

# Contents

## History

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

## Technology - Past, Present, Future

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

## Efficient Cryptographic Implementations

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

## Treachery and Perfidy

- Failure is Also an Option. . . . . 161  
*Antoine Amarilli, Marc Beunardeau, Rémi Géraud, and David Naccache*

How to (Carefully) Breach a Service Contract? . . . . . 166  
*Céline Chevalier, Damien Gaumont, David Naccache,  
and Rodrigo Portella Do Canto*

**Information Security**

SpoofKiller: You Can Teach People How to Pay, but Not How  
to Pay Attention . . . . . 177  
*Markus Jakobsson and Hossein Siadati*

Cyber-Physical Systems Security. . . . . 195  
*Dieter Gollmann and Marina Krotofil*

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

**Cryptanalysis**

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

Dual EC: A Standardized Back Door. . . . . 256  
*Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen*

An Improved Differential Attack on Full GOST . . . . . 282  
*Nicolas T. Courtois*

Cryptographic Hash Functions and Expander Graphs: The End  
of the Story? . . . . . 304  
*Christophe Petit and Jean-Jacques Quisquater*

**Side-Channel Attacks**

Polynomial Evaluation and Side Channel Analysis . . . . . 315  
*Claude Carlet and Emmanuel Prouff*

Photonic Power Firewalls. . . . . 342  
*Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache,  
and Assia Tria*

A Heuristic Approach to Assist Side Channel Analysis of the Data  
Encryption Standard . . . . . 355  
*Christophe Clavier and Djamel Rebaïne*

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

**Randomness**

Randomness Testing: Result Interpretation and Speed . . . . . 389  
*Marek Sýs and Vashek Matyáš*

A Fully-Digital Chaos-Based Random Bit Generator . . . . . 396  
*Marco Bucci and Raimondo Luzzi*

**Embedded System Security**

Secure Application Execution in Mobile Devices . . . . . 417  
*Mehari G. Msgna, Houda Ferradi, Raja Naeem Akram,  
and Konstantinos Markantonakis*

Hardware-Enforced Protection Against Buffer Overflow Using Masked  
Program Counter. . . . . 439  
*Jean-Luc Danger, Sylvain Guilley, Thibault Porteboeuf, Florian Praden,  
and Michaël Timbert*

**Public-Key Cryptography**

Hierarchical Identities from Group Signatures and Pseudonymous  
Signatures . . . . . 457  
*Julien Bringer, Hervé Chabanne, Roch Lescuyer, and Alain Patey*

Secure ElGamal-Type Cryptosystems Without Message Encoding. . . . . 470  
*Marc Joye*

Safe-Errors on SPA Protected Implementations  
with the Atomicity Technique. . . . . 479  
*Pierre-Alain Fouque, Sylvain Guilley, Cédric Murdica,  
and David Naccache*

**Models and Protocols**

Clever Arbiters Versus Malicious Adversaries: On the Gap  
Between Known-Input Security and Chosen-Input Security . . . . . 497  
*Serge Vaudenay*

Security Analysis of the Modular Enhanced Symmetric Role Authentication  
(mERA) Protocol . . . . . 518  
*Jean-Sébastien Coron*

Crypto Santa ..... 543  
*Peter Y.A. Ryan*

**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