

Table of Contents

Personal Tributes and Re-visits of Jean-Jacques's Legacy

The Hidden Side of Jean-Jacques Quisquater	1
<i>Michaël Quisquater</i>	
On Quisquater's Multiplication Algorithm	3
<i>Marc Joye</i>	
A Brief Survey of Research Jointly with Jean-Jacques Quisquater	8
<i>Yvo Desmedt</i>	
DES Collisions Revisited	13
<i>Sebastiaan Indestege and Bart Preneel</i>	
Line Directed Hypergraphs	25
<i>Jean-Claude Bermond, Fahir Ergincan, and Michel Syska</i>	

Symmetric Cryptography

Random Permutation Statistics and an Improved Slide-Determine Attack on KeeLoq	35
<i>Nicolas T. Courtois and Gregory V. Bard</i>	
Self-similarity Attacks on Block Ciphers and Application to KeeLoq	55
<i>Nicolas T. Courtois</i>	
Increasing Block Sizes Using Feistel Networks: The Example of the AES	67
<i>Jacques Patarin, Benjamin Gittins, and Joana Treger</i>	
Authenticated-Encryption with Padding: A Formal Security Treatment	83
<i>Kenneth G. Paterson and Gaven J. Watson</i>	

Asymmetric Cryptography

Traceable Signature with Stepping Capabilities	108
<i>Olivier Blazy and David Pointcheval</i>	
Deniable RSA Signature: The Raise and Fall of Ali Baba	132
<i>Serge Vaudenay</i>	

Autotomic Signatures	143
<i>David Naccache and David Pointcheval</i>	
Fully Forward-Secure Group Signatures	156
<i>Benoît Libert and Moti Yung</i>	
Public Key Encryption for the Forgetful	185
<i>Puwen Wei, Yuliang Zheng, and Xiaoyun Wang</i>	
Supplemental Access Control (PACE v2): Security Analysis of PACE Integrated Mapping	207
<i>Jean-Sébastien Coron, Aline Gouget, Thomas Icart, and Pascal Paillier</i>	

Side Channel Attacks

Secret Key Leakage from Public Key Perturbation of DLP-Based Cryptosystems	233
<i>Alexandre Berzati, Cécile Canovas-Dumas, and Louis Goubin</i>	
EM Probes Characterisation for Security Analysis	248
<i>Benjamin Mounier, Anne-Lise Ribotta, Jacques Fournier, Michel Agoyan, and Assia Tria</i>	
An Updated Survey on Secure ECC Implementations: Attacks, Countermeasures and Cost	265
<i>Junfeng Fan and Ingrid Verbauwhede</i>	
Masking with Randomized Look Up Tables: Towards Preventing Side-Channel Attacks of All Orders	283
<i>François-Xavier Standaert, Christophe Petit, and Nicolas Veyrat-Charvillon</i>	

Hardware and Implementations

Efficient Implementation of True Random Number Generator Based on SRAM PUFs	300
<i>Vincent van der Leest, Erik van der Sluis, Geert-Jan Schrijen, Pim Tuyls, and Helena Handschuh</i>	
Operand Folding Hardware Multipliers	319
<i>Byungchun Chung, Sandra Marcello, Amir-Pasha Mirbaha, David Naccache, and Karim Sabeg</i>	
SIMPL Systems as a Keyless Cryptographic and Security Primitive	329
<i>Ulrich Rührmair</i>	

Cryptography with Asynchronous Logic Automata	355
<i>Peter Schmidt-Nielsen, Kailiang Chen, Jonathan Bachrach, Scott Greenwald, Forrest Green, and Neil Gershenfeld</i>	
A Qualitative Security Analysis of a New Class of 3-D Integrated Crypto Co-processors	364
<i>Jonathan Valamehr, Ted Huffmire, Cynthia Irvine, Ryan Kastner, Çetin Kaya Koç, Timothy Levin, and Timothy Sherwood</i>	
Smart Cards and Information Security	
The Challenges Raised by the Privacy-Preserving Identity Card	383
<i>Yves Deswarte and Sébastien Gambs</i>	
The Next Smart Card Nightmare: Logical Attacks, Combined Attacks, Mutant Applications and Other Funny Things	405
<i>Guillaume Bouffard and Jean-Louis Lanet</i>	
Localization Privacy	425
<i>Mike Burmester</i>	
Dynamic Secure Cloud Storage with Provenance	442
<i>Sherman S.M. Chow, Cheng-Kang Chu, Xinyi Huang, Jianying Zhou, and Robert H. Deng</i>	
Efficient Encryption and Storage of Close Distance Messages with Applications to Cloud Storage	465
<i>George Davida and Yair Frankel</i>	
As Diverse as Jean-Jacques' Scientific Interests	
A Nagell Algorithm in Any Characteristic	474
<i>Mehdi Tibouchi</i>	
How to Read a Signature?	480
<i>Vanessa Gratzner and David Naccache</i>	
Fooling a Liveness-Detecting Capacitive Fingerprint Scanner	484
<i>Edwin Bowden-Peters, Raphael C.-W. Phan, John N. Whitley, and David J. Parish</i>	
Physical Simulation of Inarticulate Robots	491
<i>Guillaume Claret, Michaël Mathieu, David Naccache, and Guillaume Seguin</i>	
Author Index	501