Lecture Notes in Computer Science **10737**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7410

Jerzy Kaczorowski · Josef Pieprzyk
Jacek Pomykała (Eds.)

Number-Theoretic Methods in Cryptology

First International Conference, NuTMiC 2017
Warsaw, Poland, September 11–13, 2017
Revised Selected Papers

Springer

Editors
Jerzy Kaczorowski
Adam Mickiewicz University
Poznań
Poland

Jacek Pomykała
University of Warsaw
Warsaw
Poland

Josef Pieprzyk
Queensland University of Technology
Brisbane, QLD
Australia

and

Institute of Computer Science
Polish Academy of Sciences
Warsaw
Poland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-76619-5 ISBN 978-3-319-76620-1 (eBook)
https://doi.org/10.1007/978-3-319-76620-1

Library of Congress Control Number: 2018934356

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The First Number-Theoretic Methods in Cryptology (NuTMiC) Conference was held at the University of Warsaw, Poland, during September 11–13, 2017. The aim of the conference is to cross-pollinate number theory and cryptology. Besides the well-established connections between the two domains such as primality testing, factorization, elliptic curves, lattices (to mention a few), the conference endeavors to forge new ones that would encompass number theory structures and algorithms that have never been used in cryptology before. It is expected that these new connections will lead to novel, more efficient and secure cryptographic systems and protocols (such as one-way functions, pseudorandom number generators, encryption algorithms, digital signatures, etc.). The conference topics include lattice-based cryptography, elliptic curves and bilinear-based cryptography, L-functions with applications to cryptology, large sieve methods in cryptography and exponential sums over finite fields and randomness extractors.

We received 32 submissions. The review process was conducted in two phases. In the first, the papers were lightly reviewed with emphasis on helpful comments and feedback. There were 21 papers that were chosen for conference presentation. The final papers were collected after the conference for these proceedings. The papers and were subject to a rigorous review. The proceedings include 15 peer-reviewed papers and three invited talks.

We would like to thank the Program Committee members and the external reviewers for their time and effort. We also thank the local organizers who made the conference a success. In particular, Marek Janiszewski, Aleksandra Dolot, Daniel Waszkiewicz, and Marcin Tunia took care of the conference website, helped us with EasyChair, and manned the conference desk. Bartosz Źrałek helped us with e-mail communication and financial overview. We would like to express our appreciation to Springer for their support and help in the production of the conference proceedings. We thank the EasyChair team for letting us use the server.

Last but not least, we highly appreciate the support the conference received from the Faculty of Mathematics, Informatics, and Mechanics of the University of Warsaw (MIMUW) and Warsaw Center of Mathematics and Computer Science (WCMCS). In particular, the Dean of MIMUW, Professor Paweł Strzelecki, welcomed the participants and hosted the conference in his department facilities. Professor Krzysztof Barański, Director of the Institute of Mathematics, and Professor Anna Zdunik, Chair WCMCS MIMUW, supported the conference financially. We gladly acknowledge the continuous assistance of the university administration units: financial, international collaboration, and audiovisual/technical services.

December 2017

Jerzy Kaczorowski
Josef Pieprzyk
Jacek Pomykała

NuTMiC 2017

The First Conference on Number-Theoretic Methods in Cryptology
Warsaw University, Warsaw, Poland
September 11–13, 2017

In Co-operation with IACR

General Co-chairs

Jacek Pomykała	University of Warsaw, Poland
Piotr Sapiecha	Warsaw University of Technology, Poland

Organizing Committee

Chris Charnes	IAP(T) TU Darmstadt, Germany
Aleksandra Dolot	Warsaw University of Technology, Poland
Robert Dryło	Warsaw School of Economics, Poland
Konrad Durnoga	University of Warsaw, Poland
Marek Janiszewski	Warsaw University of Technology, Poland
Mariusz Skałba	University of Warsaw, Poland
Krzysztof Szczypiorski	Warsaw University of Technology, Poland
Janusz Szmidt	Military Communication Institute, Poland
Marcin Tunia	Warsaw University of Technology, Poland
Daniel Waszkiewicz	Warsaw University of Technology, Poland
Konrad Wrona	NATO Communications and Information Agency, The Netherlands
Bartosz Żrałek	University of Warsaw, Poland

Program Co-chairs

Jerzy Kaczorowski	Adam Mickiewicz University and Institute of Mathematics, Polish Academy of Sciences, Poland
Josef Pieprzyk	Queensland University of Technology, Australia and Institute of Computer Science, Polish Academy of Sciences, Poland
Jacek Pomykała	University of Warsaw, Poland

Program Committee

Tomasz Adamski	Warsaw University of Technology, Poland
Andrzej Białynicki-Birula	University of Warsaw, Poland
Xavier Boyen	Queensland University of Technology, Australia
Chris Charnes	IAP(T) TU Darmstadt, Germany
Henri Cohen	Université de Bordeaux, France
Nicolas Courtois	University College London, UK
Andrzej Dąbrowski	University of Szczecin, Poland
Gerhard Frey	University of Duisburg-Essen, Germany
Jerzy Gawinecki	Military University of Technology, Warsaw, Poland
Katalin Gyarmati	Eötvös Loránd University, Hungary
Harald Helfgott	Georg-August-Universität Göttingen, Germany and École Normale Supérieure, Paris, France
Jerzy Jaworski	Adam Mickiewicz University, Poland
Zbigniew Jelonek	Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland
Przemysław Koprowski	University of Silesia, Poland
Mieczysław Kula	University of Silesia, Poland
Zbigniew Kotulski	Warsaw University of Technology, Poland
Bogdan Ksieżopolski	Maria Curie-Skłodowska University, Poland
Alessandro Languasco	Università di Padova, Italy
Tomasz Łuczak	Adam Mickiewicz University, Poland
Giuseppe Molteni	Università di Milano, Italy
Andrew Odlyzko	University of Minnesota, USA
Andrzej Paszkiewicz	Warsaw University of Technology, Poland
Rene Peralta	Computer Security Division, NIST, USA
Alberto Perelli	Università di Genova, Italy
Jerzy Pejaś	West Pomeranian University of Technology, Poland
Olivier Ramarè	Aix Marseille Universitè, France
András Sárközy	Eötvös Loránd University, Hungary
Andrzej Schinzel	Institute of Mathematics, Polish Academy of Sciences, Poland
Jennifer Seberry	University of Wollongong, Australia
Igor Shparlinski	University of New South Wales, Australia
Mariusz Skałba	University of Warsaw, Poland

Marian Srebrny	Institute of Computer Science, Polish Academy of Sciences, Poland
Janusz Stokłosa	Poznań University of Technology, Poland
Janusz Szmidt	Military Communication Institute, Zegrze, Poland
Huaong Wang	Nanyang Technological University, Singapore

Steering Committee

Xavier Boyen	Queensland University of Technology, Australia
Nicolas Courtois	University College London, UK
Chris Charnes	IAP(T) TU Darmstadt, Germany
Gerhard Frey	University of Duisburg-Essen, Germany
Jerzy Kaczorowski	Adam Mickiewicz University and Institute of Mathematics, Polish Academy of Sciences, Poland
Rene Peralta	Computer Security Division, NIST, USA
Josef Pieprzyk	Queensland University of Technology, Australia and Institute of Computer Science, Polish Academy of Sciences, Poland
Jacek Pomykała	University of Warsaw, Poland
Igor Shparlinski	University of New South Wales, Australia
Huaong Wang	Nanyang Technological University, Singapore

Additional Reviewers

Konrad Durnoga
Robert Dryło
Maciej Grześkowiak
Renata Kawa
Piotr Sapiecha
Daniel Waszkiewicz
Bartosz Źrałek

Abstracts of Invited Talks

Arithmetic Geometry: Deep Theory, Efficient Algorithms and Surprising Applications

Gerhard Frey

University of Duisburg-Essen

One of the most astonishing success stories in recent mathematics is arithmetic geometry, which unifies methods from classical number theory with algebraic geometry ("schemes"). In particular, an the extremely important role is played by the Galois groups of base schemes like rings of integers of number fields or rings of holomorphic functions of curves over finite fields. These groups are the algebraic analogues of topological fundamental groups, and their representations induced by the action on divisor class groups of varieties over these domains yielded spectacular results like Serre's Conjecture for two-dimensional representations of the Galois group of $\mathbb{Q}$, which implies for example the modularity of elliptic curves over $\mathbb{Q}$ and so Fermat's Last Theorem (and much more).

At the same time the algorithmic aspect of arithmetical objects like lattices and ideal class groups of global fields became more and more important and accessible, stimulated by and stimulating the advances in theory. An outstanding result is the theorem of F. Heß and C.Diem yielding that the addition in divisor class groups of curves of genus g over finite fields $\mathbb{F}_q$ is (probabilistically) of polynomial complexity in g (fixed) and $\log(q)$ (g fixed). So one could hope to use such groups for public key cryptography, e.g. for key exchange, as established by Diffie-Hellman for the multiplicative group of finite fields.

The obtained insights play not only a constructive role but also a destructive role for the security of such systems. Algorithms for fast scalar multiplication and point counting (e.g. the algorithm of Schoof-Atkin-Elkies) make it possible to find divisor class groups in cryptographically relevant ranges but, at the same time, yield algorithms for the computation of discrete logarithms that are in many cases "too fast" for security. The good news is that there is a narrow but not empty range of candidates usable for public key cryptography and secure against all known attacks based on conventional computer algorithms: carefully chosen curves of genus 1 (elliptic curves) and hyperelliptic curves of genus ≤ 3 over prime fields.

In the lecture we gave an overview on the methods and results for the rather satisfying situation of elliptic and hyperelliptic cryptography–as long as we restrict the algorithms to classical bit-operations. But the possibility of the existence of quantum computers in a not too far future forces to look for alternatives.

Therefore we formulated a rather abstract setting for Diffie-Hellman key exchange schemes using (closely related) categories for the exchange partners, for which push-outs exist and are computable. The DL-systems with cyclic groups are the easiest realizations (and by Shor's algorithm cracked in polynomial time), the next level are G-sets (G a semi group) with a commutativity condition. If G is abelian (e.g. equal to $\mathbb{N}$)

then an algorithm of Kuperberg for the hidden shift problem with subexponential complexity can be applied, for general groups no such algorithm is known (but the commutation condition is difficult to realize).

Using fundamental results of M. Deuring about isogenies of elliptic curves we described the system of Couveignes-Stolbunov for key exchange using the isogeny graph of ordinary elliptic curves with endomorphism ring O, which is a G-set with $G = \mathrm{Pic}(O)$ and so only of subexponential security under quantum computing, and the system of De Feo using supersingular elliptic curves (and nicely fitting into our categorical frame) for which no non-exponential quantum computer attack is known till now.

A Babystep-Giantstep Method for Faster Deterministic Integer Factorization

Markus Hittmeir

University of Salzburg, Hellbrunnerstraße 34, 5020 Salzburg
markus.hittmeir@sbg.ac.at

We consider the problem of computing the prime factorization of integers. In practice, a large variety of probabilistic and heuristic methods is used for this task. However, none of these algorithms is efficient and the problem itself is assumed to be computationally hard. The difficulty of factoring large numbers is fundamental for the security of several cryptographical systems, one of which is the public-key scheme RSA.

A more theoretical aspect of integer factorization concerns deterministic algorithms and the rigorous analysis of their runtime complexities. In the years from 1974 to 1977, Pollard and Strassen developed such a method and proved that it runs in time $\widetilde{O}(N^{1/4})$. Since the seventies, the logarithmic factors in the bound have been refined and other deterministic algorithms running in $\widetilde{O}(N^{1/3})$ have been found. However, the bound $\widetilde{O}(N^{1/4})$ has been state of the art for the last forty years.

In this paper, we obtain an improvement by a superpolynomial factor. The runtime complexity of our algorithm is of the form

$$\widetilde{O}\left(N^{1/4}\exp(-C\log N/\log\log N)\right).$$

To describe our approach, we consider the case $N=pq$, where p and q are unknown prime factors and $p<q$. We will employ a refined babystep-giantstep method to solve the discrete logarithm problem $a^X \equiv a^{N+1} \bmod N$ for a certain $a \in \mathbb{Z}$ coprime to N. The purpose of this procedure is to determine $S := p+q$. Knowing S allows us to factor N immediately.

Let $\Delta \leq N^{1/2}$ be a parameter. The scheme for our main algorithm is as follows:

1. Use the Pollard-Strassen approach to search for p in the interval $[1,\Delta]$. If p is found, stop. If p is not found, go to Step 2.
2. Use $\Delta < p < N^{1/2}$ to find $S := p+q$, the sum of the prime factors of N.
3. Knowing N and S, compute p and q.

To speed up the application of the babystep-giantstep method in Step 2 and to optimize the value for Δ, we will consider so called modular hyperbolas $\mathcal{H}_{N,m}$. They are defined as the sets of solutions (x,y) to the congruence equation $N \equiv xy \bmod m$. Clearly, the corresponding set $\mathcal{L}_{N,m}$ consisting of the elements $x+y \bmod m$ for $(x,y) \in \mathcal{H}_{N,m}$ contains the residue of S modulo m. If r is prime, than the cardinality of $\mathcal{L}_{N,r}$ is about half

of the possible residue classes modulo r. Considering all primes up to a suitable bound B, we deduce significant information about S. For example, let $N = 3823 \cdot 2069$ and $m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Then $\mathcal{L}_{N,m}$ contains only 40 elements. As a result, the residue of S modulo m is restricted to $40/2310 = 1.7\%$ of all residue classes modulo m. The information obtained by this idea yields the main contribution to our improvement.

A Crossbred Algorithm for Solving Boolean Polynomial Systems

Antoine Joux[1] and Vanessa Vitse[2]

[1] Chaire de Cryptologie de la Fondation de l'UPMC, Sorbonne Universités, UPMC Univ Paris 06, CNRS, LIP6 UMR 7606, Paris, France
antoine.joux@m4x.org

[2] Institut Fourier, Université Grenoble-Alpes, Grenoble, France
vanessa.vitse@univ-grenoble-alpes.fr

Abstract. We consider the problem of solving multivariate systems of Boolean polynomial equations: starting from a system of m polynomials of degree at most d in n variables, we want to find its solutions over $\mathbb{F}_2$. Except for $d = 1$, the problem is known to be NP-hard, and its hardness has been used to create public cryptosystems; this motivates the search for faster algorithms to solve this problem. After reviewing the state of the art, we describe a new algorithm and show that it outperforms previously known methods in a wide range of relevant parameters. In particular, the first named author has been able to solve all the Fukuoka Type I MQ challenges, culminating with the resolution of a system of 148 quadratic equations in 74 variables in less than a day (and with a lot of luck).

Contents

Number Theory

Pseudorandomness

Algebraic Structures and Analysis