Fundamenta Informaticae 114 (2012) i-ii
DOI 10.3233/FI-2012-625
IOS Press

Cryptology in Progress: 10th Central European Conference on Cryptology, Będlewo Poland, 2010

Preface

The Central European Conferences on Cryptology (CECC) were inaugurated in 2000 at the 14th Czech and Slovak International Conference on Number Theory in Liptovský Ján, Slovak Republic with a special crypto session. Since 2001 the CECC have been organized every year in a selected Central European country: in the Slovak Republic (three times), in Hungary and the Czech Republic (twice each), and in Poland and Austria (once each). The jubilee 10th CECC was held in Poland in 2010. The conference was organized by the Stefan Banach International Mathematical Center, the Adam Mickiewicz University of Poznań, and the University of Silesia.

The aim of the CECC was to gather people involved in cryptology. The talks covered a wide range of topics including symmetric or asymmetric algorithms and protocols, digital signatures and hash functions, (pseudo)random sequences as well as some practical and theoretical aspects of computer security and computational number theory.

About 60 participants from 6 countries attended the conference. Two plenary lectures were delivered by Prof. Simon Blackburn of the Royal Holloway University of London, and by Prof. Jerzy Kaczorowski of the Adam Mickiewicz University of Poznań. Four invited lectures were given by young researches selected by the Program Committee.

The scientific program was supplemented by Dr. Marek Grajek's lecture on *Roots of Victory* dedicated to the memory of the Polish mathematicians Marian Rejewski, Jerzy Różycki and Henryk Zygalski, who broke the military version of the famous Enigma code in 1932/1933. In 1933 they were able to read the first intercepted messages. Six years later, just before attack on Poland, full technical information about the decryption methods, including copies of the German cipher machine and auxiliary devices used to cryptanalyze it, were transferred to French and English intelligence agencies, which greatly accelerated the Allied cryptanalytic effort and shortened the war.

This special issue of Fundamenta Informaticae contains research and survey articles selected from 20 submissions. They are authored by conference speakers and a few invited experts who were unable to attend the conference. All the papers were reviewed, usually by at least two reviewers. We wish to express our deep appreciation to the authors for their contributions, and to the reviewers for their careful, insightful and constructive reviews.

Special issue editors

Jerzy Jaworski
Faculty of Mathematics and Computer Science
Adam Mickiewicz University
Poznań, Poland
jaworski@amu.edu.pl

Mieczysław Kula
Institute of Mathematics
University of Silesia in Katowice
Katowice, Poland
kula@ux2.math.us.edu.pl

Damian Niwiński
Institute of Informatics
University of Warsaw
Warsaw, Poland
niwinski@mimuw.edu.pl

Jerzy Urbanowicz
Institute of Computer Science
and Institute of Mathematics
Polish Academy of Sciences
Warsaw, Poland
J.Urbanowicz@ipipan.waw.pl

December, 2011