Workshop on Cryptographic Hardware and Embedded Systems

Lausanne
OLYMPIC CAPITAL

CHES 2009
September 6th – 9th

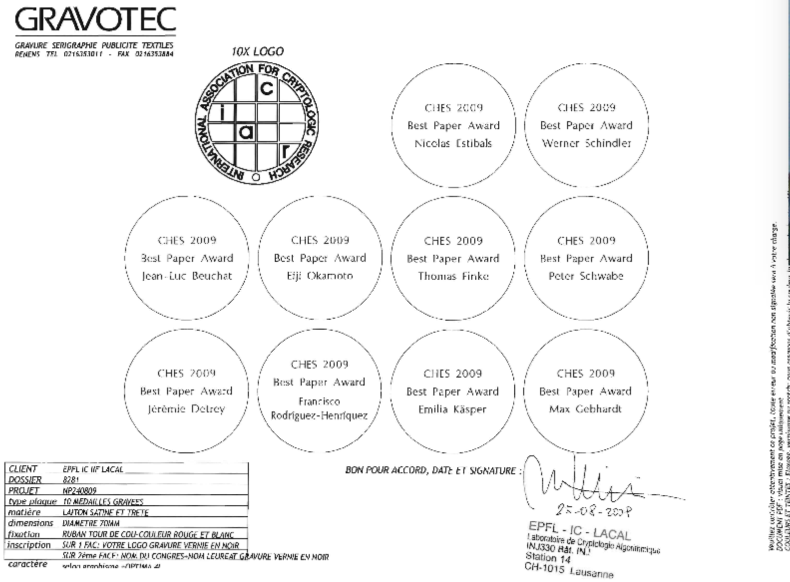
Switzerland

© LT/Régis Colombo - www.diapo.ch

Best Paper Award Presentations

Best Paper Awards

Personalized Medals



GRAVOTEC
GRAVURE SERIGRAPHIE PUBLICITE TEXTILES
RENENS TEL 0216353011 - FAX 0216353884

10X LOGO

CHES 2009
Best Paper Award
Nicolas Estibals

CHES 2009
Best Paper Award
Werner Schindler

CHES 2009
Best Paper Award
Jean-Luc Beuchat

CHES 2009
Best Paper Award
Eiji Okamoto

CHES 2009
Best Paper Award
Thomas Finke

CHES 2009
Best Paper Award
Peter Schwabe

CHES 2009
Best Paper Award
Jérémie Detrey

CHES 2009
Best Paper Award
Francisco
Rodriguez-Henriquez

CHES 2009
Best Paper Award
Emilia Käsper

CHES 2009
Best Paper Award
Max Gebhardt

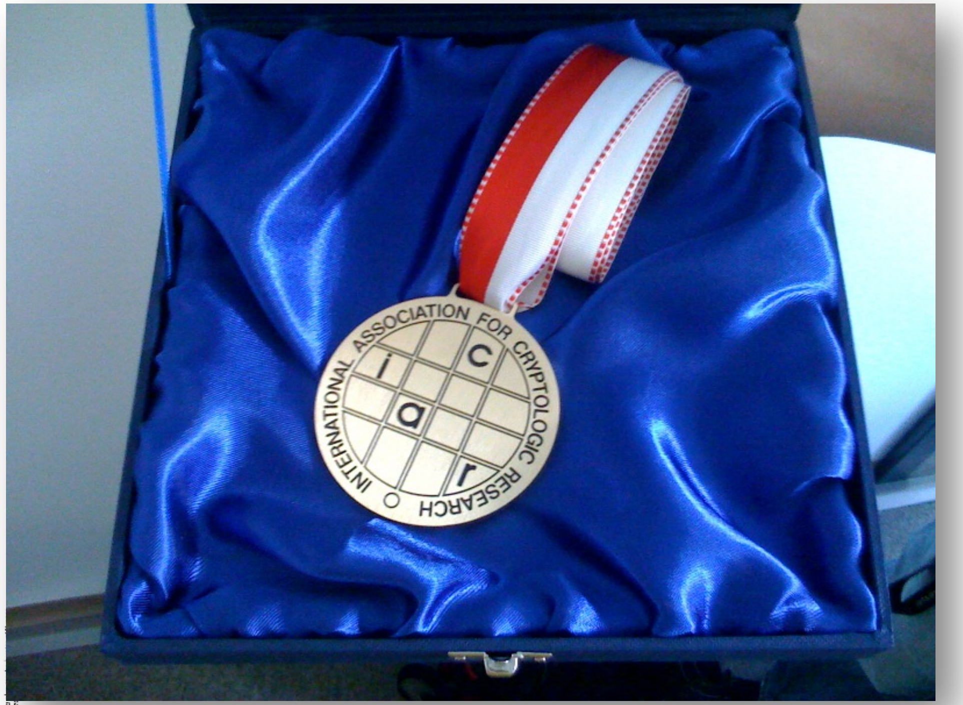
CLIENT	EPFL IC IIF LACAL
DOSSIER	8281
PROJET	NP240809
type plaque	10 MEDAILLES GRAVEES
matière	LAITON SATINE ET TRETE
dimensions	DIAMETRE 70MM
fixation	RUBAN TOUR DE COU-COULEUR ROUGE ET BLANC
inscription	SUR 1 FAC: VOTRE LOGO GRAVURE VERNIE EN NOIR SUR 2ème FACE: NOM DU CONGRES-NOM LEUREAT GRAVURE VERNIE EN NOIR
caractère	selon graphisme -OPTIMA-

BON POUR ACCORD, DATE ET SIGNATURE :

25-08-2009

EPFL - IC - LACAL
Laboratoire de Cryptologie Algorithmique
INJ330 Bât. INJ
Station 14
CH-1015 Lausanne

Veuillez contrôler attentivement ce projet, toute erreur ou modification non signalée sera à votre charge.
DOCUMENT PDF : visuel mise en page uniquement
COULEURS ET TEINTES : Eloxage, vernissage ou scotch: nous essayons d'obtenir la couleur la
GRAPHISME : nous nous efforçons de respecter au mieux votre graphisme selon exigences te



Selection Process

- Two papers with the highest average reviewer scores nominated by Program Chairs

- One more paper nominated by a Program Committee Member

- Vote of the Program Committee

Vote Results & Final Decision

- Coincidentally, all candidate papers received an equal amount of
  27 points.

- Decision by the PC to exceptionally award three equivalent awards

Topics

- efficient and secure **software implementations** of **secret key cryptography** (AES-GCM)

- efficient **hardware implementations** of **public key cryptography** (pairing)

- **side-channel attacks** and countermeasures (RSA prime number generation).

Best Paper Award

Emilia Käsper
Katholieke Universiteit Leuven, ESAT/COSIC

Peter Schwabe
Department of Mathematics and Computer Science
Technische Universiteit Eindhoven

Faster and Timing-Attack Resistant AES-GCM

Best Paper Award

Jean-Luc Beuchat[1],
Jérémie Detrey[2],
Nicolas Estibals[2],
Eiji Okamoto[1], and
Francisco Rodríguez-Henríquez[3]

[1]University of Tsukuba, Japan
[2]LORIA, INRIA Nancy, France
[3]CINVESTAV-IPN, Mexico

Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers

Best Paper Award

Thomas Finke
Max Gebhardt
Werner Schindler

BSI, Germany

A New Side-Channel Attack on RSA Prime Generation

Congratulations to all winners!!!