Indocrypt 2012 – Program Schedule

Session: **Time:**		**Morning I** **9:30 – 11:00**		**Morning II** **11:30 – 13:00**		**Afternoon I** **14:30 – 16:00**		**Afternoon II** **16:30 – 18:00**
Day 1 **09/12**	*Morning Tea and Snacks*	**Tutorial I**	*Tea Break*	**Tutorial I**	*Lunch at the Guest House*	**Tutorial II**	*Tea Break*	**Tutorial II**
Day 2 **10/12**		*Inauguration* --- Protocol		**Invited Talk I** --- Side Channel		**Tutorial III**		Cryptanalysis: Hash and Stream Ciphers
Day 3 **11/12**		Cryptanalysis: Block Ciphers		**Invited Talk II** --- Time Memory Trade Off		Hardware		*Banquet* *on River Ganges*
Day 4 **12/12**		Elliptic Curve		**Invited Talk III** --- Digital Signature		Symmetric Key Design and Provable Security		*Vote of Thanks*

Day I : Sunday – 9 December 2012

09:00-09:30 : Morning Tea and Snacks (Venue: Platinum Jubilee Auditorium)

09:30-13:00 : Tutorial Talk by Steven Galbraith
Title: Lattices and their applications to cryptography and cryptanalysis.

13:00-14:30 : Lunch (Venue: ISI Guest House)

14:30-18:00 : Tutorial Talk by Francisco Rodriguez-Henriquez
Title: Hardware design of cryptographic algorithms.

Day II : Monday – 10 December 2012

09:00-09:20 : Morning Tea and Snacks (Venue: Platinum Jubilee Auditorium)

09:20-09:30 : Brief Inauguration Program

09:30-11:10 : Session 1 : Protocol (Session Chair : Ramachandran Balasubramanian)

Title: A Unified Characterization of Completeness and Triviality for Secure Function Evaluation
Authors: Hemanta K. Maji, Manoj Prabhakaran, Mike Rosulek

Title: On the Non-Malleability of the Fiat-Shamir Transform
Authors: Sebastian Faust, Markulf Kohlweiss, Giorgia Azzurra Marson, Daniele Venturi

Title: Another Look at Symmetric Incoherent Optimal Eavesdropping against BB84
Authors: Arpita Maitra and Goutam Paul

Title: On-Line/Off-Line Leakage Resilient Secure Computation Protocols
Authors: Chaya Ganesh, Vipul Goyal, Satya Lokam

11:10-11:30 : Tea Break (Venue: Platinum Jubilee Auditorium)

11:30-12:30 : Invited Talk by Vinod Vaikuntanathan
Title: How to Compute Encrypted Data.

12:30-13:20 : Session 2 : Side Channel (Session Chair : Daniel J. Bernstein)

Title: Leakage Squeezing of Order Two
Authors: Claude CARLET, Jean-Luc DANGER, Sylvain GUILLEY, Houssem MAGHREBI

Title: ROSETTA for Single Curve Analysis
Authors: Christophe Clavier, Benoit Feix, Georges Gagnerot, Christophe Giraud, Mylne Roussellet, Vincent Verneuil

13:20-14:50 : Lunch (Venue: ISI Guest House)

14:50-16:20 : Tutorial by Subhamoy Maitra
Title: Four Lines of Design to Forty Papers of Analysis: The RC4 Stream Cipher.

16:20-16:30 : Tea Break (Venue: Platinum Jubilee Auditorium)

16:30-18:10 : Session 3 : Cryptanalysis of Hash and Stream Ciphers
(Session Chair : Yu Sasaki)

Title: Collision Attack on the Hamsi-256 Compression Function
Authors: Mario Lamberger, Florian Mendel, Vincent Rijmen

Title:Generalized Iterated Hash Functions Revisited: New Complexity Bounds for Multicollision Attacks.
Authors: Tuomas Kortelainen, Ari Vesanen, Juha Kortelainen

Title: A Differential Fault attack on the Grain family under Reasonable assumptions
Authors: Subhadeep Banik, Subhamoy Maitra, Santanu Sarkar

Title: Cryptanalysis of Pseudo-Random Generators based on Vectorial FCSRs
Authors: Thierry P. BERGER, Marine MINIER

18:10-18:30 : Evening Tea and Snacks (Venue: Platinum Jubilee Auditorium)

Day III : Tuesday – 11 December 2012

09:00-09:20 : Morning Tea and Snacks (Venue: Platinum Jubilee Auditorium)

09:20-11:00 : Session 4 : Cryptanalysis of Block Ciphers (Session Chair : Nicolas Sendrier)

Title: Faster Chosen-Key Distinguishers on Reduced-Round AES
Authors: Patrick Derbez, Pierre-Alain Fouque, Jeremy Jean

Title: The Higher-Order Meet-in-the-Middle Attack and Its Application to the Camellia BlockCipher
Authors: Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, Enes Pasalic

Title: Double-SP is Weaker than Single-SP : Rebound Attacks on Feistel Ciphers with Several Rounds.
Authors: Yu Sasaki

Title: Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers
Authors: Shengbao Wu, Mingsheng Wang

11:00-11:15 : Tea Break (Venue: Platinum Jubilee Auditorium)

11:15-12:15 : Invited Talk by Orr Dunkelman
Title: From Multiple Encryption to Knapsacks — Efficient Dissection of Composite Problems.

12:15-13:05 : Session 5 : Time Memory Trade Off (Session Chair : Sanjit Chatterjee)

Title: High-Speed Parallel Implementations of the Rainbow Method in a Heterogeneous System
Authors: Jung Woo Kim, Jungjoo Seo, Jin Hong, Kunsoo Park, Sung-Ryul Kim

Title: Computing Small Discrete Logarithms Faster
Authors: Daniel J. Bernstein, Tanja Lange

13:05-14:30 : Lunch (Venue: ISI Guest House)

14:30-15:20 : Session 6 : Hardware (Session Chair: Francisco Rodriguez-Henriquez)

Title: Embedded Syndrome-Based Hashing
Authors: Ingo von Maurich, Tim Goneysu

Title: Compact Hardware Implementations of the Block Ciphers mCrypton, NOEKEON, and SEA
Authors: Thomas Plos, Christoph Dobraunig, Alexander Oprisnik, Markus Hofinger, Christoph Wiesmeier, Johannes Wiesmeier

16:00-21:00 : Banquet on River Ganges.

Day IV : Wednesday – 12 December 2012

09:00-09:20 : Morning Tea and Snacks (Venue: Platinum Jubilee Auditorium)

09:20-11:00 : Session 7 : Elliptic Curve (Session Chair : Tanja Lange)

Title: A New Model of Binary Elliptic Curves
Authors: Hongfeng Wu, Chunming Tang, Rongquan Feng

Title: Efficient arithmetic on elliptic curves in characteristic 2
Authors: David Kohel

Title: Analysis of Optimum Pairings in Protocols at High Security Levels
Authors: Xusheng Zhang, Dongdai Lin

Title: Constructing Pairing-Friendly Genus 2 Curves with Split Jacobian
Authors: Robert Drylo

11:00-11:15 : Tea Break (Venue: Platinum Jubilee Auditorium)

11:15-12:15 : Invited Talk by Nigel Smart
Title: Using the Cloud to Determine Key Strengths.

12:15-13:05 : Session 8 : Digital Signature (Session Chair: David Kohel)

Title: Faster Batch Forgery Identification
Authors: Daniel J. Bernstein and Jeroen Doumen, Tanja Lange, Jan-Jaap Oosterwijk

Title: Implementing CFS
Authors: Gregory Landais,Nicolas Sendrier

13:05-14:30 : Lunch Break (Venue: ISI Guest House)

14:30-16:10 : Session 9 : Symmetric Key Design and Provable Security
(Session Chair : Rana Barua)

Title: SipHash: A Fast Short-Input PRF
Authors: Jean-Philippe Aumasson, Daniel J. Bernstein

Title: A Novel Permutation-based Hash Mode of Operation FP and the Hash Function SAMOSA
Authors: Souradyuti Paul, Ekawat Homsirikomol, Kris Gaj

Title: Resistance Against Adaptive Plaintext-Ciphertext Iterated Distinguishers
Authors: Asli Bay, Atefeh Mashatan, Serge Vaudenay

Title: Sufficient Conditions on Padding Schemes of Sponge Construction and Sponge-based Authenticated-Encryption Scheme.
Authors: Donghoon Chang

16:10-16:30: Vote of Thanks and End of the Conference.