VĚDECKÉ SPISY VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ

Edice PhD Thesis, sv. 669

ISSN 1213-4198

Ing. Jan Hajný

Authentication Protocols and Privacy Protection

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

Ing. Jan Hajný

AUTHENTICATION PROTOCOLS AND PRIVACY PROTECTION

AUTENTIZAČNÍ PROTOKOLY A OCHRANA SOUKROMÍ

ZKRÁCENÁ VERZE PH.D. THESIS

Obor: Teleinformatika
Školitel: doc. Ing. Karel Burda, CSc.
Oponenti: doc. Ing. Miroslav Vozňák, Ph.D.
Ing. Tomáš VANĚK, Ph.D.
Datum obhajoby: 10. 9. 2012

KEYWORDS
Privacy, authentication, digital identity protection, cryptography, anonymity, smart-cards.

KLÍČOVÁ SLOVA
Soukromí, autentizace, ochrana digitální identity, kryptografie, anonymita, smart-karty.

Disertační práce je k dispozici na Vědeckém oddělení děkanátu FEKT VUT v Brně, Technická 10, Brno, 616 00

ISBN 978-80-214-4591-8

ISSN 1213-4198

CONTENTS

Introduction **5**

1 Current State Analysis **7**
1.1 Existing Techniques for Revocation 7
1.2 Existing Attribute Authentication Systems 8

2 Thesis Objectives **11**

3 Cryptography and Notation **12**
3.1 Used Cryptographic Primitives 12
3.1.1 DL Commitments 12
3.1.2 Σ-protocols 12
3.1.3 Okamoto-Uchiyama Trapdoor One-Way Function 13
3.1.4 Bao's Verifiable Encryption 13
3.2 Notation 13

4 Novel Scheme for Attribute Authentication **15**
4.1 Additional Contribution 16
4.2 General Overview 17
4.3 Cryptographic Design 18

5 Conclusion **23**

Bibliography **25**

INTRODUCTION

User authentication is a service crucial for many electronic transactions. Without a secure verification of users, it would be impossible to provide many services both on the Internet and during everyday life. We need authentication services for the verification of identities and persons' authorizations. The most common examples of systems, where authentication is a fundamental service, are the electronic banking systems, information systems or physical access systems. In addition to these fundamental systems, there are many non-critical applications which are used on daily basis like employee ID cards, library cards or discount cards. With the steep increase of the number of services provided electronically, it is reasonable to expect a strengthening demand for secure and reliable authentication systems. On the other hand, it is not only the security of service providers what is needed to protect. The security and privacy of users must be also protected. It is very important to keep in mind the fact that users release a lot of personal information by using authentication services. Every time we use an authentication system to get an access to a service, we release our identity, which can be abused by the service providers for tracking our behavior, profiling our usage of the service or even for impersonation. That is the reason why modern authentication systems provide privacy enhancing features protecting users' identities and private data. In this thesis, the aspects of existing privacy enhancing authentication systems are analyzed and a new authentication scheme providing advanced features for privacy protection is developed.

The classical authentication systems, like RADIUS, Diameter or Kerberos, are frequently used for the identity verification. Based on the identity of a user, the system usually decides about the authorization. Therefore, the primal goal of these systems is to provide a user with some secret information and then do the verification of the possession of that secret. This approach is used in most present authentication systems because it is simple and allows many variations based on many forms of users' secrets. The user passwords, secret keys, private asymmetric keys or even biometric data can be used. The classical authentication systems provide a relatively safe way to verify the identity of a user. On the other hand, underlying cryptographic primitives are usually simple and don't allow building mathematical proofs of security. That is the reason why more complex authentication protocols have been developed in the end of 90's.

The advanced authentication protocols allow a deeper mathematical analysis. These protocols are usually based on assumptions about underlying cryptographic primitives. In authentication systems, the use of so called *Zero-Knowledge* primitives have become very popular for the design of new protocols. These primitives allow building mathematical proofs of security. It is possible to prove that an authentication protocol based on Zero-Knowledge primitives releases exactly no more information about a user than it is designed for. This is very useful because the user can be then sure that no private information is released during the execution of the protocol. The Zero-Knowledge protocols are used in many practical systems today. Even advanced systems, which provide not only authentication but also more complex features, use the Zero-Knowledge cryptographic primitives. We describe the cryptographic background in Section 3 and build a new system from related primitives in Section 4.

Unfortunately, the verification of user identity brings some risks. Let us leave out the risk of stolen passwords or keys and let us consider the authentication protocols secure from this perspective. Even in that case, the service providers always learn the identities of users who are trying to use their

services. The identities can be considered privacy-sensitive information, from the privacy-protecting perspective it would be desirable that the service providers learn as little private information as possible. With the information about users' identities, it is possible to track users, analyze their behavior and create user profiles. Based on this information, a more focused advertisement, prediction of user behavior or even the revelation of other personal information can be done. In this thesis, it is shown that more granularity to user authentication is needed. There are many services, like libraries, video archives or private Internet databases, where the identity disclosure is not necessary for authorization. In many cases, only the verification of some personal attributes (like age, license possession or citizenship) is sufficient for receiving a service. In these cases, disclosing identity is unnecessary and creates security risks. That is the reason why the *attribute authentication* systems have been introduced. In these systems, only a user-selected subset of private attributes can be disclosed. As a result, the users can stay anonymous during the use of services while their attributes are securely verified. These systems provide the maximum level of privacy protection - the users can reveal specifically only those private attributes which are needed by the service providers.

There are many reasons why the mentioned privacy preserving authentication systems are not yet used in commercial systems. Among others, it is the unwillingness of service providers who don't want to provide their services to anonymous users. They want to protect their assets by being able to revoke invalid users and identify malicious users. Unfortunately, it is very difficult to achieve privacy and anonymity for honest users together with the ability to revoke and identify attackers. Currently, none of existing systems provides reliable and practical revocation of malicious users. Therefore, the goal of this thesis is to provide a cryptographic attribute authentication scheme with working revocation features.

In this thesis, the main focus is put on the privacy-preserving attribute authentication systems. They represent the most recent step in the development of authentication systems. To explicitly show the difference between classical authentication and attribute authentication, the following two definitions are included.

Classical Authentication [36]: "Entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired)."

Attribute Authentication: Attribute authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the possession of particular attributes (like age, citizenship or driving license ownership) of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired).

Chapter 1 describes the main competitors of the newly proposed cryptographic scheme which are the U-Prove of Microsoft and Idemix of IBM. Chapter 2 defines the objectives of the thesis. The requirements on the new authentication systems are stated here. The main output of this thesis, the new attribute authentication scheme, is described in Chapter 4. The information about the implementation on a smart-card platform, performance results and formal security proofs are provided in the full version of the thesis. The conclusion and proposals for future development are given in Chapter 5.

1 CURRENT STATE ANALYSIS

In the first part of this chapter, the existing revocation techniques are analyzed and their weaknesses are described. To author's best knowledge, there is currently no scheme providing practical, multi-level revocation which is implementable on smart-cards.

In the second part of the chapter, the analysis of existing attribute authentication systems is provided. Currently, there are only two schemes which provide attribute authentication capabilities and have the potential to become widespread. They are the U-Prove and idemix, both analyzed in this chapter. These systems, both supported by large IT companies, are compared with the proposal. The weaknesses and missing features, which make them less practical, are identified.

1.1 Existing Techniques for Revocation

Revocation, a feature crucial for both attribute issuers and service providers, allows an authentication token to be revoked after its misuse, expiration, theft or loss. By omitting revocation, there is no mechanism for revoking malicious users, stolen verification tokens or lost verification smart-cards. Missing revocation is a strong reason why the service providers do not accept existing systems. It is too dangerous for them to provide their assets without being able to revoke invalid users, charge attackers for potential damage or identify clients who use stolen identities. The problem of missing revocation has been unsuccessfully addressed by many authors in papers dealing with privacy enhancing cryptography. A short overview of revocation techniques used in existing systems is provided there together with reasons why they were found impractical.

Blacklisting of Token IDs

Some systems, for example U-Prove [37], use a token identifier embedded to each transaction. The identifier is a public, unique and unchangeable number linked to the token. This number can be used to revoke the token by putting it on a blacklist. Nevertheless, this approach destroys unlinkability (the unique token identifier creates a link among all user's verification sessions). Furthermore, a token can be revoked only by verifiers who already saw the token before and there is no mechanism for revoking tokens by their issuers. That is why the issuers have no power to revoke invalid, stolen or expired tokens.

Blacklisting of Secrets

The technique for blacklisting of secrets, used, for example, in [21], allows an invalid token to be revoked by using the knowledge of secret keys used for its construction. This technique can be used in cases where secret keys of users are revealed and for example made public on the Internet. In that case, a revocation authority can create a blacklist of these keys to prevent verifiers from accepting tokens based on leaked keys. Nevertheless, this technique works only if the user secrets are revealed. But in most cases, the secret keys never leave a protected device (like a smart-card), therefore they cannot be revoked. Moreover, lost, stolen or expired tokens (e.g., stored on a smart-card) cannot be revoked because their secret keys never become public.

Epochs of Lifetime

Epochs of lifetime are the official revocation technique of idemix [29]. Here, a credential carries an epoch of validity as a special attribute. In this case, the verifier can check whether the credential is fresh. The user is required to renew his credential for every new epoch. The disadvantage of this mechanism is that the revocation of credentials is never immediate, the revoker must wait until their expiration and the issuer must stop issuing new credentials to revoked users. The second major disadvantage is that the user must periodically run the issuance protocol with the issuer (or designated entity) to update his credential.

Accumulator Proofs

The most recent technique, analyzed in [35], allows both issuers and verifiers to revoke tokens immediately by publishing so called whitelists. In this technique, a user must provide a proof that his token is included on a list of valid tokens. This can be done anonymously and efficiently using so called accumulators which accumulate all non-revoked users. Most efficient techniques are based on bilinear maps [25, 38, 41, 25]. The disadvantage of these solutions is that the user must update his secrets every time any other user is revoked from the system. This is not a big problem when the user uses an on-line computer for his verification. On the other hand, if the user uses only an off-line device, like a smart-card, then he is unable to update his secrets. Therefore, the user is unable to use his token after some other users are revoked from the system. The objective of this thesis is to provide a system which can be used for everyday verification in libraries, pubs or hotels, therefore the smart-card implementation is crucial. That is the reason why the accumulator based techniques are considered impractical.

Verifiable Encryption of Secrets

The user identity or personal secrets can be encrypted inside a token in such a manner that only a trusted authority can do the revocation or identity disclosure by decryption. In this case, the system might be considered insecure from the perspective of a user who does not fully trust the authority. In fact, this is a likely problem since users would not welcome a scheme where a fixed third party can learn all information about their verification sessions, including their identities. In practical scenarios, the user would have no choice from more trusted authorities. This even more degrades his trust in such a dictated authority. Furthermore, there is a problem with unlinkability because the verifiable encryption must be randomized for each session, which might be inefficient. Even though mentioned in some papers, this technique has not been used for revocation in any well-known system for anonymous attribute authentication.

1.2 Existing Attribute Authentication Systems

There are two privacy preserving authentication systems which have the potential of getting largely widespread. They are the idemix of IBM [29] and the U-Prove of Microsoft [37].

Let us start with Microsoft's U-Prove scheme developed by Stefan Brands [19]. Using U-Prove, a user can run the issuing protocol with an issuer to get a token with requested attributes. Then, the token can be presented to a service provider, who is able to verify the attributes and their

Tab. 1.1: Comparison to existing privacy preserving schemes.

	U-Prove	**Idemix**	**Proposed**
Security	DL	sRSA	DL
Anonymity	•	•	•
Attributes	•	•	•
Untraceability	•	•	•
Selective disclosure	•	•	•
Smart-cards	O	•	•
Practical revocation	O	O	•
Anonymity revocation	O	O	•
Speed	(1+u) exp.	(9+u) exp.	6 exp.

Glossary: O = Unsupported, • = Supported.

ownership. The user might decide to reveal only a subset of attributes. A hardware device might be enforced to participate during the presentation protocol. The scheme provides user anonymity, since the verifier is unable to identify a user who is presenting an attribute (if the user wishes so). Similarly, the issuer is unable to trace issued tokens. Nevertheless, the scheme does not provide the unlinkability of verification sessions, the recommendation of U-Prove authors is to use a different token for every verification session. This solution certainly works if the user has a computer connected to a network always available. In that case, he has enough resources to recompute tokens for every verification session. U-Prove also does not provide efficient revocation. It is possible to revoke tokens using their IDs, nevertheless this destroys unlinkability and is not available for Issuers. Unofficial mechanisms [20] need on-line token updates, thus require users' devices connected to the Internet and are computationally inefficient. The solution is also impractical for computationally slow devices. U-Prove does not seem to aim to the verification based solely on smart-cards. Unfortunately, many systems (e.g. [45, 46]) have this limitation too, because they are unable to provide a user with a long-term token which can be spent many times without being linkable.

The attacks using linking of verification sessions are not applicable to credential systems. These systems were introduced by Chaum [34], improved by Camenisch and Lysyanskaya [26, 27] and since then they have been redefined or improved many times to become idemix of IBM [29]. Similarly to U-Prove, these systems allow a user to be verified as a member of an organization, more generally as a holder of an attribute. This can be done efficiently, anonymously, untraceably a provably securely. There is also no need for token re-registration, computation delegation or communication with third party entities. The system has already been implemented in both computer and smart-card environment [33, 21]. Unlike U-Prove, idemix can run solely on smart-cards (JavaCards) without losing unlinkability. That is the reason why idemix can be implemented as an eID, where the verification sessions cannot be linked together. Nevertheless, also idemix lacks some important features. The basic revocation of users is still not fully resolved, since the initial proposal [26] is too computationally inefficient for a smart-card implementation, more recent solutions require credential updates [35, 28, 29], are not supported by current smart-card platforms [38, 41] or both [25]. Furthermore, the idemix does not provide mechanisms for the identification of malicious users. This feature has been proposed, but is not implementable on smart-cards due to high complexity [26], or is focused rather on accountability and the fulfillment of a predefined contract [24]. Full identification of internal mali-

cious users is considered very important in this thesis, since it protects service providers' assets. It is supposed that any system lacking the ability to identify and charge malicious users cannot be widely accepted by commercial service providers. Moreover, the verification time of idemix implementation [21] is around 10 s for the basic version[1]. Although it is a dramatical improvement in comparison to previous schemes, it can be still considered quite a long time for verification in a real life.

An overview of features supported by the proposed scheme and its main competitors, U-Prove and idemix, is provided in Table 1.1. In Speed row, the letter "u" represents the number of undisclosed attributes. Speed is measured by the number of exponentiations (exp). The comparison is based on information from the official U-Prove [37] and idemix [29, 21] specification.

[1] JCOP v2.2/41, restricted attribute security model, no revocation, no malicious user identification.

2 THESIS OBJECTIVES

The general objective of this thesis is to provide more privacy and identity protection in user authentication. Although it may sound contradictory to provide both privacy and authentication, there are systems which partially allow that. With attribute authentication systems, it is possible that users only prove the possession of some personal attributes (for example age, citizenship or driving license ownership) without disclosing their identity. More types of systems can be called attribute authentication systems. Therefore, the analysis of existing systems is the first objective of this thesis. The most promising ones, credential schemes and anonymous tokens, are introduced in Chapter 1. Unfortunately, these complex cryptographic systems do not provide all required features. Therefore, the main objective of this thesis is to design a new cryptographic scheme which will support all following privacy preserving features.

- **Security**: the novel scheme will be built using strong cryptographic primitives.
- **Anonymity**: the scheme will protect user's identity by providing anonymity during the verification session.
- **Untraceability**: no entity in the scheme will be able to trace a particular user.
- **Selective disclosure of attributes**: users will be able to disclose and prove the possession of any subset of their private attributes.
- **Non-transferability**: user's will be strongly discouraged by used cryptography from lending their attributes to other entities.
- ***Practical, complex* revocation**: invalid credentials will be revocable and malicious users will be traceable or even identifiable while honest users will stay anonymous.

The above enlisted privacy enhancing features are partially supported by existing systems. From these features, *revocation* is very hard to obtain. For revocation, some authority or authorities must be able to reveal all sessions of a particular user and invalidate them. This virtually contradicts anonymity, untraceability and unlinkability. Currently, satisfactory revocation is not supported by existing practical solutions. The new scheme for attribute authentication designed in this thesis will provide *all* required features, including revocation.

Furthermore, it is necessary to provide guarantees for service providers that the new system cannot be abused by users who want to exploit anonymity. Such guarantees are not provided by existing systems which leads to their rejection by the commercial sector. Therefore, a complex revocation of malicious user anonymity must be provided and users' responsibility for their acts must be assured.

By providing all mentioned privacy-enhancing features, particularly the practical revocation, it will be possible to construct new practical authentication systems which will be protecting user privacy and digital identity much more than current solutions do.

3 CRYPTOGRAPHY AND NOTATION

This chapter describes the cryptographic constructions and the notation used in this thesis. The cryptographic primitives are described here because they are used in subsequent chapters describing the related work and the proposed scheme. Most cryptographic primitives use the concept of provable security. In this concept, mathematical models giving proofs about primitives' features can be built. Thus, it is possible to build proofs about the security of protocols. The primitives used in this thesis are shown here together with related proofs and definitions. The notation is also described here because it is used not only in chapters devoted to the novel scheme design but also during the analysis of most related systems.

The first construction, cryptographic commitments, is used in cases where a user needs to commit to a number without disclosing it. Two versions of commitments are shown here, the computationally hiding and perfectly binding commitments and the perfectly hiding and computationally binding commitments. Then, the Σ-protocols are introduced. They represent an efficient and practical variant of ZK protocols. The Σ-protocols for proofs of knowledge, representation and discrete logarithm equivalence are described in next sections because they are very frequently used in Chapter 4. Using above mentioned primitives, more complex constructions can be built. The Okamoto-Uchiyama Trapdoor One-Way Function and Bao's Verifiable Encryption are described as they are used in the design of the proposed scheme.

3.1 Used Cryptographic Primitives

Most cryptographic primitives described in this section exist in more variants. In this thesis, the variants working with modular arithmetics and groups where a discrete logarithm is hard to compute are used.

3.1.1 DL Commitments

To commit to a secret value $w < q$, where q is a large prime, we use a simple computationally hiding and perfectly binding commitment. Let $p : q|p-1$ be a large prime and g a generator of order q in $\mathbb{Z}_p^*$. Then, $c = g^w \bmod p$ is a simple commitment scheme secure under the DL assumption. After publishing c, the secret w is computationally hidden (hiding property) but the committer is perfectly bound to his w (binding property) and unable to change w without changing c.

3.1.2 Σ-protocols

Σ-protocols [22] can be used for proving the knowledge of secrets and for proving the construction correctness without leaking additional information. We use the protocols described in [30] to prove the knowledge of a discrete logarithm (the protocol $PK\{\alpha : c = g^\alpha\}$), discrete logarithm equivalence (the protocol $PK\{\alpha : c_1 = g_1^\alpha \wedge c_2 = g_2^\alpha\}$) and discrete logarithm representation with respect to public generators (the protocol $PK\{(\alpha, \beta, \gamma) : c = g_1^\alpha g_2^\beta g_3^\gamma\}$). These protocols can be translated to full zero-knowledge protocols [23] thus they can be proven to leak no more information than intended. They can run non-interactively with computational security using [32]. With some restrictions, the protocols can be used in groups with hidden order by sending answers in $\mathbb{Z}$ [31]. Various types of

Tab. 3.1: Overview of used cryptographic constructions.

Construction	**Group**	**Where Used**	**Notation**
DL Commitments	DSA	R	$c = commit(w)$
Proofs of Knowledge	DSA, OU	R	$PK\{w : c = g^w\}$
Proofs of Representation	DSA, OU	V	$PK\{w, w' : c = g_1^w g_2^{w'}\}$
Proofs of DL Equivalence	DSA, OU	R, V	$PK\{w : c_1 = g_1^w \wedge c_2 = g_2^w\}$
OU Trapdoor OWF	OU	R, Rev	$c = g^w \bmod n$
Verifiable Encryption	OU	V, Rev	$VE\{x : c = g^x\}$

Glossary:
OU: Okamoto Uchiyama [43]
DSA: Digital Signature Algorithm [39]
OWF: One-Way Function
R, V, Rev: Registration, Verification and Revocation protocol of the proposed scheme

proofs of knowledge and a framework for creating proofs can be found in [30].

3.1.3 Okamoto-Uchiyama Trapdoor One-Way Function

Let $n = r^2 s$ and r, s be large primes. Pick $g \in \mathbb{Z}_n$ such that $g \bmod r^2$ is a primitive element of $\mathbb{Z}^*_{r^2}$. Then $c = g^x \bmod n$ is a trapdoor one-way function with r as a trapdoor. Value x can be computed using the trapdoor as $x = \dfrac{((c^{r-1} \bmod r^2) - 1)/r}{((g^{r-1} \bmod r^2) - 1)/r} \bmod r$ [43]. The function is secure if the factorization of n is hard [43]. Size recommendations for n are the same as for RSA [44].

3.1.4 Bao's Verifiable Encryption

The above mentioned primitives are used in Bao's Verifiable Encryption (VE) scheme [18] for discrete logarithms. Using VE, a Prover is able to convince a Verifier about the correctness of given encryption of discrete logarithm of some public value. Although the Verifier cannot decrypt, he is convinced that some other entity, which is able to decrypt, will really get the correct discrete logarithm of the given public value after the decryption. The idea is to put the exponent as an input to the Okamoto-Uchiyama function and prove the discrete log equivalence between the original public value and the output of the OU function. After seeing such a proof, the Verifier is convinced without actually seeing the exponent. Later, a third person who knows the OU trapdoor can invert the function and get the exponent (decrypt).

The overview of used cryptographic constructions and their placement in the scheme proposed in Chapter 4 is in Table 3.1.

3.2 Notation

The notation common in cryptographic protocol design is used in this thesis. The same notation is used for both the related work description and the novel scheme design description.

A Discrete Logarithm (DL) commitment c to a value w is denoted as $c = commit(w)$. For various proofs of knowledge or representation, the efficient notation introduced by Camenisch and Stadler [30] is used. The first step of PK protocols is denoted as PK_{step1}. Bao's Verifiable Encryption of x inside $c = g^x \bmod n$ is denoted as $VE\{x : c = g^x\}$. A signature using some PKI by a user U on some data is denoted as $Sig_U(data)$. The symbol ":" means "such that", "|" means "divides", "$a||b$" is the concatenation of strings a and b, "$|x|$" is the bitlength of x and "$x \in_R \{0,1\}^l$" is a randomly chosen bitstring of maximum bitlength l. "$x \in_R \mathbb{Z}_q$" denotes a randomly chosen integer less than q. "$\mathbb{Z}_q^*$" denotes an integer multiplicative group modulo q.

4 NOVEL SCHEME FOR ATTRIBUTE AUTHENTICATION

The cryptographic design of a novel scheme for attribute authentication is provided in this chapter. The proposed attribute authentication scheme supports the basic functionality of anonymously proving the possession of attributes. Additionally, the scheme provides the privacy-enhancing features defined in the thesis objectives chapter. Namely, following features are provided.

- Security
- Anonymity
- Untraceability
- Selective disclosure of attributes
- Non-transferability
- *Practical, complex* revocation

It is shown in the Chapter 2 that it is very difficult to provide some of the above specified features. Especially, the *revocation* feature is very difficult to support. Even the most advanced schemes, like U-Prove and idemix, do not support both this feature. The goal of the new scheme proposal is to fix this problem and provide all features. Moreover, the scheme design is focused on providing more complex revocation so that service providers are more willing to use the newly designed system in practical scenarios. That is the reason why a scalable revocation mechanism is provided in the proposed scheme. For a practical system, it is also very important to be computationally efficient. Thus, the proposed scheme is designed to be as fast as possible on weak devices such as smart-cards.

The proposed scheme is built on cryptographic constructions defined in Chapter 3. The cryptographic commitments, proofs of knowledge (PK) and verifiable encryption (VE) are frequently used. All constructions are based on the discrete logarithm (DL) assumption. Two domains (multiplicative groups) are used. They are the DSA subgroup modulo prime p and the Okamoto-Uchiyama subgroup modulo prime product n. Although multiple subgroups are used, the reader might still use the description of cryptographic constructions in the Chapter 3 as a reference. The properties and mechanisms remain the same for all used settings (distinguished by different moduli). The cryptographic background is specified before the actual scheme is described.

Additionally to DSA subgroup, the Okamoto-Uchiyama group is used. The difference is mainly in the used modulus and in the fact that the group order is hidden in OU group. Therefore, the third message of Σ-protocols, the answer, must be sent as a non-reduced integer instead of the reduced answer in $\mathbb{Z}_q$ sent in the DSA version. The OU group, used in proofs of knowledge and verifiable encryptions, can be easily identified by used modulus n. The full scheme is based on following assumptions.

Assumptions

The Generalized Discrete Logarithm Problem (GDLP) assumption
Based on [36] it is assumed that given a finite cyclic group G[1] of order q, a generator g and an element $\beta \in G$ it is hard to find an integer $0 \leq x \leq q-1$ such that $g^x \equiv \beta$.

Factorization hardness assumption

[1] In our case, the DSA and OU group.

Based on [43] it is assumed that it is hard to factor $n = r^2 s$, where r, s are large safe primes.

The DSA subgroup, introduced in Chapter 3, is defined by public parameters h (generator), q (prime order) and p (prime modulus). The OU group is defined by public bases g_1, g_2, g_3 and product modulus n such that $n = r^2 s$, where primes r, s are secret. The commitments, proofs of knowledge, proofs of DL equivalence and verifiable encryptions are used in the full scheme. All primitives are defined in the Chapter 3 which can be used as a cryptographic reference. The difference between the DSA subgroup, from which all examples in Chapter 3 come, and groups with hidden order is mainly in sending the final answer in integers. The communication pattern remains, further information can be found in [31, 18].

4.1 Additional Contribution

In this chapter, an attribute authentication scheme with practical, efficient multi-level revocation is provided. From user's perspective, the scheme is extremely efficient, providing following features. These features are additional to the privacy-enhancing features defined in Chapter 2 and their purpose is to further enhance privacy and practicality of the scheme.

- **Practical Revocation**
  - **Immediate Revocation**: there is no need to wait for the token lifetime expiration, tokens can be revoked immediately.
  - **Issuer and Verifier Revocation**: revocation is available to both attribute issuers and verifiers. Any of these entities can initiate the revocation process.
  - **Verifier Local Revocation (VLR)**: valid users do not have to update their tokens or download any values after some other users are revoked.
  - **Practical Revocation**: computational complexity of the verification protocol does not depend on the number of revoked users.
- **Scalability**: computational complexity of the verification protocol does not depend on the number of all users.
- **Off-line Verification**: the verification session runs between the user and verifier only. There is no need to contact other parties.
- **Computationally Efficient Verification**: the verification protocol with a revocation check needs only 6 modular exponentiations, 6 multiplications and 4 additions. The complexity of the protocol does not depend on the number of undisclosed attributes[2].

The token revocation is an extremely important feature but in some cases it is not enough to just revoke users from the system. In cases where damage was done, the service providers need a mechanism for learning the identity of attackers to make them responsible. More granularity to revocation is added to the scheme by allowing the revocation of particular privacy enhancing features. The revocation of following features is supported.

[2]The protocol independence on undisclosed attributes seems obvious and easy to provide but is currently missing in leading related schemes.

- **Token Validity Revocation**: in most practical cases, like token expiration, loss or theft, the token can be revoked without identifying the owner.
- **Anonymity Revocation**: in critical policy breaches, it is possible to revoke the anonymity of a user to make him responsible for his acts.

It is acknowledged that these revocation features must be strongly protected against a misuse. That is the reason why the ability to do revocation is spread over more entities. In the system, the issuer, verifier and a third authority must cooperate to revoke any privacy enhancing feature. By such distribution, the probability of misusing the revocation by a single authority is limited. To provide more security (and user trust in the system), the third party can be distributed using multi-party computations. Moreover, the user should have the freedom to choose his own attribute issuer among many commercial subjects, therefore, he does not have to trust a fixed designated revocation authority but rather liberally choose an entity he trusts most.

4.2 General Overview

There are 4 types of players in the scheme. They are the User (U), Issuer (I), Verifier (V) and Public Authority (PA). Their roles are described in the following section.

- **User:** a player who wants to get verified using a smart-card with a token issued by I and PA.
- **Issuer:** a player who issues attributes to users and collaborates during revocation. There are more Issuers, the Issuer can be chosen by the User depending on his preferences and trust.
- **Verifier:** a player who verifies Users' attributes and collaborates during revocation.
- **Public Authority:** a (distributed) entity that issues tokens to Users and collaborates during revocation.

The scheme is based on the interaction among these four entities. The User owns a smart-card with a token construction created using information from both PA and Issuer. The token can be used for attribute authentication, since the Verifier is able to check token's validity. This is done without the revelation of User's real identity. But when the User breaks some rules of the Verifier, e.g. destroys some data, the Verifier can ask the Issuer and Public Authority to "open" the token and reveal the identity of the User. The User is then held responsible for his past behavior. There are more levels of User revocation (from token revocation to anonymity revocation) and PA is trusted not to revoke tokens in unjustified cases.

The scheme provides security features which prevent entities from misusing their powers. V alone, I alone or PA alone cannot track or identify a User at all. PA cannot falsely accuse a particular User, but has to be trusted not to misuse its data for accusing random Users during revocation. To lower such trust, distributed PA can be introduced. Only the joint cooperation of V, I and PA can do the revocation, by sharing their inputs.

The scheme consists of 4 protocols - setup, registration (attribute issuance), verification and optional revocation. User's goal of the registration is to get data from I and PA necessary to construct the token. The token is then used during the Verification phase to prove User's membership, attribute

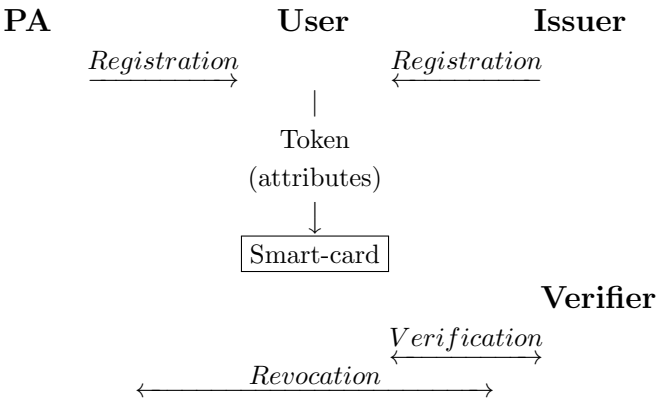

Fig. 4.1: Communication pattern of proposed scheme.

ownership or any other authorization given by I's organization. In case of disputes, loss of a smart-card or system policy breaches, the revocation phase can be introduced. Based on the level of dispute, the User can be removed, traced or identified. The revocation is possible only if I, V and PA cooperate, assuming PA cooperates only in cases where sufficient policy violation logs are given by V's organization. The communication pattern is depicted in Figure 4.1.

4.3 Cryptographic Design

The scheme consists of four protocols: Setup, Registration Protocol, Verification Protocol and Revocation Protocol.

Setup

The goal of the setup phase is to generate all necessary initial parameters. It is assumed that a public key infrastructure and valid keypairs for the User and Issuer exist. They will be used during registration. The security parameters are k, l, m (k is the length of the challenge/hash function used, l relates to the length of Users' secrets, and m is the verification error parameter). The Issuer generates the DSA subgroup G defined by a large prime modulus p, generator h of prime order $q : |q| = l$ and $q|p-1$. The Public Authority generates groups G_1, G_3 for the Okamoto-Uchiyama Trapdoor One-Way Function. G_1, G_3 are defined by the modulus $n = r^2 s$ with r, s large primes ($|r| \geq 350, |r| > 2l, |n| \geq 1024$), generators $g_1, g_3 \in_R \mathbb{Z}_n$ of order $ord(g_1 \bmod r^2) = ord(g_3 \bmod r^2) = r(r-1)$ in $\mathbb{Z}^*_{r^2}$ and $ord(g_1) = ord(g_3) = rr's'$ in $\mathbb{Z}^*_n$. PA also randomly chooses its secrets $S_1, S_2 : |S_1| = l, |S_2^{-1} \bmod \phi(n)| = l$ and $\mathrm{GCD}(S_2, \phi(n)) = 1$. Finally, PA computes a token $A = g_1^{S_1} \bmod n$ (public, common for all Users) and a value $g_2 = g_1^{S_2} \bmod n$. There might be more types of tokens (different A_i's) related to different attributes Users want to prove. In that case, each unique A_i represents one attribute, e.g. nationality, driving permission or legal voting age.[3] These attributes can be aggregated together by multiplying mod$n$. In the rest of the paper, only one A representing a general group membership is considered for simplicity.

[3] A represents a unique attribute. A public list of available attributes and their assigned values of A should be maintained by PA.

The values $q, p, h, n, g_1, g_2, g_3, A$ are made public, while $r, s,\ S_1, S_2$ are securely stored at PA or secretly shared in PA's distributed environment.

Registration Protocol

We assume a secure, authenticated (non-anonymous) channel between the User and the Issuer during the registration phase. The User randomly chooses a secret value w shorter than l bits, makes a signed commitment c_I to it and proves the knowledge of $\log_h c_I$ to the Issuer. The User binds his identity to the commitment by the signature. The Issuer might require additional actions like payments, proofs of authorization by another entity or, for example, proofs of some (e.g. driving) license possession. When the Issuer does all the checks and allows the User to get the attribute, the User gets his commitment back, signed by the Issuer. After this step, all communication of the User is anonymous if he adheres to the rules.

In the second step, the user must get information necessary to construct the private key (w, w'). These values form the discrete logarithm representation of A with respect to generators (g_1, g_2) so that $A = g_1^w g_2^{w'} \bmod n$ holds. The values (w, w') cannot be computed by the User because he does not know S_1 and the factorization of n. But it cannot be provided by PA either since these keys must be known by the User only. Therefore, the key is computed jointly so that PA does not learn (w, w') but U does[4]. The User's smart-card computes a credential seed $A' = g_1^w g_2^{w'_U} \bmod n$ where $w'_U \in_R \{0,1\}^l$ is User's random contribution to the key. User sends A', c_I and I's signature to PA and proves that the key part w is present in both A' and c_I. This can be proven in zero-knowledge using $PK\{w : c_I = h^w \bmod p \wedge A' = g_1^w g_2^{w'_U} \bmod n\}$. PA verifies the proof, check if c_I is not used by any other user and answers with his key contribution w'_{PA}. The w'_{PA} is computed as $w'_{PA} = \dfrac{(((A * A'^{-1}) \bmod n)^{r-1} \bmod r^2 - 1)/r}{(g_2^{r-1} \bmod r^2 - 1)/r} \bmod r$ so that $A = g_1^w g_2^{w'_U} g_2^{w'_{PA}} \bmod n$ holds. The User's smart-card sets $w' = w'_U + w'_{PA}$ and stores the credential $(A, (w, w'))$.

By using the described registration protocol, all Users share the same A for a particular attribute but use different keys. Users are stuck to their keys, because without $S_1, S_2, \phi(n)$ they are unable to compute different valid keys. The registration protocol is depicted in Figure 4.2.

Verification Protocol

The verification protocol runs over an anonymous channel (using either anonymous routing or smart-cards). The User proves the knowledge of representation of A using (w, w'). By doing so, he remains completely anonymous, since the proof of representation can be a Zero-Knowledge protocol. To get the ability to revoke invalid Users, a subprotocol must be added. User cannot give a commitment to his w, since this would make his sessions linkable. Therefore, he creates a verifiable encryption of the randomness used in the first step of the proof of representation protocol (denoted as PK_{step1}). Such encryption will be always different, thus untraceable. Nevertheless, if decrypted by PA, it can be used to trace a User or even to identify him. The User has to prove that the randomness in VE is the same as the one used in the proof of representation. PA is not involved during the verification at all, therefore the verification, including the revocation check, can run off-line. The protocol is

[4]Due to security reasons, (w, w') are never accessible to users directly but are stored in smart-card's protected memory. Keys are never extracted, all operations involving them are done on the smart-card.

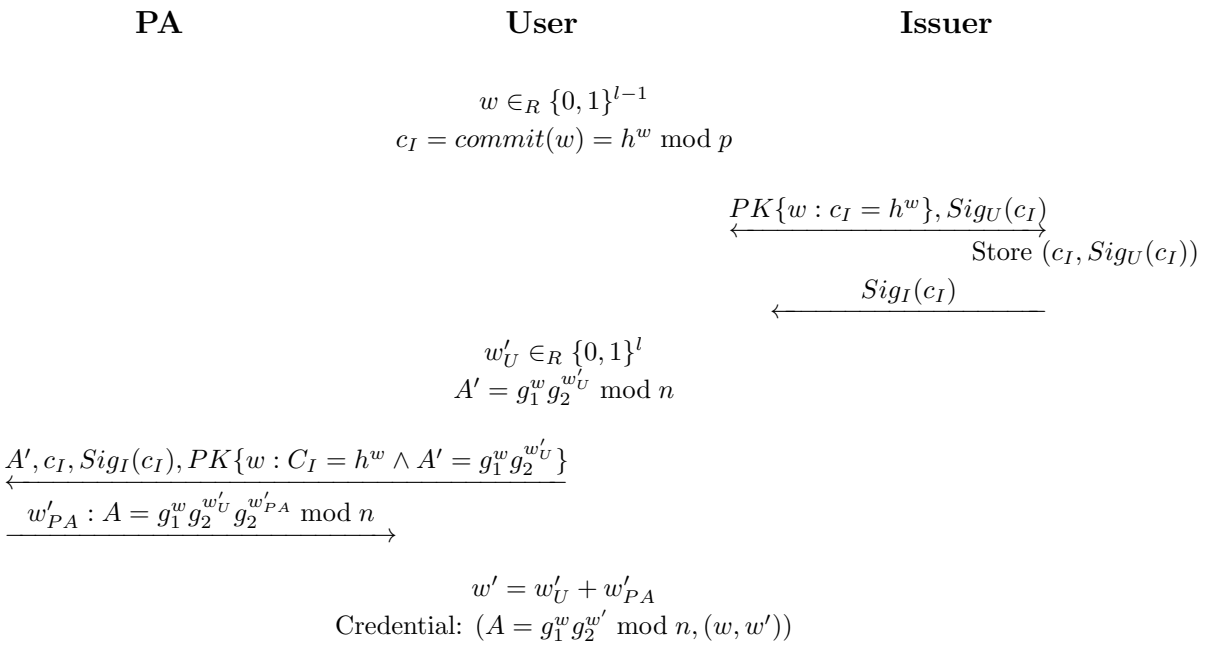

Fig. 4.2: Registration Protocol

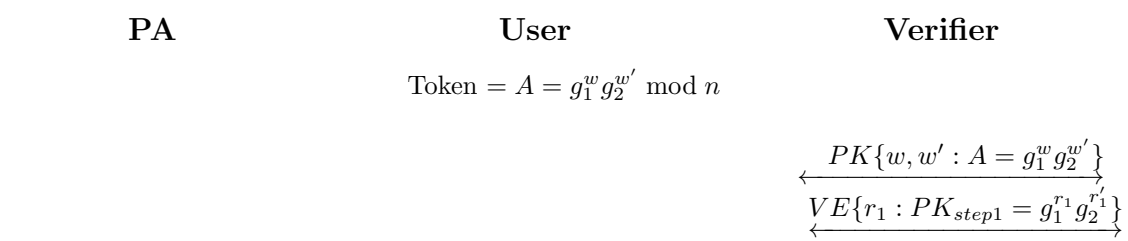

Fig. 4.3: Simplified verification.

depicted in Figure 4.3. A detailed description of the verification protocol with all the checks needed to support revocation is given in Figure 4.4.

Revocation Protocol

The revocation protocol is the fundamental part of the system, assuming a good balance between anonymity and accountability is required. Practical credential schemes [29, 37] do not implement scalable revocation and theoretical proposals [26] are not efficient enough to be implementable. In the proposed scheme, there is no way of identifying or tracing a User unless more entities cooperate. The verification protocol transcript must be given to (distributed) PA entity with an evidence of a breach of a policy. PA can then decide what type of revocation will be applied: revocation or identity revelation. Revocation can be done by PA, but in the case of identity revelation, the real identity is readable only to the Issuer (previously chosen by the User), so no unnecessary data about Users ever leak, even if Users break Verifier's policies.

Revocation (Token Revocation): PA, using its secret factorization of n, can decrypt the ran-

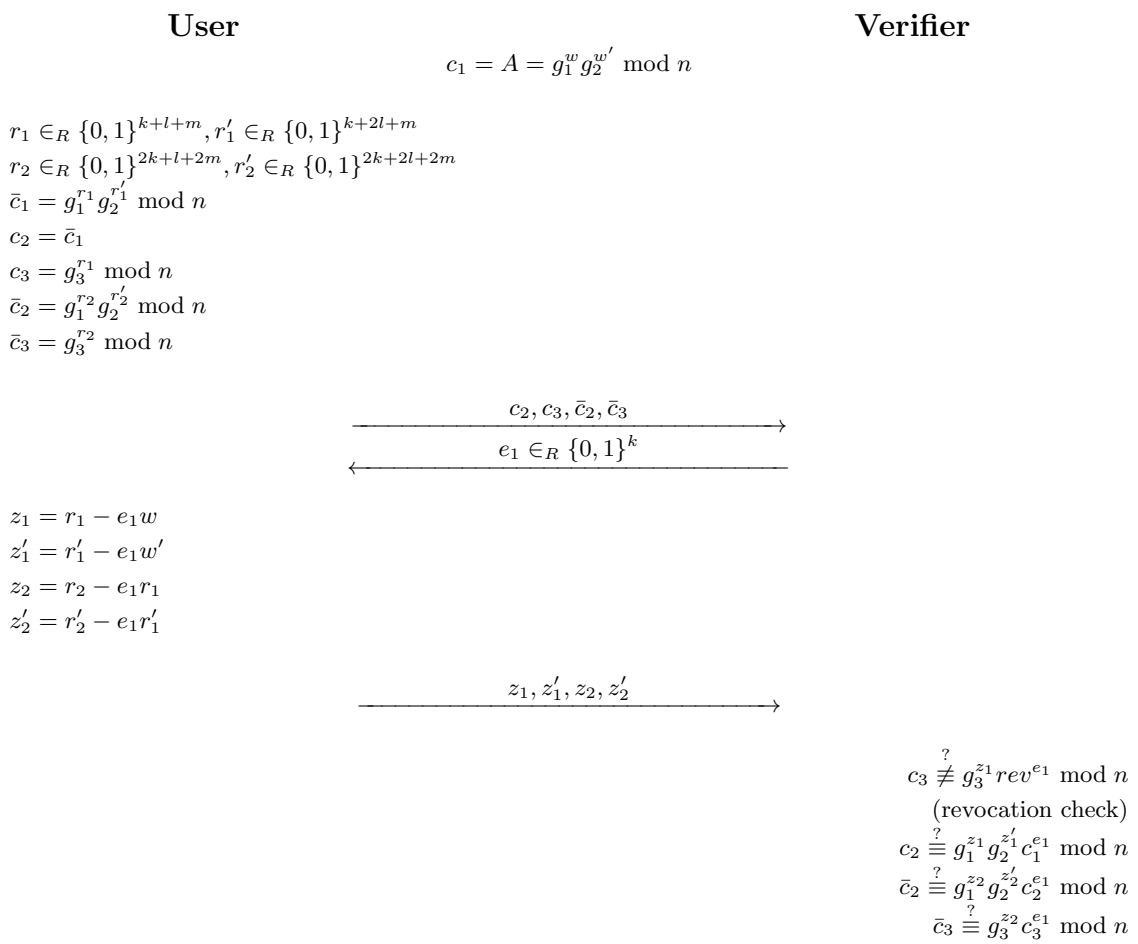

Fig. 4.4: Verification protocol (optimized).

domness inside VE[5], thus it can get User's unique w[6] (but not the real identity!). To prevent identity revelation, PA can release a commitment to w in the form of $rev = g_3^w \bmod n$. Using rev, the Verifier can always check whether the User has been revoked or not without de-anonymizing the User. The revocation check is described in Figure 4.4.

Identity Revelation (Anonymity Revocation): in the worst cases of rule breaking, PA can reveal w to the Issuer, who can compute an adequate commitment $c_I = h^w \bmod p$ and charge the User who signed that commitment during the registration.

The above described Revocation Protocol provides full anonymity to honest users. Malicious users, whose communication is submitted to one of three types of revocation, can be revealed, because their secret keys can be disclosed by PA. In our design, PA is trusted not to disclose User's secrets if insufficient policy violation proofs are submitted. It is the next goal of following research to design a scheme were such a trust in PA is removed. In the time of writing this thesis, a solution based on disclosing commitments of keys is being developed.

[5]With respect to Figure 4.4, randomness is obtained as $r_1 = \dfrac{(c_3^{r-1} \bmod r^2 - 1)/r}{(g_3^{r-1} \bmod r^2 - 1)/r} \bmod r$

[6]With respect to Figure 4.4, User's secret can be obtained as $w = ((r_1 - z_1)e_1^{-1}) \bmod r$

In this chapter, the novel scheme for anonymous attribute authentication was presented. Using the scheme, a User can anonymously convince a Verifier about the possession of an attribute, typically about the authorization to use services. By staying anonymous and having the control over all released data, the users can protect their privacy during the verification process. The full scheme supports all required features, so far supported only individually, in one practical solution, which is even easily implementable on smart-cards. Additionally to being computationally efficient, the scheme can be proven secure[7], since it is based on strong cryptographic primitives, mostly proofs of knowledge or representation, Okamoto-Uchiyama OWF and DL commitments.

Additionally, features unavailable before are included, mainly scalable and implementable revocation with malicious user identity revelation. These new features make the scheme acceptable by service providers, without whose support any scheme is without a chance for being widely accepted.

[7]Security depends also on underlying tools, like the anonymous routing protocol (TOR) and the smart-card.

5 CONCLUSION

The main objective of this thesis is to bring more privacy and digital identity protection to user authentication. This intention is motivated by the increasing number of new types of services and technologies which bring new threats to our privacy and digital identity. Technologies like electronic IDs, cloud services or ubiquitous smart-cards intensively work with our personal data although we cannot be sure if the protection is adequately high. Thus, a novel cryptographic scheme assuring personal data protection is proposed in this thesis. The scheme directly reacts on official U.S. and EU requests [42, 40] for new authentication services with the support of user-centric, attribute-based approach to authentication. Besides privacy-enhancing features, the proposed scheme provides also higher security because it is built on strong cryptographic constructions with provable features.

The proposed scheme is based on a new concept called attribute authentication. In this concept, a user can give proofs not only about his identity but also about the possession of attributes. The attributes represent any personal data, e.g. age, citizenship or nationality. With the increasing number of services, where identity disclosure is not necessary but the verification of some attribute is required, the user can anonymously prove that he is a justified holder of that attribute. By using attribute authentication, honest users can give proofs about their age, nationality or any authorization while staying completely anonymous. To protect assets of verifiers, the scheme allows the de-anonymization of malicious users so that they can be held responsible for their behavior. By allowing attribute authentication, the users can precisely manage what personal data are being released and are assured that the verifier is unable to identify, trace and profile their behavior.

An extensive analysis of current state in the field of cryptographic privacy protection is provided in this thesis. Due to missing support of privacy protection in classical protocols like RADIUS, EAP or Diameter, more advanced cryptosystems have been analyzed. The most promising technologies, U-Prove and idemix, were examined. Major weaknesses were found in these systems, namely missing revocation feature.

Due to the absence of these important features, a new scheme supporting all privacy-enhancing features including advanced revocation was designed. Particularly, it is the revocation feature, which virtually prevented existing systems from being commercially enrolled. Revocation was the main topic of many research papers from the last decade but it has been still unresolved, especially on low-performance, off-line devices. Without revocation, it is impossible to revoke invalid, expired, lost or stolen authentication tokens. The scheme presented in this thesis is the first solution which is both providing practical revocation and highly practical on devices like smart-cards. With the proposed scheme, it is now possible to significantly enhance the privacy of users of electronic services. The solution is the first one which provides strong authentication with privacy protection together with the protection of service providers. Moreover, the scheme is practical on devices like off-line smart-cards which allows the application to electronic IDs.

An extensive verification of the proposed scheme is presented in the full version of the thesis. Both theoretical and practical verification is included. Three key properties, soundness, completeness and anonymity of verification phase, are formally proven. The scheme is verified on a mathematical model using Mathematica software. An experimental smart-card implementation of the verification phase is provided. The time of verification is around 30% faster than in related existing implementations. The results have been published at international conferences, awarded prizes (Keymaker

2011, Brno Ph.D. Talent, Fulbright Stipend) and presented at key institutions (University of Minnesota, National Institute of Standards and Technology (NIST), USA, Goethe-University Frankfurt (ABC4Trust Project Leader), DE).

Although the proposed scheme is fully functional, there is a potential for future development. The full implementation has been currently started as a TACR project with a commercial partner. Also, there are several aspects of the scheme which can be cryptographically improved. These aspects are being investigated by the author and foreign partners. The goal is improving the verification and revocation procedure so that user keys are not fully learnt by PA, more attributes are proven more quickly and the trust in key entities like PA is even more lowered. All these three improvements are the core subjects of follow-up research.

BIBLIOGRAPHY

Author's selected publications

[1] Hajný, J. Úvod do zero- knowledge protokolů. *Crypto-World*. 2008, vol. 10, pp. 7–13. ISSN 1801-2140.

[2] Hajný, J. Anonymita v globální síti. *Crypto-World*. 2009, vol. 11, pp. 7–11. ISSN 1801-2140.

[3] Hajný, J. Flexible authentication framework. In *Proceedings of the 15th conference Student EEICT 2009* EEICT, 2009. pp. 468–472. ISBN 978-80-214-3870-5.

[4] Hajný, J. Anonymous authentication for smartcards. *Radioengineering*. 2010, vol. 19, pp. 363–368. ISSN 1210-2512.

[5] Hajný, J.; Malina, L. Implementation results of anonymous authentications scheme. *Elektrorevue*. 2010, vol. 2010, pp. 1–8. ISSN 1213-1539.

[6] Hajný, J.; Martinásek, Z. Kryptografický systém pro ochranu identity. In *Proceedings of the MKB 2011* 2011. pp. 67–68. ISBN 978-80-904257-3- 6.

[7] Hajný, J.; Malina, L. Secure authentication for smart-cards. In *Proceedings of the 17th conference Student EEICT 2011* EEICT, 2011. pp. 1–5. ISBN 978-80-214-4273- 3.

[8] Hajný, J.; Malina, L.; Pelka, T. Zero- knowledge for anonymous authentication. In *Proceedings of the 33rd International Conference on Telecommunication and Signal Processing* TSP, 2010. pp. 1–6. ISBN 978-963-88981-0-4.

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

[10] Hajný, J.; Pelka, T. Univerzální autentizační rámec. *Sdělovací technika*. 2009, vol. 2009, pp. 3–6. ISSN 0036-9942.

[11] Hajný, J.; Pelka, T. Univerzální autentizační rámec. *Elektrorevue*. 2009, vol. 2009, pp. 1–6. ISSN 1213-1539.

[12] Hajný, J.; Pelka, T.; Lambertová, P. Flexible authentication framework. In *Proceedings of the IEEE Xplore. Network and Service Security* IEEE Xplore, 2009. pp. 1–5. ISBN 978-2-9532-4431-1.

[13] Hajný, J.; Pelka, T.; Lambertová, P. Universal authentication framework: Requirements and phase design. In *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2009)* ICETE, 2009. pp. 57–60. ISBN 978-989-674-005-4.

[14] Hajný, J.; Pelka, T.; Zeman, V. Privacy protection for user authentication. In *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2010)* ICETE, 2010. pp. 90–93. ISBN 978-989-8425-18-8.

[15] Hajný, J.; Zeman, V. Anonymous authentication with spread revelation. *Cryptologia*. June 2011, vol. 35, pp. 235–246. ISSN 0161-1194.

[16] Malina, L.; Hajný, J. Secure authentication in privacy protection systems. In *Proceedings of the 16th conference Student EEICT 2010* EEICT, 2010. pp. 1–3. ISBN 978-80-214-4079-1.

[17] Malina, L.; Hajný, J. Accelerated modular arithmetic for low- performance devices. In *Proceedings of the 34th International Conference on Telecommunication and Signal Processing* TSP, 2011. pp. 1–5. ISBN 978-1-4577-1409-2.

Other's publications

[18] Bao, F. An efficient verifiable encryption scheme for encryption of discrete logarithms. In *Proceedings of the The International Conference on Smart Card Research and Applications*. London, UK, UK: Springer-Verlag, 2000. CARDIS '98, pp. 213–220. ISBN 3-540-67923-5.

[19] Brands, S. A. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge, MA, USA: MIT Press, 2000. ISBN 0262024918.

[20] Brands, S.; Demuynck, L.; De Decker, B. A practical system for globally revoking the unlinkable pseudonyms of unknown users. In *Proceedings of the 12th Australasian conference on Information security and privacy*. Berlin, Heidelberg: Springer-Verlag, 2007. ACISP'07, pp. 400–415. ISBN 978-3-540-73457-4.

[21] Bichsel, P. et al. Anonymous credentials on a standard java card. In *Proceedings of the 16th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2009. CCS '09, pp. 600–610. ISBN 978-1-60558-894-0.

[22] Cramer, R. *Modular Design of Secure, yet Practical Cryptographic Protocols*, PhD thesis University of Amsterdam, 1996.

[23] Cramer, R.; Damgård, I.; MacKenzie, P. D. Efficient zero-knowledge proofs of knowledge without intractability assumptions. In *Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography*. London, UK, UK: Springer-Verlag, 2000. PKC '00, pp. 354–372. ISBN 3-540-66967-1.

[24] Camenisch, J.; Gross, T.; Heydt-Benjamin, T. S. Rethinking accountable privacy supporting services: extended abstract. In *Proceedings of the 4th ACM workshop on Digital identity management*. New York, NY, USA: ACM, 2008. DIM '08, pp. 1–8. ISBN 978-1-60558-294-8.

[25] Camenisch, J.; Kohlweiss, M.; Soriente, C. An accumulator based on bilinear maps and efficient revocation for anonymous credentials. In *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography: PKC '09*. Berlin, Heidelberg: Springer-Verlag, 2009. Irvine, pp. 481–500. ISBN 978-3-642-00467-4.

[26] Camenisch, J.; Lysyanskaya, A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*. London, UK: Springer-Verlag, 2001. EUROCRYPT '01, pp. 93–118. ISBN 3-540-42070-3.

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

[28] Camenisch, J.; Lysyanskaya, A. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*. London, UK, UK: Springer-Verlag, 2002. CRYPTO '02, pp. 61–76. ISBN 3-540-44050-X.

[29] Camenisch, J.; et Al. *Specification of the Identity Mixer Cryptographic Library* IBM Research - Zurich, 2012. Technical report.

[30] Camenisch, J.; Stadler, M. *Proof Systems for General Statements about Discrete Logarithms* IBM, 1997. Technical report.

[31] Damgård, I.; Fujisaki, E. A statistically-hiding integer commitment scheme based on groups with hidden order. In *Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*. London, UK: Springer-Verlag, 2002. ASIACRYPT '02, pp. 125–142. ISBN 3-540-00171-9.

[32] Fiat, A.; Shamir, A. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology - CRYPTO 86*. Editor Andrew Odlyzko Springer Berlin / Heidelberg, 1987. Lecture Notes in Computer Science; vol. 263, pp. 186–194. ISBN 0-387-18047-8.

[33] Camenisch, J.; Van Herreweghen, E. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2002. CCS '02, pp. 21–30. ISBN 1-58113-612-9.

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

[35] Lapon, J. et al. Performance analysis of accumulator-based revocation mechanisms. In *Security and Privacy – Silver Linings in the Cloud*. Editors Kai Rannenberg, Vijay Varadharajan a Christian Weber Springer Boston, 2010. IFIP Advances in Information and Communication Technology; vol. 330, pp. 289–301. ISBN 978-3-642-15256-6.

[36] Menezes, A. J. et al. *Handbook of Applied Cryptography*. CRC Press, 1997. ISBN 978-0849385230.

[37] Paquin, C. *U-Prove Cryptographic Specification V1.1* Microsoft Corporation, 2011. Technical report.

[38] Nguyen, L. Accumulators from bilinear pairings and applications. In *Topics in Cryptology CT-RSA 2005*. Editor Alfred Menezes Springer Berlin / Heidelberg, 2005. Lecture Notes in Computer Science; vol. 3376, pp. 275–292. ISBN 978-3-540-24399-1.

[39] 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. pp. 1 online resource (ix, 119 p.) :.

[40] Naumann, I.; Hogben, G. Privacy features of eid cards. *Network Security Newsletter*. 2008, vol. 2008, pp. 9–13. ISSN 1353-4858.

[41] Nguyen, L.; Safavi-Naini, R. Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings. In *ASIACRYPT'04, LNCS 3329* Springer-Verlag, 2004. pp. 372–386. ISBN 3-540-23975-8.

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

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

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

[45] Schaffer, M.; Schartner, P. Anonymous authentication with optional shared anonymity revocation and linkability. In *Proceedings of the 7th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications.* Berlin, Heidelberg: Springer-Verlag, 2006. CARDIS'06, pp. 206–221. ISBN 3-540-33311-8, 978-3-540-33311-1.

[46] Teranishi, I.; Furukawa, J.; Sako, K. k-times anonymous authentication (extended abstract). In *ASIACRYPT, VOLUME 3329 OF LNCS* Springer, 2004. pp. 308–322. ISBN 3-540-23975-8.

CURRICULUM VITAE

Jan Hajný

Affiliation	Brno University of Technology, Brno, CZ
	International Association for Cryptologic Research (IACR)
Contact	+420608823522, hajny@feec.vutbr.cz

EDUCATION

2008 - 2012	Doctoral program at Brno University of Technology, CZ
	Faculty of Electrical Engineering and Communication
	Research topic: "Authentication protocols and privacy protection"
2010 - 2011	Department of Mathematics, Department 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"
	Grade average for whole program (1 - excellent 4 - failed): 1.08
2003 - 2006	Bachelor's program at Brno University of Technology, CZ
	Bachelor's thesis "Methods for LAN protecting"
	Grade average for whole program (1 - excellent 4 - failed): 1.37

WORK EXPERIENCE

2008 - Present	Computer and communication security lab instructor
2006 - 2007	Network security consultant

LANGUAGE SKILLS

Czech language	Native
English language	Fluent, certified
German language	Intermediate

CERTIFICATIONS

General	Graduate Record Examination GRE General Test (780/800 in QR)
Language	University of Cambridge, Certificate of Advanced English - C1 Level
	ETS TOEFL (Test of English as a Foreign Language) iBT, score 108/120

PRIZES AND HONORS

2011	1. Prize in Keymaker cryptography competition in Ph.D. section
2010	Fulbright stipend for internship at University of Minnesota, USA
2010	Brno Ph.D. Talent prize
2010	AVG prize for security projects
2009	EEICT 2009 - first prize in Ph.D. section "Information Systems"
2008	Master degree with honors
2006	Bachelor degree with honors

SELECTED PROJECTS

2012 - 2014	TA02011260: Cryptographic system for the protection of electronic identity
2012 - 2014	FR-TI3/170: Integration server with cryptographic protection
2009 - 2012	JCMM Brno Ph.D. Talent: Cryptographic identity protection
2012	FRVŠ 823/2012: Innovation of cryptography and computer security courses
2010	FRVŠ 2833/2010: Inclusion of application firewalls to security courses
2010	FEKT-J-10-5: Authentication and authorization in modern computer networks
2008 - 2011	2C08002: Universal and complex authentication and authorization
	for computer networks

SELECTED INVITED PRESENTATIONS

2012	Authentication and privacy protection at SmartCard Forum
2011	Privacy Protection by Attribute Authentication at NIST
2011	Cryptographic System for Identity Protection at MKB 2011

PUBLICATIONS IN NUMBERS

Impacted journals	3 publications
Journals	6 publications
Int. conferences	7 publications
Czech conferences	7 publications
Total	23 publications

SUPERVISED COURSE LABS

2008, 2009, 2011	Information systems security
2009, 2010	Design, administration and security of computer networks

ABSTRACT

This dissertation thesis deals with the cryptographic constructions for user authentication. Rather than classical authentication protocols which allow only the identity verification, the attribute authentication systems are the main topic of this thesis. The attribute authentication systems allow users to give proofs about the possession of personal attributes. These attributes can represent any personal information, for example age, nationality or birthplace. The attribute ownership can be proven anonymously and with the support of many features for digital identity protection. These features include, e.g., untraceability, selective disclosure of attributes or efficient revocation. Currently, the attribute authentication systems are considered to be the successors of existing authentication systems by the official strategies of USA (NSTIC) and EU (ENISA). The necessary features are partially provided by existing cryptographic concepts like U-Prove and idemix. But at this moment, there is no system providing all privacy-enhancing features which is implementable on computationally restricted devices like smart-cards. Among all weaknesses of existing systems, the absence of practical revocation is the most critical one. Without this features, it is currently impossible to invalidate expired users, lost or stolen authentication cards and cards of malicious users. Therefore, a new cryptographic scheme is proposed in this thesis to fix the weaknesses of existing schemes. The resulting scheme, which is based on established primitives like Σ-protocols for proofs of knowledge, cryptographic commitments and verifiable encryption, supports all privacy-enhancing features. At the same time, the scheme is easily implementable on smart-cards. This thesis includes the full cryptographic specification, the formal verification of key properties, the mathematical model for functional verification in Mathematica software and the experimental implementation on .NET smart-cards. Although the scheme supports all privacy-enhancing features which are missing in related work, the computational complexity is the same or lower, thus the time of verification is shorter than in existing systems. With all these features and properties, the resulting scheme can significantly improve the privacy of users during their verification, especially when used in electronic ID systems, access systems or Internet services.