

**4th International Conference on Cryptology
And Information Security
AFRICACRYPT 2011: PROGRAM
July 05-07, 2011, Dakar, Senegal**

Monday, July 04, 2011

18:00 - 21:30 **Registration**
19:30 - 21:30 **Welcome reception**

Tuesday, July 05, 2011

08:00 - 08:30 **Registration**
08:30 - 08:40 **Opening remarks**

Session 1:	Protocols I	Chair:
1) 08:40 - 09:10	Secure Outsourced Computation Jake Loftus and Nigel P. Smart	
2) 09:10 - 09:40	Fully Simulatable Quantum-Secure Coin-Flipping and Applications Carolin Lunemann and Jesper Buus Nielsen	
3) 09:40 - 10:10	Efficient and Secure General Pattern Matching via Fast Fourier Transform Damien Vergnaud	

10:10 - 10:20 **Free**

Special Session:	Chair: Pr Mamadou Sanghare
10:20 - 11:20	Official Ceremony

11:20 - 11:30 **Coffee break**

Session 2:	Protocols II	Chair:
4) 11:40 - 12:10	Identification Schemes from Key Encapsulation Mechanisms Hiroaki Anada and Seiko Arita	

12:10 - 13:10	Invited talk 1: The NIST SHA-3 Competition: A Perspective on the Final Year Bart Preneel
----------------------	--

13:10 - 15:10 **Lunch break**

Session 3:	Cryptanalysis	Chair:
5) 15:10 - 15:40	Attacking Bivium and Trivium with the Characteristic Set Method Zhenyu Huang and Dongdai Lin	

AFRICACRYPT 2011: PROGRAM

Contacts Fax: 00 221 33 824 63 18, Tel: 00 221 77 184 74 79, 00 221 76 591 34 72 - Email: sowdjibab@ucad.sn, sowdjibab@yahoo.fr

- 6)** 15:40 – 16:10 **Improved Cryptanalysis of the Multi-Prime Φ -Hiding Assumption**
Mathias Herrmann
- 7)** 16:10 – 16:40 **FPGA Implementation of a Statistical Saturation Attack against PRESENT**
Stéphanie Kerckhof, Baudoin Collard and François-Xavier Standaert

16:40 – 17:00 **Coffee break**

- 8)** 17:00 – 17:30 **Collisions of MMO-MD5 and Their Impact on Original MD5**
Yu Sasaki

Session 4: **Secret-Key Cryptography** **Chair:**

- 9)** 17:30 – 18:00 **Really fast syndrome-based hashing**
Daniel J. Bernstein, Tanja Lange, Christiane Peters and Peter Schwabe
- 10)** 18:00 – 18:30 **Montgomery's Trick and Fast Implementation of Masked AES**
Laurie Genelle, Emmanuel Prouff and Michaël Quisquater

Wednesday, July 06, 2011

Session 5: **Efficient Implementations** **Chair:**

- 11)** 09:00 – 09:30 **Memory-Constrained Implementations of Elliptic Curve Cryptography in Co-Z Coordinate Representation**
Michael Hutter, Marc Joye and Yannick Sierra
- 12)** 09:30 – 10:00 **Efficient Multiplication in Finite Field Extensions of Degree 5**
Nadia El Mrabet, Aurore Guillevic and Sorina Ionica

10:00 – 10:30 **Coffee break**

Session 6: **Cryptographic Schemes** **Chair:**

- 13)** 10:30 – 11:00 **Achieving Optimal Anonymity in Transferable E-cash with a Judge**
Olivier Blazy, Sébastien Canard, Georg Fuchsbauer, Aline Gouget, Hervé Sibert and Jacques Traoré
- 14)** 11:00 – 11:30 **Revocable Attribute-Based Signatures with Adaptive Security in the Standard Model**
Alex Escala, Javier Herranz and Paz Morillo

11:30 – 12:30 **Invited talk 2:**
Some Key Techniques on Pairing Vector Spaces
Tasuaki Okamoto and Katsuyuki Takashima

12:40 – 14:30 **Lunch break**

Wednesday, July 06, 2011: 14:30 – 18:00 Excursion

AFRICACRYPT 2011: PROGRAM

Contacts Fax: 00 221 33 824 63 18, Tel: 00 221 77 184 74 79, 00 221 76 591 34 72 - Email: sowdjabab@ucad.sn, sowdjabab@yahoo.fr

19:00 – 20:30

Rump Session

Chair:

21:00 – 23:30

Gala dinner

Thursday, July 07, 2011

Session 7:

Algorithmic Problems

Chair:

15) 09:00 – 09:30

Using the Inhomogeneous Simultaneous Approximation Problem for Cryptographic Design
Frederik Armknecht, Carsten Elsner and Martin Schmidt

16) 09:30 – 10:00

Analyzing standards for RSA integers
Daniel Loebenberger and Michael Nüsken

10:00 – 10:30

Coffee break

Session 8:

Elliptic Curves

Chair:

17) 10:30 – 11:00

Hashing into Hessian Curves
Reza Rezaeian Farashahi

18) 11:00 – 11:30

On Randomness Extraction in Elliptic Curves
Abdoul Aziz Ciss and Djiby Sow

11:30 – 12:30

Invited talk 3:

Efficient Zero-Knowledge Proofs
Jens Groth

12:40 – 14:30

Lunch break

Session 9:

Fault Analysis

Chair:

19) 14:30 – 15:00

Fault Analysis of Grain-128 by Targeting NFSR
Sandip Karmakar and Dipanwita Roy Chowdhury

20) 15:00 – 15:30

Differential Fault Analysis of Sosemanuk
Yaser Esmaeili-Salehani, Aleksandar Kircanski and Amr Youssef

21) 15:30 – 16:00

An Improved Differential Fault Analysis on AES-256
Sk Subidh Ali and Debdeep Mukhopadhyay

16:00 – 16:30

Coffee break

Session 10:

Security Proofs

Chair:

22) 16:30 – 17:00

Benaloh's Dense Probabilistic Encryption Revisited
Laurent Fousse, Pascal Lafourcade and Mohamed Alnuaimi

23) 17:00 – 17:30

On the Security of the Winternitz One-Time Signature Scheme
Johannes Buchmann, Erik Dahmen, Sarah Ereth, Andreas Huelsing and Markus Rueckert

17:30 – 17:45

Closing remarks

AFRICACRYPT 2011: PROGRAM

Contacts Fax: 00 221 33 824 63 18, Tel: 00 221 77 184 74 79, 00 221 76 591 34 72 - Email: sowdijibab@ucad.sn, sowdijibab@yahoo.fr

Contacts

Program Chair:

Professor David Pointcheval

Crypto Team, Computer Science Dept, Ecole Normale Supérieure, Paris, France
Email: david.pointcheval@ens.fr, www.di.ens.fr/users/pointche

General Chair

Professor Mamadou Sangharé

Address: Mr Mamadou Sangharé (Directeur de l'Ecole Doctorale Mathématiques et Informatique)
Département de Mathématiques et d'Informatique
Université Cheikh Anta Diop de Dakar
B P. 5005 Dakar-Fann - SENEGAL
Fax: 00 221 33 824 63 18, Tel: 00 221 77 520 40 82
Email: mamsanghare@ucad.sn, mamsanghare@hotmail.com

Co-Program Chair:

Professor Abderrahmane Nitaj,

University of Caen ,France, Email: nitaj@math.unicaen.fr

Local Organization Committee

Dr Djiby SOW

Address: Département de Mathématiques et d'Informatique, Université Cheikh Anta Diop de Dakar
B P. 5005 Dakar-Fann - SENEGAL
Fax: 00 221 33 824 63 18, Tel: 00 221 77 184 74 79, 00221 76 591 34 72
Email: sowdjibab@ucad.sn, sowdjibab@yahoo.fr

Mr. Babacar Alassane NDAW

Chef du Service Technique Central des Chiffres et de la Sécurité des Télécommunications
Adress: Présidence de la République
BP : 4026 Dakar – Sénégal, Fax : 00 221 33 8232840, Tel : 00 221 33 880 8342 – 00 221 77 638 70 13
Email : babacar_ndaw@orange.fr; stccdir@stcc.presidence.sn

Dr Oumar Diankha

Address: Département de Mathématiques et d'Informatique, Université Cheikh Anta Diop de Dakar
B P. 5005 Dakar-Fann - SENEGAL
Fax: 00 221 33 824 63 18, Tel: 00 2215196267
Email: oumar.diankha@ucad.edu.sn, odiankha@ucad.sn

Dr Cheikh Thiécoumba Gueye

Address: Département de Mathématiques et d'Informatique, Université Cheikh Anta Diop de Dakar
B P. 5005 Dakar-Fann - SENEGAL
Fax: 00 221 33 824 63 18, Tel: 00 22177 630 47 70
Email: cheikht.gueye@ucad.edu.sn, thgueye@yahoo.fr

AFRICACRYPT 2011: PROGRAM

Contacts Fax: 00 221 33 824 63 18, Tel: 00 221 77 184 74 79, 00 221 76 591 34 72 - Email: sowdjibab@ucad.sn, sowdjibab@yahoo.fr