Indocrypt 2018: Program

Sunday, December 9, 2018 (Tutorials)

Venue: Juniper Hall, India Habitat Center

10:00 - 11:00 **Tutorial 1: (Session Chair: Debrup Chakraborty)**
Introduction to the sponge and duplex constructions
Gilles Van Assche

11:00 - 11:30 Break

11:30 - 12:30 **Tutorial 2 (Session Chair: Debrup Chakraborty)**
Cryptographic properties of Keccak
Gilles Van Assche

12:30 - 14:00 **Lunch**

14:00 - 15:00 **Tutorial 3 (Session Chair: Bimal Roy)**
Public Key Encryption and Security against Chosen Ciphertext Attacks- I
Takahiro Matsuda

15:00 - 15:30 **Break**

15:30- 16:30 **Tutorial 4 (Session Chair: Bimal Roy)**
Public Key Encryption and Security against Chosen Ciphertext Attacks- II
Takahiro Matsuda

Monday, December 10, 2018, *Venue: Silver Oak Hall, India Habitat Centre*

8:30-09:00 **Registration**

09:00-09:40 **Inaugural Program**

09:40- 11:10 **High Tea**

11:10-12:10 **Invited Talk 1 (Session Chair**: **Tetsu Iwata**)
On dec(k) functions
Gilles Van Assche

12:10-13:00 **Session 1: Outsourced Computation and Searchable Encryption (Session Chair: Srinivas Vivek)**
Revisiting Single-server Algorithms for Outsourcing Modular Exponentiation
Jothi Rangasamy and Lakshmi Kuppusamy

Keyword Search Meets Membership Testing: Adaptive Security from SXDH
Sanjit Chatterjee and Sayantan Mukherjee

13:00-14:30 **Lunch**

14:30-15:45 **Session 2 : Symmetric Key Cryptography and Format Preserving Encryption (Session chair: Rajesh Pillai)**
Tweakable HCTR: A BBB Secure Tweakable Enciphering Scheme
Avijit Dutta and Mridul Nandi

Reconsidering Generic Composition: the Tag-then-Encrypt case
Francesco Berti, Olivier Pereira, and Thomas Peters

On Diffusion Layers Of SPN Based Format Preserving Encryption Schemes: Format Preserving Sets Revisited
Rana Barua, Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray

15:45-16:15 **Tea Break**

16:15-17:05 **Session : Fault Attacks and Hash Functions (Session Chair: Gilles Van Assche)**
Differential Fault Attack on SIMON with Very Few Faults
Ravi Anand, Akhilesh Siddhanti, Subhamoy Maitra, Sourav Mukhopadhyay

Cryptanalysis of 2 round Keccak-384
Rajendra Kumar, Nikhil Mittal, and Shashank Singh

17:30-18:00 **CRSI Meeting**

Tuesday, December 11, 2018, *Venue: Silver Oak Hall, India Habitat Centre*

10:00 - 11:00 **Invited talk 2 (Session Chair: Bimal Roy)**
Public Key Encryption Secure against Related Randomness Attacks
Takahiro Matsuda

11:00 - 11: 30 **Tea Break**

11:30 - 13:10 **Session 4: Post Quantum Cryptography**
(Session Chair: Indivar Gupta)
A faster way to the CSIDH
Michael Meyer and Steffen Reith

A note on the security of CSIDH
Jean-François Biasse, Annamaria Iezzi, and Michael J. Jacobson Jr

Constructing Canonical Strategies For Parallel Implementation Of Isogeny Based Cryptography
Aaron Hutchinson and Koray Karabina

More Efficient Lattice PRFs from Keyed Pseudorandom Synthesizers
Hart W. Montgomery

13:10- 14:30 **Lunch**

14:30-15:45 **Session 5: Asymmetric Key Cryptography and Cryptanalysis**
(Session Chair: Takahiro Matsuda)
A Las Vegas algorithm to solve the elliptic curve discrete logarithm problem
Ayan Mahalanobis, Vivek Mallick, and Ansari Abdullah

Pairing-Friendly Twisted Hessian Curves
Chitchanok Chuengsatiansup and Chloe Martindale

A Family of FDH Signature Schemes Based on the Quadratic Residuosity Assumption
Giuseppe Ateniese, Katharina Fech, and Bernardo Magri

15:45-16:15 **Tea Break**

16:15 - 17:05 **Session 6 : Symmetric Key Cryptanalysis**
(Session Chair: R C Singh)
Using MILP in Analysis of Feistel Structures and Improving Type II GFS by Switching Mechanism
Mahdi Sajadieh and Mohammad Vaziri

Tools in analyzing linear approximation for Boolean functions related to FLIP
Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy, and Pantelimon Stanica

19:00 - **Conference dinner**

Wednesday, December 12, 2018

Venue: Silver Oak Hall, India Habitat Centre

10:00 - 11:00 **Invited talk 3**
(Session Chair: P.K. Saxena)
How To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC
Mridul Nandi

11:00 - 11:30 **Tea Break**

11:30 - 12:20 **Session 7: Theory**
(Session chair: A.H. Siddiqui)
Non-malleable Codes against Lookahead Tampering
Divya Gupta, Hemanta K. Maji, and Mingyuan Wang

Obfuscation from Low Noise Multilinear Maps
Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, Pratyay Mukherjee

12:20 - 13:10 **Session 8: Secure Computations and Protocols**
(Session Chair: N. B. Singh)
Non-Interactive and Fully Output Expressive Private Comparison
Yu Ishimaki and Hayato Yamana

Secure Computation with Constant Communication Overhead using Multiplication Embeddings
Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen

13:10-14:30 **Lunch**

END OF CONFERENCE