Preface

Jacek Pomykała

Faculty of Mathematics Informatics and Mechanics,
Institute of Mathematics,
University of Warsaw,
Banacha 2, 02-097 Warsaw, Poland
E-mail: pomykala@mimuw.edu.pl

Jerzy Pejaś

Faculty of Computer Science and Information Technology,
West Pomeranian University of Technology,
71-210 Szczecin, Poland
E-mail: jpejas@wi.zut.edu.pl

Biographical notes: Professor Jacek Pomykała works in Mathematical Institute at the Faculty of Mathematics Informatics and Mechanics of Warsaw University. His scientific interests are number theory, cryptology, computational complexity, security of computer systems and cybercrimes. He was the invited speaker of many international conferences in the area of mathematics and computer science and the author of over 40 publications in these domains. He is an author of one book on the modelling and security of information systems and the co-editor of collected papers concerning the cryptographic and biometrics authentication.

Dr. Jerzy Pejaś works in West Pomeranian University of Technology, at Faculty of Computer Science and Information Technology. His main subject of interest are: the theoretical and practical aspects of information and computer network security, in particular the problems of public key infrastructure (PKI) and the services provided by its mechanisms. He is also interested in the problems of access control to sensitive information, as well as new trends in cryptography. Currently, he works in the area of distributed systems for secure signature which are consistent with European Directive on Electronic Signature and Polish Law. He published over 40 papers and chapters of books in the area of PKI design, access control systems and authentication protocols.

This special issue on *Authentication and Non-repudiation in Biometrics and Cryptography* concerns the concepts, surveys, state-of-the-art, research, standards, implementations and running experiments. The practical case studies of different aspects of authentication and non-repudiation are achieved as a result of application of biometric and cryptographic methods. Furthermore some authors of the contributed papers investigate other relations between biometrics and cryptography, for example the watermarking techniques.

Generally speaking, the important connection between the biometric methods, on the one hand and the authentication and non-repudiation features on the other, is the credibility of information assured by the given entity. How can we prove the authenticity or the non-repudiation of the handwritten message, an e-mail or simply the record in the computer storage? How can we check the suitable connection between the source and the message it generates? In this connection, the unique biometrical (behavioural) features of the entity or the knowledge it possesses can be applied to create such undeniable evidence (connection). Therefore, the same goal may be attained by completely different methods. To recognise the biometrical pattern of the handwritten signature, the biological neural network provides us with a relatively good tool to solve the problem. In the case when secret knowledge is somehow hidden in the message encryption process, the cryptographic tool is the right way to verify this linkability. In some contributed papers, this process is described in a more detailed way.

The integrated 'match in card' security system was investigated in the paper *Biometric Cards with Advanced Signing System*. The proposed solution referring to certificate-based digital signatures, as well as the certificateless user authentication system, was investigated in detail. The security-enhanced model, when compared with the classical Id-based signature scheme, refers to the threat of the compromising of the user private key or master key of the corresponding PKG-party. The related protocol is based on the application of the bilinear map in the so-called Gap Diffie-Hellman groups. This implies good performance of the system and the corresponding digital signature scheme to be provably secure.

Certainly, we have to be aware of the positive and negative false verifications. On the other hand, the cryptographic authentication is free of this weakness. However, in practice, both kinds of authentication are used frequently in one integrated security system. An example is the electronic passport system that was the subject of one contributed paper – *Security and Privacy in Electronic Passports*. Both the public key infrastructure and the biometry-based authentication system appear as the components of the whole integrated security system. Describing some vulnerabilities of the system, the author points out the necessity of the electronic passport system to be more secure. The solutions applied in the different countries provide us with good examples of the case studies.

Some very important aspects of the biometrics feature are analysed in the work *Biometrics for Non-repudiation: Security and Legal Aspect*. This paper is very controversial because it attempts to refute many of general opinions on the non-repudiation of digital signatures and biometrics from the security and legal aspects point of view. It is obvious to many experts that digital signature provides non-repudiation, but when assigning the same requirement to biometric authentication we are forced to rethink this opinion again.

The authors of the paper *Handwritten Signatures Recognition using Liquid State Machine* apply Liquid State Machine and neural network for the task of the off-line signature recognition and verification. They obtained interesting results as well as posed the valuable suggestions related to further development of this method. For instance, measuring the impact of the variable parameters on the optimal performance of the system should be investigated in the future.

Intellectual property protection of digital images and multimedia has been a challenge for many researchers for many years. There is no effective and secure solution to this problem, since almost all approaches are merely trying to increase the resistance of the proposed techniques to known attacks. The method proposed in the paper *A Robust Biometric Dual Watermarking Technique with Hand Vein Patterns for Digital Images* also belongs to the same class of solutions. However, in comparison with previous ones, the method proposed in this paper is based on the handvein biometric watermarking technique providing high security to prevailing watermarking techniques.

The authors of published papers have not responded to all important questions concerning the authentication and non-repudiation in biometric and cryptographic systems, for example, the mutual relation between different aspects of digital signatures and biometrics. However, we believe that the contributed papers may serve as a good starting point for further research in this important and interesting area of subject.