Issue 1: Cryptography

Cryptography and security systems are two fields of security research that strongly interact and complement each other. The series of International Conferences on Cryptography and Security Systems (CSS) is a forum for presentation of theoretical and applied research papers, case studies, implementation experiences, as well as work-in-progress results in these two disciplines. The conference especially invites young researchers and PhD students who have an opportunity to share their results with colleagues, invited keynote lecturers, and the Program Committee members actively participating in conference sessions. The research papers presented during the Third International Conference on Cryptography and Security Systems (CSS 2014) held during September 22–24, 2014, in Lublin, Poland are published in three special volumes. One of them is vol. 448 of the Springer Communications in Computer and Information Science series. It includes seventeen regular papers, seven of which concern different areas of cryptography, while the remaining ten deal with recent problems of cryptographic protocols. Two other volumes are special issues of the journal Annales UMCS, ser. Informatica (vol. 14, no. 1 and 2). Thirteen papers in these issues are mainly short and work-in-progress papers; seven papers of Issue 1 concern cryptography and related problems while six remaining included in issue 2 deal with security systems. This issue of Annales UMCS, ser. Informatica is entitled "Cryptography". It includes seven papers presented during Short and Work-in-Progress Papers Session of the Third International Conference on Cryptography and Security Systems (CSS 2014). First five papers concern cryptographic algorithms and protocols. The paper "On multivariate cryptosystems based on computable maps with invertible decomposition" by Vasyl Ustimenko proposes new multivariate encryption maps induced by special walks in the algebraically defined extremal graphs of increasing girth. More results in multivariate cryptography are presented in the paper of Aneta Wróblewska and Vasyl Ustimenko entitled "On new examples of families of multivariate stable maps and their cryptographical applications". The authors construct a new family of stable elements with invertible decomposition. This is the first construction of the family of maps based on walks on the bipartite algebraic graphs defined over a general finite commutative ring, which are not edge transitive. Another recent cryptographic topic, which is a duplex construction, is a subject of the paper "Cryptographic Applications of the Duplex Construction" by Mariusz Borowski. Such a construction equipped with one ideal permutation and appropriate security parameters is suitable for building provably secure cryptographic primitives. The next paper of this issue: Christian Franck, "Dining Cryptographers with 0.924 Verifiable Collision Resolution" proposes a computationally secure dining cryptographers protocol with collision resolution that achieves a maximum stable throughput of 0.924 messages per round and which allows to easily detect disruptors. The last paper of this series, "Modified Alternating Step Generators with Non-Linear Scrambler" written by Robert Wicik, Tomasz Rachwalik and Rafał Gliwa deals with pseudorandom generators suitable for cryptographic purposes. The authors

propose to use a non-linear scrambler at the output of keystreams for stream ciphers produced by the exclusive- or sum of outputs of alternately clocked linear feedback shift registers to increase their security. Two remaining papers of this issue concern important cryptography-related problems. In the first one, "Cheap and Easy PIN Entering Using Eye Gaze" by Paweł Kasprowski and Katarzyna Harężlak a novel method of the PIN entering was proposed. Instead of using a numerical keyboard, the PIN may be entered by eye gazes, which is a hands-free, easy and robust technique. The second paper "A fingerprint-based digital images watermarking for identity authentication" by Wioletta Wójtowicz proposes the combination of fingerprint verification methods with watermarking technology as a new protocol of providing copyright protection and authentication of digital images.

Zbigniew Kotulski
Bogdan Księżopolski
Katarzyna Mazur