THESIS SUMMARY

„Improving confidentiality for the public systems which manage personal information"

Author: Eng. Narcis-Florentin ANTONIE

Email: narcis.antonie@yahoo.com, tel: 0744 753 198

Ph.D. supervisor: Professor Eng. Ciprian Răcuciu, PhD

The paper begins with an introductory part which presents some basic elements in the field of cryptography as well as historical elements that led to the evolution of cryptography.

Chapter 1 describes the basic notions in cryptography, the terminology used, and basic elements in communications such as protocols and the need to standardize them. There are general elements presented from the point of view of communications security and the operation of several block type encryption algorithms is detailed as well as the OTP algorithm. The chapter ends by describing an alternative in the field of cryptography, namely quantum cryptography.

Chapter 2 describes one of the most popular and widely implemented suites of security protocols, IPSec. The chapter ends with the description of laboratory tests performed by the author to determine the delay performance of different block-type encryption algorithms.

Chapter 3 introduces the concept of a distributed computing structure and describes elements of information security in such structures. Here, the cloud storage services are presented as well as the issues which arise in such systems. This chapter describes the solutions to solve some of these problems.

Chapter 4 describes in detail two public systems that manage personal information, the national electronic health insurance system and the national electronic population records system. These systems are those targeted in this work to make confidentiality more effective by introducing anonymous signatures.

Chapter 5 describes the concept of anonymous signatures in the context of its differentiation from standard digital signatures. The concepts of anonymous signature proposed by other authors are described and the applicability of these schemes in practice is also described through four practical examples of applicability.

This chapter ends by describing three variants of innovative anonymous digital signature schemes proposed by the author of this thesis. These anonymous signature variants involve the introduction into the anonymous signature scheme of a symmetric encryption algorithm described in Chapter 1 of this paper.

Chapter 6 represents the actual proposals of the author to make confidentiality more effective for the two public personal information management systems described in Chapter 4. Both proposals are based on an anonymous signature scheme designed by the author in Chapter 5. Also presented is a future research idea for the introduction of anonymous signatures within a comprehensive population accounting and personal information management system that uses smart cards and biometric data.

Chapter 7 describes the practical implementation of an anonymous signature described in Chapter 5 using a smart card. The chapter begins with a description of smart cards and continues with the description of the practical implementation algorithm of the solution. It describes the developed application and how it works with the results of author-designed test scenarios.

Chapter 8 is the section of conclusions and experimental results evaluating the results of the work done during the doctoral school and as a result of the research activities that are found in this paper. Modern scientific concepts regarding the confidentiality of personal data and ensuring the requirements imposed by the European legislation in force (GDPR – General Data Protection Regulation) are specified.

At the end of the chapter the journalistic activity and the research stages conducted by the author are mentioned in relation to the topics approached in the doctoral thesis. Possible future research directions are also described and the elements of personal contribution and originality brought by the author in the studied subject are highlighted.

The last sections in the structure of the paper are the bibliographic references, the glossary of abbreviations, the list of figures and tables and the appendices to the paper detailing some practical aspects described in the thesis.