally equivalent algorithms in a fair and balanced manner is a challenging task. I will briefly highlight the difficulties and present tools for fair, comprehensive, and automated evaluation of hardware implementations, developed by CERG, and software implementations.

Biography

Jens-Peter Kaps is an assistant professor of electrical and computer engineering at the Volgenau School of Engineering at George Mason University (GMU) since 2006. He received a PhD in Electrical and Computer Engineering from Worcester Polytechnic Institute in 2006. He is co-director of the Cryptographic Engineering Research Group (CERG) at GMU. His research interests include ultra-low power cryptographic hardware design, side-channel analysis, computer arithmetic, efficient cryptographic algorithms, and ubiquitous computing. He was general co-chair for the Cryptographic Hardware and Embedded Systems conference (CHES) in 2008 and general chair for the Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS) workshop in 2012. Dr. Kaps is a member of the IEEE Computer Society and the International Association for Cryptologic Research (IACR)