Technical Program
Workshop and Conference
Indocrypt 2010

December 12th
Workshop
Morning Session

- ## Registration

Time	Venue
08:30-09:30 Hrs	Sapphire Ballroom

- ## Tutorial

Time	Title	Speaker
09:30-11:00 Hrs	Lightweight Cryptography for RFID Systems	Guang Gong

- ## Tea Break

Time	Venue
11:00-11:30 Hrs	Sapphire Ballroom - 1

- ## Tutorial

Time	Title	Speaker
11:30-13:00 Hrs	Lightweight Cryptography for RFID Systems	Guang Gong

- ## Lunch Break

Time	Venue
13:00-14:00 Hrs	Sapphire Ballroom - 1

December 12th
Workshop
Afternoon Session

- ## Tutorial

Time	Title	Speaker
14:00-15:30 Hrs	Pairing Based Cryptography	Sanjit Chatterjee

- ## Tea Break

Time	Venue
15:30-16:00 Hrs	Sapphire Ballroom - 1

- ## Tutorial

Time	Title	Speaker
16:00-17:30 Hrs	Pairing Based Cryptography	Sanjit Chatterjee

December 13th
Morning Session

• Registration

Time	Venue
08:30-09:30 Hrs	Marriott Convention Center

• Inaugural Function

Time	Venue
09:30-11:00 Hrs	Marriott Convention Center

• High Tea

Time	Venue
11:00-11:30 Hrs	Marriott Convention Center

• Invited Talk

Time	Title	Speaker
11:30-12:30 Hrs	Getting a Few Things Right and Many Things Wrong	Neal Koblitz

• Session 1: Security of RSA and Multivariate Schemes

Time	Title	Authors
12:45-13:15 Hrs	Partial Key Exposure Attack on RSA – Improvements for Limited Lattice Dimensions	Santanu Sarkar, Sourav Sen Gupta , and Subhamoy Maitra
13:15-13:45 Hrs	Towards Provable Security of the Unbalanced Oil and Vinegar Signature Scheme under Direct Attacks	Stanislav Bulygin, Albrecht Petzoldt, and Johannes Buchmann
13:45-14:15 Hrs	CyclicRainbow- A Multivariate Signature Scheme with a Partially Cyclic Public Key	Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann

December 13th
Afternoon Session

- ## Lunch

Time	Venue
14:15-15:15 Hrs	Marriott Convention Center

- ## Session 2: Security Analysis, Pseudorandom Permutations and Applications

Time	Title	Authors
15:15-15:45 Hrs	Combined Security Analysis of the One- and Three-pass Unified Model Key Agreement Protocols	Sanjit Chatterjee, Alfred Menezes and Berkant Ustaoglu
15:45-16:15 Hrs	Indifferentiability Beyond the Birthday Bound for the Xor of Two Public Random Permutations	Avradip Mandal, Jacques Patarin and Valerie Nachef
16:15-16:45 Hrs	The Characterization of Luby-Rackoff and Its Optimum Single-Key Variants	Mridul Nandi
16:45-17:15 Hrs	Versatile Pret a Voter: Handling Multiple Election Methods with a Unified Interface	Zhe Xia, Chris Culnane, James Heather, Hugo Jonker, Peter Ryan, Steve Schneider and Sriramkrishnan Srinivasan

- ## Tea Break

Time	Venue
17:15-17:45 Hrs	Marriott Convention Center

December 14th
Morning Session

- ## Invited Talk

Time	Title	Speaker
09:30-10:30 Hrs	Cryptographic Hash Functions: Theory and Practice	Bart Preneel

- ## Tea Break

Time	Venue
10:30-11:00 Hrs	Marriott Convention Center

- ## Session 3: Attacks on Block Ciphers and Stream Ciphers

Time	Title	Authors
11:00-11:30 Hrs	New Boomerang Attacks on ARIA	Ewan Fleischmann, Christian Forler, Michael Gorski and Stefan Lucks
11:30-12:00 Hrs	Algebraic, AIDA/Cube and Side Channel Analysis of KATAN Family of Block Ciphers	Gregory Bard, Nicolas Courtois, Jorge Nakahara Jr, Pouyan Sepehrdad and Bingsheng Zhang
12:00-12:30 Hrs	The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA	Cihangir Tezcan
12:30-13:00 Hrs	Greedy Distinguishers and Nonrandomness Detectors	Paul Stankovski

- ## Lunch Break

Time	Venue
13:00-14:00 Hrs	Marriott Convention Center

December 14th
Afternoon Session

- ## Session 4: Hash Functions

Time	Title	Authors
14:00-14:30 Hrs	Cryptanalysis of Tav-128 Hash function	Ashish Kumar, Somitra Sanadhya, Praveen Gauravaram, Masoumeh Safkhani and Majid Naderi
14:30-15:00 Hrs	Near-Collisions for the Reduced Round Versions of Some Second Round SHA-3 Compression Functions using Hill Climbing	Meltem Sonmez Turan and Erdener Uyan
15:00-15:30 Hrs	Speeding Up The Wide-pipe: Secure and Fast Hashing	Mridul Nandi

- ## Tea Break

Time	Venue
15:30-16:00 Hrs	Marriott Convention Center

- ## Session 5: Fast Cryptographic Computation

Time	Title	Authors
16:00-16:30 Hrs	Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity	Sedat Akleylek, Murat Cenk and Ferruh Ozbudak
16:30-17:00 Hrs	Random Euclidean Addition Chain Generation and Its Apllication to Point Multiplication	Fabien Herbaut, Pierre-Yvan Liardet, Nicolas Meloni, Yannick Teglia and Pascal Veron

December 15th
Morning Session

- ## Session 6: Cryptanalysis of AES

Time	Title	Authors
09:30-10:00 Hrs	Attack on a Higher-Order Masking of the AES Based on Homographic Functions	Thomas Roche and Emmanuel Prouff
10:00-10:30 Hrs	Improved Impossible Differential Cryptanalysis of 7- round AES-128	Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen and Mahmood Modarres-Hashemi
10:30-11:00 Hrs	Cryptanalysis of a Perturbated White-Box AES Implementation	Yoni De Mulder, Brecht Wyseur and Bart Preneel

- ## Tea Break

Time	Venue
11:00-11:30 Hrs	Sapphire Ballroom - 1

- ## Session 7: Efficient Implementation

Time	Title	Authors
11:30-12:00 Hrs	A Program Generator for Intel AES-NI Instructions	Raymond Manley and David Gregg
12:00-12:30 Hrs	ECC2K-130 on NVIDIA GPUs	Daniel Bernstein, Hsi-Chung Chen, Chen-Mou Cheng, Tanja Lange, Ruben Niederhagen, Peter Schwabe and Bo-Yin Yang
12:30-13:00 Hrs	One Byte per Clock: A Novel RC4 Hardware	Sourav Sen Gupta, Koushik Sinha, Subhamoy Maitra and Bhabani P. Sinha

- ## Lunch Break

Time	Venue
13:00-14:00 Hrs	Sapphire Ballroom - 1