Foreword

Second Workshop on Mathematical Cryptology

This issue of the Journal of Mathematical Cryptology collects selected papers on work presented to the meeting WMC 2008, held in Santander (Spain), October 23–25, 2008.

The result of the evolution of technology and science is that today we are witnesses of an explosive growth in the applications of mathematics in cryptology. There is growing interest among mathematicians and cryptographers in cryptosystems based on algebraic problems and in related cryptanalysis.

The Workshop on Mathematical Cryptology (WMC 2008) is the second of a series of meetings where the main purpose is to learn and discuss recent developments and emerging open problems derived from cryptology and having mathematical interest. It was organized by the research group Algorithmic Mathematics and Cryptography of the University of Cantabria, formed by: Paula Bustillo, Domingo Gómez, Jaime Gutierrez, Álvar Ibea and David Sevilla. The workshop consisted of invited lectures, short contributed talks and posters. In WMC 2008, fourteen speakers were invited to give a talk. They were Simon R. Blackburn (Royal Holloway, University of London), Joan-Josep Climent (University of Alicante), Jean-Charles Faugère (INRIA, Paris), Joachin von zur Gathen (BiT, Bonn), Alexander May (Ruhr University, Bochum), Carles Padró (Technical University of Catalonia, Barcelona), Kenny Paterson (Royal Holloway, University of London), Michael E. Pohst (Technical University of Berlin), Oriol Serra (Technical University of Catalonia, Barcelona), Tony Shaska (Oakland University, Rochester MI), Igor Shparlinski (Macquarie University, Sydney), Vladimir Shpilrain (The City College of New York), Rainer Steinwandt (Florida Atlantic University) and Arne Winterhof (RICAM, Linz).

After a detailed refereeing process, including in most cases three or four different reviews, we have chosen eight articles from the many excellent submissions we received. We hope that the reader will find an interesting perspective of this rich and active area. Let us say here a few words about each of the selected papers. In the paper by Luk Betttale, Jean-Charles Faugère and Ludovic Perret, Gröbner basis theory is used to present an improved approach to solve multivariate systems over finite fields. The paper by Simon R. Blackburn shows that a certain class of groups is not suitable as a platform for discrete logarithm based cryptography. The paper by Gérald Bourgeois and Jean-Charles Faugère presents an algebraic attack on a restricted NTRU using the method of the Witt vectors. In the paper by Nina Brandstätter and Arne Winterhof, character sum techniques are used to analyse the linear complexity of some sequences. Simon Fischer, Willi Meier and Dirk Stegemann study several properties of the feedback with carry shift registers (FCSR), which are extensively discussed in the context of pseudorandom number generation and as building blocks for stream ciphers. The paper by István Gaál and Michael E. Pohst provides general effective methods for solving norm
equations in global function fields, which is crucial for a variety of applications in cryptography. The paper by Mario Lamberger, Tomislav Nad and Vincent Rijmen gives a new approach to apply numerical methods in the cryptanalysis of stream ciphers, in particular for Trivium. In the paper by John B. Friedlander and Igor E. Shparlinski, Riemann Hypothesis is used to show that a certain set of primes which is of importance for the theory of pseudorandom sequences is of positive relative density.

The preparation of this special issue has only been possible with the help of many colleagues. We would like to thank all the authors who have submitted their precious manuscript to this issue and to ask for their understanding for our possible mistakes. The refereeing process went very smoothly and we thank the anonymous reviewers who accepted evaluating in detail these submissions. We also thank the managing editors of the Journal of Mathematical Cryptology, specially Rainer Steinwandt, who offered us the opportunity to do this job. Finally, but not least, we also would like to express our sincere gratitude to Álvar Ibeas who has done a tremendous job in all steps on the preparation process of this volume.

JAIME GUTIERREZ

University of Cantabria, Santander, Spain