Africacrypt2008
June 11-14, 2008, Casablanca, Morocco

Program

Tuesday, June 10, 2008

17:00 - 20:30	**Registration**
18:00 - 20:30	**Welcome reception**

Wednesday, June 11, 2008

08:00 – 09:00	**Registration**
09:00 – 09:10	**Opening remarks**

Session 1: AES — Chair: Serge Vaudenay

09:10 – 09:40	**Improving Integral Attacks against Rijndael-256 up to 9 Rounds** *Samuel Galice, Marine Minier*
09:40 – 10:10	**Implementation of the AES-128 on Virtex-5 FPGAs** *Philippe Bulens, François-Xavier Standaert, Jean-Jacques Quisquater, Pascal Pellegrin, Gaël Rouvroy*
10:10 – 10:40	**Coffee break**

Session 2: ANALYSIS OF RFID PROTOCOLS — Chair: Serge Vaudenay

10:40 – 11:10	**Weaknesses in a Recent Ultralightweight RFID Authentication Protocol** *Paolo D'Arco, Alfredo De Santis*
11:10 – 11:40	**Differential Cryptanalysis of Reduced-Round PRESENT** *Meiqin Wang*
11:40 – 12:40	**Invited talk 1:** **A Brief History of Provably-Secure Public-Key Encryption** ***Alexander W. Dent***
12:40 – 14:30	**Lunch break**

Session 3: CRYPTOGRAPHIC PROTOCOLS — Chair: Jean-Jacques Quisquater

14:30 – 15:00	**An (Almost) Constant-Effort Solution-Verification Proof-of-Work Protocol based on Merkle Trees** *Fabien Coelho*
15:00 – 15:30	**Robust Threshold Schemes Based on the Chinese Remainder Theorem** *Kamer Kaya, Ali Aydın Seçuk*
15:30 – 16:00	**An Authentication Protocol with Encrypted Biometric Data** *Julien Bringer, Hervé Chabanne*
16:30 – 17:00	**Coffee break**

Session 4: AUTHENTICATION — Chair: Renate Scheidler

17:00 – 17:30	**Authenticated Encryption Mode for Beyond the Birthday Bound Security** *Tetsu Iwata*

17:30 – 18:00 **Cryptanalysis of the TRMS Signature Scheme of PKC'05**
Luk Bettale, Jean-Charles Faugère, Ludovic Perret

Thursday, June 12, 2008

Session 5: PUBLIC-KEY CRYPTOGRAPHY **Chair: Alexander Dent**

09:00 – 09:30 **New Definition of Density on Knapsack Cryptosystems**
Noboru Kunihiro

09:30 – 10:00 **Another Generalization of Wiener's Attack on RSA**
Abderrahmane Nitaj

10:00 – 10:30 **An Adaptation of the NICE Cryptosystem to Real Quadratic Orders**
Michael J. Jacobson, Jr, Renate Scheidler, Daniel Weimer

10:30 – 11:00 **Coffee break**

Session 6: PSEUDORANDOMNESS **Chair: Abdelhak Azhari**

11:00 – 11:30 **A Proof of Security in $O(2^n)$ for the Benes Scheme**
Jacques Patarin

11:30 – 12:30 Invited talk 2:
Modern Cryptography: a Historical Perspective
Jacques Stern

12:30 – 14:30 **Lunch break**

Session 7: ANALYSIS OF STREAM CIPHERS I **Chair: Mitsuru Matsui**

14:30 – 15:00 **Yet Another Attack on Vest**
Pascal Delaunay, Antoine Joux

15:00 – 15:30 **Chosen IV Statistical Analysis for Key Recovery Attacks on Stream Ciphers**
Simon Fischer, Shahram Khazaei, Willi Meier

15:30 – 16:00 **Correlated Keystreams in MOUSTIQUE**
Emilia Käsper, Vincent Rijmen, Tor E. Bjørstad, Christian Rechberger, Matt Robshaw, Gautham Sekar

16:00 – 16:30 **Coffee break**

Session 8: ANALYSIS OF STREAM CIPHERS II **Chair: Tetsu Iwata**

16:30 – 17:00 **Stream Ciphers using a Random Update Function: Study of the Entropy of the Inner State**
Andrea Röck

17:00 – 17:30 **Analysis of Grain's Initialization Algorithm**
Christophe De Canniere, Özgül Küçük, Bart Preneel

17:30 – --:-- **Rump Session** **Chair: Abderrahmane Nitaj**

21:00 – --:-- **Gala dinner**

Friday, June 13, 2008

Session 9: HASH FUNCTIONS **Chair: Daniel Bernstein**

09:00 – 09:30 **Password Recovery on Challenge and Response: Impossible Differential Attack on Hash Function**
Yu Sasaki, Lei Wang, Kazuo Ohta, Noboru Kunihiro

09:30 – 10:00 **How (Not) to Efficiently Dither Blockcipher-Based Hash Functions?**
Jean-Philippe Aumasson and Raphael C.-W. Phan

10:00 – 10:30 **Coffee break**

Session 10: BROADCAST ENCRYPTION **Chair: Tanja Lange**

10:30 – 11:00 **Attribute-Based Broadcast Encryption Scheme Made Efficient**
David Lubicz, Thomas Sirvent

11:00 – 11:30 **Lower Bounds for Subset Cover Based Broadcast Encryption**
Per Austrin, Gunnar Kreitz

11:30 – 12:30 Invited talk 3:
The Psychology of Security
Bruce Schneier

12:30 – 14:30 **Lunch break**

Session 11: IMPLEMENTATION **Chair: Marc Joye**

14:30 – 15:00 **On Compressible Pairings and their Computation**
Michael Naehrig, Paulo S. L. M. Barreto, Peter Schwabe

15:00 – 15:30 **Twisted Edwards Curves**
Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters

15:30 – 16:00 **Efficient Multiplication in $F_{3^{lm}}$**
Murat Cenk, Ferruh Özbudak

16:00 – 16:05 **Closing remarks**

Saturday - Sunday, June 14-15, 2008: Excursion to Marrakech

Departure for Marrakech : Saturday, June 14, 2008 at 09:00
Return to Casablanca : Sunday, June 15, 2008 at 10:00