VĚDECKÉ SPISY VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ
Edice Habilitační a inaugurační spisy, sv. 529
ISSN 1213-418X

Jan Hajný

CRYPTOGRAPHIC PROOFS OF KNOWLEDGE AND THEIR USAGE IN SYSTEMS PROTECTING DIGITAL IDENTITY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta elektrotechniky a komunikačních technologií
Ústav telekomunikací

Ing. Jan Hajný, Ph.D.

CRYPTOGRAPHIC PROOFS OF KNOWLEDGE AND THEIR USAGE IN SYSTEMS PROTECTING DIGITAL IDENTITY

KRYPTOGRAFICKÉ DŮKAZY ZNALOSTI A JEJICH VYUŽITÍ V SYSTÉMECH CHRÁNÍCÍCH DIGITÁLNÍ IDENTITU

Zkrácená verze habilitační práce
v oboru Teleinformatika

VUTIUM

BRNO 2015

KEYWORDS

Cryptography, proofs of knowledge, digital identity, privacy, anonymity, attribute-based authentication, anonymous credentials.

KLÍČOVÁ SLOVA

Kryptografie, důkazy znalosti, digitální identita, soukromí, anonymita, atributová autentizace, anonymní pověření.

MÍSTO ULOŽENÍ PRÁCE

Habilitační práce je k dispozici na Vědeckém oddělení děkanátu FEKT
VUT v Brně, Technická 10, Brno, 61600.

ISBN 978-80-214-5313-5
ISSN 1213-418X

CONTENTS

Ing. Jan Hajný, Ph.D.

Faculty of Electrical Engineering and Communications
Brno University of Technology
Technická 3082/12, 616 00 Brno
E-mail: hajny@feec.vutbr.cz

Professional Experience

2015	Visiting researcher at IBM Research Laboratories Zurich, Switzerland
2012 - Present	Scientist at SIX Center, BUT
2008 - Present	Academic worker, Department of Telecommunications, BUT

Education

2008 - 2012	Doctoral program at FEEC, BUT Dissertation topic: "Authentication protocols and privacy protection"
2010 - 2011	Fulbright scholar at Department of Mathematics, Dept. of Computer Science University of Minnesota, USA
2008	Department of Computer Science (Crypto-Group) University of Arhus, Denmark
2006 - 2008	Master's program at Brno University of Technology, CZ Master's thesis: "Analysis and design of authentication systems"
2003 - 2006	Bachelor's program at Brno University of Technology, CZ Bachelor's thesis "Methods for LAN protecting"

Selected Projects

2014 - 2017	TA04010476 (Lead): Secure systems for electronic services user verification
2014 - 2017	GP14-25298P (Lead): Research into cryptographic primitives for secure authentication and digital identity protection
2012 - 2014	TA02011260: Cryptographic system for the protection of electronic identity
2009 - 2012	JCMM Brno Ph.D. Talent (Lead): Cryptographic protection of identity
2008 - 2011	2C08002: Complex authentication and authorization for computer networks

Publications in Numbers

Impacted Journals	6 publications
Scientific Journals	7 publications
Conf. in Scopus	32 publications
Czech Conferences	8 publications
Total	53 publications
h-index	2 (Thomson Reuters), 6 (Google Scholar)

Taught Courses

To be started	ICT security 1
To be started	Cryptologic protocol theory
2013 - Present	Fundamentals of cryptography
2013 - 2015	Computers and programming
2008, 2009, 2011	Security of information systems
2009, 2010	Design, administration and security of computer networks

INTRODUCTION

The purpose of this habilitation thesis is to provide a unified description of cryptographic primitives used for the digital identity protection and to summarize the author's results achieved in the field of the design of digital identity protection schemes.

The text contains new proposals of protocols for secure authentication, access control and privacy-sensitive data transfer. The proposals of protocols contained in this thesis, as well as author's other past results, have a common feature: they are constructed using the modular composition of fundamental functional blocks, so called primitives. By the combination and parametric settings of the primitives, novel systems are constructed. The main unifying aspect of all schemes proposed in this thesis, besides the focus on digital identity protection, is the usage of the same building blocks, particularly the proofs of knowledge about discrete logarithms.

The proposals of new cryptographic systems are not the only contribution of this thesis. The text contains also a comprehensive overview of the current state and a deep analysis of primitives used not only in our proposals but also in most modern cryptographic schemes. The analysis contains the description of primitives including their security aspects and potential usage. The text is intended to work as a study material for teaching modern cryptography.

The text is structured in a way that a reader obtains the basic theoretical knowledge about fundamental building blocks in the first chapters. Next, the overview of the current state in digital identity protection is provided. This knowledge is later used for explaining the construction of privacy-enhanced schemes. The examples of using the primitives in novel schemes proposed by the author are provided in the latter sections. The expected pedagogical aim of this thesis is that the broader theoretic background together with practical examples will allow readers to understand the principles of the usage of modular proof of knowledge protocols and to obtain the ability to construct own systems. It is expected that parts of the material will be used in the courses of the Information Security study program at Brno University of Technology, where the author is involved.

The habilitation thesis covers the digital identity protection merely from the technical perspective. However, it is very important to note that practical systems are always based on the combination of technical and non-technical instruments. It would be a huge mistake to omit, for example, legal, social or economical aspects. This overlap of disciplines is respected in both pedagogical and scientific activities of the author. Yet, this thesis provides only technical solutions due to author's specialization.

1 THESIS OVERVIEW

This chapter contains a brief overview of the thesis. We present the motivation for writing this text in Sec. 1.1 and the goals we are aiming at in Sec. 1.2. The contribution to current state and the relation to author's past work is described in Sec. 1.3. Finally, the structure of the text is analyzed in Sec. 1.4.

1.1 Motivation

The role of cryptography in modern communication systems is crucial. As the number and variety of electronic services grow, the need for better protection is becoming more and more urgent. New technologies, such as social networks, cloud computing, smart metering or wearable devices, are already there, ready for usage. Despite the fact that many services, and thus our activities, are moving to an electronic space, the protection of digital identity is weak. There were many stories about identity thefts, private data leaks or unauthorized tracing of people presented in both mass medias and scientific publications. The ubiquitous communication devices, easy-to-access social networks and cloud services make the protection of digital identity even more actual topic.

Cryptography has been traditionally the solution to many security-related problems in the information and communication technologies (ICT) area. There are well-known solutions that fulfill the traditional demands, for example on data confidentiality and authenticity. Such solutions, based on technologies like RSA [45], DSA [40], DH [34] or AES [23], are using cryptographic primitives that are known mostly since 1980's. However, the development in cryptography was ongoing in recent two decades and many new concepts and schemes have appeared. Many of these concepts are particularly suitable for digital identity protection. The new cryptographic schemes, such as group signatures [31], anonymous attribute-based credentials [30] or provable identification systems [35], couldn't be designed without recent advances in cryptography.

While the classical cryptography protecting confidentiality and authenticity is present almost everywhere, the outcomes of modern cryptography are less frequently used in practical systems. One of the domains, where the recent cryptography results might play an important role, is the privacy and digital identity protection. Being already included in national plans and strategies [47, 41], privacy-enhancing technologies represent an important next step in ICT security. The main focus of this text is on the fundamental cryptographic technologies used for digital identity protection, their composition into systems and finally their implementation aspects. By covering these topics, we want to support digital identity protection, in particular help readers understand the underlying concepts and contribute to this field by proposing novel solutions.

1.2 Goals

This text has the ambition to provide readers with the basic background necessary to understand modern digital identity protection systems, describe the state of the art in this area and propose new cryptographic schemes with novel or improved functionality. In addition to the chapters focused on theory, that constitute the majority of the text, a chapter about practical implementation aspects of modern cryptographic systems is included. The goals of the thesis are summarized below.

- *Explain and provide study resources* on the fundamentals of cryptographic primitives necessary for digital identity protection technologies. The cryptographic commitments, interactive proof systems, zero-knowledge protocols and proofs of knowledge will be covered. All these primitives are frequently used as the building blocks of more complex privacy-enhancing systems.
- *Analyze* state of the art in digital identity protection systems. Three domains related to identity protection are selected and will be analyzed. The authentication protocols are selected because they are the most frequently used cryptographic systems dealing with user identity. The anonymous credentials are covered because they are considered by many documents to be the future successors of classical authentication systems due to their privacy protection features. The data collection systems were selected because they are complementary to above systems as they protect privacy by restricting unauthorized data analysis and profiling. These domains were also chosen due to their big potential for the usage of modern cryptography, in particular of the proof of knowledge protocols.
- *Design* novel digital identity protection schemes. The outcomes of author's research into modern cryptographic schemes will be presented. Novel schemes addressing problems of existing systems will be described here in full details.
- *Verify* practical usability of systems proposed. The proposed theoretical systems will be analyzed according to their practical implementability on low resource devices like smart-cards and smart-phones.

1.3 Contribution

This text is designed and written to have both pedagogical and scientific contribution. Therefore, it should serve the non-experts in the field of cryptography and students to gain basic knowledge of concepts used in modern cryptographic systems. Furthermore, the chapters devoted to the state of art analysis of digital identity protection systems are written in a way that allows readers to easily understand how these systems work and what technologies they rely on. After these introductory chapters, the text describes the outcomes of author's own research into systems based on cryptographic proofs of knowledge. Novel authentication schemes, anonymous credential systems and data collection systems are presented there. The contribution of the text can be summarized as follows.

- *Pedagogical contribution*: Chap. 2 and 3 are written to have a pedagogical contribution in the field of modern cryptography. The concepts of cryptographic commitments, interactive proof systems, interactive proof arguments, zero-knowledge protocols and proofs of knowledge are covered in Chap. 2. These concepts represent the fundamentals of modern cryptography and the understanding of underlying theory is essential for understanding the digital identity protection systems, that are covered later in Chap. 3. The latter chapter does not cover all the cryptographic digital identity protection systems exhaustively. Instead of that, only three areas most closely related to digital identity protection and the usage of modern cryptography were selected. The existing technologies in strong authentication, anonymous credentials and data collection systems are covered here. After reading Chap. 2 and 3, a reader should have solid understanding of modern cryptographic digital identity protection systems and underlying concepts.
- *Scientific contribution*: the Chap. 4 contains original author's results in the domains identified

and analyzed in Chap. 3. A novel protocol for strong authentication in physical access control systems is presented in Sec. 4.1. A novel anonymous credential scheme is presented in Sec. 4.2. Finally, a novel scheme for privacy-friendly data collection is presented in Sec. 4.3. All these outcomes are based on cryptographic fundamentals described in Chap. 2. Therefore, the schemes proposed are very related according to their cryptographic structure and primitives used, although they belong to different application areas. In particular, all schemes proposed are based on cryptographic proofs of knowledge. To prove the readiness of the novel schemes for a practical implementation, we also describe implementation results in Chap. 5.

1.3.1 Relation to Author's Other Publications

This section provides a brief overview of past publications of this thesis's author that are related to this text. The cryptographic primitives, that are used for the construction of systems for the protection of digital identity, have been intensively studied by the author in the past decade [6, 4, 16]. The links to relevant papers are provided throughout the text to provide further information. This applies mainly to the introductory sections of this text, particularly Chap. 2, 3, where the cryptographic primitives are introduced.

The chapters containing new results, namely Chap. 4 and 5, are based on recent original scientific work of the author, in particular papers published in the period from 2012 to 2015 [14, 20, 17, 22, 16, 9, 18, 12, 21, 11, 10, 15]. The section devoted to anonymous credentials (Chap. 4, Sec. 4.2) is related to author's Ph.D. thesis [8] that covered attribute-based authentication protocols. In this section, we build on the results of the Ph.D. thesis to construct a novel cryptographic scheme with improved security (by providing protection against collusion attacks) and privacy protection (by preventing unauthorized linkability of verification sessions). None of the results presented in this thesis was published in the author's Ph.D. thesis or any past author's theses.

1.4 Structure

This text is structured into 6 chapters. The Chap. 1 Thesis Overview gives the general overview of the scope and goals of the text. Sections describing motivation (Sec. 1.1), goals (Sec. 1.2), contribution (Sec. 1.3) and text structure (Sec. 1.4) are contained.

The Chap. 2 Cryptography Fundamentals provides readers with the background from cryptography necessary for understanding modern cryptographic proof of knowledge protocols and the protocols for digital identity protection. Sections devoted to basic cryptographic primitives, namely cryptographic commitments, interactive proof systems (IPS) and interactive arguments (IA), zero-knowledge protocols (ZK) and proofs of knowledge (PK), are included.

In Chap. 3, the description of the current state and the analysis of existing systems are provided. The cryptographic systems covered here are divided into three groups according to their purpose. In this chapter, proofs of identity (Sec. 3.1), anonymous credentials (Sec. 3.2) and data collection systems (Sec. 3.3) are covered.

Based on the current state analysis, novel protocols and schemes based on proofs of knowledge are proposed in Chap. 4. New cryptographic schemes are described and their contribution is defended in Sec. 4.1 (proofs of identity), 4.2 (anonymous credentials) and 4.3 (data collection systems).

Our goal is to design and propose cryptographic technologies that are practical and usable on off-the-shelf devices. To prove that fundamental cryptographic primitives and higher systems are not only theoretical but also practically implementable on low-resource devices, we included Chap. 5. It describes the implementation aspects of cryptographic primitives and of relevant systems.

The last Chap. 6 concludes the text.

2 CRYPTOGRAPHY FUNDAMENTALS

This chapter contains the basic theory necessary for understanding the cryptographic protocols and schemes used in the digital identity protection systems. In the full version of the thesis, we provide a brief overview of existing primitives that are the fundamental building blocks of complex cryptographic systems. We introduce basic constructions that are later combined into more complex systems. We start with the description of multi-purpose primitives called cryptographic commitments (Sec. 2.4), we proceed with the introduction of the concepts of interactive proof systems and interactive arguments (Sec. 2.5). Using these concepts, we introduce the zero-knowledge protocols in Sec. 2.6. The practical variants of zero-knowledge protocols, particularly the Σ-protocols, are described in Sec. 2.7. The composition of zero-knowledge protocols into proof of knowledge systems, that are the main cryptographic construction used in the thesis, is presented in Sec. 2.8.

2.1 Notation

We specify the notation used throughout the text here. We use the standard notation commonly used in cryptography and applied mathematics. For various proofs of knowledge or representation, we use the simplified CS notation introduced by Camenisch and Stadler [29]. The protocol for proving the knowledge of discrete logarithm of c with respect to g is denoted as "$PK\{\alpha : c = g^{\alpha}\}$". The proof of discrete logarithm equivalence with respect to different generators g_1, g_2 is denoted as "$PK\{\alpha : c_1 = g_1^{\alpha} \wedge c_2 = g_2^{\alpha}\}$". A signature by a traditional asymmetric signature scheme (e.g., RSA) of a user U on some data is denoted as "$Sig_U(data)$". The symbol ":" means "such that", "$\forall$" means "for all", "$|$" means "divides", "$|x|$" is the bitlength of x and "$x \in_R \{0,1\}^l$" is a randomly chosen bitstring of maximum length l. G denotes the respective group. The symbol "$ord(g)$" denotes the order of an element g in the respective group. The symbol "$\mathcal{H}$" denotes a hash function. The symbol "$\mathbb{Z}_p^*$" denotes a modular multiplicative group with prime modulus p. The typical example of such a group is the structure used by the DSA algorithm [40]. The symbol "$\mathbb{Z}_n^*$" denotes a modular multiplicative group with composite modulus n. The typical example is the RSA group [45] where $n = rs$ and r, s are primes.

This text is devoted to cryptographic proofs of knowledge and their practical applications. The proofs of knowledge are (usually) protocols running between two entities. Since the text includes many examples of both existing and newly proposed protocols, we unify their description by using a common layout. In Fig. 2.1, the placement of entities, shared values, private values, algorithms running at only one side and messages interchanged is shown. Any block can be omitted or repeated more times.

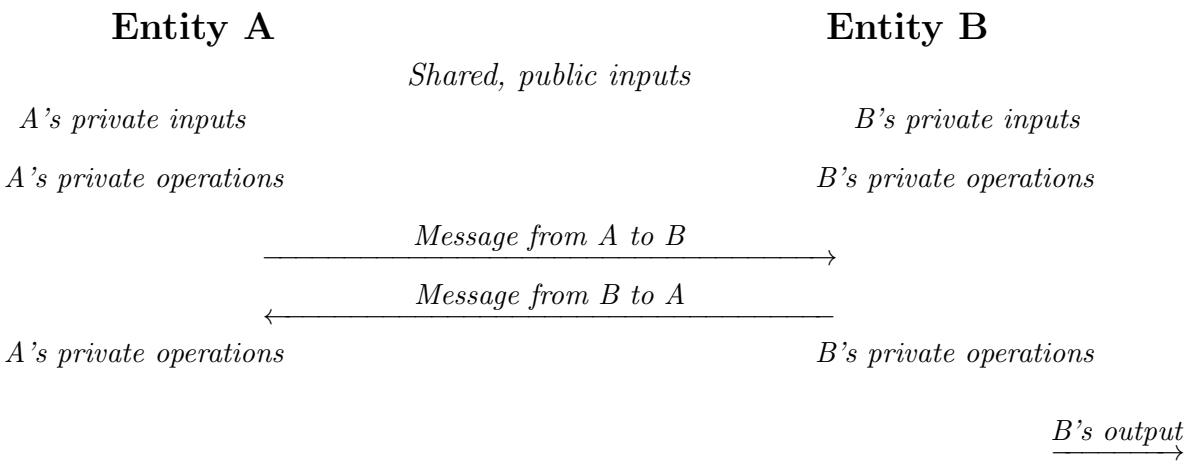

Fig. 2.1: Unified layout of protocol description.

3 EXISTING SYSTEMS USING PROOFS OF KNOWLEDGE

In this chapter, we provide the overview of selected existing systems that are based on cryptographic proofs of knowledge. We consider only systems directly related to digital identity protection, i.e., authentication and identification systems (Sec. 3.1), anonymous credential systems (Sec. 3.2) and data collection systems (Sec. 3.3). This selection directly agrees with the structure of the Chap. 4 where novel systems are proposed. Therefore, this chapter can be considered a broad analysis of existing systems related to our proposals. The detailed state of the art analyses with particular focus on our contribution are included later in Chap. 4, ahead of sections where novel schemes are proposed.

Even though we are focusing only on systems based on proofs of knowledge and providing digital identity protection, it is impossible to cover all schemes available. Therefore, the chapter describes the systems that are particularly important due to one or more reasons from the list below.

- **Milestone proposals:** we include systems that are particularly fundamental, first of their kind.
- **Existing practical implementation:** systems, that are already implemented in existing applications, are preferred due to practical scope of this text and its focus on implementations.
- **Latest outcomes in the field:** to illustrate the latest advances in the field, we also provide readers with the description of some latest proposals, not older than 3 years.

3.1 Authentication and Identification Schemes

Authentication and identification schemes are cryptographic constructions that are particularly interesting from the perspective of digital identity protection. Using these schemes, a user is able to prove his identity to a verifier. The identity is being proven using users' secrets, for example passwords, private keys, etc. Since the difference between authentication and identification schemes is often unclear even in scientific literature, we provide the definition from [35] below.

- Authentication schemes: U can prove to V that he is U, but someone else cannot prove to V that he is U.
- Identification schemes: U can prove to V that he is U, but V cannot prove to someone else that he is U.

From the informal definition above we can see that the identification schemes have higher level of user protection. While in authentication systems the dishonest verifier is able to impersonate users, in identification systems this is not possible. The authentication schemes are often implemented using symmetric cryptography in contrast to identification schemes, that are based on asymmetric primitives.

We selected three schemes that illustrate both the fundamentals and latest advances in the area of identification schemes. The Schnorr authentication scheme [46] is very simple, almost the same as the proof of knowledge of a discrete logarithm protocol. Yet, it is one of the most frequently used construction in digital identity protection systems even today. The Fiat-Shamir (FS) scheme is one of the first identification schemes, it has been improved in many modifications and also implemented in

real applications. While the Schnorr and FS scheme represent quite dated proposals (from 1990's), the Peeter-Hermans scheme represents a recent identification scheme that has additional privacy-enhancing features. All examples provided in Sec. 3.1 are schemes designed for the implementation in RFID identification systems. This is exactly the purpose of our novel protocol proposed in Chap. 4, Sec. 4.1.

3.2 Anonymous Credentials

Anonymous Attribute-Based Credentials (ABCs) allow users to anonymously prove the ownership of their personal attributes. The attributes like age, citizenship, ticket ownership or driving license can be proven anonymously and without anyone's ability to trace or link the proving transactions. The ABC schemes usually employ the following entities.

- *Issuer (I)*: validates the applications for attributes, issues attributes to Users.
- *User (U)*: gets issued an attribute from the Issuer and anonymously proves its possession to Verifiers.
- *Verifier (V)*: receives the attribute ownership proof generated by the User, verifies its validity.
- *Revocation Referee (RR)*: revokes invalid attributes and credentials.

The entities engage in the following protocols.

- `Issue Attribute`: a User gets issued an attribute from an Issuer, based on past physical interaction, electronic interaction or no communication at all. By issuing an attribute we mean the issuance of a private key that can be used to prove attribute's ownership.
- `Prove Attribute`: using the private attribute key obtained by the `Issue Attribute` protocol, it is possible to build an attribute *proof* using the `Prove Attribute` protocol. The proof is anonymized and randomized. By running the `Prove Attribute` protocol, the User proves his ownership of attributes without disclosing any other personal information.
- `Revoke`: in special cases (e.g., attribute storage loss, theft or damage), the issued attributes can be revoked or even the malicious Users can be de-anonymized. In that case, the *proof* transcript is sent by the Verifier to a special revocation entity who decides about the justification and type of revocation.

The entities and protocols used in ABCs are depicted in Fig. 3.1.

In the thesis, we cover the most well-known schemes that are based on proven cryptographic protocols and have working implementations. The Idemix from IBM [27] and U-Prove from Credentica (Microsoft) [44] are covered. We provide only an introduction describing the basic functionality of these schemes, since details on particular features that are important for our work and have relevance to proposed schemes are covered in Chap. 4.

3.3 Group Signatures, Data Collection Schemes

In the past sections, we dealt mainly with identification and (attribute-based) authentication schemes. These schemes allow users to construct proofs about their identity or personal attributes. However, there are also systems where the requirement on the protection of digital identity is not so straightforward, but still very relevant. This is the case of group signature schemes (GS) and data collection

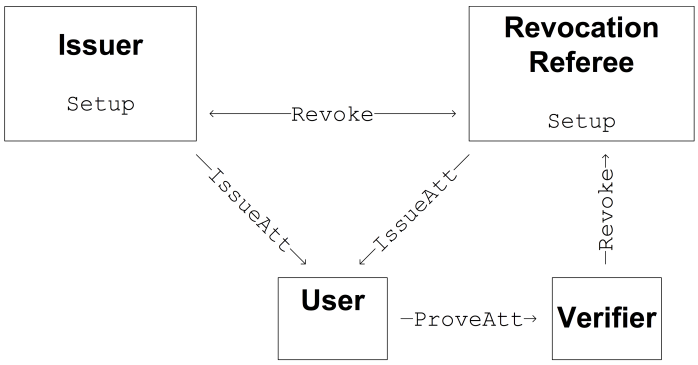

Fig. 3.1: Architecture of ABCs.

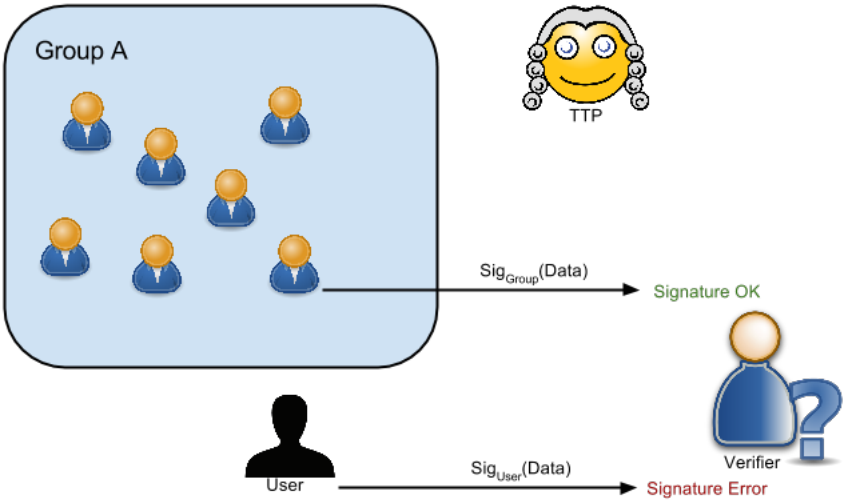

Fig. 3.2: Principle of group signatures.

schemes (DC). In these schemes, data is being signed by a user to prove their origin, authenticity and integrity. The examples of applications of group signatures and data collection schemes include smart-metering, vehicular networks, sensor networks and cloud-based applications.

The group signatures, originally proposed in [31], are the analogy of standard digital signature schemes. In contrast to standard signature schemes, data is not signed on behalf of a concrete user but on behalf of a certain group. In a typical scenario, data is signed by a user belonging to some group and the signature reveals only the information that it was created by a group member. However, the concrete signer's identity stays hidden. The identification is possible only in case disputes arise. In that case, a trusted third party is employed to identify a concrete user that created the signature. The group signatures are very useful in scenarios where we are interested more in the group origin than the concrete authorship of data. The principle of a group signature is depicted in Fig. 3.2.

The group signatures are basic primitives that are usually used as the building blocks in more complex cryptographic systems. Data collection systems are very often based on group signatures. Here, many users send signed data to a central distribution center that verifies the group origin of data, executes some processing and distributes anonymized results to another users. It is the typical

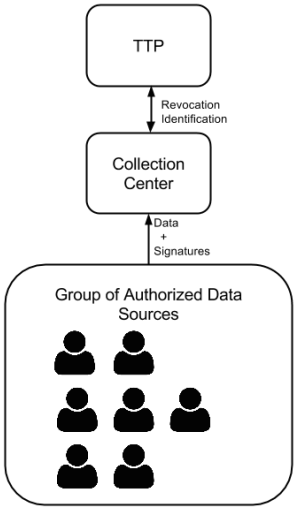

Fig. 3.3: Principle of data collection systems.

example of a many-to-one communication pattern-based system. In this system, both data integrity and authenticity is assured without disclosing the identity of signers. The concrete examples of data collection systems are the smart-metering systems, where data about consumption are collected from households to providers, the vehicular networks, where data about traffic and accidents are collected and distributed to drivers, or the cloud applications, where users' data is sent from PCs to cloud infrastructures for processing. All applications require privacy protection as well as data authenticity and integrity at the same time. The principle of a general data collection system is depicted in Fig. 3.3.

The group signature schemes are the fundamental building blocks of many privacy-enhancing schemes, including the data collection schemes. There is a large number of group signature schemes that have been proposed in past 20 years, for example [46, 28, 25, 33, 37, 26, 32, 36, 38, 20]. In the thesis, we cover only schemes that are particularly important for privacy-enhancing technologies and introduce significant novel functionality. We informally describe Schnorr's signature [46], Camenisch-Lysyanskaya's (CL) signature [28], Boneh, Boyen and Shacham's (BBS) signature [25] and provide an overview of other signatures and schemes.

4 NOVEL SYSTEMS USING PROOFS OF KNOWLEDGE

This chapter contains the original work of the author, that is the proposals of three cryptographic schemes based on the proof of knowledge protocols. Each scheme is designed for a different application, namely the identification of users, attribute-based authentication using anonymous credentials and data collection in vehicular networks.

4.1 Authentication and Identification Schemes

In this section, we provide the full description of a novel scheme for secure and privacy-friendly identification in physical access control systems. The amended version of the text below is part of the the official Secrypt 2015 conference proceedings [11] including further details.

4.1.1 Introduction to PACs

We use Physical Access Control systems (PACs) many times a day. We open parking lot gates, office complex doors or operate elevators by attaching our chipcards or RFID (Radio Frequency Identification) tags to electronic readers. Using PACs, the identification and authentication process is easy and fast. The chipcard just transmits the identifier stored in its memory to the reader. In more advanced systems, a cryptographic authentication protocol is additionally implemented to avoid the eavesdropping of identifiers by attackers.

The general architecture of physical access control systems is described in this section. Regardless the manufacturer, the existing commercial systems usually respect the architecture shown in Fig. 4.1.

Although some modifications might occur in concrete implementations, we will assume this architecture because it sufficiently reflects the most of existing systems and perfectly reflects the implementation we are aiming at with our scheme. We provide the list of key PAC entities and describe their roles in the system here.

- **User Device:** a smartcard or a smartphone used by a user for authentication. The User Device transmits the identifier or executes the authentication protocol with a reader via RFID interface. The expected range is upto 5 centimeters.
- **Reader:** a simple device receiving the identifier or authentication data. In trivial implementations, the reader just re-sends data received by the RFID interface to Access Terminal via a one-way Wiegand three-wire interface. In more complex implementations, the Reader is able to verify the cryptographic data received and re-send user's identifier only in case he provides correct proofs. In this case, the Reader is often equipped by SAM (Secure Access Module). Using SAM, the verification of cryptographic data might be faster and more secure due to the use of special cryptographic co-processors. The SAM is usually realized by a programmable smart-card, such as JavaCard [43] or MultOS card [39].
- **Access Terminal:** a device connected to Readers by a one-way Wiegand interface and to Central Servers by a two-way interface (e.g., LAN). The Access Terminal maintains a list of identifiers of authorized users. This list gets updated from Central Servers. After receiving

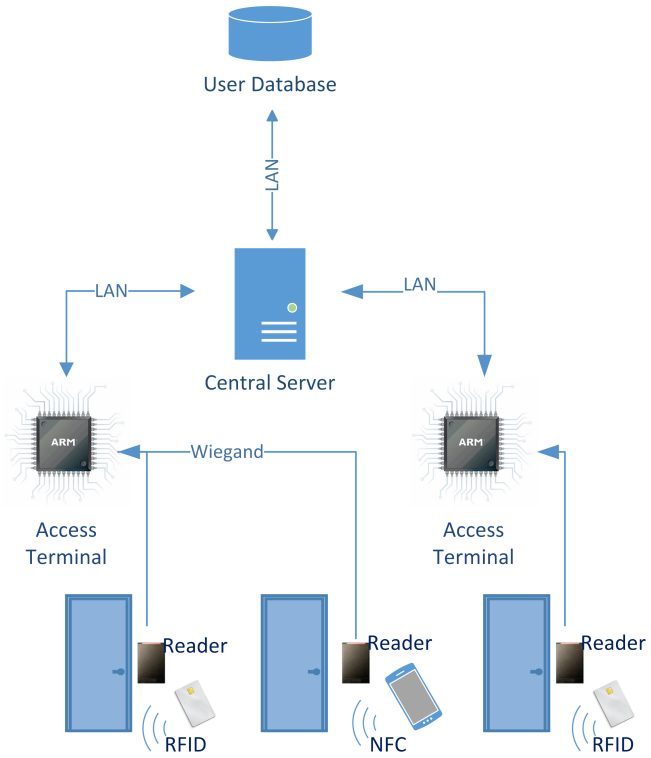

Fig. 4.1: General architecture of physical access control systems.

an identifier from the Reader, the Terminal checks its presence on its list and decides about authorization.

- **Central Server:** the Central Server is the central point of administration. Using Central Server, it is possible to add, remove, block and manage all users. The information necessary for authentication (user identifiers, their keys) are distributed to other devices from here.
- **User Database:** all user information is stored in a central database directly connected to the Central Server.

The weakest point of the above described architecture from the security perspective is the communication between the User Device and the Reader. That is due to its wireless nature and the fact that it is not protected physically (like the other interfaces might be, for example by running wires inside walls or private areas of the building). Therefore, most cryptographic protocols are aiming on securing the communication between users' smart-cards and SAMs inside Readers.

4.1.2 Our Contribution

We specify a novel cryptographic scheme called SPAC addressing the weaknesses of existing schemes. In particular, the SPAC scheme is designed to provide the following features.

- **Provable Security:** our SPAC scheme is based on cryptographic primitives with provable security, particularly on the interactive Schnorr-based proof of knowledge of discrete logarithm [46] in the RSA group [45]. We provide the full security analysis in the thesis.
- **Privacy Protection Features:** the SPAC scheme provides features for the protection of users' privacy and digital identity, namely user ID hiding and authentication sessions unlinka-

bility.

- **Non-Repudiation:** the SPAC scheme is based on asymmetric cryptography. The user is proving his identity using a private cryptographic key known only by him, not by anyone else. Therefore, users cannot repudiate their past transactions like in symmetric schemes.
- **Local Key Storage:** unlike existing schemes, the user authentication key is stored in user's device only, not in the verifier's device. That makes the key protection much easier.
- **Computational and Communication Efficiency:** the SPAC scheme is computationally efficient enough to run on low-resource devices like smart-cards and SAMs. The communication is realized by a simple 3-way protocol.

4.1.3 SPAC Summary

In the full version of the thesis, we provide the cryptographic specification of a novel physical access control scheme called SPAC. In comparison to existing schemes, SPAC is based on modern asymmetric primitives, that provide features currently unavailable in existing systems, such as provable security, local key storage, non-repudiation and authentication session randomization. The scheme is designed to be practical even on low-resource devices, such as smart-cards. The scheme shows the practical application of proof of knowledge protocols.

4.2 Anonymous Credentials

The full thesis contains the cryptographic specification of an original anonymous Attribute-Based Credential scheme (ABC) based on proof of knowledge protocols. The scheme was designed to address weaknesses of author's past schemes presented in [14, 8]. The amended version of the text below including further details is part of the official ACM CCS 2014 conference proceedings [9] and author's paper in the Security and Communication Networks journal published by Wiley [10].

4.2.1 Introduction to ABCs

By using attribute-based credentials, users can anonymously prove their possession of some attributes. These attributes can represent any personal data such as age, citizenship or valid driver's license. In contrast to classical authentication, the identity of attribute holders is never released. Thus, the verification process is anonymous and with many additional features protecting users' privacy. To provide user privacy, a verification session must be totally anonymous, unlinkable to other sessions and revealing no personal or traceable information. In contrast to this requirement, some linking is required in situations where the device containing credentials is lost, stolen or destroyed. In these cases, the credential must be revoked so that it cannot be used any time in future. Furthermore, there must be a mechanism for the identification of misbehaving users. The problem of existing attribute-based credentials is that they do not support the revocation of credentials and the identification of malicious users, if off-line, computationally weak devices (such as smart-cards) are used for storing attributes. We provide a short overview of revocation techniques used in existing credential systems in the thesis, together with reasons why we consider them impractical.

4.2.2 Our Contribution

In paper [14], we described a novel ABC scheme with efficient revocation. In the thesis, we update the scheme to be implementable with strong security even on devices not protected by hardware means. That allows the implementation on devices like smart-phones. The update requires complex redesign of the scheme and changes in both issuing and verifying protocols to avoid attacks on fixed value discrete logarithm proofs [24]. While the new scheme is more secure and preserves all the features of the original scheme (referred as HM12), we still consider the previous scheme more suitable for small, smart-card-based implementations due to its higher performance. However, if computationally strong devices like smart-phones are available as end-user devices, the scheme presented in this section is the preferred choice.

The scheme presented in thesis is able to provide anonymous, unlinkable, untraceable attribute verification. At the same time, a practical offline revocation mechanism is available. The scheme presented in this text thus eliminates all major technical problems of existing schemes - the missing *unlinkability* of verification sessions, the problematic *revocation* and the *collusion attack* susceptibility.

The scheme is particularly useful in physical access control (PAC) applications where offline, low-performance user devices are used. The existing solutions have weaknesses in these applications, since U-Prove protocol sessions are linkable unless many tokens are pre-issued, and Idemix lacks a method for immediate revocation that is practical on offline, low-performance user devices.

4.2.3 ABC Summary

In the full version of the thesis, we describe an ABC scheme that is the evolution of our HM12 scheme presented in [14]. The new scheme provides the cryptographic collusion protection at the cost of higher computational requirements and higher complexity. In particular, the collusion protection is achieved by requiring users to prove their knowledge of a discrete logarithm representation with respect to generators that are unique per user. Providing both HM12 and this scheme allows service providers to choose whether the system is protected by hardware means (that is the case of the HM12 scheme) or by cryptographic means (that is the case of the scheme presented here). Each approach suits different applications depending on hardware, security requirements, type of services, etc.

4.3 Group Signatures, Data Collection Schemes

In the past sections, we showed how the proof of knowledge protocols can be used to construct identification and attribute-based authentication schemes. Here, we show how a data collection scheme can be easily obtained from an ABC scheme. We present a scheme for secure data collection designed for vehicular networks. Using the scheme, traffic information can be collected from trusted sources (registered users) without any privacy risks. The novel scheme, called SVANET (Simple Vehicular Ad-Hoc Network), is built using modified protocols of our HM12 scheme described in [14]. The amended version of the text below is part of the the official Secrypt 2013 conference proceedings [17] including further details.

4.3.1 Introduction to VANETs

Vehicular Ad-hoc NETworks (VANETs) provide, so far mostly theoretically, mechanisms for the communication among cars in daily traffic. By implementing VANETs, it would be possible to share information about traffic accidents, road conditions, traffic density or road closures. Moreover, VANETs would also allow easier monitoring of traffic in cities and on highways. This would improve route planning. Improved traffic monitoring would significantly improve the efficiency, time demands and ecology of traveling.

VANETs allow the communication among cars, which are equipped with special devices called On-Board Units (OBUs). These built-on-purpose devices are wirelessly connected to stationary devices along roads called Road-Side Units (RSUs). Additionally to vehicles with OBUs and RSUs, many existing schemes also use additional third party entities (e.g., registration authorities, revocation authorities, etc.). We consider this concept too complex and impractical for a real-world implementation. It would be too demanding (both financially and logistically) to equip roads with special electronic devices on side (RSUs). Also, it would be very difficult to equip all cars with new, built-on-purpose devices (OBUs). Thus, we propose a new concept called SVANETs, which needs only smart-phones in participating cars. By simplifying the concept of VANETs, we hope that these communication networks will become more efficient and subsequently more commercially interesting and easier to deploy.

The security of VANETs plays a crucial role in the whole system. First, it is necessary to provide confidentiality and authenticity of messages. In addition to classical security requirements, like the confidentiality and authenticity of messages, the VANETs must also provide new means of privacy protection. Many security problems of existing VANETs are connected to the privacy of users. It must be assured that drivers are not traceable by attackers or by any other entity in the system. The protection of users' privacy plays an important role when the system is about to be deployed commercially and in a large scale. A system which allows the monitoring of drivers and their unwanted tracing would be surely rejected by customers.

In the Sec. 4.3, we propose a novel cryptographic scheme which is both highly computationally efficient and supporting all security requirements. It provides both the authenticity of messages and the privacy of users. The cryptographic scheme described in the thesis is a practical representation of the SVANET concept.

4.3.2 Our Contribution

Based on the analysis of existing schemes, we lack a practical scheme which is able to provide both basic security features (message confidentiality and authenticity) as well as advanced privacy-preserving features (in particular, the anonymity, untraceability and unlinkablity of drivers and no trusted third parties).

In our proposal, we get rid of costly Road-Side Units (RSU) and replace On-Board Units (OBUs) with users' smart-phones. We call the new concept Simple VANETs (SVANETs). Our concept supports both the basic security features, such as message confidentiality and authenticity, and advanced privacy-enhancing features. Still, the scheme remains highly practical on mobile devices.

4.3.3 SVANET Summary

The Sec. 4.3 in the full version of the thesis shows how the proof of knowledge protocols can be used to construct a simple VANET scheme. Using our novel scheme called SVANET, traffic information can be securely interchanged among cars without weakening user privacy. The scheme is a direct application of the ABC scheme specified in [14]. If a better protection against collusion attacks is required, the ABC scheme presented in the Sec. 4.2 can be used analogously.

5 IMPLEMENTATION ASPECTS

All schemes presented in Chap. 4 were designed to be practically implementable on real, off-the-shelf devices. Special attention was paid to provide not only theoretical constructions, but also practical systems that can be directly deployed in real products. Therefore, computationally costly operations, such as bilinear pairings, were ruled out from the architecture of schemes, although this decision made the design more difficult. To prove the efficiency and implementability of our proposals on real devices, we shortly analyze the implementation aspects of our cryptographic constructions in this chapter.

5.1 Implementation of Primitive Operations

Although the schemes proposed are quite complex, they are built using the modular composition of simpler protocols, mainly the proof of knowledge protocols. Furthermore, the proof of knowledge protocols are the composition of modular arithmetic operations and simple cryptographic operations like hash functions. In this section, we analyze the performance of the fundamental building blocks on resource restricted devices like smart-cards and smart-phones.

The information presented in this chapter and further details can be found in author's papers [16, 18] presented at DPM 2013 and IWSEC 2014 conferences, both published in Springer LNCS.

Smart-cards

It was possible to implement all required operations on all selected cards with the exception of MultOS ML2-80K-65 card which is lacking the support of 2048b modular exponentiation. In many operations, the JavaCard Oberthur ID-one v7.0a is very fast (in particular, in random number generation and 1024b modular exponentiation). Often, the bitlength of inputs (cryptographic group size) does play a significant role, for example in the case of modular exponentiation. Thus, we recommend to plan ahead before implementing and choose the right balance between speed and security (group size). Even with modern smart-cards, operations in 2048 b groups might be too demanding. When implementing complex privacy-enhancing schemes, operations in 2048 b groups would be probably too slow. Also, a big difference among cards appears when the modular multiplication and non-modular operations are needed. This is the case of all PK protocols where a group with unknown order is used (such as RSA group [45], OU group [42]). Then, the MultOS cards are much faster than the rest due to their direct support of these operations in API, in particular due to their built-in support of accelerated modular multiplication.

Android Devices

It is no surprise that most operations are several hundred times faster on Android devices than on smart-cards. All primitives can be easily implemented on Android. Due to the high performance, we recommend using larger (and safer) 2048-bit groups and more recent primitives (e.g., SHA-2 instead of SHA-1 or MD5).

5.1.1 Pilot Results

Our attribute-based credential system described in [14], that has a structure based on primitives similar to those used in schemes presented in this thesis, has been experimentally deployed at the university during the fall semester of 2013. The goal of the pilot deployment was to verify, whether the attribute-based credentials can be practically deployed for privacy-enabled access control. An attribute indicating student group membership has been issued to 30 smart-cards. Then, the students used the smart-cards to gain access to university laboratories. In this pilot deployment, the students remained anonymous and untraceable while the university had the ability to control access to its premises.

The attribute issuance phase is represented by the IssueAtt protocol and is realized via communication between the student's smart-card and the issuance terminal. The attribute issuance took around 4.5 s, including the time necessary for user key generation and data transfer. The operation needs to be done only once in a lifetime. After attribute issuance, the students were able to use the smart-card to access laboratories. The access was granted after successful completion of the ProveAtt protocol. The attribute proof generation and verification took around 2.9 s, including the time necessary for session randomization, revocation check and data transfer. During the pilot, the 1024 b version of all protocols was used. Using a mobile phone as an authentication devices, the proving phase takes under 1 s.

5.2 Implementation Summary

We present the complete implementation of all necessary building blocks and all protocols of the HM12 scheme, namely the attribute issuance protocol, the attribute verification protocol and the revocation protocol. All protocols were implemented on the MultOS ML3 smart-cards with only 16 b CPU and 2 kB of RAM available. We showed the results of our pilot deployment. The HM12 scheme, presented by the author of this thesis in [14], is the fundamental building block for our novel schemes presented in Chap. 4. The implementation results confirm that our cryptographic schemes presented here are 1) practically implementable on widely available hardware and 2) fully functional in real applications.

6 CONCLUSION

The main purpose of this thesis was to 1) provide a comprehensive, unified description of fundamental cryptographic constructions used in modern privacy-enhancing schemes, and 2) propose novel schemes for the protection of digital identity with improved features. The expected contribution is both pedagogical, i.e., to produce a missing study resource, and scientific, i.e., to produce schemes with currently unavailable features.

The *pedagogical contribution* is addressed in Chap. 2 and Chap. 3 where we provide a deep analysis of fundamental cryptographic building blocks used in systems for digital identity protection. In particular, we explain the principles and analyze the features and security aspects of commitment schemes, zero-knowledge protocols and proofs of knowledge about discrete logarithms. These primitives are the crucial building blocks of most modern privacy-enhancing schemes, not only those presented in this work. We also provide the overview of schemes most related to digital identity protection, i.e. identification schemes (Sec. 3.1), credential schemes (Sec. 3.2) and data collection schemes (Sec. 3.3). The sections in Chap. 2 and Chap. 3 contain necessary theoretical background to understand all the schemes presented in later chapters and most of existing schemes based on cryptographic proofs of knowledge. The text was written to serve the students of courses on modern cryptography, in particular courses taught by the author in the Information Security program at Brno University of Technology.

The *scientific contribution* is addressed in Chap. 4. Here, we propose novel cryptographic schemes based on cryptographic proofs of knowledge introduced in earlier chapters. Although applications in different domains are described, the common purpose of all schemes is digital identity protection. Schemes for physical access control (Sec. 4.1), anonymous credentials (Sec. 4.2) and secure data collection (Sec. 4.3) are proposed. All schemes presented have been peer-reviewed and accepted for publication in an impacted journal or at a renowned conference focused solely on cryptography. In addition to the theoretical verification by the scientific community, we also present the implementation results in Chap. 5. The fundamental building blocks were implemented and the performance was measured on low-resource devices. The results prove the practical implementability of our schemes on existing hardware and can be used to evaluate the performance of other schemes based on the same primitives.

Most of the schemes presented here are being implemented into products. The author of the thesis and his team works further on improving the schemes and adding new features in many projects involving both fundamental and applied research.

BIBLIOGRAPHY

Author's selected publications

[1] Hajny, J. *Flexible Authentication Framework.* In Proceedings of the 15th conference Student EEICT 2009, pp. 468–472. EEICT, 2009. ISBN 978-80-214-3870-5.

[2] Hajný, J. *Anonymous Authentication for Smartcards.* Radioengineering, 19:363–368, 2010. ISSN 1210-2512.

[3] Hajny, J. and Malina, L. *Implementation Results of Anonymous Authentications Scheme.* Elektrorevue, 2010:1–8, 2010. ISSN 1213-1539.

[4] Hajny, J., Malina, L., and Pelka, T. *Zero- Knowledge for Anonymous Authentication.* In Proceedings of the 33rd International Conference on Telecommunication and Signal Processing, pp. 1–6. TSP, 2010. ISBN 978-963-88981-0-4.

[5] Hajny, J., Malina, L., and Zeman, V. *Practical anonymous authentication - Designing anonymous authentication for everyday use.* In Proceedings of the 8th International Conference on Security and Cryptography (SECRYPT 2011), pp. 405–408. 2011. ISBN 978-989-8425-18- 8.

[6] Hajný, Jan. *Úvod do Zero- Knowledge protokolů.* Crypto-World, 10:7–13, 2008. ISSN 1801-2140.

[7] Hajný, Jan. *Anonymita v globální síti.* Crypto-World, 11:7–11, 2009. ISSN 1801-2140.

[8] Hajny, Jan. Authentication Protocols and Privacy Protection. Ph.D. thesis, Brno University of Technology, 2012.

[9] Hajny, Jan, Dzurenda, Petr, and Malina, Lukas. *Privacy-PAC: Privacy-Enhanced Physical Access Control.* In Proceedings of the 13th Workshop on Privacy in the Electronic Society, pp. 93–96. New York, NY, USA: ACM, 2014. ISBN 978-1-4503-3148-7. doi: 10.1145/2665943.2665969.
URL `http://doi.acm.org/10.1145/2665943.2665969`

[10] Hajny, Jan, Dzurenda, Petr, and Malina, Lukas. *Attribute-Based Credentials with Cryptographic Collusion Prevention.* Security and Communication Networks, p. In Print, 2015.

[11] Hajny, Jan, Dzurenda, Petr, and Malina, Lukas. *Secure Physical Access Control with Strong Cryptographic Protection.* In Proceedings of the 12th International Conference on Security and Cryptography (SECRYPT 2015), pp. 220–227. 2015. ISBN 978-989-758-117-5. doi:10.5220/0005524202200227.

[12] Hajny, Jan, Dzurenda, Petr, Malina, Lukas, and Zeman, Vaclav. *Cryptography for Privacy- Preserving Electronic Services*. In 37th International Conference on Telecommunications and Signal Processing (TSP). 2014. ISBN 978-80-214-4983-1.

[13] Hajny, Jan and Malina, Lukas. *Practical Revocable Anonymous Credentials*. In Bart De Decker and DavidW. Chadwick, editors, Communications and Multimedia Security, vol. 7394 of *Lecture Notes in Computer Science*, pp. 211–213. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-32804-6. doi:10.1007/978-3-642-32805-3_22.
URL http://dx.doi.org/10.1007/978-3-642-32805-3_22

[14] Hajny, Jan and Malina, Lukas. *Unlinkable Attribute-Based Credentials with Practical Revocation on Smart-Cards*. In Stefan Mangard, editor, Smart Card Research and Advanced Applications, vol. 7771 of *Lecture Notes in Computer Science*, pp. 62–76. Springer Berlin Heidelberg, 2013. ISBN 978-3-642-37287-2. doi:10.1007/978-3-642-37288-9_5.
URL http://dx.doi.org/10.1007/978-3-642-37288-9_5

[15] Hajny, Jan, Malina, Lukas, and Dzurenda, Petr. *Practical Privacy-Enhancing Technologies*. In 38th International Conference on Telecommunications and Signal Processing (TSP). 2015. ISBN 978-1-4799-8498-5.

[16] Hajny, Jan, Malina, Lukas, Martinasek, Zdenek, and Tethal, Ondrej. *Performance Evaluation of Primitives for Privacy-Enhancing Cryptography on Current Smart-Cards and Smart-Phones*. In Joaquin Garcia-Alfaro, Georgios Lioudakis, Nora Cuppens-Boulahia, Simon Foley, and William M. Fitzgerald, editors, Data Privacy Management and Autonomous Spontaneous Security, vol. 8247 of *Lecture Notes in Computer Science*, pp. 17–33. Springer Berlin Heidelberg, 2014. ISBN 978-3-642-54567-2. doi:10.1007/978-3-642-54568-9_2.
URL http://dx.doi.org/10.1007/978-3-642-54568-9_2

[17] Hajny, Jan, Malina, Lukas, Martinasek, Zdenek, and Zeman, Vaclav. *Privacy-preserving SVANETs - Privacy-preserving Simple Vehicular Ad-hoc Networks*. In SECRYPT 2013 - Proceedings of the 10th International Conference on Security and Cryptography, Reykjavík, Iceland, 29-31 July, 2013, pp. 267–274. 2013. ISBN 978-989-8565-73-0.

[18] Hajny, Jan, Malina, Lukas, and Tethal, Ondrej. *Privacy-Friendly Access Control Based on Personal Attributes*. In Maki Yoshida and Koichi Mouri, editors, Advances in Information and Computer Security, vol. 8639 of *Lecture Notes in Computer Science*, pp. 1–16. Springer International Publishing, 2014. ISBN 978-3-319-09842-5.

[19] Hajny, Jan and Zeman, Vaclav. *Anonymous Authentication with Spread Revelation*. Cryptologia, 35(3):235–246, 2011. ISSN 0161-1194. doi:10.1080/01611194.2011.584777.
URL http://dx.doi.org/10.1080/01611194.2011.584777

[20] Malina, Lukas, Castellà-Roca, Jordi, Vives-Guasch, Arnau, and Hajny, Jan. *Short-Term Linkable Group Signatures with Categorized Batch Verification.* In Joaquin Garcia-Alfaro, Frédéric Cuppens, Nora Cuppens-Boulahia, Ali Miri, and Nadia Tawbi, editors, Foundations and Practice of Security, vol. 7743 of *Lecture Notes in Computer Science*, pp. 244–260. Springer Berlin Heidelberg, 2013. ISBN 978-3-642-37118-9. doi: 10.1007/978-3-642-37119-6_16.

[21] Malina, Lukas and Hajny, Jan. *Privacy-preserving framework for geosocial applications.* Security and Communication Networks, 7(11):1764–1779, 2014. ISSN 1939-0122.

[22] Malina, Lukas, Hajny, Jan, and Martinasek, Zdenek. *Efficient Group Signatures with Verifier-local Revocation Employing a Natural Expiration.* In SECRYPT, pp. 555–560. 2013. ISBN 978-989-8565-73-0.

Other publications

[23] *Federal Information Processing Standards Publication (FIPS 197). Advanced Encryption Standard (AES)*, 2001.

[24] Alpar, Gergely, Hoepman, Jaap-Henk, and Lueks, Wouter. *An Attack Against Fixed Value Discrete Logarithm Representations*. Cryptology ePrint Archive, Report 2013/120, 2013.

[25] Boneh, Dan, Boyen, Xavier, and Shacham, Hovav. *Short group signatures*. In Advances in Cryptology - CRYPTO'04. 2004. ISBN 3-540-22668-0.

[26] Boneh, Dan and Shacham, Hovav. *Group signatures with verifier-local revocation*. In Proceedings of the 11th ACM conference on Computer and communications security, pp. 168–177. ACM, 2004.

[27] Camenisch, Jan and et Al. *Specification of the Identity Mixer Cryptographic Library*. Tech. rep., IBM Research - Zurich, 2012.

[28] Camenisch, Jan and Lysyanskaya, Anna. *A signature scheme with efficient protocols*. In Proceedings of the 3rd international conference on Security in communication networks, SCN'02, pp. 268–289. Berlin, Heidelberg: Springer-Verlag, 2003. ISBN 3-540-00420-3.

[29] Camenisch, Jan and Stadler, Markus. *Efficient group signature schemes for large groups*. In Burton Kaliski, editor, Advances in Cryptology - CRYPTO '97, vol. 1294 of *Lecture Notes in Computer Science*, pp. 410–424. Springer Berlin / Heidelberg, 1997. ISBN 978-3-540-63384-6.

[30] Chaum, David. *Security without identification: transaction systems to make big brother obsolete*. Commun. ACM, 28:1030–1044, 1985. ISSN 0001-0782.

[31] Chaum, David and Van Heyst, Eugène. *Group signatures*. In Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques, EUROCRYPT'91, pp. 257–265. Berlin, Heidelberg: Springer-Verlag, 1991. ISBN 3-540-54620-0.

[32] Chu, Cheng-Kang, Liu, Joseph K, Huang, Xinyi, and Zhou, Jianying. *Verifier-local revocation group signatures with time-bound keys*. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 26–27. ACM, 2012.

[33] Delerablée, Cécile and Pointcheval, David. *Dynamic fully anonymous short group signatures*. In Progress in Cryptology-VIETCRYPT 2006, pp. 193–210. Springer, 2006.

[34] Diffie, W. and Hellman, M. *New Directions in Cryptography*. IEEE Trans. Inf. Theor., 22(6):644–654, 2006. ISSN 0018-9448. doi:10.1109/TIT.1976.1055638.
URL `http://dx.doi.org/10.1109/TIT.1976.1055638`

[35] Feige, Uriel, Fiat, Amos, and Shamir, Adi. *Zero-knowledge proofs of identity.* Journal of Cryptology, 1(2):77–94, 1988. ISSN 0933-2790. doi:10.1007/BF02351717. URL http://dx.doi.org/10.1007/BF02351717

[36] Ferrara, Anna Lisa, Green, Matthew, Hohenberger, Susan, and Pedersen, Michael Østergaard. *Practical Short Signature Batch Verification.* In Topics in Cryptology - The Cryptographers' Track at the RSA Conference, vol. 5473, pp. 309–324. Springer, 2009.

[37] Hwang, Jung Yeon, Lee, Sokjoon, Chung, Byung-Ho, Cho, Hyun Sook, and Nyang, DaeHun. *Short group signatures with controllable linkability.* In Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), 2011 Workshop on, pp. 44–52. IEEE, 2011.

[38] Kim, Kitae, Yie, Ikkwon, Lim, Seongan, and Nyang, Daehun. *Batch Verification and Finding Invalid Signatures in a Group Signature Scheme.* IJ Network Security, 13(2):61–70, 2011.

[39] MultOS. *MultOS Webpage.* "http://www.multos.com", 2015.

[40] National Institute of Standards and Technology (U.S.) . Digital Signature Standard (DSS) [electronic resource]. U.S. Dept. of Commerce, National Institute of Standards and Technology, Gaithersburg, MD :, 2009.

[41] Naumann, Ingo and Hogben, Gilles. *Privacy Features of eID Cards.* Network Security Newsletter, 2008:9–13, 2008. ISSN 1353-4858.

[42] Okamoto, Tatsuaki and Uchiyama, Shigenori. *A new public-key cryptosystem as secure as factoring.* In Kaisa Nyberg, editor, Advances in Cryptology - EUROCRYPT 98, vol. 1403 of *Lecture Notes in Computer Science*, pp. 308–318. Springer Berlin / Heidelberg, 1998. ISBN 3-540-64518-7.

[43] Oracle. *Java Card Webpage.* "http://www.oracle.com/technetwork/java/embedded/javacard/overview/index.html", 2015.

[44] Paquin, Christian. *U-Prove Cryptographic Specification V1.1.* Tech. rep., Microsoft Corporation, 2011.

[45] Rivest, R. L., Shamir, A., and Adleman, L. *A method for obtaining digital signatures and public-key cryptosystems.* Commun. ACM, 21:120–126, 1978. ISSN 0001-0782.

[46] Schnorr, C. P. *Efficient signature generation by smart cards.* Journal of Cryptology, 4:161–174, 1991. ISSN 0933-2790.

[47] The White House. *National Strategy for Trusted Identities in Cyberspace*, 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

LIST OF ABBREVIATIONS

Acronym	Meaning	Remark
3DES	Triple Data Encryption Standard	Block cipher.
ABC	Attribute-Based Credentials	Cryptographic schemes.
AES	Advanced Encryption Standard	Block cipher.
API	Application Programming Interface	
BBS	Boneh Boyen Shacham	Group signature.
CL	Camenisch Lysyanskaya	Group signature.
CPU	Central Processing Unit	
CS	Camenisch Stadler	Notation for proofs of knowledge.
DC	Data Collection	
DH	Diffie-Hellman	
DES	Data Encryption Standard	Block cipher.
DH	Diffie Hellman	
DL	Discrete Logarithm	
DSA	Data Signature Algorithm	Signature scheme in Digital Signature Standard.
E	Encrypt	
EC	Elliptic Curve	
ECC	Elliptic Curve Cryptography	
FS	Fiat Shamir	Heuristic for non-interactive proofs.
GCD	Greatest Common Divisor	
GDLP	Generalized Discrete Logarithm Problem	
GS	Group Signature	
HM12	HM12 Protocol	ABC scheme.
HVZK	Honest Verifier Zero Knowledge	
I	Issuer	
IA	Interactive Argument	
ID	Identifier	
IPS	Interactive Proof System	
IPTM	Interactive Pair of Turing Machines	
ITM	Interactive Turing Machine	
KAC	Key Authentication Center	Entity in Schnorr's authentication scheme.
LAN	Local Area Network	
NFC	Near Field Communication	
NIST	National Institute for Standards and Technology	U.S. Standardization body.
NIZK	Non-Interactive Zero Knowledge	
NP	Non Polynomial	
OBU	On Board Unit	
OU	Okamoto Uchiyama	Group used by Okamoto Uchiyama cryptosystem.
P	Prover	
P*	Prover	Any, even dishonest prover.
PAC	Physical Access Control	
PK	Proof of Knowledge	
PRNG	Pseudo Random Number Generator	
RAM	Random Access Memory	
RFID	Radio Frequency Identification	
RNG	Random Number Generator	
RR	Revocation Referee	
RSA	Rivest Shamir Adleman	Encryption/signature scheme.
RSU	Road Side Unit	
SAM	Secure Access Module	
SPAC	Secure Privacy Access Control	

SPK	Signature Proof of Knowledge	Signature scheme based on PKs.
SRSA	Strong RSA	Assumption.
SVANETs	Simple Vehicular Ad-Hoc Network	
TTP	Trusted Third Party	
U	User	
UID	Unique Identifier	
V	Verifier	
V*	Verifier	Any, even dishonest prover.
VANETs	Vehicular Ad-Hoc Networks	
VE	Verifiable Encryption	
VLR	Verifier-Local Revocation	Revocation not affecting remaining users.
ZK	Zero Knowledge	

ABSTRACT

This thesis deals with the fundamental building blocks of cryptographic systems for the protection of digital identity, especially with the cryptographic proofs of knowledge. The first part of the text contains the description and analysis of primitives used during the construction of modern protocols, in particular the cryptographic commitment schemes, interactive proof systems, Σ-protocols and proofs of knowledge. The analysis of primitives allows readers to understand current proposals of protocols and schemes for the digital identity protection, such as authentication, identification, access control systems, and systems with enhanced privacy protection, such as attribute-based authentication systems or anonymous credentials. The first part of the text, which is written as a complex introduction to the area of cryptographic protection of digital identity, contains also the current state analysis.

In the next chapters, own cryptographic schemes based on aforementioned primitives are proposed. The schemes for physical access control, attribute-based authentication and secure data collection are specified. Using the proposals, the modularity and versatility of the primitives are demonstrated in various applications. The main contributions of the schemes are novel privacy-enhancing features and features for the identification of malicious users using revocation and de-anonymization methods. The existing systems either lack these features completely or provide only inefficient solutions that cannot be implemented on real devices. The efficiency of our methods is proven in the final chapter devoted to implementation aspects.