COLLECTIO CIPHRARUM

Book Series

2

COLLECTIO CIPHRARUM

Book Series

The method is capable of dispatching with accuracy every kind of urgent messages, but in practice it requires care and exact attention.
(Polybius 150 BC)

La collana Collectio Ciphrarum pubblica atti di convegni e workshop in crittografia e argomenti affini, inclusi cicli di seminari di ampia durata. La collana ospita con preferenza non esclusiva atti di convegni in Italia o organizzati congiuntamente da sedi italiane e straniere. Di norma ogni volume ospita tra dieci e venti interventi, in formato di extended abstract ciascuno in lingua inglese, più eventuali survey tematici dietro invito degli editor. Gli abstract possono anche riassumere risultati già pubblicati in altre sedi. Tutti i contributi sono referati in maniera anonima da esperti internazionali. Gli organizzatori di un workshop sono invitati a proporre la pubblicazione degli atti nella Collectio Ciphrarum contattando il Board.

The book series Collectio Ciphrarum presents proceedings papers of talks given at workshops/conferences in Cryptography and related matters, including talks given at organized seminar series. Collectio Ciphrarum has a keen interest in workshops/conferences that are either held in Italy or co-organized by at least one Italian research institution. A book will usually contain ten to twenty extended abstracts, sketching research that may be published in another publication venue, plus invited surveys, which are meant to be published exclusively here. All papers are refereed by anonymous international experts. Any organizer of a workshop/conference, falling in the book series scope, is invited to contact the Editorial Board for proposing a new volume.

DE CIFRIS CRYPTANALYSIS

SELECTED PAPERS FROM THE ITASEC2020 WORKSHOP *CRYPTANALYSIS A KEY TOOL IN SECURING AND BREAKING CIPHERS*

edited by

ROBERTO LA SCALA, MARCO PEDICINI, ANDREA VISCONTI

preface by

MASSIMILIANO SALA

Contributions of

STEFANO BARBERO, MARCO CIANFRIGLIA, MICHELE ELIA, ROBERTO LA SCALA
NADIR MURRU, ELIA ONOFRI, MARCO PEDICINI, SERGIO POLESE
GIORDANO SANTILLI, SHARWAN K. TIWARI, ANDREA VISCONTI

aracne

ISBN
979–12–5994–865–6

FIRST EDITION
ROMA 16 MARCH 2022

Index

Part I
INTRODUCTION

De Cifris Cryptanalysis
ISBN 979-12-5994-865-6
DOI 10.53136/97912599486561
pp. 11-11 (March 2022)

Preface

Massimiliano Sala

The national initiative "De Componendis Cifris" aims at fostering teaching and research of cryptography in Italy, including its applicative aspects. Under the guidance of the late Michele Elia, we have started several publishing projects. The book in your hands is the second volume of our new book series "Collectio Ciphrarum", which is devoted to proceedings.

This book, titled "De Cifris Cryptanalysis" by its editors, represents a daring tentative to put in plain sight (part of) cryptanalytic research taking place in Italy. Cryptanalysis is probably the most fascinating aspect of cryptology, but it is often surrounded by a mix of doubt and suspicion. We believe that only rigourous explanations of modern cryptanalytic methods can reveal this discipline for what it is: a beautiful research area where advanced mathematical theories and tools intertwine with practical estimates of the security of real-life cryptosystems.

The short abstracts presented here will give you a (tiny) sample of the active research lines, while the two surveys will introduce you to two of the most appealing mathematical theories at the frontier of modern cryptanalysis. My sincere thanks to the editors for their careful choice of the volume contributions and their quality. I do hope that this book will be for you the beginning of a journey into this not-so-mysterious not-so-obscure area.

De Cifris Cryptanalysis
ISBN 979-12-5994-865-6
DOI 10.53136/97912599486562
pp. 13-14 (March 2022)

Introduction

Roberto La Scala Marco Pedicini Andrea Visconti

The first Italian Workshop on Cryptanalysis was held at Ancona, Italy, in February 2020 during the Italian Conference on Cyber Security (ITASEC20). The workshop entitled "CRYPTANALYSIS: a key tool in securing and breaking cyphers" was organized by Roberto La Scala, Marco Pedicini, Massimiliano Sala and Andrea Visconti in collaboration with De Componendis Cifris (https://www.decifris.it). This event gathered Italian researchers and professionals working in the field of cryptography and security, including academia, industries, research institutions, and government. The organizers invited Italian researchers to contribute to this initiative and take part in it, giving several talks both theoretical and applied. The speakers also provided a manuscript that summarizes their presentations. Manuscripts received for publication in the proceedings were reviewed by experts and were collected in two categories: extended abstracts and surveys. These papers intended to explain to the crypto community that cryptanalysis has become an irreplaceable tool for raising awareness of the fact that crypto algorithms get old and should be continuously tested, maintained and improved. The paper "Methods for Rotational Cryptanalysis of ARX ciphers" by Stefano Barbero deals with a special class of block ciphers. Block ciphers are traditionally considered harder to break than stream ciphers or public-key cryptosystems. However, new approaches are showing some unexpected deviation from the ideal (random) behaviour of their encoding functions and this brings new light into their resistance. This paper deals with a special case of interest. The second paper "Systems of difference equations and stream ciphers " focuses on stream ciphers. This paper, authored by Roberto La Scala and Sharwan K. Tiwari, introduces a modeling of such ciphers based on systems of explicit difference equations defining the evolution of their internal state. By means of this modeling, special algebraic and symbolic methods for cryptanalysis can be applied. Trivium and Bivium ciphers are considered in the paper and experimental results illustrated. The last two papers in the extended abstracts

section deal with the Cube Attack, a new methodology settled in their Eurocrypy2009 paper by Itai Dinur and Adi Shamir. In the first contributed paper "Novel notation on cube attack" by Elia Onofri and Marco Pedicini a new notation to express the technical intricacies of the cube attack is introduced. In this paper, the authors suggest that this notation could simplify the analysis of cryptosystems and leads light to the discovery of more effective attacks. The second paper on cube attacks is a short presentation of the software package, the authors, Marco Cianfriglia and Marco Pedicini, performed some practical tests of the kite-attack with a way to organise computations of the cube attack to better adapt to GPU architectures. The second section of this volume is constituted of three invited surveys on cryptanalysis: the first one "RSA Cryptanalysis and Factoring: An Overview" by Michele Elia and Nadir Murru, is a compendium of algebraic methods applied to the analysis of integer factorization. The algorithmic complexity of attacks is illustrated in various cases: factorization by elliptic curves algorithm, by Pollard's $p-1$ method, by the Quadratic Sieve, by Shank's method, by the General Number Field Sieve and by the quantum algorithm introduced by Peter Shor. Another interesting survey is presented by Giordano Santilli in "A survey on cryptanalysis of Elliptic Curve Cryptography" where notions at the basis of ECC are introduced and three kinds of attacks on these cryptographic methods are reported: general attacks on ECDLP (Baby step - Giant step, Pollard's rho, Pohlig-Hellman), weak parameters attacks (anomalous curves) and faulty implementations. Finally, we could have not missed a survey on hash functions, fundamental primitives for the current development of many branches of cryptography. The gentle presentation by Sergio Polese and Andrea Visconti entitled "Survey: Attacks on Hash Functions" gives a clear idea of the many types of attacks that can be crafted against hash functions: from the fundamental probabilistic considerations of the birthday paradox to the more sophisticated multi-block collision search. Editors wish to thank the authors for their interesting contributions, as well as for their timely collaboration in the preparation of the manuscripts. We would like to thank the reviewers for their hard work, useful suggestions, and feedback that helped the authors to improve their manuscripts. To close, we also would like to sincerely thank De Componendis Cifris and its secretary, Elisa Cermignani, for the support in the organisation of the workshop.

Part II

EXTENDED ABSTRACTS