prisma cloud

Report on Privacy-Enhancing Cryptography

Deliverable D4.8

Editor Name	Thomas Groß (UNEW)
Type	Report
Dissem. Level	CO
Release Date	July 29, 2017
Version	1.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644962.

More information available at https://prismacloud.eu.

Copyright Statement

Executive Summary

PRISMACLOUD aims at bringing novel cryptographic concepts and methods to practical application to improve the security and privacy of cloud based services and make them usable for providers and users.

The purpose of this report is to document the progress on research activities within the **Task 4.3 Privacy enhancing cryptography** in the second period (i.e., up to M30) of the PRISMACLOUD project. We thereby focus on privacy-preservation for users of cloud services as well as service providers. In particular, we will improve and propose privacy-enhancing cryptography such as signature schemes for constructing anonymous credentials as well as group signature schemes for the cloud environment with a focus on user's access privacy in authentication and authorization, private billing for the use of cloud services as well as privacy for cloud providers enabling them to selectively prove properties about their certified infrastructure without disclosing the blueprint of their infrastructure.

To this end, this task conducts research in the following fields.

4.3.1 Privacy-Preserving Cryptography for the Cloud. In this task, we investigate privacy-preserving cryptographic protocols and in particular anonymous credential systems and group signature schemes. Most such privacy preserving schemes as (updatable/stateful) anonymous one-show/multi-show credentials, or group signatures are obtained by means of (generic) transformations from signature schemes enjoying specific properties (such as blind/partially blind signing support, support for signing commitments, randomizability and compatibility with efficient zero-knowledge proofs). We will on the one hand perform research in anonymous credential systems that do not follow the traditional proof-of-knowledge paradigm, but are based on alternative constructions (such as ideas from malleable signatures), which make them conceptually simpler as well as to integrate additional features such as a state and updateability. Furthermore, we will investigate these approaches focusing on identifying difficulties and trade-offs that have to be made when targeting for implementations in resource constrained hardware. In this deliverable we present three publications related to this task.

4.3.2 Certified and Verifiable Infrastructure for Cloud Services. In this task we develop a signature scheme on committed graphs with a zero-knowledge proof system and optimize it for practical use in virtualized infrastructures. Such a scheme allows an auditor to analyze the configuration of a cloud, and issue a signature on its topology. The signature encodes the topology as a graph in a special way, such that the cloud provider can use it to prove in zero-knowledge high-level security properties such as isolation of tenants to verifiers, such as the tenants, without disclosure of secret information. By that the verifying tenant can be confident that the infrastructure is configured securely as promised by the provider and be assured at the same time that no information about his resource pool is leaked to other tenants. In this deliverable, we present research to establish hardware-protected minimal functional units that can then be certified as trustworthy vertices in the

topology certification.

Table of Contents

Document information

Project Context

Work Package	WP4 Advancement of enabling cryptographic primitives, protocols and schemes
Task	T4.3 Privacy enhancing cryptography
Dependencies	D4.6, D4.7, D5.6, D5.7, D5.9, D6.4, D6.5, D.6.6

Author List

Organization	Name	E-mail
UNEW	Thomas Groß	thomas.gross@newcastle.ac.uk
TU Graz	Daniel Slamanig	daniel.slamanig@tugraz.at
UNEW	Ioannis Sfyrakis	ioannis.sfyrakis@newcastle.ac.uk
TU Graz	David Derler	david.derler@iaik.tugraz.at

Reviewer List

Organization	Name	E-mail
AIT	Christoph Striecks	christoph.striecks@ait.ac.at
UNI PASSAU	Henrich Poehls	hp@sec.uni-passau.de

Version History

Version	Date	Reason/Change	Editor
0.1	2017-05-31	1st Draft	Daniel Slamanig
0.2	2017-06-01	Input TU Graz	Daniel Slamanig
0.3	2017-07-13	Input UNEW	Ioannis Sfyrakis
0.4	2017-07-20	Update contribution	Ioannis Sfyrakis
0.5	2017-07-22	Final version for internal review	David Derler
1	2017-07-28	Incorporate reviewer comments	David Derler

1 Introduction

1.1 Scope of this Document

The objective of this task is to conduct research in privacy-enhancing cryptographic schemes for application in privacy-preserving authorisation, privacy preserving (aggregated) billing for the privacy protected service usage in the cloud and for structural integrity and certification of virtualised infrastructures. To this end, Task 4.3 conducts research on the following tasks:

Task 4.3.1 Privacy-Preserving Cryptography for the Cloud

Task 4.3.2 Certified and Verifiable Infrastructure for Cloud Service

In the following sections we describe the research goals of the respective subtasks.

1.1.1 Privacy-Preserving Cryptography for the Cloud

For many services in the cloud, it is important that users are given means to prove that they are authorised to perform or delegate a certain task. However, it is usually not necessary that users reveal their full identity to the cloud, but only to prove by some means that they are authorised, e.g., possess certain rights. Traditional access mechanisms thereby typically reveal the user's identity and additional information (e.g., certain attributes about the user). When using a privacy-friendly means to authentication, i.e., minimising the data disclosed to the service or even anonymous authentication, the the main obstacle is that a cloud provider must still be cryptographically reassured that the user is authorised.

Anonymous credential (AC) systems have proved to be an important and versatile concept for such privacy-preserving and data minimising applications, as they allow users to authenticate in an anonymous way without revealing any more information than necessary to be authenticated at a service. The underlying cryptographic building blocks of state-of-the-art anonymous credential systems moreover can be used in the design of various related concepts such as group signatures, privacy protecting multi-coupon systems, anonymous subscriptions, e-cash systems and many more.

While the design of anonymous credential systems in their early days has been quite ad-hoc, many more recent works in the field propose a quite generic composition of a few building blocks with specific properties. Recently, also some results on instantiating various types of anonymous credentials (typically with some restrictions) from so called malleable signature schemes have been proposed (e.g., [BCKL08a, CKLM13]). Some of these tools are very interesting, but often they lack in efficiency.

We improve the state-of-the-art in anonymous credential system and group signature schemes with a particular focus on their application in cloud computing services.

1.1.2 Certified and Verifiable Infrastructure for Cloud Service

For services in the cloud, it is imperative that users can gain assurance that the cloud is configured securely and fulfils their security requirements. The user may, for instance, require that their resources are well isolated from all other tenants, that their resources fulfil deployment requirements, or that dependencies of their services are covered. These security requirements on confidentiality, integrity and availability are in tension with the cloud provider's and other tenants requirements on the confidentiality of the overall system. Hence, there are requirements on the verification of clouds as well as on their confidentiality-preserving security assurance.

Both aspects are with respect to a system-of-systems model of the infrastructure and a graph representation to abstract away the low-level details of the cloud configuration, that is, of hypervisors and management hosts. While there has been a body of research on modelling clouds in graph representations as well as dedicated information flow analysis or model checking on them, recent verification approaches investigated in PRISMACLOUD focus on dynamically changing clouds and graph model checking as tool of choice for the analysis.

For the certification and security assurance towards a verifier, we base our research on a legacy of anonymous credential (AC) systems. Whereas traditional anonymous credential systems focus on the certification and proof of knowledge of integers and bit strings as message space, the research in PRISMACLOUD focuses on certification and proof of knowledge of entire graphs. Hence, this thrust of research establishes graph signatures as a new cryptographic primitive and enables versatile and efficient signing for applications in the cloud.

We aim at creating a new graph signature scheme with a wide range of applications, which shall be efficient enough in its signing and proof of knowledge operations to satisfy the needs of large dynamically changing infrastructures. This research seeks to enable a cloud provider to obtain a graph signature certifying the current state of a cloud from an auditor, which the cloud provider can subsequently use to prove to multiple tenants that their security requirements are fulfilled without disclosing the blueprint of the infrastructure.

1.2 Relation to Other Project Work

This deliverable is connected to the following PRISMACLOUD deliverables:

- Deliverables D4.6 and D4.7 in WP 4: This deliverable builds upon the results presented in D4.6 as well as D4.7 and presents additional research results.
- Deliverables D5.6, D5.7 and D5.9 in WP5: This deliverable is directly related to the deliverables in WP5 concerned with the description of the PRISMACLOUD tools. In particular, results from Task 4.3.1 is integrated within the FLEXAUTH tool and the research in Task 4.3.2 is at the heart of the TOPOCERT tool.

- Deliverables D6.4, D6.5 and D6.6 in WP 6: This deliverable is also related to software implementation of cryptographic primitives and protocols as well as their documentation in WP 6. In particular, implementations of the core cryptographic concepts dealt within this line of deliverables will be at the heart of the FLEXAUTH and TOPOCERT tools and consequently their implementation. WP 6 deliverables also document how this cryptographic functionality can be used within the PRISMACLOUD services.

1.3 Structure of the Document

This document is structured as follows. In Section 2 we present research on privacy-preserving cryptography for the cloud. In particular, we present three research contributions dealing with so called structure-preserving signature schemes on equivalence classes and their applications to multi-show attribute-based anonymous credential (ABC) systems as well as group signatures. Moreover, we present research on the novel paradigm of witness encryption and its applications to privacy enhancing cryptography. In Section 3, we present research on certified and verifiable infrastructure for cloud services. In particular, creating trustworthy compartments in virtualized infrastructures.

Section 4 presents a brief overview of all the research papers presented in this report and finally Section 5 concludes this report.

2 Privacy-Preserving Cryptography for the Cloud

In this task, we investigate privacy-preserving cryptographic primitives and protocols and their underlying signatures schemes. In particular, we study multi-show attribute-based anonymous credential (ABC) systems and group signature schemes which enable more privacy-friendly cloud applications. Moreover, we study the novel paradigm of witness encryption with respect to efficient constructions and applications to privacy enhancing cryptography.

In particular, in Section 2.1 we investigate structure-preserving signatures on equivalence classes (SPS-EQ) and their application to efficient multi-show attribute-based credential (ABC) systems.

In Section 2.2 we present a novel approach to construct group signatures from SPS-EQ. This yields extremely efficient group signatures and outperforms the fastest constructions providing anonymity in the BSZ model known to date.

In Section 2.3 we present an efficient instantiation of the novel primitive of witness encryption for a restricted class of languages which has interesting applications to privacy-enhancing cryptography.

We want to stress that we reuse large parts of the introductions of the respective papers (verbatim) for the overviews presented below. Also note that the following sections are intended to give a high-level overview of our results. For a more formal treatment we refer the reader to the full papers which can be accessed via the Prismacloud website.

2.1 Structure-Preserving Signatures on Equivalence Classes and Constant-Size Anonymous Credentials

Digital signatures are an important cryptographic primitive that provide a means for integrity protection, non-repudiation and authenticity of messages in a publicly verifiable way. In most signature schemes, the message space consists of integers in $\mathbb{Z}_{\mathrm{ord}(\mathbb{G})}$ for some group $\mathbb{G}$, or of arbitrary strings mapped to either integers in $\mathbb{Z}_{\mathrm{ord}(\mathbb{G})}$ or elements of a group $\mathbb{G}$ via a cryptographic hash function. In the latter case, the hash function is often modeled as a random oracle (thus, one effectively signs random group elements).

Structure-preserving signature (SPS) schemes [Fuc09, AHO10, AFG+10, AGHO11, ACD+12, AGOT14a, AGOT14b, BFF+15, KPW15, Gha16] sign group elements without requiring any prior encoding. In particular, SPS are defined over two groups $\mathbb{G}_1$ and $\mathbb{G}_2$, equipped with a bilinear map (pairing), and messages are vectors of group elements (from either $\mathbb{G}_1$ or $\mathbb{G}_2$, or both). Moreover, public keys and signatures also consist of group elements only and signatures are verified by deciding group membership of their elements and evaluating the pairing on elements from the public key, the message and the signature. Fully SPS schemes [AKOT15, Gro15b] also require the secret key to consist of group elements.

Randomization is a useful feature of signature schemes that lets anyone transform one signature into a new one that looks like a freshly generated signature on the same message.

There have been various constructions of randomizable signatures [CL03, CL04, BBS04a, Wat05, PS16] and SPS schemes supporting some types of randomization (inner, sequential, etc.) [AFG+10, AGOT14b].

In this paper, we extend this randomization, in particular, we construct SPS schemes that in addition to randomizing signatures also enable randomization of the signed *messages* in particular ways, and adaptation of the corresponding signatures. As we show, such signature schemes are particularly interesting for applications in privacy-enhancing cryptographic protocols.

2.1.1 Previous Work

Signatures. Blazy et al. [BFPV11] introduce a new primitive, termed *signatures on randomizable ciphertexts* for which they modify Waters' signature scheme [Wat05]. Given a signature on a ciphertext, anyone can randomize the ciphertext and adapt the signature accordingly, knowing neither signing key nor encrypted message. Their construction is only practical for very small message spaces, which makes it unsuitable for our purposes.

Another related approach is the proofless variant of the Chaum-Pedersen signature [CP93], used for self-blindable certificates by Verheul [Ver01]. The certificate as well as the initial message can be randomized using the same scalar, preserving the validity of the certificate. This approach works for the construction in [Ver01], but (as also observed in [Ver01]) it is not a secure signature scheme due to its homomorphic property and the possibility of efficient existential forgeries.

Linearly homomorphic signatures [BFKW09, CFW12, Fre12] allow to sign any subspace of a vector space by publishing a signature for every basis vector with respect to the same (file) identifier; this identifier "glues" together the single vectors (of a file). Given a sequence of scalar/signature pairs $(\beta_i, \sigma_i)_{i\in[\ell]}$ for vectors $\vec{v}_i$ (with the same identifier), one can publicly compute a signature for the vector $\vec{v} = \sum_{i\in[\ell]} \beta_i \vec{v}_i$.

If one uses a different identifier for every signed vector $\vec{v}$ then such signatures would support a functionality similar to signature adaptation in SPS-EQ, that is, publicly compute signatures for vectors $\vec{v}' = \beta\vec{v}$ (although they are not structure-preserving). Various constructions also provide a privacy feature called strongly/completely context-hiding [ALP12, ALP13], requiring that a signature resulting from homomorphic operations is indistinguishable from a fresh one. Nevertheless, homomorphic signatures do not help in our context: for SPS-EQ unforgeability, we must prevent combination of signatures on several (independent) vectors; so every vector must be assigned a unique identifier. Then however, our unlinkability notion cannot be satisfied as every signature can be linked to its initial signature via the unique identifier. The same arguments also apply to structure-preserving linearly homomorphic signatures [LPJY13]. Homomorphic signatures supporting richer classes of admissible functions (beside linear ones) have also been considered, but are not applicable in our context either (cf. [ABC+12, ALP12] for an overview). We note that the general framework of *P-homomorphic signatures* [ABC+12, ALP12] is related to our approach in terms of unforgeability and privacy guarantees, but there are no

existing instantiations for the functionality that we require (and we find our formalization more natural).

Chase et al. [CKLM14] introduce *malleable signatures* that let one derive, from a signature on a message m, a signature σ' on $m' = T(m)$ for an "allowable" transformation T. This generalizes signature schemes, including quotable [ABC+12, ALP13] or redactable signatures [SBZ02, JMSW02] with an additional context-hiding property. Letting messages be pseudonyms and allowable transformations map one pseudonym to another one, the authors use malleable signatures to construct anonymous credential systems and *delegatable* anonymous credential systems [BCC+09]. The general construction in [CKLM14] however relies on malleable zero-knowledge proofs [CKLM12] and is not practically efficient—even when instantiated with the Groth-Sahai proof system [GS08]. Although the above framework is conceptually totally different from our approach, we note that SPS-EQ can be cast into the definition of malleable signatures: the evaluation algorithm takes only a single message vector with corresponding signature and there is a single type of allowable transformation. However, our construction is practical and moreover Chase et al. [CKLM14] only focus on transformations of single messages (pseudonyms) and do not consider multi-show ABCs, which is the main focus of our construction.

Set Commitments. The best-known approach for commitments to (ordered) sets are *Merkle hash trees* (MHTs) [Mer88], where for a set S the commitment size is $O(1)$ and the opening of a committed set element is of size $O(\log |S|)$. Boneh and Corrigan-Gibbs [BC14] propose an alternative MHT construction using a novel commitment scheme based on a bivariate polynomial modulo RSA composites. In contrast to MHTs, their construction supports succinct proofs of knowledge (PoK) of committed values.

Kate, Zaverucha and Goldberg [KZG10] introduce *polynomial-commitment* schemes that allow to commit to polynomials and support (batch) openings of polynomial evaluations. They can be used to commit to ordered sets (by fixing an index set) or to sets by identifying committed values with roots. Their two constructions are analogues to DL and Pedersen commitments and have $O(1)$-size commitments and openings. Recently, Camenisch et al. [CDHK15] proposed a variant of the Pedersen version from [KZG10]. A related commitment scheme, called *knowledge commitment*, was proposed by Groth [Gro10] and later generalized by Lipmaa [Lip12].

Other commitments to ordered sets are generalized Pedersen [Ped92] or Fujisaki-Okamoto [FO98] commitments. Both have commitment size $O(1)$, but opening proofs are of size $O(|S|)$. For completeness, let us also mention *vector commitments* [CF13], which allow to open specific positions as well as subsequent updates at specific positions (but do not necessarily require hiding). *Zero-knowledge sets* [MRK03] are another primitive in this context. They allow to commit to a set and to perform membership and non-membership queries on values without revealing any further information on the set. In [DHS15], it was shown that zero-knowledge sets imply commitments in a black-box way.

ABCs. Signatures providing randomization features together with efficient zero-knowledge PoKs of committed values can be used to generically construct ABC systems. The most

prominent example are CL credentials [CL03, CL04], based on Σ-protocols. With the advent of Groth-Sahai proofs [GS08], which provide efficient non-interactive proofs in the CRS model without random oracles, various constructions of non-interactive anonymous credentials [BCKL08b, ILV11] and delegatable (hierarchical) anonymous credentials [BCC+09, Fuc11] have been proposed. These have a non-interactive showing protocol, that is, the show and verify algorithms do not interact when demonstrating credential possession (also the recent model for conventional ABCs in [CKL+14] demands showings to be non-interactive). We note that although such credential systems with non-interactive protocols extend the scope of applications of anonymous credentials, the most common use case (i.e., authentication and authorization), essentially relies on interaction (to provide freshness/liveness). We emphasize that our goal is not to construct non-interactive anonymous credentials.

2.1.2 Contribution

Our contributions can be broken down as follows: (1) Introduction and instantiation of SPS on equivalence classes (SPS-EQ), which are defined on group element vectors; (2) a randomizable set commitment scheme that enables constant-size opening of subsets of the committed set; and building on these primitives (3) a new construction approach for multi-show attribute-based anonymous credentials, which we efficiently instantiate and analyze in a comprehensive security model we propose.

Structure-Preserving Signature Scheme on Equivalence Classes. Inspired by randomizable signatures, we introduce a variant of SPS. Instead of signing message vectors as in previous SPS schemes, our variant signs classes of a projective equivalence relation $\mathcal{R}$ defined over $\mathbb{G}^\ell$ with $\ell > 1$. These classes are lines going through the origin and are determined by the mutual ratios of the discrete logarithms of the vector components. By multiplying each component by the same scalar, a different representative of the same equivalence class is obtained. If the DDH assumption holds in group $\mathbb{G}$ then it is hard to decide whether two vectors belong to the same equivalence class.

In SPS-EQ an equivalence class is signed by signing an arbitrary representative of the class. From this signature one can later derive a signature for any other representative of the same class, without having access to the secret key. Unforgeability for SPS-EQ is defined with respect to classes. Thus, after obtaining signatures on representatives of its choice, no adversary should be able to compute a signature on a representative of a class that is different from the ones signed. We also require that adaptation of signatures leads to freshly distributed ones; in combination with unlinkability of equivalence classes this implies the following: given a representative and a signature on it, a random representative of the same class and an adapted signature on it are indistinguishable from a completely random message and a fresh signature on it.

We present a definitional framework for SPS-EQ including game-based security definitions and present an efficient construction whose signatures are short and their length is independent of the message-vector length ℓ. We prove our construction secure in the

generic-group model [Sho97].

Set Commitments. We propose a new type of commitment scheme that lets one commit to sets and open arbitrary subsets. We first propose a model for this primitive and then give an efficient construction, which we prove secure in this model. It lets one commit to subsets of $\mathbb{Z}_p$ and a commitment and a subset-opening both consist of a single bilinear-group element. Our scheme is computationally binding, perfectly hiding, and computationally subset-sound, meaning that given a commitment to a set S it is hard to produce a subset-opening for some $T \not\subseteq S$.

We prove security under a generalization of the strong Diffie-Hellman assumption [BB04].

The scheme also enables commitment randomization, which is compatible with the randomization of our SPS-EQ scheme (i.e., multiplication by a scalar). Randomization is perfect and the witness used for subset opening can be adapted accordingly. This property has not been achieved by existing constructions without relying on costly zero-knowledge proofs of randomization.

A Multi-Show Attribute-Based Anonymous Credential System. *Attribute-based anonymous credentials* provide means for anonymous authentication. A credential system is a multi-party protocol involving a user, an organization (or issuer) and a verifying party. The user can obtain a credential on multiple attributes, such as her nationality or age, from an organization and present the credential to some verifier later on, revealing only certain attributes. While not learning any information about the user *(anonymity)*, the verifier can still be sure that presented information (the shown attributes) is authentic *(unforgeability)*. In a *multi-show* credential system, a user obtains a credential from an organization, typically in a non-anonymous way, and can later perform an arbitrary number of unlinkable showings.

We propose a new way of building multi-show attribute-based anonymous credentials (often called Privacy-ABCs; we simply write ABCs) from SPS-EQ and set commitments. Using our instantiations, we construct the first standard-model multi-show ABC with anonymity holding against malicious organization keys.

An SPS-EQ scheme allows to randomize a vector of group elements together with a signature on it, a property we use to achieve unlinkability of credential showings. We use set commitments to commit to a user's attributes. To issue a credential, the issuer signs a message vector containing this set commitment; the credential is essentially this signature together with its message. During a showing, a subset of the issued attributes can then be opened. Unlinkability of showings is achieved via the rerandomization properties of both the signature scheme and the set-commitment scheme, whose rerandomizations are compatible with each other. Furthermore, to thwart replay attacks of showings, we add a short constant-size proof of knowledge, which guarantees freshness.

We emphasize that our approach to constructing ABCs differs considerably from existing ones, as we do not use zero-knowledge proofs to selectively disclose attributes during showings. This makes *constant-size* showings possible, as achieved by our construction.

In particular, the size of credentials as well as the bandwidth required when showing a credential are independent of the number of possible attributes as well as those contained in the credential; it is a small constant number of group elements. This is the first ABC system with this feature. We note that Camenisch et al. [CDHK15] recently proposed an approach with identical asymptotic complexity.

We introduce a game-based security model for ABCs in the vein of the Bellare, Shi and Zhang's [BSZ05] model for group signatures and prove our ABC system secure in it. We note that there are no other comprehensive models for attribute-based credential systems (apart from independently developed very strong simulation-based notions in [CKL+14, CDHK15]). Our model considers replays and provides a strong form of anonymity against organizations that may generate malicious keys—both of which are not considered by earlier models. Replay attacks have often been considered an implementation issue, but we believe that such attacks should already be considered in the formal analysis, avoiding from the beginning problems that might later appear within an implementation.

We note that the independently proposed formal model by Camenisch et al. [CKL+14] and the ABC construction in [CDHK15]—using a different model—do consider replays and malicious keys too, although the former in a seemingly weaker sense and the latter only assuming a CRS.

Finally, we discuss a variant of our scheme with smaller organization key sizes that is concurrently secure in the CRS model. We provide a comparison of our ABC system to other existing multi- and one-show ABC approaches.

2.2 Fully-Anonymous Short Dynamic Group Signatures Without Encryption

Group signatures, initially introduced by Chaum and van Heyst [CvH91], allow a group manager to set up a group so that every member of this group can later anonymously sign messages on behalf of the group. Thereby, a dedicated authority (called opening authority) can open a given group signature to determine the identity of the actual signer. Group signatures were first rigorously formalized for static groups by Bellare et al. in [BMW03]. In this setting, all members are fixed at setup and also receive their honestly generated keys at setup from the group manager. This model was later extended to the dynamic case by Bellare et al. in [BSZ05] (henceforth denoted by BSZ model), where new group members can be dynamically and concurrently enrolled to the group. Further, it separates the role of the issuer and the opener so that they can operate independently. Moreover, the BSZ model requires a strong anonymity notion, where anonymity of a group signature is preserved even if the adversary can see arbitrary key exposures and arbitrary openings of other group signatures. A slightly weaker model, which is used to prove the security (and in particular anonymity) of the popular BBS group signature scheme was introduced by Boneh et al. [BBS04b]. This model is a relaxation of the BSZ model, and in particular weakens anonymity so that the adversary can not request openings for signatures. As it is common, we refer to this anonymity notion as CPA-full anonymity, whereas we use CCA2-full anonymity to refer to anonymity in the sense of BSZ.

2.2.1 Previous Work

Over the years, two main construction paradigms for group signatures have been established. The first one is the widely used sign-encrypt-prove (SEP) paradigm [CS97]. Here, a signature is essentially an encrypted membership certificate together with a signature of knowledge, where the signer demonstrates knowledge of some signed value in the ciphertext [ACJT00, BBS04b, NS04, BSZ05, KY05, DP06, BW07, BW06, Gro07, LPY15, LLM+16, LMPY16]. As an alternative to this paradigm, Bichsel et al. in [BCN+10] proposed an elegant design paradigm for group signatures which does not require to encrypt the membership certificate to produce signatures. Henceforth we call this paradigm sign-randomize-proof (SRP). Essentially, they use a signature scheme which supports (1) randomization of signatures so that multiple randomized versions of the same signature are unlinkable, and (2) efficiently proving knowledge of a signed value. In their construction, on joining the group, the issuer uses such a signature scheme to sign a commitment to the user's secret key. The user can then produce a group signature for a message by randomizing the signature and computing a signature of knowledge on the message, which demonstrates knowledge of the signed secret key. To open signatures, in contrast to constructions following SEP which support constant time opening by means of decrypting the ciphertext in the signature, constructions in this paradigm require a linear scan, i.e., to check a given signature against each potential user. Bichsel et al. proposed an instantiation based on the randomizable pairing-based Camensich-Lysyanskaya (CL) signature scheme [CL04] (whose EUF-CMA security is based on the interactive LRSW assumption). Recently, Pointcheval and Sanders [PS16] proposed another randomizable signature scheme (whose EUF-CMA security is proven in the generic group model), which allows to instantiate the approach due to Bichsel et al. more efficiently. We note that while these two existing constructions do not explicitly use public key encryption, the required assumptions for the scheme imply public key encryption. Yet, it seems to be beneficial regarding performance to avoid to explicitly use public key encryption.

The main drawback of existing constructions following the SRP paradigm is that they rely on a security model that is weaker than the BSZ model [BSZ05]. In particular, anonymity only holds for users whose keys do not leak. This essentially means that once a user key leaks, all previous signatures of this user can potentially be attributed to this user. Furthermore, the model used for SRP constructions assumes that the opening authority and the issuing authority are one entity, meaning that the issuer can identify all signers when seeing group signatures. Both aforementioned weakenings can be highly problematic in practical applications of group signatures. It is thus a natural question to ask whether it is possible to prove that constructions following the SRP paradigm provide CPA- or even CCA2-full anonymity. Unfortunately, for existing constructions, we have to answer this negatively. Even when allowing to modify the existing constructions in [BCN+10, PS16] to allow the explicit use of encryption upon joining the group (which might solve the separability issue regarding issuer and opener), it is easy to see that knowledge of the user secret key breaks CCA2- as well as CPA-full anonymity for both constructions.[1] Since

[1] Each valid group signature contains a valid randomizable signature on the secret key of the user. While group signatures only contain a proof of knowledge of the signed secret key, being in possession of secret

CCA2-full anonymity straight forwardly implies anonymity in the SRP model, this example confirms that CCA2-full anonymity is a strictly stronger notion. The notion of CPA-full anonymity is somewhat orthogonal to the anonymity notion used by the SRP model: it appropriately models the leakage of user secret keys, but restricts the open oracle access. Yet, in practice it seems that the risk that a user secret key leaks is extremely hard to quantify, which is why we deem CPA-full anonymity to be more desirable. This is also underpinned by the fact that—to the best of our knowledge—no attacks arising from the restriction of the open oracle access in CPA-full anonymity are known.

2.2.2 Contribution

Group signatures have received significant attention from the cryptographic community and also gain increasing practical relevance due to technological innovations in intelligent transportation systems (e.g., floating car data, toll systems) as well as public transportation systems (i.e., smart ticketing), where user privacy is considered to play an important role (cf. EU Directive 2010/40/EU). These developments make it important to have particularly efficient group signature candidates at hand. As an illustrative example for the importance of very fast signature generation and verification times, consider public transportation system where every user needs to sign on passing a gate.

Despite their increasing practical importance, no progress has been made with respect to computational efficiency improvements of group signature schemes providing the more desirable notions of CPA- as well as CCA2-full anonymity within the last decade. The most efficient schemes known to date are the BBS group signature scheme [BBS04b] (which achieves CPA-full anonymity) and the XSGS group signature scheme [DP06] (which achieves CCA2-full anonymity).

We tackle the following open questions, which are of both theoretical and practical interest:

- *Is it possible to construct schemes providing the more desirable* CPA*-full and* CCA2*-full anonymity notions, where compelling efficiency is reached by (1) avoiding the explicit encryption of the membership certificate upon signing, yet (2) allowing to explicitly use encryption during the joining of a group?*
- *Is it possible to further push the computational efficiency limits of group signature schemes providing those more desirable anonymity notions?*

We, henceforth, refer to such schemes as "without encryption".

We answer both questions posed above to the affirmative by contributing a novel approach to construct group signatures "without encryption". Our approach is a composition of structure preserving signatures on equivalence classes (SPS-EQ) [HS14, FHS17] (cf. also Section 2.1), conventional digital signatures, public key encryption, non-interactive zero-knowledge proofs, and signatures of knowledge. Although these tools may sound quite

key candidates allows to simply test them using the verification algorithm of the randomizable signature scheme. This clearly provides a distinguisher against CCA2- as well as CPA-full anonymity.

heavy, we obtain surprisingly efficient group signatures, which provably provide CCA2-full anonymity in the strongest model for dynamic group signatures, i.e., the BSZ model. In doing so, we obtain the first construction which achieves this strong security notion without an encrypted membership certificate in the signature. In addition to that, we introduce an even more efficient CPA-fully anonymous variant of our scheme.

We also show how to instantiate our constructions in the random oracle model (ROM) to obtain particularly efficient schemes. We are thereby able to further push the long standing computational efficiency limits for both CPA- and CCA2-fully anonymous schemes regarding signature generation and verification. When comparing to the popular BBS group signature scheme [BBS04b] (which achieves CPA-full anonymity in the ROM), besides being more efficient we surprisingly even obtain shorter signatures. Ultimately, when comparing to instantiations in the vein of Bichsel et al. (which provide a less desirable anonymity notion), our instantiations provide comparable computational efficiency.

2.3 Practical Witness Encryption for Algebraic Languages Or How to Encrypt Under Groth-Sahai Proofs

Witness encryption (WE) is a recent powerful encryption paradigm introduced by Garg et al. [GGSW13]. In WE, an encryption scheme is defined for some **NP**-language L with witness relation R so that $L = \{x \mid \exists\, w : R(x, w) = 1\}$. The encryption algorithm takes an alleged word x from L (instead of an encryption key) and a message m and produces a ciphertext c. Using a witness w such that $R(x, w) = 1$, anyone can decrypt c to obtain m. Decryption only works if $x \in L$ and a ciphertext c hides m if c has been computed with respect to some $x \notin L$.

Constructions of WE. The first construction of WE for any language in **NP** in [GGSW13] has been for the **NP**-complete problem *exact cover* and uses approximate multilinear maps (MLMs). Later, Gentry et al. [GLW14] introduced the concept of positional WE, which allows to prove the aforementioned construction secure. In [GGH+13], Garg et al. showed that indistinguishability obfuscation implies WE. Goldwasser et al. proposed the stronger notion of *extractable* WE in [GKP+13]. While the security for WE is only with respect to $x \notin L$, extractable WE requires that any successful adversary against semantic security of the WE, given an encryption with respect to x, implies the existence of an extractor that extracts a witness w to $x \in L$. Thereby, the adversary and the extractor additionally get an auxiliary input. Garg et al. [GGHW14] have shown that under the assumption that special-purpose obfuscation exists, extractable WE for all languages in **NP** cannot exist.[2] Zhandry [Zha16] introduced the concept of witness PRFs, which essentially generalizes WE. Zhandry also proposes (CCA secure) *reusable* WE, which introduces an additional global setup and thus allows to reuse certain parameters. This drastically reduces the size of ciphertexts in WE schemes. We observe that our generic constructions of WE bear similarities to how WE is constructed from witness PRFs. Yet, Zhandry aims at building witness PRFs for any **NP**-language, where we aim at practical instantiations. All these

[2] Even if such special-purpose obfuscation exists, this does not rule out that extractable WE for a sufficiently large interesting subset of **NP** exists.

constructions build upon MLMs and/or obfuscation and are thus far from being practical. To this end, Abusalah et al. [AFP16] recently introduced the notion of *offline* WE as a step towards more practical WE. They split encryption into an expensive offline phase and a much more efficient online phase, which allows them to achieve practical efficiency for the online part. Nevertheless, the offline part and the decryption still requires obfuscation and thus cannot be considered to be practical. Besides imposing a huge computational overhead, MLM and obfuscation are still in a "break-repair" state and it is currently unknown if one can come up with candidate constructions being secure under well established assumptions.

Restricting Languages. In concurrent and independent work, Faonio et al. [FNV15] introduced the concept of predictable arguments of knowledge (PAoK). They are one-round interactive protocols in which the verifier generates a challenge and can at the same time predict the prover's answer to that challenge. Faonio et al. show that PAoKs are equivalent to extractable WE [GKP+13]. Regarding concrete instantiations of PAoKs (and thus extractable WE), they show how to construct PAoKs from extractable hash proof systems (Ext-HPS) as defined by Wee in [Wee10]. Although their approach to constructing WE can thus be seen as related to our approach, firstly ours is conceptually simpler and secondly the languages covered by Ext-HPSs are very basic and very restricted, i.e., [Wee10] presents two instantiations; one for the iterated squaring relation and one for the Diffie Hellman relation. It is also not clear if efficient instantiations for more expressive languages can be found. We also note that due to the lack in expressiveness of Ext-HPS as used in [FNV15], their constructions are not suitable for what we are targeting at. Earlier work on (private) conditional oblivious transfer [COR99, JL09] can be viewed as as an interactive version of (extractable) WE for very specific and restricted languages not suitable for achieving our goals. Finally, [GGSW13] mentioned along the lines that earlier work on SPHFs can be interpreted as establishing the existence of WE for certain restricted languages and an informal sketch of a construction of WE from SPHFs was recently given in [ABP15].

Applications of WE. WE in general extends the scope of encryption as it allows to encrypt a message using the description of a hard problem and only someone who knows a solution to this problem is able to decrypt. WE is thus intuitively related to time-lock puzzles [RSW96] and WE indeed has been used to realize a related concept denoted as time-lock encryption, i.e., a method to encrypt a message such that it can only be decrypted after a certain deadline has passed, but then very efficiently and by everyone. An approach to realize such schemes from WE and so called computational reference clocks has been proposed by Jager in [Jag15]. Liu et al. [LKW15] also propose to use their WE construction for time-lock encryption based on the Bitcoin protocol. Bellare and Hoang [BH15] proposed to use WE to realize asymmetric password-based encryption, where the hash of a password can be used to encrypt a message (acting as a public key) and only the knowledge of the respective password allows decryption. Moreover, it has already been shown in the seminal work [GGSW13] that WE can be used to construct identity-based encryption (IBE) [BF01] as well as attribute-based encryption (ABE) [SW05] for circuits.

2.3.1 Previous Work

SPHFs (denoted as hash proof systems) were initially used to construct CCA2 secure public key encryption [CS98] without requiring the random oracle heuristic. Later it was observed that SPHFs are sufficient to construct such encryption schemes [CS02]. They use the SPHF exactly the other way round as we use it, i.e., in their setting decryption is done with the knowledge of the hashing key and without the witness. This paradigm can also be viewed as an implicit construction of publicly evaluable pseudorandom functions [CZ14].

Hybrid Encryption. Kurosawa and Desmedt [KD04] used the paradigm described above for hybrid encryption. A series of works follow their paradigm (e.g., [KPSY09]) and use SPHFs to obtain CCA2 secure hybrid encryption schemes. Similar to [CS02], they use the SPHF exactly the other way round as we are going to use it.

Key-Exchange. A line of work following Gennaro and Lindell [GL06] uses SPHFs for password-based authenticated key exchange (PAKE) between two parties. This concept was later extended to one-round PAKE [KV11] and generalized to language-authenticated key exchange (LAKE) for various algebraic languages over bilinear groups in [BBC+13] (and we note that follow-up work on various aspects exists). Most recently, in [BC16] it was shown how to construct so called structure preserving SPHFs, which can use GS proofs as witnesses. Even though this may sound somewhat related to our work, apart from not constructing WE, the approach in [BC16] to build SPHFs is diametrically opposed to our approach. In particular, our WE approach requires GS proofs to be public and that they must not to be useful to reconstruct the hash value. So, applying our approach to construct WE to the SPHFs in [BC16] does not help us.

2.3.2 Contribution

Motivation. While having WE schemes that support *all languages* in **NP** is appealing, it is the main source of inefficiency. We aim to make WE practical, but in contrast to offline WE as introduced in [AFP16] we focus on all aspects, i.e., encryption and decryption, to be efficient. Our approach to improving the efficiency is by restricting the class of supported languages from any **NP**-language to languages that are expressive enough to cover many problems encountered in cryptographic protocol design. In particular, we aim at *algebraic languages defined over bilinear groups*. Such languages are very relevant for the design of cryptographic protocols as statements in these languages cover statements that can be proven in a zero-knowledge (or witness indistinguishable) fashion using the Groth-Sahai (GS) non-interactive proof framework [GS08]. Our techniques yield a novel way of encryption, where one can encrypt messages with respect to a GS proof so that only the prover, i.e., the party that computed the respective proof, can decrypt. We assume that there are many interesting applications that could benefit from our technique.

Our contributions are as follows.

- We provide a generic construction of WE from SPHFs and prove that if there exists an SPHF for a language L, then there exists an adaptively sound WE scheme for language L. Thereby, we define WE to provide an additional setup algorithm as also done in [AFP16, Zha16], since this notion makes the schemes more efficient and more convenient to use in protocol design.
- Using well known techniques such as universal hashing and secure symmetric encryption schemes, we obtain a WE scheme for messages of arbitrary length.
- We present practical instantiations of our generic approach to WE for algebraic languages in the bilinear group setting. We, thereby, achieve compatibility with statements from the GS proof system. Besides being practically efficient, our constructions only require standard assumptions (i.e., DLIN).[3]
- We observe that the existing security notions for WE are unsuited when using WE in combination with other primitives. To this end, we introduce a stronger security notion for WE which considers the combination of WE with GS proofs and prove that our instantiation satisfies this notion.
- We present an approach to use our WE construction for GS statements to elegantly encrypt messages with respect to NIZK/NIWI proofs for statements in the frequently used GS proof system so that only the one who computed the proof can decrypt. This yields a novel way of encryption.
- To illustrate the aforementioned concept, we discuss two potential applications of our techniques in the context of privacy preserving exchange of information.

[3] Our approach is also easily portable to the SXDH setting (and thus relying on DDH).

3 Certified and Verifiable Infrastructure for Cloud Service

In this section, we describe the research on certified and verifiable infrastructure for cloud service, especially in advances on graph signatures used for the representation of cloud infrastructures. Overall, this research is concerned with analyzing clouds, certifying the outcomes of that analysis and subsequently enabling a cloud provider to prove security properties to verifiers, such as tenants. This work is predominantly in the area of privacy-enhancing cryptography, however, we briefly introduce techniques for analyzing virtualized infrastructures as well as certifiable compartmentalization, deriving graph representations and proving their security properties as well, because they are a vital precondition to the certification.

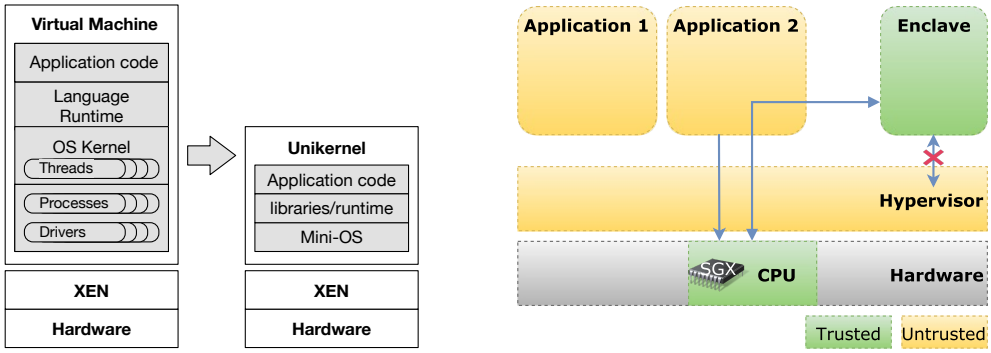
Consequently, we introduce one work on the systems' foundations for certified secure cloud infrastructures.

Section 3.1 outlines research on creating trustworthy compartments in virtualized infrastructures that are protected using a hardware-based mechanism. This research addresses one of the major shortcomings of the topology certification present in PRISMACLOUD: The topology certification with graph signatures [Gro15a, Gro14] only covers topological properties and is dependent on the control of the behavior of certified units (e.g., virtual machines or network devices) by other means. Whereas there are proposals for creating trustworthy compartments in virtualized infrastructures such as Trusted Platform Module (TPM) [Tru14] and ARM TrustZone [ARM09], this proposal is the first one to protect unikernels leveraging a hardware-based security mechanism. As a result, vertices in a topology certification are trustworthy and in extension we provide a trustworthy graph representation to the auditor for topology certification.

3.1 UniGuard: Protecting Unikernels using Intel SGX

Previous research on certified and verifiable virtualized infrastructures represents virtual machines as monolithic computation units. Virtual machines can represent vertices and their labels can contain information such as their operating system, platform and software image. In addition, virtual machines execute multi-purpose computations and have a large attack surface if we consider all their internal components. Another dimension, is the trustworthiness of computations in virtual machines where privileged software can ascertain information about computations. For a certified and verifiable virtualized infrastructure it is desirable to assure the trustworthiness of the vertices which results in a correct topology certification.

The *UniGuard* project aims at realizing a unikernel-based virtualized infrastructure that employs Intel Software Guard Extensions (SGX) to create a trusted execution environment where privileged software cannot tamper with the execution of unikernels. Even though unikernels [MRS+13] do not have a guest operating system or extraneous functionality, they are still vulnerable to attacks from adversaries that have access to privileged software and access to hardware.



(a) Unikernels (b) Intel SGX

Figure 1: Unikernel and Intel SGX architectures

3.1.1 Previous Work

Unikernels [MRS+13] are specialized, minimal single-address virtual machines that have system libraries, language runtime, and application and configuration files baked in, but no general purpose-operating system. Figure 1a gives an overview of this paradigm.

The *UniGuard* work is based on Intel SGX [AGJS13] which is a mechanism integrated into an Intel CPU that enables the creation of Trusted Execution Environments (TEE). A Trusted Execution Environment is an environment that executes trusted applications in isolation inside an operating system. Intel SGX includes a set of hardware instructions that are used for generating secure software containers called enclaves. Enclaves are isolated regions of memory for code and data

Haven [BPH15] was one of the first attempts to use Intel SGX. Haven executes unmodified Windows applications inside a secure enclave. This approach requires the whole Windows library OS inside the enclave to execute full Windows applications, which creates a large Trusted Computing Base (TCB). This means that a vulnerability in the operating system can compromise the security of the enclave. Figure 1b illustrates the conceptual architecture of Intel SGX.

Scone [ATG+16] proposes a secure container mechanism for Docker that uses Intel SGX to protect containers from an external malicious user. Even though Scone uses a smaller TCB than Haven it still can be reduced if it was also supporting unikernels.

Sanctum [CLD16] provides a different approach than the previous works focusing in providing strong software isolation with minimal hardware changes to a RISC-V core. This work's main improvement in comparison with Intel SGX is that it does not allow software attacks that analyze memory access patterns to gain confidential information. However, it only focuses on software attacks in the threat model, while Intel SGX includes certain hardware attacks in its threat model.

Other examples of using Intel SGX include VC3 [SCF+15] and Graphene-SGX [TPV17]. VC3 is focusing on MapReduce computations and uses Intel SGX to execute them in an

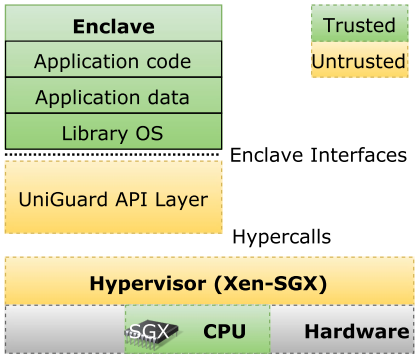


Figure 2: UniGuard high-level architecture

untrusted virtualized infrastructure. Although, VC3 has a small TCB and low performance overhead it only supports the Hadoop application. In contrast, Graphene-SGX supports a wide range of unmodified applications and offers comparable performance overhead.

3.1.2 Contribution

The main contribution of this work is the architecture and realization of *UniGuard*, a system that integrates Intel SGX with unikernels. We depict the architecture in Figure 2. *UniGuard* makes it possible to deploy minimal specialized virtual machines, which execute their trusted part in a secure enclave using Intel SGX. As a result, the unikernel is protected from a number of software and hardware attacks.

The unikernel approach enables certification and verification of virtualized infrastructures [Gro14] on smaller functional units for compute resources and thereby a more fine-grained representation. Whereas fully-fledged VMs may be connected to network and storage vertices for each of their ingrained functionalities without differentiation, the unikernel-based deployments can be restricted to the network and storage resources required for the designated function. Executing a unikernel in a secure enclave results in a trustworthy vertex and in extend in a trustworthy graph representation.

UniGuard achieves its goal by creating a MirageOS library that interfaces with the Intel SGX API. The library creates a thin layer between the unikernel and the secure enclave. In essence, we can have a number of enclaves performing the secure computation inside them or have only one enclave per unikernel. Since unikernels have a minimal footprint the relationship between enclaves and unikernels is one-to-one.

Figure 2 illustrates the high-level architecture of *UniGuard*. We are using a particular Xen hypervisor version that supports Intel SGX. The UniGuard API layer provides a wrapper for enclave interfaces that create the hypercalls required for managing the enclave lifecycle. The enclave hosts a version of MirageOS which includes a library responsible for integrating a unikernel with the enclave.

The above approach is specialized for infrastructures that include a hypervisor. A similar

approach can be taken when we use a container-based infrastructure where the operat ing system plays the role of the hypervisor. The operating system kernel includes and SGX driver that manages the lifecycle of the enclave and a library OS is included inside the enclave.

4 Abstracts of Research Papers

4.1 Privacy-Preserving Cryptography for the Cloud

- Georg Fuchsbauer, Christian Hanser and Daniel Slamanig: "Structure-Preserving Signatures on Equivalence Classes and Constant-Size Anonymous Credentials", in *Journal of Cryptology 2017* [FHS17]

  Structure-preserving signatures (SPS) are a powerful building block for cryptographic protocols. We introduce SPS on equivalence classes (SPS-EQ), which allow joint randomization of messages and signatures. Messages are projective equivalence classes defined on group element vectors, so multiplying a vector by a scalar yields a different representative of the same class. Our scheme lets one adapt a signature for one representative to a signature for another representative without knowledge of any secret; and given a signature, an adapted signature for a different representative is indistinguishable from a fresh signature on a random message. We propose a definitional framework for SPS-EQ and an efficient construction in Type-3 bilinear groups, which we prove secure against generic forgers.

  We also introduce a set-commitment scheme that lets one open subsets of the committed set. From this and SPS-EQ we then build an efficient multi-show attribute-based anonymous credential system for an arbitrary number of attributes. Our ABC system avoids costly zero-knowledge proofs and only requires a short interactive proof to thwart replay attacks. It is the first credential system whose bandwidth required for credential showing is independent of the number of its attributes, i.e., constant-size. We propose strengthened game-based security definitions for ABC and prove our scheme anonymous against malicious organizations in the standard model; finally, we give a concurrently secure variant in the CRS model.

- David Derler and Daniel Slamanig: "Fully-Anonymous Short Dynamic Group Signatures Without Encryption", in submission [DS16]

  Group signatures are a central tool in privacy-enhancing crypto, which allow members of a group to anonymously sign on behalf of the group. Ideally, group signatures are dynamic and thus allow to dynamically and concurrently enroll new members to a group. For such schemes Bellare et al. (CT-RSA'05) proposed a strong security model (BSZ model) that preserves anonymity of a group signature even if an adversary can see arbitrary key exposures or arbitrary openings of other group signatures. All previous constructions achieving this strong anonymity notion follow the so called sign-encrypt-prove (SEP) paradigm. In contrast, all known constructions which avoid this paradigm and follow the alternative "without encryption" paradigm introduced by Bichsel et al. (SCN'10), only provide a weaker notion of anonymity (which can be problematic in practice). Until now it was not clear if constructions following this paradigm, while providing strong anonymity in the sense of BSZ even exist.

  We answer this question to the affirmative by proposing a novel approach to dynamic group signature schemes following this paradigm, which is a composition of

structure preserving signatures on equivalence classes (Asiacrypt'14) and other standard primitives. Our results are interesting for various reasons: We can prove our construction following this "without encryption" paradigm secure without requiring random oracles. Moreover, when opting for an instantiation in the ROM, the so obtained scheme is extremely efficient and outperforms the fastest constructions providing anonymity in the BSZ model known to date. Regarding constructions providing a weaker anonymity notion than BSZ, we surprisingly outperform the popular short BBS group signature scheme (Crypto'04) and thereby even obtain shorter signatures.

- David Derler and Daniel Slamanig: "Practical Witness Encryption for Algebraic Languages Or How to Encrypt Under Groth-Sahai Proofs", in submission [DS15]

  Witness encryption (WE) is a recent powerful encryption paradigm, which allows to encrypt a message using the description of a hard problem (a word in an **NP**-language) and someone who knows a solution to this problem (a witness) is able to efficiently decrypt the ciphertext. Recent work thereby focuses on constructing WE for **NP** complete languages (and thus **NP**). While this rich expressiveness allows flexibility w.r.t. applications, it makes existing instantiations impractical. Thus, it is interesting to study practical variants of WE schemes for subsets of **NP** that are still expressive enough for many cryptographic applications.

  We show that such WE schemes can be generically constructed from smooth projective hash functions (SPHFs). In terms of concrete instantiations of SPHFs (and thus WE), we target languages of statements proven in the popular Groth-Sahai (GS) non-interactive witness-indistinguishable and zero-knowledge proof framework. This allows us to provide a novel way to encrypt. In particular, encryption is with respect to a GS proof and efficient decryption can only be done by the respective prover. The so obtained constructions are entirely practical. To illustrate our techniques, we apply them in context of privacy-preserving exchange of information.

4.2 Certified and Verifiable Infrastructure for Cloud Service

- Ioannis Sfyrakis and Thomas Groß: "UniGuard: Protecting Unikernels using Intel SGX", UNEW Research Report [SG17]

  Malicious insiders exploit vulnerabilities in the software layer of cloud infrastructures namely hypervisors, management virtual machines, and guest virtual machines. Computations inside virtual machines can leak information to privileged users and operating systems or hypervisors as numerous vulnerabilities have shown in recent times.

  Computations executed in lightweight virtual machines called unikernels have a minimal attack surface, however they are still prone to leaking information to the operating system or to the hypervisor that hosts them. Indeed the multi-platform deployment of unikernels requires a uniform protection mechanism to ensure that information does not leak from unikernels.

In this paper, we present UniGuard, a uniform protection mechanism that leverages Intel Software Guard Extension (SGX) to protect computations inside unikernels. We believe that unikernels are an excellent match for Intel SGX leveraging their advantages and creating a Trusted Execution Environment (TEE). Our main contribution is the design and implementation of a multi-platform library that gives access to the Intel SGX API for unikernel developers to create unikernels that execute the trusted part of the unikernel inside an Intel SGX enclave.

5 Conclusion

This deliverable has described the research conducted within Task 4.3 during the second year of the PRISMACLOUD project with its two subtasks: privacy-preserving cryptography for the cloud (Task 4.3.1) and certified and verifiable infrastructure for cloud service (Task 4.3.2).

In Task 4.3.1 we have focused our research on privacy-friendly authentication methods using privacy-enhancing cryptography that enables the application of cloud computing or are enabled by the existence of cloud computing. In particular, we have studied structure-preserving signatures on equivalence classes that are a central building block to blind signatures, one- and multi-show attribute-based anonymous credentials as well as group signatures. We present an efficient multi-show ABC system and a highly efficient approach to construct group signatures. Finally, we have investigated efficient approaches to witness encryption for restricted classes of languages and have investigated their application to privacy protection.

In Task 4.3.2 we have focused our research on two strands: one is to establish the systems foundations to enable a certified and verifiable infrastructures, the other is to advance the capabilities of the topology certification to represent virtualized infrastructures and proofs on their security properties. In particular, we have studied the possibility of establishing trustworthy unikernel-based computation units using a hardware-based mechanism that results in trustworthy graph representation for topology certification.

List of Acronyms

ABC	Attribute-Based Anonymous Credential
AC	Anonymous Credential
BSZ	Bellare, Shi and Zhang
CCA2	Adaptively Chosen Ciphertext Attack
CL	Camenisch-Lysyanskaya
CPA	Chosen Plaintext Attack
CRS	Common Reference String
GS	Groth Sahai
GS	Group Signatures
GSS	Group Signature Scheme
NIZKP	Non-Interactive Zero-Knowledge Proof
NP	Nondeterministic Polynomial Time
PoK	Proof of Knowledge
ROM	Random Oracle Model
SEP	Sign-And-Encrypt-And-Prove
SPHF	Smooth Projective Hash Function
SPS	Structure-Preserving Signature
SPS-EQ	Structure-Preserving Signature on Equivalence Classes
WE	Witness Encryption
ZK	Zero-Knowledge
ZKPK	Zero-Knowledge Proof of Knowledge

List of Figures

References

[ABC+12] Jae Hyun Ahn, Dan Boneh, Jan Camenisch, Susan Hohenberger, abhi shelat, and Brent Waters. Computing on authenticated data. In Ronald Cramer, editor, *TCC 2012: 9th Theory of Cryptography Conference*, volume 7194 of *Lecture Notes in Computer Science*, pages 1–20, Taormina, Sicily, Italy, March 19–21, 2012. Springer, Heidelberg, Germany.

[ABP15] Michel Abdalla, Fabrice Benhamouda, and David Pointcheval. Disjunctions for hash proof systems: New constructions and applications. In *EUROCRYPT*, 2015.

[ACD+12] Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 4–24, Beijing, China, December 2–6, 2012. Springer, Heidelberg, Germany.

[ACJT00] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In *CRYPTO*, volume 1880 of *LNCS*, pages 255–270. Springer, 2000.

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In *CRYPTO*, pages 209–236, 2010.

[AFP16] Hamza Abusalah, Georg Fuchsbauer, and Krzysztof Pietrzak. Offline witness encryption. In *ACNS*, 2016.

[AGHO11] Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 649–666, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany.

[AGJS13] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In *Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy*, volume 13, 2013.

[AGOT14a] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Structure-preserving signatures from type II pairings. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 390–407, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Heidelberg, Germany.

[AGOT14b] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 688–712, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany.

[AHO10] Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010. http://eprint.iacr.org/2010/133.

[AKOT15] Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi. Fully structure-preserving signatures and shrinking commitments. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 35–65, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

[ALP12] Nuttapong Attrapadung, Benoît Libert, and Thomas Peters. Computing on authenticated data: New privacy definitions and constructions. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 367–385, Beijing, China, December 2–6, 2012. Springer, Heidelberg, Germany.

[ALP13] Nuttapong Attrapadung, Benoît Libert, and Thomas Peters. Efficient completely context-hiding quotable and linearly homomorphic signatures. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013: 16th International Conference on Theory and Practice of Public Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 386–404, Nara, Japan, February 26 – March 1, 2013. Springer, Heidelberg, Germany.

[ARM09] ARM ARM. Security Technology-Building a Secure System using TrustZone Technology. Technical report, 2009.

[ATG+16] Sergei Arnautov, Bohdan Trach, Franz Gregor, Thomas Knauth, Andre Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Dan O'Keeffe, Mark Stillwell, et al. Scone: Secure linux containers with intel sgx. In *OSDI*, pages 689–703, 2016.

[BB04] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73, Interlaken, Switzerland, May 2–6, 2004. Springer, Heidelberg, Germany.

[BBC+13] Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud. Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages. In *PKC*, 2013.

[BBS04a] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

[BBS04b] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short Group Signatures. In *CRYPTO*, volume 3152 of *LNCS*, pages 41–55. Springer, 2004.

[BC14] Dan Boneh and Henry Corrigan-Gibbs. Bivariate polynomials modulo composites and their applications. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 42–62, Kaoshiung, Taiwan, R.O.C., December 7–11, 2014. Springer, Heidelberg, Germany.

[BC16] Olivier Blazy and Céline Chevalier. Structure-preserving smooth projective hashing. In *ASIACRYPT*, 2016.

[BCC+09] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable proofs and delegatable anonymous credentials. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 108–125, Santa Barbara, CA, USA, August 16–20, 2009. Springer, Heidelberg, Germany.

[BCKL08a] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. P-signatures and Noninteractive Anonymous Credentials. In *TCC*, volume 4948 of *LNCS*, pages 356–374. Springer, 2008.

[BCKL08b] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. P-signatures and noninteractive anonymous credentials. In Ran Canetti, editor, *TCC 2008: 5th Theory of Cryptography Conference*, volume 4948 of *Lecture Notes in Computer Science*, pages 356–374, San Francisco, CA, USA, March 19–21, 2008. Springer, Heidelberg, Germany.

[BCN+10] Patrik Bichsel, Jan Camenisch, Gregory Neven, Nigel P. Smart, and Bogdan Warinschi. Get Shorty via Group Signatures without Encryption. In *SCN*, 2010.

[BF01] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO*, 2001.

[BFF+15] Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi. Strongly-optimal structure preserving signatures from type II pairings: Synthesis and lower bounds. In Jonathan Katz, editor, *PKC 2015: 18th International Conference on Theory and Practice of Public Key Cryptography*, volume 9020 of *Lecture Notes in Computer Science*, pages 355–376, Gaithersburg, MD, USA, March 30 – April 1, 2015. Springer, Heidelberg, Germany.

[BFKW09] Dan Boneh, David Freeman, Jonathan Katz, and Brent Waters. Signing a linear subspace: Signature schemes for network coding. In Stanislaw Jarecki and Gene Tsudik, editors, *PKC 2009: 12th International Conference on Theory and Practice of Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 68–87, Irvine, CA, USA, March 18–20, 2009. Springer, Heidelberg, Germany.

[BFPV11] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Signatures on randomizable ciphertexts. In *PKC*, pages 403–422, 2011.

[BH15] Mihir Bellare and Viet Tung Hoang. Adaptive Witness Encryption and Asymmetric Password-Based Cryptography. In *PKC*, 2015.

[BMW03] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *EUROCRYPT*, 2003.

[BPH15] Andrew Baumann, Marcus Peinado, and Galen Hunt. Shielding applications from an untrusted cloud with haven. *ACM Transactions on Computer Systems (TOCS)*, 33(3):8, 2015.

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In *CT-RSA*, volume 3376 of *LNCS*, pages 136–153. Springer, 2005.

[BW06] Xavier Boyen and Brent Waters. Compact Group Signatures Without Random Oracles. In *Advances in Cryptology – EUROCRYPT 2006*, pages 427–444, 2006.

[BW07] Xavier Boyen and Brent Waters. Full-Domain Subgroup Hiding and Constant-Size Group Signatures. In *PKC*, 2007.

[CDHK15] Jan Camenisch, Maria Dubovitskaya, Kristiyan Haralambiev, and Markulf Kohlweiss. Composable and modular anonymous credentials: Definitions and practical constructions. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 262–288, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

[CF13] Dario Catalano and Dario Fiore. Vector commitments and their applications. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013: 16th International Conference on Theory and Practice of Public Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 55–72, Nara, Japan, February 26 – March 1, 2013. Springer, Heidelberg, Germany.

[CFW12] Dario Catalano, Dario Fiore, and Bogdan Warinschi. Efficient network coding signatures in the standard model. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in*

Computer Science, pages 680–696, Darmstadt, Germany, May 21–23, 2012. Springer, Heidelberg, Germany.

[CKL+14] Jan Camenisch, Stephan Krenn, Anja Lehmann, Gert Læssøe Mikkelsen, Gregory Neven, and Michael Østergaard Pedersen. Formal treatment of privacy-enhancing credential systems. Cryptology ePrint Archive, Report 2014/708, 2014. http://eprint.iacr.org/2014/708.

[CKLM12] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Malleable proof systems and applications. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 281–300, Cambridge, UK, April 15–19, 2012. Springer, Heidelberg, Germany.

[CKLM13] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Malleable Signatures: Complex Unary Transformations and Delegatable Anonymous Credentials. IACR Cryptology ePrint Archive, 2013. http://eprint.iacr.org/.

[CKLM14] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Malleable signatures: New definitions and delegatable anonymous credentials. In *IEEE 27th Computer Security Foundations Symposium, CSF 2014*, pages 199–213, 2014.

[CL03] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN 02: 3rd International Conference on Security in Communication Networks*, volume 2576 of *Lecture Notes in Computer Science*, pages 268–289, Amalfi, Italy, September 12–13, 2003. Springer, Heidelberg, Germany.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 56–72, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

[CLD16] Victor Costan, Ilia A Lebedev, and Srinivas Devadas. Sanctum - Minimal Hardware Extensions for Strong Software Isolation. *USENIX Security Symposium*, 2016.

[COR99] Giovanni Di Crescenzo, Rafail Ostrovsky, and Sivaramakrishnan Rajagopalan. Conditional Oblivious Transfer and Timed-Release Encryption. In *EUROCRYPT*, 1999.

[CP93] David Chaum and Torben P. Pedersen. Wallet databases with observers. In Ernest F. Brickell, editor, *Advances in Cryptology – CRYPTO'92*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105, Santa Barbara, CA, USA, August 16–20, 1993. Springer, Heidelberg, Germany.

[CS97] Jan Camenisch and Markus Stadler. Efficient Group Signature Schemes for Large Groups. In *Advances in Cryptology – CRYPTO 1997*, pages 410–424, 1997.

[CS98] Ronald Cramer and Victor Shoup. A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack. In *CRYPTO*, pages 13–25, 1998.

[CS02] Ronald Cramer and Victor Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. In *EUROCRYPT*, 2002.

[CvH91] David Chaum and Eugène van Heyst. Group Signatures. In *EUROCRYPT*, volume 547 of *LNCS*, pages 257–265. Springer, 1991.

[CZ14] Yu Chen and Zongyang Zhang. Publicly evaluable pseudorandom functions and their applications. In *SCN*, 2014.

[DHS15] David Derler, Christian Hanser, and Daniel Slamanig. Revisiting cryptographic accumulators, additional properties and relations to other primitives. In Kaisa Nyberg, editor, *Topics in Cryptology – CT-RSA 2015*, volume 9048 of *Lecture Notes in Computer Science*, pages 127–144, San Francisco, CA, USA, April 20–24, 2015. Springer, Heidelberg, Germany.

[DP06] Cécile Delerablée and David Pointcheval. Dynamic Fully Anonymous Short Group Signatures. In *Progress in Cryptology – VIETCRYPT 2006*, pages 193–210, 2006.

[DS15] David Derler and Daniel Slamanig. Practical witness encryption for algebraic languages or how to encrypt under groth-sahai proofs. *IACR Cryptology ePrint Archive*, 2015:1073, 2015.

[DS16] David Derler and Daniel Slamanig. Fully-anonymous short dynamic group signatures without encryption. *IACR Cryptology ePrint Archive*, 2016:154, 2016.

[FHS17] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. *Journal of Cryptology (accepted, to appear)*, 2017. http://eprint.iacr.org/2014/944.

[FNV15] Antonio Faonio, Jesper Buus Nielsen, and Daniele Venturi. Predictable arguments of knowledge. *IACR Cryptology ePrint Archive, to appear at PKC 2017*, 2015.

[FO98] Eiichiro Fujisaki and Tatsuaki Okamoto. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In Kaisa Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 32–46, Espoo, Finland, May 31 – June 4, 1998. Springer, Heidelberg, Germany.

[Fre12] David Mandell Freeman. Improved security for linearly homomorphic signatures: A generic framework. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 697–714, Darmstadt, Germany, May 21–23, 2012. Springer, Heidelberg, Germany.

[Fuc09] Georg Fuchsbauer. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. Cryptology ePrint Archive, Report 2009/320, 2009. http://eprint.iacr.org/2009/320.

[Fuc11] Georg Fuchsbauer. Commuting signatures and verifiable encryption. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 224–245, Tallinn, Estonia, May 15–19, 2011. Springer, Heidelberg, Germany.

[GGH+13] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits. In *FOCS*, 2013.

[GGHW14] Sanjam Garg, Craig Gentry, Shai Halevi, and Daniel Wichs. On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input. In *CRYPTO*, 2014.

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness Encryption and its Applications. In *STOC*, 2013.

[Gha16] Essam Ghadafi. Short structure-preserving signatures. In Kazue Sako, editor, *Topics in Cryptology – CT-RSA 2016*, volume 9610 of *Lecture Notes in Computer Science*, pages 305–321, San Francisco, CA, USA, February 29 – March 4, 2016. Springer, Heidelberg, Germany.

[GKP+13] Shafi Goldwasser, Yael Tauman Kalai, Raluca A. Popa, Vinod Vaikuntanathan, and Nickolai Zeldovich. How to Run Turing Machines on Encrypted Data. In *CRYPTO*, 2013.

[GL06] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange[1]. *ACM Trans. Inf. Syst. Secur.*, 9(2), 2006.

[GLW14] Craig Gentry, Allison B. Lewko, and Brent Waters. Witness Encryption from Instance Independent Assumptions. In *CRYPTO*, 2014.

[Gro07] Jens Groth. Fully Anonymous Group Signatures Without Random Oracles. In *ASIACRYPT*, 2007.

[Gro10] Jens Groth. Short pairing-based non-interactive zero-knowledge arguments. In Masayuki Abe, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 321–340, Singapore, December 5–9, 2010. Springer, Heidelberg, Germany.

[Gro14] Thomas Groß. Efficient certification and zero-knowledge proofs of knowledge on infrastructure topology graphs. In *Proceedings of the 6th edition of the ACM Workshop on Cloud Computing Security (CCSW 2014)*, pages 69–80. ACM, 2014.

[Gro15a] Thomas Groß. Signatures and efficient proofs on committed graphs and NP-statements. In *19th International Conference on Financial Cryptography and Data Security (FC 2015)*, pages 293–314, 2015.

[Gro15b] Jens Groth. Efficient fully structure-preserving signatures for large messages. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 239–259, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT*, pages 415–432, 2008.

[HS14] Christian Hanser and Daniel Slamanig. Structure-Preserving Signatures on Equivalence Classes and their Application to Anonymous Credentials. In *ASIACRYPT*, 2014. Full Version: Cryptology ePrint Archive, Report 2014/705.

[ILV11] Malika Izabachène, Benoît Libert, and Damien Vergnaud. Block-wise P-signatures and non-interactive anonymous credentials with efficient attributes. In Liqun Chen, editor, *13th IMA International Conference on Cryptography and Coding*, volume 7089 of *Lecture Notes in Computer Science*, pages 431–450, Oxford, UK, December 12–15, 2011. Springer, Heidelberg, Germany.

[Jag15] Tibor Jager. How to Build Time-Lock Encryption. *IACR Cryptology ePrint Archive*, page 478, 2015.

[JL09] Stanislaw Jarecki and Xiaomin Liu. Private Mutual Authentication and Conditional Oblivious Transfer. In *CRYPTO*, 2009.

[JMSW02] Robert Johnson, David Molnar, Dawn Xiaodong Song, and David Wagner. Homomorphic signature schemes. In Bart Preneel, editor, *Topics in Cryptology – CT-RSA 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 244–262, San Jose, CA, USA, February 18–22, 2002. Springer, Heidelberg, Germany.

[KD04] Kaoru Kurosawa and Yvo Desmedt. A New Paradigm of Hybrid Encryption Scheme. In *CRYPTO*, 2004.

[KPSY09] Eike Kiltz, Krzysztof Pietrzak, Martijn Stam, and Moti Yung. A New Randomness Extraction Paradigm for Hybrid Encryption. In *EUROCRYPT*, 2009.

[KPW15] Eike Kiltz, Jiaxin Pan, and Hoeteck Wee. Structure-preserving signatures from standard assumptions, revisited. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 275–295, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[KV11] Jonathan Katz and Vinod Vaikuntanathan. Round-Optimal Password-Based Authenticated Key Exchange. In *TCC*, 2011.

[KY05] Aggelos Kiayias and Moti Yung. Group signatures with efficient concurrent join. In *EUROCRYPT*, 2005.

[KZG10] Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg. Constant-size commitments to polynomials and their applications. In Masayuki Abe, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 177–194, Singapore, December 5–9, 2010. Springer, Heidelberg, Germany.

[Lip12] Helger Lipmaa. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. In Ronald Cramer, editor, *TCC 2012: 9th Theory of Cryptography Conference*, volume 7194 of *Lecture Notes in Computer Science*, pages 169–189, Taormina, Sicily, Italy, March 19–21, 2012. Springer, Heidelberg, Germany.

[LKW15] Jia Liu, Saqib A. Kakvi, and Bogdan Warinschi. Extractable witness encryption and timed-release encryption from bitcoin. *IACR Cryptology ePrint Archive*, page 482, 2015.

[LLM+16] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, pages 373–403, 2016.

[LMPY16] Benoît Libert, Fabrice Mouhartem, Thomas Peters, and Moti Yung. Practical "Signatures with Efficient Protocols" from Simple Assumptions. In *Asia CCS*, 2016.

[LPJY13] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Linearly homomorphic structure-preserving signatures and their applications. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 289–307, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[LPY15] Benoît Libert, Thomas Peters, and Moti Yung. Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions. In *CRYPTO*, 2015.

[Mer88] Ralph C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378, Santa Barbara, CA, USA, August 16–20, 1988. Springer, Heidelberg, Germany.

[MRK03] Silvio Micali, Michael O. Rabin, and Joe Kilian. Zero-knowledge sets. In *44th Annual Symposium on Foundations of Computer Science*, pages 80–91, Cambridge, MA, USA, October 11–14, 2003. IEEE Computer Society Press.

[MRS+13] Richard Mortier, Charalampos Rotsos, David J Scott, Balraj Singh, Thomas Gazagnaire, Steven Smith, Jon Crowcroft, Anil Madhavapeddy, and Steven Hand. Unikernels: Library Operating Systems for the Cloud . *Architectural Support for Programming Languages and Operating Systems, ASPLOS*, pages 461–472, 2013.

[NS04] Lan Nguyen and Reihaneh Safavi-Naini. Efficient and Provably Secure Trapdoor-Free Group Signature Schemes from Bilinear Pairings. In *Advances in Cryptology – ASIACRYPT 2004*, pages 372–386, 2004.

[Ped92] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140, Santa Barbara, CA, USA, August 11–15, 1992. Springer, Heidelberg, Germany.

[PS16] David Pointcheval and Olivier Sanders. Short randomizable signatures. In Kazue Sako, editor, *Topics in Cryptology – CT-RSA 2016*, volume 9610 of *Lecture Notes in Computer Science*, pages 111–126, San Francisco, CA, USA, February 29 – March 4, 2016. Springer, Heidelberg, Germany.

[RSW96] Ronald L. Rivest, Adi Shamir, and David A Wagner. Time-lock puzzles and timed-release crypto. Technical report, Massachusetts Institute of Technology, 1996.

[SBZ02] Ron Steinfeld, Laurence Bull, and Yuliang Zheng. Content extraction signatures. In Kwangjo Kim, editor, *ICISC 01: 4th International Conference on Information Security and Cryptology*, volume 2288 of *Lecture Notes in Computer Science*, pages 285–304, Seoul, Korea, December 6–7, 2002. Springer, Heidelberg, Germany.

[SCF+15] Felix Schuster, Manuel Costa, Cédric Fournet, Christos Gkantsidis, Marcus Peinado, Gloria Mainar-Ruiz, and Mark Russinovich. Vc3: Trustworthy data analytics in the cloud using sgx. In *IEEE Symposium on Security and Privacy (2015)*, pages 38–54. IEEE, 2015.

[SG17] Ioannis Sfyrakis and Thomas Groß. UniGuard: Protecting Unikernels using Intel SGX. Technical Report CS-TR, Newcastle University, 2017.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *Advances in Cryptology – EUROCRYPT'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266, Konstanz, Germany, May 11–15, 1997. Springer, Heidelberg, Germany.

[SW05] Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. In *EUROCRYPT*, 2005.

[TPV17] Chia-Che Tsai, Donald E Porter, and Mona Vij. Graphene-sgx: A practical library os for unmodified applications on sgx. In *2017 USENIX Annual Technical Conference (USENIX ATC)*, 2017.

[Tru14] Trusted Computing Group. Trusted Platform Module Library Part 1: Architecture. Technical report, 2014. https://trustedcomputinggroup.org/tpm-library-specification/.

[Ver01] Eric R. Verheul. Self-blindable credential certificates from the Weil pairing. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 533–551, Gold Coast, Australia, December 9–13, 2001. Springer, Heidelberg, Germany.

[Wat05] Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.

[Wee10] Hoeteck Wee. Efficient Chosen-Ciphertext Security via Extractable Hash Proofs. In *CRYPTO*, 2010.

[Zha16] Mark Zhandry. How to Avoid Obfuscation Using Witness PRFs. In *TCC 2016-A*, 2016.