

Rump Session 2016



The New Codebreakers: a challenge

Jean-Jacques Quisquater

UCLouvain, Belgium

The New Codebreakers

A Celebration of the 80th Birthday of David Kahn



Université du Luxembourg - Campus Limpertsberg

Luxembourg, June 28-29, 2010

Home

Programme

Organizers

Registration

Conference Venue

Social Event and News

Travel and Accommodation

Sponsors

The logo for SNT (Société Nationale de Télécommunications) features the letters 'SNT' in a bold, sans-serif font. A horizontal bar below the letters is divided into three segments of red, blue, and green.

The logo for the University of Luxembourg features the letters 'uni.lu' in a stylized font where the 'i' and 'l' are connected. Below it, the text 'UNIVERSITÉ DU LUXEMBOURG' is written in a smaller, sans-serif font.

The logo for CSC (Computer Science and Communications Research Unit) features the letters 'CSC' in a large, bold, sans-serif font. To the right, the full name 'Computer Science and Communications Research Unit' is written in a smaller font.

The logo for LACS (Luxembourg Academic Centre for Security) features the letters 'LACS' in a bold, sans-serif font. The letters are filled with a colorful, abstract pattern.

The logo for the Fonds National de la Recherche Luxembourg features a stylized 'L' shape composed of two overlapping squares, one blue and one green. To the right, the text 'Fonds National de la Recherche Luxembourg' is written in a sans-serif font.

Background

The purpose of this event is to celebrate the 80th year of the eminent writer and historian of cryptography and intelligence [David Kahn](#).

Dr Kahn is arguably the most famous writer on these subjects. In particular, he is the author of the famed book "[The Codebreakers](#)". This appeared in the 60s and for decades was the only widely available and readable book on the making and breaking of codes and ciphers. For many researchers in the field this book was an inspiration and a key ingredient in setting them on their professional course.

The event brings together several eminent researchers in cryptography and the history of intelligence. Anyone interested in the event and in its topics is warmly invited to attend. There is no registration fee but, as we expect this to be a very popular event and the venue has limited space, we advise early registration. To register please visit our [registration page](#).

News

- *News*: Special rate for the Hotels;
- *News*: Social event location

More information on our [news page](#).



Crypto 2011 Rump Session


The Crypto 2011 Rump Session took place Tuesday 16 August 2011 from 19:30 PDT to 23:00 PDT. Daniel J. Bernstein and Tanja Lange served as chairs. Jim Hughes provided assistance in program selection. Christiane Peters served as horn-blower. Nadia Heninger prepared slides for the panel discussion. The rump session was broadcast live, and there is a [Youtube playlist](#) available.

The call for submissions has been archived on a [separate page](#). Slides and video are now available from all presenters who agreed to have their slides officially online.

	Authors	Speaker	Title	Slides	Video
	Session 1				
19:30	Bart Preneel	Bart Preneel	The 2011 IACR Fellowship Induction Ceremony		Video
19:55	Andy Clark, Whit Diffie, David Naccache, Jean-Jacques Quisquater, Peter Ryan	Jean-Jacques Quisquater	An historical call for papers ...	slides	Video
19:57	Christiane Peters	Christiane Peters	Playing "Spot the Difference" with Springer	slides	
20:00	Eli Biham, Nathan Keller, Orr Dunkelman, Adi Shamir	Orr Dunkelman	Rethinking IDEA	slides	Video
20:04	Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger	Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger	Biclique cryptanalysis of the full AES	slides	Video
20:10	Niels Ferguson	Niels Ferguson	Observations on H-PRESENT-128	slides	Video
20:14	Faith Chaza and Ian Goldberg	Faith Chaza and Ian Goldberg	An Application Of Frequency Shift Keying To Communication Resynchronisation	slides	Video

THE NEW CODEBREAKERS

rump session EUROCRYPT 2016, Wien



THE NEW CODEBREAKERS [NEW BRACKETED HEROES]

Donald Trump session EUROCRYPT 2016, Wien

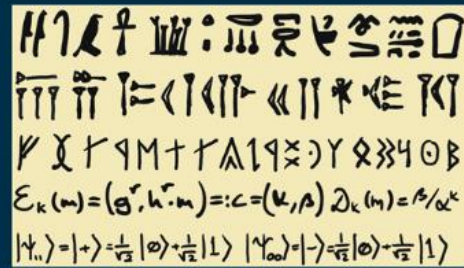
Festschrift

LNCS 9100

Peter Y.A. Ryan
David Naccache
Jean-Jacques Quisquater (Eds.)

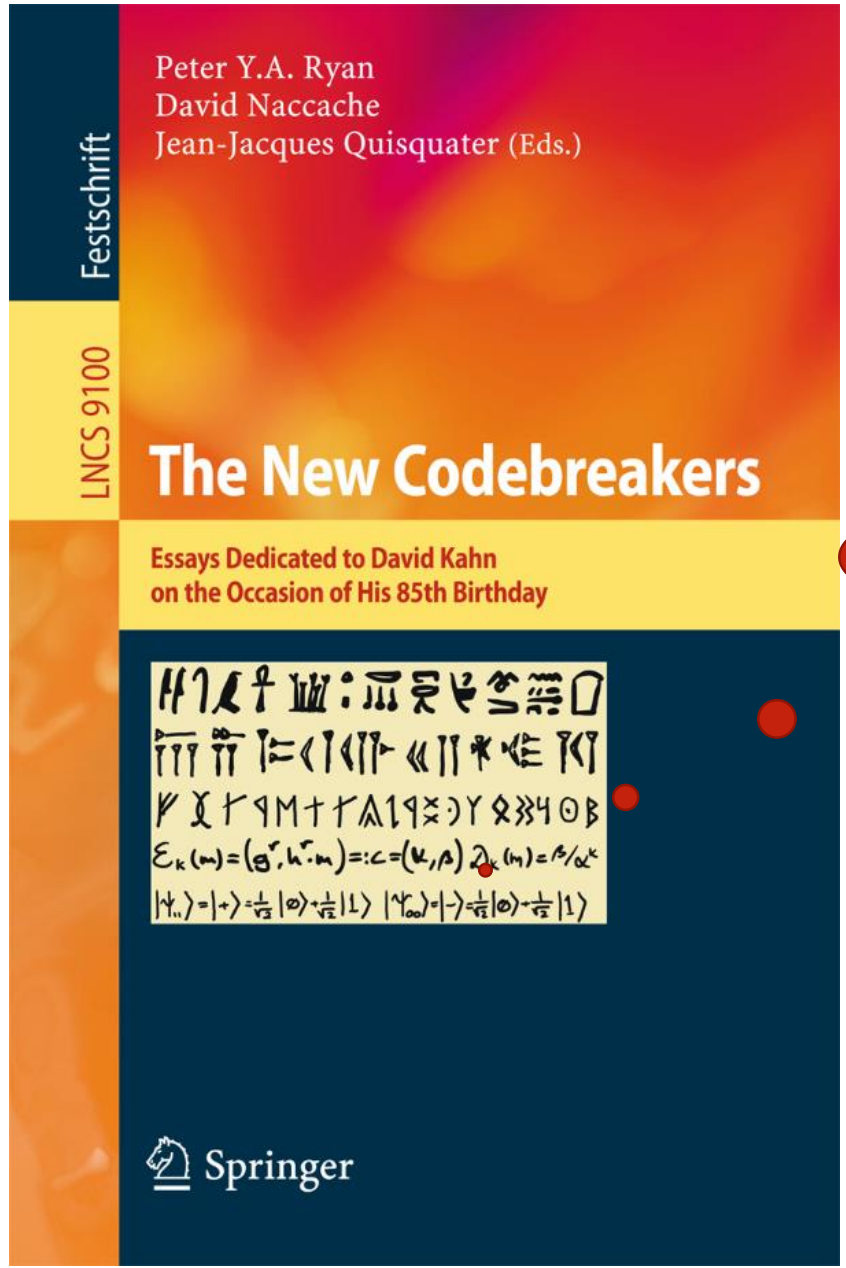
The New Codebreakers

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



$$\begin{aligned} & \text{H} \text{I} \text{J} \text{K} \text{L} \text{M} \text{N} \text{O} \text{P} \text{Q} \text{R} \text{S} \text{T} \text{U} \text{V} \text{W} \text{X} \text{Y} \text{Z} \text{[} \text{] } \\ & \text{a} \text{b} \text{c} \text{d} \text{e} \text{f} \text{g} \text{h} \text{i} \text{j} \text{k} \text{l} \text{m} \text{n} \text{o} \text{p} \text{q} \text{r} \text{s} \text{t} \text{u} \text{v} \text{w} \text{x} \text{y} \text{z} \\ & \text{A} \text{B} \text{C} \text{D} \text{E} \text{F} \text{G} \text{H} \text{I} \text{J} \text{K} \text{L} \text{M} \text{N} \text{O} \text{P} \text{Q} \text{R} \text{S} \text{T} \text{U} \text{V} \text{W} \text{X} \text{Y} \text{Z} \\ & \text{E}_k(m) = (\theta^k \cdot h^k \cdot m) = c = (u, p) \quad \mathcal{D}_k(m) = p^k / \alpha^k \\ & | \psi_n \rangle = | + \rangle = \frac{1}{\sqrt{2}} (| 0 \rangle + \frac{1}{\sqrt{2}} | 1 \rangle) \quad | \psi_{\infty} \rangle = | - \rangle = \frac{1}{\sqrt{2}} (| 0 \rangle - \frac{1}{\sqrt{2}} | 1 \rangle) \end{aligned}$$

 Springer



Peter Y.A. Ryan
David Naccache
Jean-Jacques Quisquater (Eds.)

Festschrift

LNCS 9100

The New Codebreakers

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

Handwritten-style text and mathematical formulas, including a cipher and the formula $E_k(m) = (a \cdot m) \pmod{n}$.

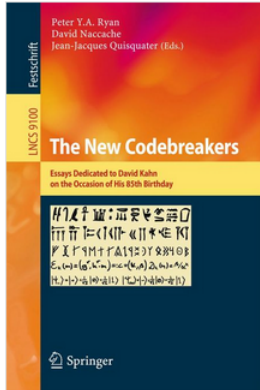
 Springer

Mozart?

Author Index

- Akram, Raja Naeem 417
Amarilli, Antoine 161
- Bellovin, Steven M. 40
Bernstein, Daniel J. 256
Beunardeau, Marc 161
Bringer, Julien 457
Bucci, Marco 396
Buchmann, Johannes A. 88
Butin, Denis 88
- Carlet, Claude 315
Chabanne, Hervé 457
Chevalier, Céline 166
Clavier, Christophe 355
Coron, Jean-Sébastien 518
Courtois, Nicolas T. 282
- Danger, Jean-Luc 374, 439
De Capitani di Vimercati, Sabrina 205
de Lastours, Sophie 34
Desmedt, Yvo 109
Do Canto, Rodrigo Portella 166
Dubois-Nayt, Armel 3
Dutertre, Jean-Max 342
- Ferradi, Houda 417
Foresti, Sara 205
Fouque, Pierre-Alain 479
- Garcia, Flavio D. 69
Gaumont, Damien 166
Géraud, Rémi 148, 161
Gollmann, Dieter 195
Göpfert, Florian 88
Guilley, Sylvain 374, 439, 479
- Hoogvorst, Philippe 374
- Jacobs, Bart 69
Jakobsson, Markus 177
Joye, Marc 470
- Koç, Çetin Kaya 125
Korkikian, Roman 134
Krotofil, Marina 195
- Lange, Tanja 256
Laurent, Sébastien-Yves 25
Lescuyer, Roch 457
Lim, Rone Kwei 125
Livraga, Giovanni 205
Luzzi, Raimondo 396
- Maimuț, Diana 148
Markantonakis, Konstantinos 417
Matyáš, Vashek 389
Mirbaha, Amir-Pasha 342
Msgna, Mehan G. 417
Murdica, Cédric 374, 479
- Naccache, David 134, 148, 161, 166,
342, 374, 479
Nacheff, Valérie 3
Niederhagen, Ruben 256
- Patarin, Jacques 3
Patey, Alain 457
Petit, Christophe 304
Petzold, Linda Ruth 125
Petzoldt, Albrecht 88
Porteboeuf, Thibault 439
Portella do Canto, Rodrigo 134
Praden, Florian 439
Prouff, Emmanuel 315
- Quisquater, Jean-Jacques 304
- Rebaine, Djamel 355
Ryan, Peter Y.A. 543
- Samarati, Pierangela 205
Siadati, Hossein 177
Sýs, Marek 389
- Timbert, Michaël 439
Tría, Assia 342
- Vaudenay, Serge 497
- Young, Adam 243
Yung, Moti 243

73 authors



THE NEW CODEBREAKERS - 2016

EDITORS Peter Y. A. Ryan • David Naccache • Jean-Jacques Quisquater

ISBN 9783662493014 • 9783662493007

DOI 10.1007/978-3-662-49301-4

[VIEW ON PUBLISHER SITE](#)

SHOW ACTIVITY FOR:

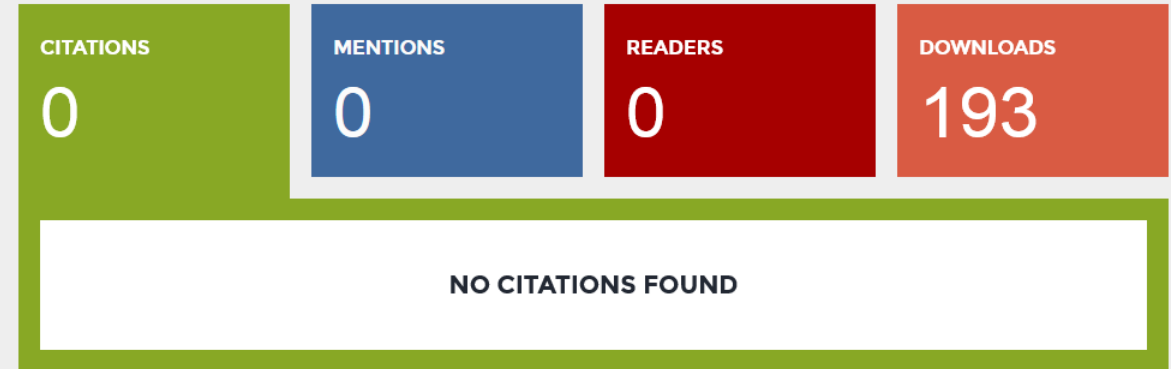
- SUMMARY** 0 2 2 8K 0
 Combined activity for all chapters
- CHAPTER 1** 0 0 0 167
 Mary of Guise's Enciphered Letters
- CHAPTER 2** 0 0 0 165
 About Professionalisation in the Intelligence Community: The French Cryptologists (ca 1870–ca 1945)
- CHAPTER 3** 0 0 0 171
 Myths and Legends of the History of Cryptology
- CHAPTER 4** 0 0 0 166

ALL ACTIVITY FOR CHAPTER:

Post-Quantum Cryptography: State of the Art

AUTHORS Johannes A. Buchmann • Denis Butin • Florian Göpfert • Albrecht Petzoldt

DOI 10.1007/978-3-662-49301-4_6





ONE VOLUME FOR YOU, THANKS TO SPRINGER

- I've one: how to share it?
- Setting a challenge!



THE AUTHOR OF THE NEXT DRAWING?

- Send me an email to jjq@uclouvain.be

