Cryptography and cryptanalysis call for efficient hardware modules. For example, when mounting an attack against a cipher, the attacker's budget and/or hardware resources are typically limited. Efficient implementation of hardware modules allows faster attack and improves cost-performance ratio.

In the first part of this thesis, the author focuses on hardware architectures operating over elements of binary finite fields in normal basis representation. Such architectures are applicable e.g. in Elliptic Curve Cryptography, which finds its use in constantly expanding areas of applications. Four new architectures of digit-serial normal basis multipliers are presented. Based on these architectures, a novel structure of a normal basis arithmetic unit is proposed. As the unit is both small and scalable, the design constraints can be met optimally.

The second part of the thesis focuses on the cryptanalysis of the A5/1 cipher used in GSM communications. Hardware architectures of two attacks against the A5/1 cipher are presented. They represent the first real-world implementations of attacks against A5/1 reported in open literature. The attacks have been implemented using an existing low-cost special-purpose hardware device: COPACOBANA. The attacks are designed to utilize both the properties of the cipher and the features of underlying reconfigurable hardware. Presented design approaches can be reused when designing attacks against similar ciphers.

Martin Novotný graduated in electrical engineering from the Czech Technical University in Prague, Czech Republic in 1992. In 2003, he started his PhD studies under the supervision of Prof. Jan Schmidt, Department of Computer Science and Engineering at CTU in Prague. Since 2007, he continued his PhD studies under the supervision of Prof. Christof Paar, Chair for Embedded Security at Ruhr-University Bochum, Germany.

His research interests include arithmetic units, cryptanalytical hardware and efficient hardware implementations of cryptographic algorithms.

BOCHUMER UNIVERSITÄTS-VERLAG
WWW.BOUDE

9 783899 663464

EUROPEAN UNIVERSITY PRESS
CON-SCIEN-TIA
COG-NI-TIO
AD USUM

ISBN 978-3-89966-346-4 • 24,90 €

IT 12

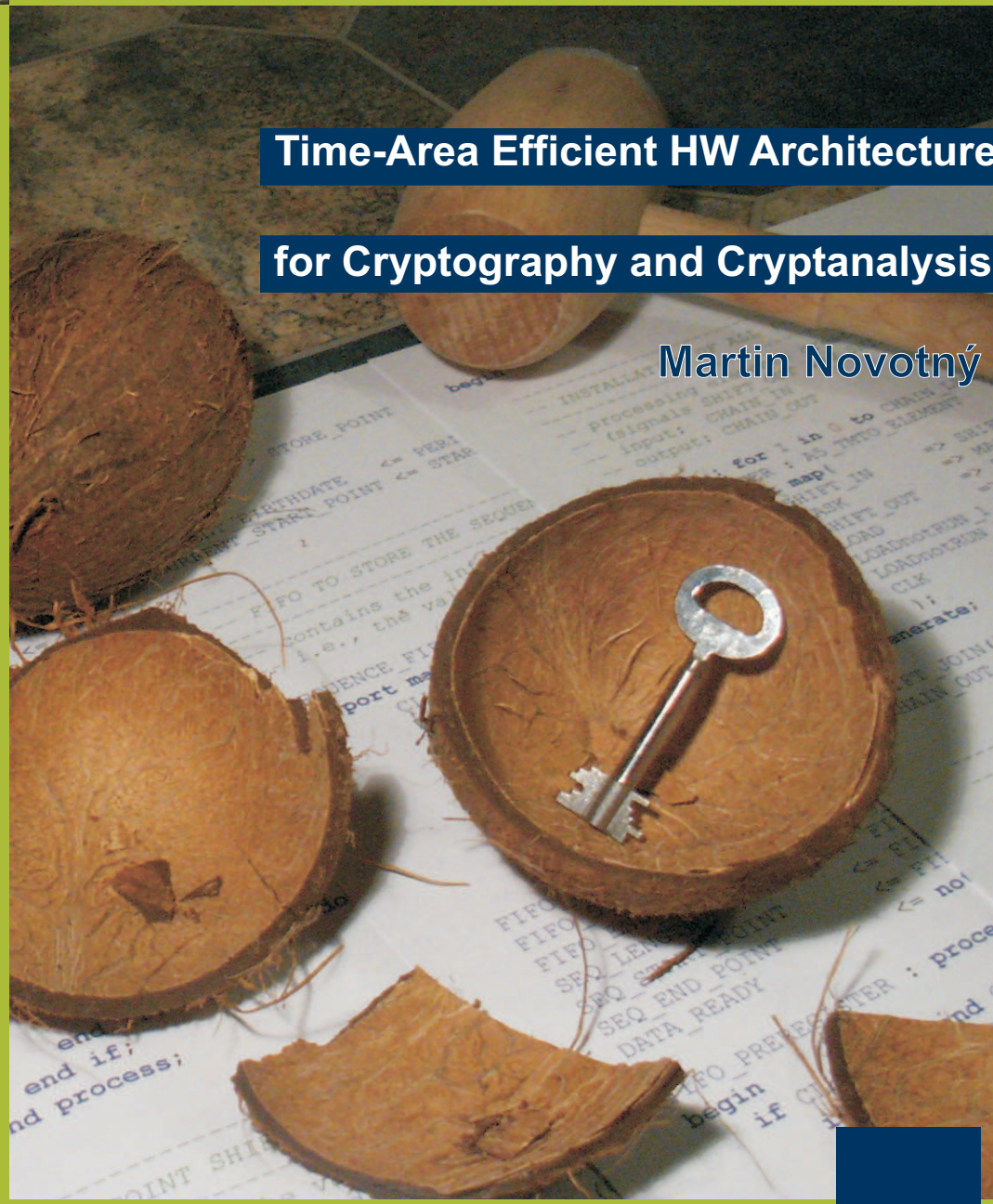
Novotný: Time-Area Efficient HW Architectures for Cryptography

RUHR-UNIVERSITÄT BOCHU

Time-Area Efficient HW Architecture

for Cryptography and Cryptanalysis

Martin Novotný



IT-SECURITY 12

RUB