Preface to Issue 3
"Cryptography and Data Protection"

Cryptography and security systems are two fields of security research that strongly interact and complement each other. The International Conference on Cryptography and Security Systems (CSS) is a forum of presentation of theoretical, 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 lecturers and the Program Committee members who actively participate in conference sessions.

In the second edition of the International Conference on Cryptography and Security Systems (CSS 2012) 18 regular presentations (selected out of 25 submitted papers by the authors from 10 countries) and 3 general invited lectures have been presented. The first lecture was given by Dr. Pascal Lafourcade from the University of Joseph Fourier in Grenoble on "Automatic Security Proof of Cryptographic Primitives : Public Encryption, Symmetric Encryption Modes, MAC...". Dr. Lafourcade presented current results of his and co-workers' research on constructing a tool for automatic verification of correctness of cryptographic protocols and their security against common attacks. After presenting the background of his tool and formal description of protocols, he concentrated on the analysis of three groups of the most popular cryptographic primitives which are public-key cryptosystems, symmetric ciphers in different modes of operation and hash functions applied in the MAC protocols.

The second general lecture was presented by Dr. Mark D. Cole from the University of Luxembourg and its subject was "Combating Cybercrime - Can Law Contribute to Enhancing Security of Communication Networks? On International, European and National Responses and Possibilities". Dr. Cole presented current problems of fighting cybercrime from the point of view of individual countries' national, European and, generally, international legal regulations. This lecture initiated interesting discussion moved on for the coffee break since the audience understood that the fundamentals of any protection method should lie in good law and international agreements on rights and licenses as well as every day cooperation.

The third invited lecture was by Dr. Krzysztof Chmiel from Poznań University of Technology. Its title was "Methods of Differential and Linear Cryptanalysis of Block Ciphers". Dr. Chmiel gave an overview and the summary of his research on cryptanalysis of symmetric block ciphers, starting with the first attacks on the DES cipher and ending with the analysis of modern PP1 encryption algorithm. He also presented different approaches to estimation of security level of cipher and methods of approximations of the most complicated ciphers' component operations.

The regular papers accepted for CSS 2012 were presented during the sessions that can be grouped into two tracks. Issue 3 of volume XII of Annales UMCS ser. Informatica is devoted to the track named "Cryptography and Data Protection". It consists of 9 papers which communicate the Authors' recent results in constructing new cryptographic

algorithms and protocols, implementation of cryptographic algorithms and steganalysis techniques. Three of those papers reflect the current stream of research inspired by the SHA-3 conquest, e.g., constructing new hash algorithms to replace the present SHA-2 standard. The paper by Anna Grocholewska-Czurylo, Janusz Stoklosa, Krzysztof Bucholc and Tomasz Bilski entitled "Parameterized Hash Functions" describes a family of highly parameterized hash functions called HaF-256, HaF-512 and HaF-1024. Such a parameterization results in high flexibility between the performance and security of the algorithm. Details of the functions structure and the method used to generate S-box is also described. Cryptanalysis of a hash function is the subject of the paper by Mateusz Buczek, "Attacks on StreamHash 2". StreamHash 2 is an algorithm presented by Michał Trojnara during the first Conference on Cryptography and Security Systems in 2011 and in its preliminary version called StreamHash introduced in 2008 during the SHA-3 Competition. The third paper on the topical subject of analysing hash algorithms was presented by Sebastien Varrette, Jakub Muszynski and Pascal Bouvry, "Hash Function Generation by Means of Gene Expression Programming". Their article investigates the ways to generate automatically the compression functions by means of Evolutionary Algorithms and to apply them for the constructs of iterative hash schemes.

Another topical problem connected with cryptographic protocols is the subject of the paper by Renata Kawa and Mieczysław Kula, "A Remark on Hierarchical Threshold Secret Sharing". The main results of this paper are theorems which provide a solution to the open problem posed by Tassa who considered hierarchical threshold access structures and showed that two extreme members of these structures are realized by secret sharing schemes that are ideal and perfect. The Authors answered the question whether other members of this access structure can be realized by the ideal and perfect schemes (the reply in general case is negative).

Next two papers concentrate on secret keys problems. Aneta Wroblewska and Vasyl Ustimenko in their paper "Dynamical Systems as the Main Instrument for the Constructions of New Quadratic Families and Their Usage in Cryptography" used the advanced mathematical approach to construct background of new symbolic key exchange protocols and public keys algorithms. Using dynamical systems approach and quadratic polynomial maps iterations they proposed new protocols and algorithms analogous to those usually applying a discrete logarithm problem. The second of the secret-key related papers by Mariusz Borowski, Marek Leśniewicz, Robert Wicik and Marcin Grzonkowski entitled "Generation of Random Keys for Cryptographic Systems" is of more practical nature. The Authors consider a one-time pad cipher that may be used to ensure perfect security and present an electronic device designed in the Military Institute of Telecommunications in Zegrze which makes it possible to generate binary random sequences with the potential output rate of 100 Mbit/s. They present the generator scheme and the results of its security and performance tests.

Algebraic graphs and their application for obtaining cryptographic primitives are the field of interest of the Authors of the following two papers. Urszula Romańczuk and Vasyl Ustimenko in the paper "On the Family of Cubical Multivariate Cryptosystems

Based on Algebraic Graph over Finite Commutative Rings of Characteristic 2" defined a family of algebraic graphs over a finite commutative ring and used them for the design of different multivariate cryptographic algorithms such as private and public key encryption and key exchange protocols. In the sequence, Low-Density Parity-Check Codes obtained from the families of algebraic graphs and their correcting properties are the subject of the paper "LDPC Codes Based on Algebraic Graphs" by Monika Polak and Vasyl Ustimenko. Such graphs come from the infinite incidence structure. The Authors describe how to construct these codes and choose their parameters.

The last paper in this issue, "Performance Evaluation of Different Universal Steganalysis Technique in JPG Files", is written by Ashraf M. Emam and Mahmoud M. Ouf. Its subject is steganography being a data security technique complementary to cryptography. The paper aims for the performance evaluation of five of the universal steganalysis techniques which are "Wavelet Based Steganalysis", "Feature Based Steganalysis", "Moments of Characteristic Function Using Wavelet Decomposition Based Steganalysis", "Empirical Transition Matrix in DCT Domain Based Steganalysis", and "Statistical Moment Using jpeg2D Array and 2D Characteristic Function". The Authors try to give algorithms recommendations for choosing a universal steganalysis method from the analyzed.

Zbigniew Kotulski
Bogdan Księżopolski