Computing (2009) 85:1–2
DOI 10.1007/s00607-009-0043-x

Editorial

C. Heuberger · V. Rijmen

Received: 8 April 2009 / Accepted: 8 April 2009 / Published online: 7 May 2009

The 8th Central European Conference on Cryptography (CECC'08) took place from 2 July to 4 July at Graz University of Technology. Previous installments of this conference series were held in Slovakia, Hungary, Poland and the Czech Republic. Around 70 participants attended the conference; the scientific program consisted of six invited and 22 contributed talks.

The present special issue contains ten revised papers corresponding to presentations at the conference, spanning various areas of cryptography.

The CECC conferences treat all the mathematical aspects of cryptography and its applications. Cryptography forms the corner stone of computer security, and as such it needs no lengthy motivation in the advent of the Internet of Things, Ambient Intelligence and Ubiquitous Computing. As has been demonstrated time and again in the last decade, strong cryptography can be achieved only on a fundament of sound mathematics.

The paper "Computational Aspects of the Expected Differential Probability of 4-Round AES and AES-like Ciphers" presents an improved analysis of the security of the Advanced Encryption Standard (AES) and similar block ciphers. In "An Approach for Stream Ciphers Design Based on Joint Computing over Random and Secret Data," a novel approach towards designing stream ciphers is presented.

Two new digital signature schemes are presented in "Step-out Group Signatures" and "Post-Quantum Cryptography: Lattice Signatures".

"A variant of Wiener's attack on RSA" defines a new class of weak exponents, which should not be used in the RSA cryptosystem. A generalization of the discrete logarithm problem is presented in "Discrete logarithms for finite groups."

C. Heuberger (✉) · V. Rijmen
Graz, Austria
e-mail: clemens.heuberger@tugraz.at

Some connections between graph theory and cryptography are explored in "On infinite families of graphs with information ratio $2 - 1/k$" and "Random Key Predistribution for Wireless Sensor Networks Using Deployment Knowledge."

"A new matrix test for randomness" presents a new method to evaluate the quality of sequences for use in cryptography.

"On affine (non)equivalence of Boolean functions" discusses equivalence classes of Boolean functions.

We thank the members of the program committee and the reviewers for their support in the selection of the speakers as well as the papers for this special issue.

We acknowledge the support of the Austrian Science Foundation FWF through its research network S96 "Analytic Combinatorics and Probabilistic Number Theory".