Invited Talk

Department of Computer Science and Engineering

Indian Institute of Technology Kanpur

September 14, 2018, Friday

Time: 5:00-6:00 PM

Venue: KD 101

Talk Title: *SymSum: Symmetric-Sum Distinguishers Against Round Reduced SHA3*

Speaker: Dhiman Saha

IIT- Bhilai

Abstract: Cryptographic Hash Functions are ubiquitous in our day-to-day digital lives. Primarily they ensure data integrity which is one of the fundamental crypto goals making the analysis of these hash functions imperative. After briefly introducing the research area, this talk will focus on devising "Distinguishers" of the latest cryptographic hash function – SHA3. "Distinguishers" constitute a specific paradigm of analyzing hash functions that deals with exhibiting non-random behavior. The talk will zoom-in to the domain of higher-order derivatives of Boolean functions and its applications to analysis of SHA3 in the form of the Zero-Sum property. Finally, our latest research result which proposes a new class of Distinguishers of SHA3 will be presented. The technique presented relies on a variant of classical higher order Boolean derivatives over special subspaces. It exploits internal symmetry of the hash function to come up with the best distinguisher on SHA3 penetrating up to 9 rounds that succeeds with probability one and outperforms the closest competitor, in terms of effort, by a factor of 4.

Brief Bio: Dhiman Saha is an Assistant Professor in the Department of Electrical Engineering and Computer Science at IIT Bhilai. Prior to that he was working as a Visiting Scientist at the R.C Bose Center for Cryptology & Security, ISI Kolkata. He received his PhD in 2017 from the Computer Science and Engineering Department, IIT Kharagpur where he also served as a Research Associate in the Crypto Research Lab. His broad area of research encompasses both theoretical and physical aspects of Cryptography. As a part of his thesis he worked on the cryptanalysis of hash functions and authenticated ciphers. He has broken three authenticated encryption schemes submitted to the on-going CAESAR competition and has been involved in the analysis of latest cryptographic hash standard - SHA3. Before joining for his PhD, he worked in the Electronic Design Automation industry for over two years. He completed his MS degree from IIT Kharagpur in 2009 with a thesis on Hardware Security. He received his BE from NIT Agartala in 2006 and was awarded the Gold Medal for Computer Science and Engineering. He was also recipient of the NEC Scholarship during his BE. Along with hash functions and authenticated ciphers, his recent research interests include randomness in public permutations, infective counter-measures in fault analysis and memory-hard functions.