

Contents

History

Mary of Guise's Enciphered Letters.	3
<i>Valérie Nachev, Jacques Patarin, and Armel Dubois-Nayt</i>	
About Professionalisation in the Intelligence Community: The French Cryptologists (ca 1870–ca 1945)	25
<i>Sébastien-Yves Laurent</i>	
Myths and Legends of the History of Cryptology	34
<i>Sophie de Lastours</i>	
Vernam, Mauborgne, and Friedman: The One-Time Pad and the Index of Coincidence	40
<i>Steven M. Bellovin</i>	

Technology - Past, Present, Future

The Fall of a Tiny Star	69
<i>Flavio D. Garcia and Bart Jacobs</i>	
Post-Quantum Cryptography: State of the Art.	88
<i>Johannes A. Buchmann, Denis Butin, Florian Göpfert, and Albrecht Petzoldt</i>	
What is the Future of Cryptography?.	109
<i>Yvo Desmedt</i>	

Efficient Cryptographic Implementations

Bitsliced High-Performance AES-ECB on GPUs.	125
<i>Rone Kwei Lim, Linda Ruth Petzold, and Çetin Kaya Koç</i>	
Buying AES Design Resistance with Speed and Energy.	134
<i>Rodrigo Portella do Canto, Roman Korkikian, and David Naccache</i>	
Double-Speed Barrett Moduli	148
<i>Rémi Géraud, Diana Maimuț, and David Naccache</i>	

Treachery and Perfidy

Failure is Also an Option.	161
<i>Antoine Amarilli, Marc Beunardeau, Rémi Géraud, and David Naccache</i>	

How to (Carefully) Breach a Service Contract?	166
<i>Céline Chevalier, Damien Gaumont, David Naccache, and Rodrigo Portella Do Canto</i>	

Information Security

SpoofKiller: You Can Teach People How to Pay, but Not How to Pay Attention	177
<i>Markus Jakobsson and Hossein Siadati</i>	

Cyber-Physical Systems Security.	195
<i>Dieter Gollmann and Marina Krotofil</i>	

Practical Techniques Building on Encryption for Protecting and Managing Data in the Cloud	205
<i>Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, and Pierangela Samarati</i>	

Cryptanalysis

Cryptography as an Attack Technology: Proving the RSA/Factoring Kleptographic Attack.	243
<i>Adam Young and Moti Yung</i>	

Dual EC: A Standardized Back Door.	256
<i>Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen</i>	

An Improved Differential Attack on Full GOST	282
<i>Nicolas T. Courtois</i>	

Cryptographic Hash Functions and Expander Graphs: The End of the Story?	304
<i>Christophe Petit and Jean-Jacques Quisquater</i>	

Side-Channel Attacks

Polynomial Evaluation and Side Channel Analysis	315
<i>Claude Carlet and Emmanuel Prouff</i>	

Photonic Power Firewalls.	342
<i>Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache, and Assia Tria</i>	

A Heuristic Approach to Assist Side Channel Analysis of the Data Encryption Standard	355
<i>Christophe Clavier and Djamal Rebaïne</i>	

Improving the Big Mac Attack on Elliptic Curve Cryptography	374
<i>Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica, and David Naccache</i>	

Randomness

Randomness Testing: Result Interpretation and Speed	389
<i>Marek Sýs and Vashek Matyáš</i>	
A Fully-Digital Chaos-Based Random Bit Generator	396
<i>Marco Bucci and Raimondo Luzzi</i>	

Embedded System Security

Secure Application Execution in Mobile Devices	417
<i>Mehari G. Msgna, Houda Ferradi, Raja Naeem Akram, and Konstantinos Markantonakis</i>	
Hardware-Enforced Protection Against Buffer Overflow Using Masked Program Counter.	439
<i>Jean-Luc Danger, Sylvain Guilley, Thibault Porteboeuf, Florian Praden, and Michaël Timbert</i>	

Public-Key Cryptography

Hierarchical Identities from Group Signatures and Pseudonymous Signatures	457
<i>Julien Bringer, Hervé Chabanne, Roch Lescuyer, and Alain Patey</i>	
Secure ElGamal-Type Cryptosystems Without Message Encoding.	470
<i>Marc Joye</i>	
Safe-Errors on SPA Protected Implementations with the Atomicity Technique.	479
<i>Pierre-Alain Fouque, Sylvain Guilley, Cédric Murdica, and David Naccache</i>	

Models and Protocols

Clever Arbiters Versus Malicious Adversaries: On the Gap Between Known-Input Security and Chosen-Input Security	497
<i>Serge Vaudenay</i>	
Security Analysis of the Modular Enhanced Symmetric Role Authentication (mERA) Protocol	518
<i>Jean-Sébastien Coron</i>	

Crypto Santa	543
<i>Peter Y.A. Ryan</i>	
Author Index	551

<http://www.springer.com/978-3-662-49300-7>

The New Codebreakers

Essays Dedicated to David Kahn on the Occasion of His
85th Birthday

Ryan, P.Y.A.; Naccache, D.; Quisquater, J.-J. (Eds.)

2016, XIV, 551 p. 135 illus., Softcover

ISBN: 978-3-662-49300-7