Project PROMETHEUS
PRivacy preserving pOst-quantuM systEms
from advanced crypTograpHic mEchanisms
Using latticeS

PROMETHEUS

D5.1

Survey of Existing Privacy-Preserving Cryptographic Protocols

Contractual submission date Month 10	Actual submisision date May 2019
Deliverable version 1.0	Main author Olivier Sanders (ORA)

http://www.h2020prometheus.eu/

h2020prometheus

PROMETHEUS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780701. The contents of this deliverable are the responsibility of the PROMETHEUS consortium, and do not necessarily reflect the official views of the European Union.

Document information

Grant agreement no.	780701
Project acronym	PROMETHEUS
Project full title	PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS
Type of action	Research and Innovation Action (RIA)
Topic	H2020-DS-06-2017-Cybersecurity PPP: Cryptography
Project dates	1st January 2018 (Month 1) / 31st December 2021 (Month 48)
Duration	48 months
Project URL	http://www.h2020prometheus.eu/
EU Project Officer	Carmen Ifrim

Work package	WP5 – Privacy-preserving protocols
Deliverable title	Survey of Existing Privacy-Preserving Cryptographic Protocols
Deliverable no.	D5.1
Deliverable version	1.0
Deliverable filename	`PROMETHEUS-WP5-D5.1.pdf`
Nature of deliverable	Report
Dissemination level	Public
Number of pages	31
Responsible partner	ORA (participant number 2)
Authors	Olivier Sanders (ORA), Javier Herranz (UPC) Thomas Ricosset ()

Abstract. This document is a survey of existing constructions for anonymous credentials, e-cash and e-voting. These primitives will be presented independently, leading to three main sections. Each section will be organized similarly, as follows. First, an introduction will explain the context and the concrete goals of the primitive. Next, the main state-of-the-art results related to the primitive will be presented, even if they do not concern lattices. For this section, we will highlight the different frameworks followed by existing constructions and present the properties that they achieve. Finally, we will describe existing lattice-based solutions, with special focus on the tools used to construct them.

Keywords: Anonymous credentials, e-cash, e-democracy.

Signatures

Written by	Olivier Sanders	ORA	May 2019
Reviewed by	Javier Herranz	UPC	12/03/2019
Approved by	Benoît Libert as WP coordinator	UPC	07/05/2019
Approved by	Sébastien Canard as Technical leader	ORA	07/05/2019

Partners

ENSL	ENS de Lyon
ORA	Orange SA
CWI	Stiching Centrum Voor Wiskunde En Informatica
IDC	IDC Herzliya
RHUL	Royal Holloway, University of London
RUB	Ruhr-Universität Bochum
SCYTL	Scytl Secure Electronic Voting, S.A.
THA	Thales Communications & Security S.A.S.
TNO	TNO
UPC	Universitat Politècnica de Catalunya · BarcelonaTech
UR1	Université de Rennes 1
WEI	Weizmann Institute of Science

1 Introduction

Privacy preserving cryptography encompasses all cryptographic initiatives that aim at minimizing the amount of information leaked by citizens/consumers in their daily lives. Although all these protocols fundamentally share the same goal, they face very different scenarios and thus need specific solutions. In this document, we will group them into three important branches, namely anonymous credentials, electronic cash (e-cash) and electronic voting.

Anonymous credential is the generic term used in cryptography to denote protocols allowing users to authenticate themselves as legitimate customers of some services, while remaining anonymous. It departs from traditional cryptography that usually relies on non-anonymous certificates (digital signatures) for this task. It is probably the most prolific area of privacy preserving cryptography and has known important industrial successes, with more than 500 millions trusted platform modules [TCG] embedding Direct Anonymous Attestations [BCC04] and billions of Intel processors implementing EPID systems [AlL16]. The hardness of designing such primitives stems from the need to retain accountability/revocability while providing anonymity. This usually implies the use of quite complex cryptographic tools which are particularly difficult to instantiate in post-quantum settings. We provide an extended survey in Section 2.

Electronic cash is the digital counterpart of conventional cash with a specific focus on users' privacy. Although it shares several commonalities with anonymous credentials, the main difficulty here is to deter money replication. Addressing this problem while retaining anonymity has proved very difficult and it took several decades to construct really practical solutions. Unfortunately, the latter are not quantum resistant and the techniques used to design them do not translate well in the lattice settings. In Section 3, we recall the main results on e-cash along with the open problems in this area.

Electronic voting is a major tool to strengthen citizen involvement in the community matters and has been increasingly adopted in the world. Beyond just mimicking traditional voting, electronic voting offers very interesting features, such as verifiability which enables any citizen to check that the voting process has been honestly carried out. Conceptually, it is quite different from previous primitives and it relies on a broader set of cryptographic building blocks, including for example mix-nets, blind signature or homomorphic encryption. Designers of such systems must additionally address several challenges that we present in Section 4.

Most of the constructions given in this document refer to some cryptographic building blocks. The aim of D5.1 is not to give all the details on these ones, but explain how they can be used to design privacy-preserving cryptographic protocols. Such additional information are given in PROMETHEUS D4.1 deliverable on "Survey of existing building blocks for practical advanced protocols" and an interested reader can refer to this document for getting those details.

2 Anonymous Credentials

2.1 Introduction

Usually, electronic authentication is done via identification, i.e., a user supplies his identity and proves possession of some secret in order to gain some service or resource. Because user identities are readily available to service providers, these latter can exchange collected data about any particular user among themselves.

Anonymous credentials allow to mitigate such privacy breaches and to give the user more control over her data. Informally, as explained in [BBB$^+$18], a user acts under an arbitrary number of unlinkable pseudonyms rather than under his identity. Any two services know a user under different pseudonyms, making it hard to link user data between the two services. A user may even generate multiple pseudonyms for the same service, allowing her to partition generated user data between several of them. In the most extreme case, a user may choose a new pseudonym for every single transaction with any service, making all user actions unlinkable. Usually, different users have different access rights to some services. In anonymous credentials, these access rights are described by *attributes*. A service provider can issue a *credential* to a user, which is parameterized with attributes. These attributes can, for example, encode access rights to a service or some user data. The user can then *prove possession of a credential* to the same or to other service providers in a privacy-preserving way. This process is called *showing* a credential. This mechanism essentially allows users to carry (authenticated) data and access restrictions when confronted with anonymous users. Note that in this scenario, the user is in full control of her data and can actively decide what parts of it to reveal to service providers.

A credential may be, for example, used to encode citizen cards issued by the government. Through this credential, the state certifies attributes such as "citizenship", "student status", and "age". The citizen can store this credential, for example, on her smartphone and use it to prove statements about her certified attributes while staying unlinkable across services. The showing of credentials will be done via wireless communications channels of the smartphone, e.g., NFC. As an example, a public transportation provider may provide ticket discounts to students, young people, and senior citizens. To get the discount in this scenario, the user would need to prove possession of a credential whose attributes satisfy the complex policy: "registered" and "country A" and ("student" or "age" ≤ 17 or "age" > 65). It is a challenge to do this without disclosing the user's specific attribute values to the transportation provider. Note that disclosing (some of) the user's specific attribute values gives the provider quite specific information about the user, which may be used to de-anonymize her. Ideally, the transportation provider only learns a single bit about the attributes, namely that they satisfy the policy.

2.2 Main Results

Anonymous credentials were first suggested by Chaum [Cha85] and efficiently realized at first by Camenisch and Lysyanskaya [CL01, CL02]. They involve one or more credential issuer(s) and a set of users who have a long-term secret key which constitutes their digital identity and pseudonyms that can be seen as commitments to their secret key. Users can dynamically obtain credentials from an issuer that only knows users' pseudonyms and obliviously certifies users' secret keys as well as (optionally) a set of attributes. Later on, users can make themselves known to verifiers under a different pseudonym and demonstrate possession of the issuer's signature on their secret key without revealing neither the signature nor the key (nor the attributes they have). Anonymous credentials typically consist of a protocol whereby the user obtains the issuer's signature on a committed message, another protocol for proving that two commitments open to the same value (which allows proving that the same secret underlies two distinct pseudonyms) and a protocol for proving possession of a secret message-signature pair.

As proven by the different constructions of Camenisch and Lysyanskaya [CL01, CL02, CL04], an anonymous credential system can be built from the following five primitives:

1. a commitment scheme,
2. a signature scheme,
3. a protocol to obtain a signature on a commited value without revealing the value to the signer (also known signature with efficient protocols),
4. a ZKPoK protocol to prove knowledge and equality of two commited values,
5. a ZKPoK protocol to prove knowledge of a signature on a committed value.

To create a practical solution, the three last primitives must be very efficient, since these typically are the bottleneck of a system. Then, most approaches aim at designing new commitment and signature schemes, from which very efficient ZKPoK protocols can be built. The first efficient constructions were given by Camenisch and Lysyanskaya under the Strong RSA assumption [CL01, CL02] or using bilinear groups [CL04]. Other solutions were subsequently given with additional useful properties such as opening (allowing an authority to lift the anonymity in case of misbehavior), non-interactivity [BCKL08], delegatability [BCC$^+$09] or support for efficient attributes [CG08a] (see [CKL$^+$14] and references therein). There are also several different approaches, based on other cryptographic building blocks, such as sanitizable signatures [CL13] or aggregate signatures [CL11].

Anonymous credentials with attributes are often obtained by having the issuer obliviously sign a multi-block message $(\mathfrak{m}_1, \ldots, \mathfrak{m}_N)$, where one block is the secret key while other blocks contain public or private attributes. Note that, for the sake of keeping the scheme compatible with zero-knowledge proofs, the blocks $(\mathfrak{m}_1, \ldots, \mathfrak{m}_N)$ cannot be simply hashed before getting signed using a ordinary, single-block signature. Such technique necessitates the use of signature schemes with efficient protocols [CL01] (a.k.a. structure-preserving signatures [AFG$^+$10]).

In a different approach, it appeared since the work of Chaum and van Heyst [Cv91] that group signatures share a lot of properties with anonymous credentials. Indeed, as mentioned in [BCN18] and [dLS18], group signatures can be constructed from non-interactive anonymous credentials with opening and vice versa.

Group signatures are a central anonymity primitive, introduced by Chaum and van Heyst [Cv91] in 1991, which allows members of a group managed by some authority to sign messages in the name of the entire group. At the same time, users remain accountable for the messages they sign since an opening authority can identify them if they misbehave.

Ateniese, Camenisch, Joye and Tsudik [ACJT00] provided the first scalable construction meeting the security requirements that can be intuitively expected from the primitive, although clean security notions were not available yet at that time. Bellare, Micciancio and Warinschi [BMW03] filled this gap by providing suitable security notions for static groups, which were subsequently extended to the dynamic setting[1] by Kiayias and Yung [KY06] and Bellare, Shi and Zhang [BSZ05]. In these models, efficient schemes have been put forth in the random oracle model [KY06, DP06] (the ROM) and in the standard model [Gro07, AFG$^+$10, ACD$^+$12].

[1] By "dynamic setting", we refer to a scenario where new group members can register at any time but, analogously to [BSZ05, KY06], we do not consider the orthogonal problem of user revocation here.

2.3 Lattice-based Construction

Lattice-based group signatures were put forth for the first time by Gordon, Katz and Vaikuntanathan [GKV10] whose solution had linear-size signatures in the number of group members. Camenisch, Neven and Rückert [CNR12] extended [GKV10] so as to achieve anonymity in the strongest sense. Laguillaumie *et al.* [LLLS13] decreased the signature length to be logarithmic in the number N of group members. While asymptotically shorter, their signatures remained space-consuming as, analogously to the Boyen-Waters group signature [BW06], their scheme encrypts each bit of the signer's identity individually. Simpler and more efficient solutions with $\mathcal{O}(\log N)$ signature size were given by Nguyen, Zhang and Zhang [NZZ15] and Ling, Nguyen and Wang [LNW15]. In particular, the latter scheme [LNW15] achieves significantly smaller signatures by encrypting all bits of the signer's identity at once. Benhamouda *et al.* [BCK$^+$14] described a hybrid group signature that simultaneously relies on lattice assumptions (in the ring setting) and discrete-logarithm-related assumptions. Recently, Libert, Ling, Nguyen and Wang [LLNW16] obtained substantial efficiency improvements via a construction based on Merkle trees which eliminates the need for GPV trapdoors [GPV08].

All these lattice-based group signatures are designed for static groups and analyzed in the model of Bellare, Micciancio and Warinschi [BMW03], where no new group member can be introduced after the setup phase. This is somewhat unfortunate given that, in anonymous credentials systems, the dynamicity property is arguably what we need. To date, it remains an important open problem to design an efficient lattice-based system that supports dynamically growing population of users in the models of [BSZ05, KY06]. Recently, Libert, Ling, Mouhartem, Nguyen and Wand [LLM$^+$16] presented a first solution to this problem built on the SIS-based signature of Böhl *et al.* [BHJ$^+$15], which is itself a variant of Boyen's signature [Boy10].

Boschini, Camenisch and Neven [BCN18] described the first efficient lattice-based anonymous credentials system. , their scheme is based on a signature and a commitment scheme with efficient zero-knowledge proofs using Lyubashevsky's Fiat-Shamir with aborts technique. Most lattice-based zero-knowledge proofs are either Fiat-Shamir proofs with single-bit challenges or Stern-type proofs [Ste96]. Because of the large soundness error (i.e. the probability that a cheating prover can convince the honest verifier that a false statement is true) of 1/2 and 2/3 that these proofs incur, respectively, they have to be repeated many times in parallel, which comes at a considerable cost in efficiency. Lyubashevsky's Fiat-Shamir with aborts technique [Lyu09] yields much more efficient proofs with large challenges, but these proofs have the disadvantage that they are relaxed, in the sense that extracted witnesses are only guaranteed to lie in a considerably larger domain than the witnesses used to construct the proof.

Del Pino, Lyubashevsky and Seiler [dLS18] presented a group signature scheme, based on the hardness of lattice problems, whose outputs are almost a 2 order of magnitude smaller than [LLM$^+$16] and an order of magnitude smaller than [BCN18]. They also provide the first experimental implementation of lattice-based group signatures demonstrating that their construction is practical with less than half a second per operation on a standard laptop. For the signing keys of the group members one needs to sample preimages of a linear map from discrete Gaussian distribution. This can, in theory, be done with GPV sampling algorithm from [GPV08], but it requires computing the Gram-Schmidt decomposition of a basis which is a prohibitively expensive operation in the high dimensions required for their scheme. They have therefore implemented the Fast Fourier Orthogonalization algorithm from [DP16] adapted to cyclotomic fields which computes a compact LDL^* decomposition of the basis that is used in a Fast Fourier Nearest Plane algorithm, also from [DP16], to sample preimages. This was done before in the Falcon signature scheme [PFH$^+$17], but contrary to Falcon, the scheme presented in [dLS18] needs arbitrary precision complex arithmetic since double precision is not enough for their larger moduli.

3 E-Cash

3.1 Introduction

Electronic payment systems offer high usage convenience to their users but at the cost of their privacy. Indeed, transaction informations, such as payee's identity, date and location, allow a third party (usually, the financial institution) to learn a lot of things about the users: individuals' whereabouts, religious beliefs, health status, etc, which can eventually be quite sensitive.

However, secure e-payment and strong privacy are not incompatible, as shown by Chaum in 1982 [Cha82] when he introduced the concept of electronic cash (*e-cash*). Informally, e-cash can be thought of as the digital analogue of regular cash with special focus on users' privacy. Such systems indeed consider three kind of parties: the bank, the user and the merchant. The bank issues coins that can be withdrawn by users and then spend to merchants. Eventually, the latter deposit the coins on their account at the bank. Compared to other electronic payment systems, the benefit of e-cash systems is that the bank is unable to identify the author of a spending. More specifically, it is unable to link a particular withdrawal -even if it knows the user's identity at this stage- to a spending nor to link two spendings performed by the same user.

At first sight, this anonymity property might seem easy to achieve: one could simply envision a system where the bank would issue the same coin (more specifically, one coin for each possible amount) to each user. Such a system would obviously be anonymous but it would also be insecure. Indeed, although e-cash aims at mimicking regular cash, there is an intrinsic difference between them: e-cash, as any electronic data, can easily be duplicated. This is a major issue because it means that a user could spend the same coin to different merchants. Of course, some hardware countermeasures (such as storing the coins on a secure element) can be used to mitigate the threat but they cannot remove it. Moreover, the prospect of having an endless (and untraceable) reserve of coins will constitute a strong incentive to attack this hardware whose robustness is not without limits.

To deter this bad behaviour, e-cash systems must therefore enable (1) detection of re-used coins and (2) identification of defrauders. Besides invalidating the trivial solution sketched above (the fact that everyone uses the same coin prevents any identification procedure) these requirements impose very strong constraints on e-cash systems. They indeed mean that users should be anonymous as long as they act honestly while being traceable as soon as they will begin to overspend even one cent.

The idea of Chaum, taken up by all subsequent works, was to associate each withdrawn coin with a unique identifier called a "serial number"[2]. The latter remains unknown to all parties, except the user, until the coin is spent. At this time, it becomes

[2] Actually, this specific terminology appeared later [CFN90] but this notion is implicit in the Chaum's paper

public and so can easily be compared to the set of all serial numbers of previously spent coins. A match then acts as a fraud alert for the bank which can then run a specific procedure[3] to identify the cheater.

Unfortunately, by reproducing the features of regular cash, e-cash also reproduces its drawbacks, in particular the problem of paying the exact amount. Worse, the inherent limitations of e-cash compound this issue that becomes much harder to address in a digital setting. This has led cryptographers to propose a wide variety of solutions to mitigate the impact on user's experience. They include for example on-line e-cash, transferable e-cash or divisible e-cash that we describe in the next section.

Finally, we note that a confusion might occur between e-cash systems and the so-called cryptocurrencies since the introduction of Bitcoin [Nak08]. Although they are all electronic payment systems, we stress that they are very different in essence. Indeed, the goal of e-cash is to provide an anonymous plug-in replacement to current electronic payment systems. In particular, e-cash does not intend to change the existing trust model nor to remove one of the actors. Contrarily, the goal of cryptocurrencies is to remove the trusted authority (namely, the bank) on which all current payment systems are built. Moreover, while most cryptocurrencies provide a certain level of anonymity we note that it is usually limited compared to e-cash. For example, the privacy of Bitcoin users is only protected by a pseudonyms system that still allows to trace user's spendings across the blockchain.

The very different natures of e-cash systems and cryptocurrences make them very difficult to compare. Nevertheless, we note that the strength of cryptocurrencies, namely the lack of trusted authority, can also be a drawback for the general public. Indeed, in case of loss or theft of his keys, a user has no one to turn to, meaning that his money is definitively lost. It is akin to a situation where a bank consumer would definitively lose access to his account if he lost his payment card. Conversely, e-cash systems efficiently support backup procedures, and more generally, can deal with any problem with a minimum impact on user's experience.

3.2 Main Results

The original solution proposed by Chaum for anonymous payment was based on the concept of blind signature. This primitive, later formalized in [PS96, PS00], allows anyone to get a signature σ on a message m that is unknown to the signer. Moreover, the latter will be unable to link the pair (σ, m) to a specific issuance. Applying this idea to the payment context leads to the following e-cash system. A coin is a blind signature issued by a bank to a user during a withdrawal. To spend his coin, the user simply shows the signature to a merchant who is able to verify it using the bank's public key. Two cases may then appear. Either the e-cash system does not allow identification of defrauders, in which case the bank must be involved in the protocol to check that this coin has not already been spent. The resulting system is then referred to as *on-line* e-cash. Otherwise, the coin may be deposited later to the bank, leading to an *off-line* e-cash system. Obviously, the latter solution is preferable since it avoids a costly connection to the servers of the bank during the payment. In the following, we will only consider off-line e-cash systems.

Theoretically, the problem of anonymous payment is thus solved by blind signatures for which several instantiations have been proposed (see *e.g.* [PS00]). However,

[3]This procedure usually consists in combining the information of the fraudulent spendings -there are at least two of them, by definition- to recover the identity of the spender

as we mention in the previous section, it remains to address the problem of paying the exact amount, which becomes trickier in a digital setting. Indeed, let us consider a consumer that owns a coin whose denomination is 10 € and that wants to pay 8.75 €. A first solution could be to contact his bank to exchange his coin against coins of smaller denominations but this would actually reintroduce the bank in the spending process and so would rather correspond to an on-line system. It then mainly remains two kind solutions: those where the merchant gives change and those that only use coins of the smallest possible denomination (*e.g.* 0.01 €). They both gave rise to two main streams in e-cash: *transferable* e-cash and *compact/divisible* e-cash.

Let us go back to our example. At first sight, the simplest solution (inspired from regular cash) is the one where the merchant gives change, by returning, for example, a coin of 0.05 €, one of 0.20 € and one of 1 €. However, by receiving coins, the user technically becomes a merchant (in the e-cash terminology) which are not anonymous during deposit. Therefore, the only way to retain anonymity in this case is to ensure transferability of the coin, meaning that the user will be able to re-spend the received coins instead of depositing them. While this is a very attractive feature, it has unfortunately proved very hard to achieve. Worse, Chaum and Pedersen [CP93] have shown that a transferable coin necessarily grows in size after each spending. Intuitively, this is due to the fact that the coins must keep information about each of its owner to ensure identification of defrauders. In the same paper, Chaum and Pedersen also proved that some anonymity properties cannot be achieved in the presence of an unbounded adversary. Their result was later extended by Canard and Gouget [CG08b] who proved that these properties were also unachievable under computational assumptions. More generally, identifying the anonymity properties that a transferable e-cash system can, and should, achieve has proved tricky [CG08b, BCFK15].

All these negative results perhaps explain the small number of results on transferable e-cash, and even quite recent constructions ([CGT08, BCF$^+$11, BCFK15]) are too complex for a large-scale deployment or rely on a very unconventional model [FPV09]. In particular, none of them achieves optimality with respect to the size, meaning that the coin grows much faster than the theoretical pace defined by Chaum and Pedersen.

Now let us consider our spending of 8.75 € in the case where all coins are of the smallest possible denomination. This means that the user no longer has a coin of 10 € but now has 1000 coins of 0.01 €. Such a system can handle any amount without change but must provide an efficient way to store and to spend hundreds of coins at once. A system offering efficient storage is said *compact* and a system supporting both efficient storage and spending is said *divisible*.

Anonymous compact e-cash was proposed by Camenisch, Hohenberger and Lysyanskaya [CHL05] and was informally based on the following idea. Let N be the amount of a wallet withdrawn by a user (*i.e.* the wallet contains N coins that all have the same value). During a withdrawal, a user gets a certificate on some secret value s[4] defining a pseudo-random function (PRF) F_s. The latter defines in turn the serial numbers of the N coins as $F_s(i)$ for $i \in [0, N-1]$.

To spend the i-th coin, a user then essentially reveals $F_s(i)$ and proves, in a zero-knowledge way, that it is well-formed, *i.e.* that (1) s has been certified and that (2) the serial number has been generated using F_s on an input belonging to the set $[0, N-1]$. All of these proofs can be efficiently instantiated in a bilinear setting. Anonymity follows from the zero-knowledge property of the proofs and from the properties of

[4]several efficient protocols exist, such as the ones described in [CL04, PS16]

the pseudo-random function: intuitively it is hard to decide if $F_s(i)$ and $F_s(j)$ have been generated using the same function F_s.

Unfortunately, compact e-cash only provides a partial answer to the practical issues of spendings: storage is very efficient but the coins must still be spent one by one which quickly becomes cumbersome. An ultimate answer to this issue was then provided by Okamoto and Ohta [OO92] and later named *divisible* e-cash. The core idea of divisible e-cash is that the serial numbers of a divisible coin[5] can be revealed by batches, leading to efficient spendings.

Intuitively, the main difference with compact e-cash is that the serial numbers are now generated by a *constrained* PRF, a notion formalized much later by Boneh and Waters [BW13]. A constrained PRF allows the owner of the secret key to output a constrained key $k_{\mathcal{S}}$ allowing to evaluate the PRF only on the elements of S. By revealing $k_{\mathcal{S}}$ during a spending, the user enables the merchant (and then, the bank) to recover all the serial numbers generated from $\mathcal{S}$. This concretely means that he only has to send one element ($k_{\mathcal{S}}$) to spend $|\mathcal{S}|$ coins at once which explains the theoretical efficiency of such systems.

However, in practice, several problems arise if one wants to ensure both anonymity and security of the resulting construction. First, (1) the validity of the constrained key should be efficiently checkable in a zero-knowledge way. Second, (2) constrained keys generated from the same master key (but for disjoint subsets) should be unlinkable. Finally, (3) the constrained key $k_{\mathcal{S}}$ should provide no information on the subset $\mathcal{S}$ itself.

Providing all these features at once in an efficient scheme has proved very difficult. The original construction of Okamoto and Ohta failed to achieve anonymity (the uses of different parts of the coins were traceable) but provided a framework that have been used for decades until very recently [PST17]. Their divisible coin was defined by a binary tree whose leaves correspond to the coins and so were associated with serial numbers. More specifically, the binary tree was defined recursively from the root: given a node, one can compute its descendants by using one-way functions as in [GGM84]. Therefore, during a spending, the user can simply reveal the value (the constrained key) associated with a node, allowing anyone to recover the 2^{ℓ} serial numbers (where ℓ depends on the depth of the node) associated with the descendant leaves of the node. Their PRF was then *prefix-constrained*.

For decades, the main goal of designers of divisible e-cash systems has then be the construction of such a PRF achieving all the features (especially compatibility with zero-knowledge proofs) presented above. The first ones to succeed were Canard and Gouget [CG07] but their scheme was totally unpractical. They later proposed an improvement [CG10] but the resulting scheme was still very complex. Meanwhile, some other solutions were proposed achieving either better efficiency [ASM08] or security (proof in the standard model) [IL13]. However, both of them were unsatisfactory: the former relies on a very unconventional model while the latter suffers from a very inefficient double-spending detection procedure.

The first efficient construction was proposed in 2015 [CPST15a] and improved in [CPST15b]. It was based on a common tree structure for all coins, leading to very efficient zero-knowledge proofs and so very efficient spendings. Indeed, implementations on a SIM card show that spendings and verification can be performed in less than 300 ms, proving that divisible e-cash can be truly practical.

[5] The terminology can be confusing here: the “divisible coin” considered by most of the papers corresponds to the “wallet” of a compact e-cash system. In particular, the divisible coin contains several coins that are all associated to a serial number

As we mention, for 25 years, divisible e-cash have used prefix-constrained PRF (inherent to the tree-based construction) leading to a logarithmic complexity of spendings since serial numbers can only be revealed by batches of 2^ℓ. Very recently, Pointcheval, Sanders and Traoré [PST17] proposed a constrained PRF allowing to generate a constrained key of constant-size for any subinterval $[i, j]$ of $[0, N-1]$. Not only does this allow to reveal any amount of serial numbers (not just powers of 2) but this also facilitates management of the coin, as explained in their paper. Moreover, their PRF complies with the requirements (1), (2) and (3) above, leading to the first efficient constant-size e-cash system.

3.3 Lattice-based Construction

As we explain, e-cash constructions that support at least compact storage, *i.e.* compact e-cash, are based on an intricate combination of zero-knowledge proofs, pseudorandom functions and digital signature schemes. Designing such schemes for cyclic groups is thus already a complex task, but it becomes even worse for lattices where each of these building blocks (in particular zero-knowledge proofs) is much harder to instantiate. This explains the lack of constructions in this setting. Actually, there exists only one system [LLNW17] that was recently proposed by Libert *et al.*

At the core of this system, there are new zero-knowledge arguments to prove the correct evaluation of LWR-based PRFs, in particular the one proposed by Boneh *et al* [BLMR13]. We indeed note that PRFs based on the LWE problem are unsuitable for e-cash since their non-deterministic errors are likely to prevent any detection of frauds. The Learning-with-Rounding problem, introduced by Banerjee, Peikert and Rosen [BPR12], seems therefore the most promising one to build lattice-based e-cash systems.

Proving correct evaluation of a LWR-based PRF requires at some step a proof that the rounding operation has been properly carried out. Concretely, this means that for some dimension $m > 1$ and moduli $q > p \geq 2$, one must prove knowledge of some vector $\mathbf{x} \in \mathbb{Z}_q^m$ such that $\mathbf{y} = \lfloor (p/q) \cdot \mathbf{x} \rfloor \bmod p$, where y is the output of the PRF. Unfortunately, this formula is not suitable for Stern-like protocols [Ste96] that constitutes the basis of the zero-knowledge arguments from [LLNW17].

However, the authors observed that the knowledge of such $\mathbf{x}$ was equivalent to the one of two vectors $\mathbf{x}$, $\mathbf{z} \in [0, q-1]^m$ such that $p.\mathbf{x} = q.\mathbf{y} + \mathbf{z}$, the latter formula being easier to handle with Stern-like protocols. Actually, it fits the Ling *et al*'s decomposition-extension framework [LNSW13] from which one can derive concrete zero knowledge arguments.

The authors additionally showed how to prove that the other steps of the PRF evaluation have been correctly carried out and so overcame the main difficulty of designing an e-cash scheme. Indeed, combining these proofs with one of knowledge of a Libert *et al*' signature [LLM$^+$16] on the seed of the PRF leads to the first e-cash system in the lattices setting.

The result of [LLNW17] is significant in the sense that it is the first lattice-based e-cash system, thus demonstrating the theoretical feasibility of this concept. Unfortunately, it suffers from a very high complexity that prevents any use on standard devices and so can only be considered as a proof of concept. Intuitively, the problem comes from its high reliance on Stern-like protocols whose soundness error is quite high (2/3). To achieve reasonable level of security, it is thus necessary to repeat such protocols a large of number of times, which entails (at least) a high communication complexity. Moreover, Stern-like proofs usually need vector whose coordinates belong to small sets (*e.g.* $\{-1, 0, 1\}$) to comply with the permutation requirements inherent to such protocols. It imposes the use of decomposition-extension techniques that are well-known but that imply an important increase of the dimensions of the involved matrices and vectors, and hence of the overall complexity.

Nevertheless, we note that the situation was similar for cyclic groups, with a first construction [CG07] that was deemed impractical [ASM08, CG10] but that encouraged new constructions culminating with truly efficient systems [CPST15a, PST17]. We may therefore hope that the Libert *et al*'s result is the first of a series of work that will dramatically improve the efficiency of this primitive in a lattice setting.

4 Electronic Voting

4.1 Introduction

Protocols for e-democracy contain several types of processes, from Internet voting systems to new tools which enforce citizen participation and involvement in the community matters, such as liquid democracy processes.

In this document we will concentrate on Internet voting systems. In recent years, several countries have been introducing electronic voting systems as a way to improve their democratic processes: e-voting allows more accurate and fast vote counts, reduces the logistic cost of organizing an election and also offers specific mechanisms for voters with disabilities to cast their votes independently. In particular, Internet voting systems provide voters with the chance to cast their votes from anywhere: their homes, hospitals, or even from foreign countries in case they are abroad at the time of the election.

Requirements for Internet voting systems include privacy and verifiability. Privacy requires both that voters are given the opportunity to cast their vote privately in conditions of confidentiality (coercion-resistance) as well as the *anonymity* of their choices: namely, that it is not possible to link the content of a vote to the identity of the voter. At the same time, it has to be ensured that only eligible voters can cast a vote, and that only one vote per voter is counted. Regarding *verifiability*, everybody should be able to check that all the parties in a voting system (voters, devices and the different entities) have behaved honestly.

A basic approach for an electronic voting scheme is to combine encryption and digital signature schemes: encryption schemes are used for providing secrecy of information transmitted among two parties, in front of external observers. Signature schemes are used in order to ensure the integrity of the transmitted messages, as well as providing assurance of the origin of such messages. This means that an external entity cannot modify or forge a message without being detected by the intended receiver.

In this basic approach, voters encrypt their messages prior to casting them, in such a way that only the intended recipient - the electoral board, or the electoral commission - is able to decrypt them and see their content. After encryption and prior to casting, voters also digitally sign their votes, in order to prove later on to the election authorities that they have been cast by eligible voters. This approach is similar to the traditional process in which a voter who casts her vote by postal mail digitally signs the outer envelope of her vote. Digital signatures allow identification of the voter who casts a vote, and therefore can also be used in order to discern whether a voter tries to cast a vote twice. Also in a similar way as in postal voting, outer envelopes are removed after verification of the signature, and prior to the recovery of the clear vote by decryption. Therefore, a clear vote cannot be connected to a voter's identity.

The security measures based on vote encryption and digital signatures seem enough to protect voters' privacy. However, these measures are only efficient during the voting process. During the election tally, decrypted votes could still be correlated with the voters who submitted them, by checking the order in which votes are decrypted: decrypted votes can be correlated to the voter identities by checking the digital signature of the encrypted votes stored in the ballot box in the same order. Therefore, encrypting and signing is not enough to ensure anonymity, and more advanced cryptographic protocols have to be used.

We review here three different ways to ensure anonymity in a voting system. The last one, tallying, is only valid for specific types of elections: a set of independent questions, each one with a small set of possible answers.

4.1.1 Anonymity (I): MixNets

In these protocols, voters cast encrypted and digitally signed votes which are stored in the ballot box until the end of the voting phase. Then, the votes are detached from their signatures and passed through a mix-net [Cha81], which is composed of several nodes which shuffle the votes sequentially using a secret permutation. The purpose of the mix-net is to output votes which cannot be linked with those that were stored in the ballot box, originally signed by the voters.

There are two kinds of mix-nets.

- Decryption mix-nets: Votes are encrypted in several layers (as many as nodes in the mix-net), using in each layer the key from the corresponding node. When encrypted votes are provided to the mix-net, each node permutes the input encrypted votes and uses its key to remove the outer encryption layer. This process is repeated at each node until it reaches the last one, where the last encryption layer is removed and the original vote contents are obtained.

- Re-encryption mix-nets: Votes are encrypted using an encryption scheme which allows re-encryption or re-randomization of the ciphertexts multiple times, while only one decryption step is needed to recover the plaintexts. Each node, in turn, permutes the input encrypted votes and re-encrypts / re-randomizes them in order to make them look totally different than in the input (the combination of permutation and re-randomization of the ciphertexts is called a shuffle). Finally, a decryption step is done in the last node of the mix-net in order to recover the plaintexts.

Due to the fact that the mix-net modifies the output votes in such a way that they cannot be related to those at the input, it may easily erase and insert votes without detection. Therefore, verification methods have to be put in place in order to ensure that the mix-net behaves properly. Verifiable mix-nets are mix-nets which provide mathematical (cryptographic) proofs which demonstrate that they do not modify the processed votes during the mixing process. These proofs are designed in such a way that they do not rely on providing secret information, as the secret permutation or private keys, for proving their correct behavior. Instead, they use zero-knowledge proofs which can be verified using public information.

For instance, in the case of re-encryption mix-nets, each mix server has to prove that its shuffling operation was properly conducted: namely, it has to demonstrate that its output ciphertexts were really obtained by permuting re-randomized versions of its input ciphertexts.

4.1.2 Anonymity (II): Two Agencies and Blind signatures

The two agencies model, first proposed in 1992, allows a voter to cast her vote anonymously, but at the same time checks that such voter is eligible to vote in the election. In order to do that, two server-side entities participate during the voting phase:

- The Validator Service: authenticates the voter, verifies her eligibility and allows her to vote in an anonymous way using an anonymous token.
- The Voting Service: receives encrypted votes with anonymous tokens from voters, and accept them after verifying that their tokens have been issued by the Validation Service.

This kind of scheme usually employs blind signatures [Cha82]. Blind signatures allow an entity to digitally sign a message without viewing its content: the requester of the signature sends a blind message to the signer, who digitally signs it and returns it to the requester. The requester can then remove the blinding factor from the message, and obtains a digitally signed message.

With this mechanism, the Validator Service can digitally sign the authorization token without viewing its content. The voter, after removing the blinding factor, sends the signed token to the Voting Service, which validates the token. A coalition of Validation Service and Voting Service cannot trace a token back to the voter since, due to the properties of blind signatures, the first one (who knows the identity of the voter), did not see the token in clear, but a blind version of it. After the voting phase, votes are decrypted to perform the tally. The voters' privacy is preserved, since the votes to be decrypted are not linked to voter identities.

The two agencies idea has also been used in [CSST06] by using a variant of group signatures called list signatures.

4.1.3 Anonymity (III): Tallying

In some elections, the final result can be thought as an (arithmetic) operation applied to all the submitted clear votes. For instance, in a referendum each voter may choose the clear vote 1 for "yes", and the clear vote 0 for "no". The sum of all the clear votes gives the number of voters who chose "yes".

Since the votes are encrypted, what is needed is an encryption scheme with homomorphic properties: combining (in a public way) an encryption of m_1 with an encryption of m_2 results in an encryption of $m_1 + m_2$, for instance.

With such an homomorphic encryption scheme, an election with tallying works as follows: (i) every signer sends his signed encrypted vote, maybe along with a proof that the encrypted vote is a valid one; (ii) votes with a valid signature pass to the final box, still encrypted, but without the signatures; (iii) all the ciphertexts are combined to produce the encrypted version of the final result of the election; (iv) the owner(s) of the secret key of the election run decryption of a single ciphertext. Since individual ciphertexts are never decrypted, the privacy and anonymity of the users is preserved.

4.1.4 Verifiability

Verifiability in e-voting has been a concern and an important research topic in the last 10 years. Verifiability means that the steps of the election process - vote casting, vote storage and vote counting - can be checked by voters, auditors or external observers. One key instrument in Internet voting verifiable systems is the Bulletin Board: a public place where all the election configuration information, as well as the votes received in the system, is published by authorized parties. In the Bulletin Board, voters can verify that their votes have been correctly received and stored on the remote server. Auditors and third parties can verify as well that the election result is correct from the information posted in the Bulletin Board, and that only eligible voters have participated by comparing the authorship of the digital signatures of the votes against the electoral roll.

Of course, since many operations in an election system are run locally, maybe involving secret keys, the verification of the correctness of these operations will be possible only if the parties give a proof of correctness. Such a proof must convince observers that the operation was done correctly, but without leaking information about secret values (like chosen voting option or secret keys). The suitable cryptographic ingredient is therefore a (non-interactive) zero-knowledge proof. We review here some examples, related to different operations described in the previous sections.

- In a mix-net, each node must prove that he has run its corresponding shuffle in a correct way, by applying a real permutation and a decryption (or re-randomization) of the inputs ciphertexts. But such a proof must reveal no information on the permutation, or on the secret key of the node (in case of decryption), or on the random elements used for re-randomization. Otherwise, the anonymity purpose of the mix-net would not be fulfilled.
- In a voting system with tallying [Gro05], the voter must prove that the clear vote he has encrypted is a valid answer to the election question; otherwise, the final result of the election could be dishonestly biased. For instance, in the case of a referendum, the voter must add a zero-knowledge proof that the clear text inside his ciphertext is either 0 or 1, without leaking any other information on the clear text.
- When a (human) voter chooses his voting option, there is a voting device (a mobile phone, a computer, etc.) which encrypts this option and sends the result to the Bulletin Board. It may be the case, due to a failure or to an attack, that this device is not encrypting the option chosen by the voter. Since the vote cast in the Bulletin Board is encrypted, the voter has no means to verify this. Therefore, to check that this operation is done correctly, the voter device should compute and publish some kind of zero-knowledge proof, which in combination to other published information (maybe by the voter, maybe by the authorities) can convince everybody that the option chosen by the voter is actually encrypted in the ciphertext.

4.2 Existing (Not Lattice-Based) Solutions

Listing all the existing results for electronic voting systems is impossible: there are annual workshops devoted to this topic, and also there are papers on the topic that are presented or published in other (more general) conferences and journals about information security and cryptography.

Therefore, the references that we include below are just a sample of the existing results in this area.

4.2.1 Mix-nets

In his initial work on mix-nets and shuffles, Chaum [Cha82] did not provide a concrete solution. Several works gave generic constructions [SK95, GI08, BG12] of verifiable shuffle based on additively homomorphic encryption.

Some of the most known and efficient verifiable mix-nets are Randomized Partial Checking [JJR02], Verificatum or Douglas Wikstrom's Commitment-Consistent Proof of a Shuffle [Wik09], or the Bayer-Groth Efficient zero-knowledge argument for correctness of a shuffle [BG12]. The main benefits of these protocols are that they can use more flexible encryption schemes than homomorphic tally protocols; they support write-ins; and they provide a better support for complex electoral processes.

Regarding efficiency, one of the protocols in [BG12] can prove the correctness of a shuffle of N ciphertexts with a communication complexity $O(\sqrt{N})$, using ElGamal cryptosystem.

4.2.2 Blind and group signatures

The way to use blind signature schemes in eVoting has been proposed in different papers. The first relevant system was due to Ohkubo et al. [OMA$^+$99], based on the use of both blind signatures and a (non universally verifiable) mix-net. Such system was in particular implemented in the Votopia system [KKLA01]. However, Canard et al. [CGT06] have shown that using a non universally verifiable mix-net is not enough in this setting and that some attacks can be mounted. The idea is then to use either a universally verifiable mix net, but in this case the blind signature is no more useful (see previous section) or a fair blind signature [SPC95].

Regarding group signature based construction, the only proposal, to the best of our knowledge, is the one given in [CSST06].

4.2.3 Tallying: homomorphic encryption

Using homomorphic tallying in electronic elections has been considered in many different works, see for instance [CGS97, AR06, MMS16] and some variants of Helios (see Section 4.2.5) like Belenios. Those constructions make use of different public key encryption schemes with homomorphic properties, such as ElGamal [ElG85], Goldwasser-Micali [GM84], Paillier [Pai99], Boneh-Goh-Nissin [BGN05], Benhamouda et al. [BHJL17].

4.2.4 Verifiability: Zero-Knowledge Proofs

There are very generic (but inefficient) results showing that one can prove any relation in NP in a zero-knowledge interactive way [GMR85]. If the proof needs to be non-interactive and secure in the standard model, then a common reference string (chosen by a trusted party) between the prover and the verifier is required [BFM88].

Regarding efficient constructions of non-interactive proofs, we can first mention the Fiat-Shamir heuristic [FS87] to transform an interactive proof into a non-interactive proof, in the random oracle model. For zero-knowledge proofs for specific relations, we can mention [CDS94] for conjunctions and disjunctions of statements, or [Bou00] for range proofs. For relations described by equations involving bilinear pairings, the non-interactive proofs of Groth-Sahai [GS08] are efficient and secure in the standard model.

In the recent years, the notion of succinct zero-knowledge proofs (SNARKs) has been proposed: the length of a proof is constant, independent of the size of the (arithmetic) circuit that describes the relation that is being proved. Some specific proposals of SNARKs exist [GGPR13], using bilinear pairings.

4.2.5 A Particular Election System: Helios

The previous sections describe cryptographic results that can be used in different parts of an election system, but we believe it may be useful to describe or comment on a specific election system. There are quite a few proposals of election systems (VoteBox, Star Vote, Wombat...), but we have chosen Helios, which is maybe the one that has received the more attention by the cryptographic community.

Helios has been widely used in academic environments, both as a voting tool (mainly student organization elections, although other organizations, such as IACR, have also used it) and as a research tool. The system has evolved over time. In version 1.0 [Adi08], it consisted on a mixing-based scheme, implementing the verifiable mix-net from Sako and Kilian [SK95]. Then, it was modified in version 2.0 to implement homomorphic tally with exponential ElGamal and distributed decryption, following a scheme similar to that described in [CGS97].

Helios has been widely studied by the academic community in the last years and has a lot of variants, which are evolutions of the Helios system or academic alternatives, some of which having their own implementations.

Helios provides cast-as-intended and recorded-as-cast verifiability in a similar way as described in a proposal from Benaloh [Ben06]: after doing her selections and prior to casting her vote, the voter is presented with the commitment of the ciphertext generated by the voting device, in the form of a hash value. At that moment the voter can decide to either cast the vote, or audit it. In case the voter chooses to cast her vote, the vote is sent to the remote server, where it is posted in the bulletin board. Otherwise, the randomness, the encryption parameters and the clear vote are provided, so that the voter can check that the generated ciphertext is correct according to these parameters, and that the clear vote matches her selections. A software application is offered by the same Helios website in order to make this audit. However, it is recommended to use a third-party software, and preferably on a device different than the one used for voting, in order to ensure independence of the verifier and the verified entities. Because the voting client does not know, at the time of generating the ciphertext and showing the commitment to the voter, which is the option she will choose, the chance of cheating without being detected is $1/2$. It is encouraged that voters perform this audit several times in order to improve this probability.

Audited ciphertexts are not cast to prevent the voter from being able to sell her vote, but the voting options are encrypted again with new randomness after the audit.

The voter is able to check that the vote she cast was accepted by the remote voting server by checking that the hash or fingerprint, which the voting device used to commit to a generated ciphertext, matches one entry of the bulletin board. Depending on the Helios variant, ciphertexts may be published alongside the voter's identifier, an alias, or no identifier at all. Also, hashes may be published instead of the full ballots.

4.3 Existing Lattice-based Solutions

4.3.1 Basic Cryptographic Tools

Blind signatures. Essentially only one blind signature scheme has been proposed in the lattice-based setting [Rüc10], later improved in [ZJZ$^+$18]. To the best of our knowledge, no fair blind signature scheme have been proposed yet based on lattices.

Mix-nets. There is only one specific proposal of a verifiable mix-net in the lattice-based setting [CMM17] but the efficiency remains too bad for a practical use.

Actually, the most popular method to construct a mix-net is by re-encryption, which is done by combining a ciphertext of an homomorphic encryption scheme with an encryption of 0 or 1 (depending on whether the homomorphism is additive or multiplicative). Therefore, the number of (re-)encryptions that are applied to a vote equals the number of nodes in the mix-net. If this number is big, then homomorphic lattice-based encryption schemes suffer from a problem that we describe in the next paragraph, because it appears (more significantly) in the scenario of elections with homomorphic tallying, where potentially millions of homomorphic operations may be applied to the initial ciphertexts.

Tallying: homomorphic encryption. The classical techniques on homomorphic encryption (ElGamal, Paillier...) do not directly carry over to the lattice setting: the problem of efficiently extending them to additively homomorphic Regev encryptions remains open, in particular if we want to retain competitive parameters. One of the difficulties arises from the noise term contained in lattice-based ciphertexts, which typically comes from a Gaussian distribution over the integers. Currently, the only simple solution that allows for properly applying many homomorphic operations to ciphertexts, other than inefficient bootstrapping as in fully homomorphic encryption, is to add a super-polynomial amount of noise to the initial noise so as to drown statistical discrepancies (via a technique known as noise flooding). The problem is that, by doing this, we need a super-polynomial large modulus and thus a much less efficient parameter choice.

Verifiability: Zero-Knowledge Proofs. Existing zero-knowledge techniques for lattice-related languages are either quite expensive or restricted to very specific languages. However, this is a very active area of research, and improved results are being published every year.

In the standard model, lattice-based NIZK proofs are only known for very specific languages [PV08]. If we enable interaction or random oracles, several techniques [JKPT12, XXW13, BKLP15] were given to prove the satisfiability of arbitrary circuits. They unfortunately decompose the statements into a circuit – thus leading to a communication complexity proportional to the circuit size. A recent result has improved from linear to logarithmic [BBC$^+$18].

Restricting oneself to particular statements allows hoping for more efficient solutions. In this direction, initial steps were taken in [Lyu08, LNSW13] for the specific task of proving knowledge of a solution to the inhomogeneous SIS problem (ISIS). However, they require the verifier's challenge to live in a small space, so that many repetitions of the same basic protocol are necessary to make sure that a dishonest prover can only cheat the verifier with negligible probability. In structured lattices, Lyubashevsky [Lyu09] showed how to work with a large challenge space so as to avoid repeating a basic protocol many times (this technique has been improved in [LS18]). On the downside, the technique of [Lyu09] is only known to work for relatively simple statements and it is not clear how to apply it in the context of higher-level privacy-preserving protocols.

Several works [LNSW13, LLNW16] extended Stern's protocol [Ste96] to prove expressive statements in the lattice setting. Unfortunately, the resulting protocols inherit the computational cost of [Ste96] due to the many repetitions incurred by the small set where verifiers' challenges have to be chosen.

So far, it remains a challenging open problem to combine the expressiveness of [LNSW13, LLNW16] and the efficiency of [Lyu09] in the context of interactive proofs, especially if they are to be made non-interactive in the quantum random oracle model. In the setting of non-interactive proofs in the standard model, the situation is even worse as general NIZK proofs are not known to be implied by lattice assumptions alone.

In the context of set membership proofs, the techniques of [CCs08] easily extend to the lattice setting but they require a setup phase where a trusted party generates a signature on all set elements and safely deletes the private signing key. In many applications, however, a trusted setup is not a realistic assumption to make.

Concerning range proofs, existing solutions either rely on homomorphic integer commitments [FO97, Bou00, Gro11] or they generically build upon set membership proofs [CCs08] (or both). In the lattice setting, it is not clear how these techniques can be adapted under standard hardness assumptions. The main reasons are that these techniques usually rely on homomorphic commitments over exponentially large domains. Hence, any direct adaptation of the same ideas in the lattice setting ends up with a super-polynomial modulus, which significantly impacts the efficiency or the strength of the underlying assumption.

Other languages where specific and efficient zero-knowledge proofs have been proposed include relations between committed integers [LLNW18] and relations between encrypted and committed integers [BKLP15].

Regarding succing zero-knowledge proofs (SNARKs), the only proposal in the lattice-based setting [GMNO18] works for designated verifiers: the proof can be verified by the owner of a specific secret key, only.

4.3.2 Particular Election Systems

In the literature, there are three papers describing whole election systems with post-quantum security, based on lattices. The two proposals in [CGGI16, GS17] use techniques from fully-homomorphic encryption [Gen09], for instance to replace some of the zero knowledge proofs (verifiability), and also bootstrapping to decrease the noise produced when several homomorphic operations are done. Unfortunately, the use of fully homomorphic techniques is quite far from being practical, today.

Finally, in [dLNS17] a different lattice-based election system, EVOLVE, has been proposed, which does not make use of fully homomorphic encryption techniques. Actually EVOLVE does not use encryption for privacy, but secret sharing techniques: voters split their votes in shares, and send these shares, privately, to different voting authorities (this generic idea was firstly proposed in [CFSY96]), along with commitments to these shares and zero-knowledge proofs of the fact that the shared vote is either a 0 or a 1, because EVOLVE is proposed for this particular setting of referendums.

The voting authorities also help in computing part of the zero-knowledge proofs, to decrease the cost at the voters' side, and because in this way they can use amortized techniques to prove many instances (all the votes together) at the same time. Finally, each authority combines the valid shares that it got, and publishes the resulting share of the final result. The combination of these shares yields the final result of the election; since the result is computed using tallying, shuffling is not used.

5 Conclusion

In the context of privacy-preserving cryptographic protocols, the maturity of related work in the standard setting is very high. In the lattice setting, the observation is much less shining and there are only a few papers, and a lot of open problems. Within WP5 of PROMETHEUS project, our aim is to find solutions to most of these open problems in order to push to demonstrators (within WP6) the most relevant cryptographic specifications.

References

[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, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 4–24. Springer, Heidelberg, December 2012.

[ACJT00] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 255–270. Springer, Heidelberg, August 2000.

[Adi08] Ben Adida. Helios: Web-based open-audit voting. In *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*, pages 335–348, 2008.

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, Heidelberg, August 2010.

[AlL16] Guy AlLee. EPID for iot identity, 2016.

[AR06] Ben Adida and Ronald L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In *Proceedings of the 2006 ACM Workshop on Privacy in the Electronic Society, WPES 2006, Alexandria, VA, USA, October 30, 2006*, pages 29–40, 2006.

[ASM08] Man Ho Au, Willy Susilo, and Yi Mu. Practical anonymous divisible e-cash from bounded accumulators. In Gene Tsudik, editor, *FC 2008*, volume 5143 of *LNCS*, pages 287–301. Springer, Heidelberg, January 2008.

[BBB+18] Kai Bemmann, Johannes Blömer, Jan Bobolz, Henrik Bröcher, Denis Diemert, Fabian Eidens, Lukas Eilers, Jan Haltermann, Jakob Juhnke, Burhan Otour, Laurens Porzenheim, Simon Pukrop, Erik Schilling, Michael Schlichtig, and Marcel Stienemeier. Fully-featured anonymous credentials with reputation system. pages 42:1–42:10, 2018.

[BBC+18] Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafaël del Pino, Jens Groth, and Vadim Lyubashevsky. Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 669–699. Springer, Heidelberg, August 2018.

[BCC04] Ernest F. Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick McDaniel, editors, *ACM CCS 2004*, pages 132–145. ACM Press, October 2004.

[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, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 108–125. Springer, Heidelberg, August 2009.

[BCF+11] Olivier Blazy, Sébastien Canard, Georg Fuchsbauer, Aline Gouget, Hervé Sibert, and Jacques Traoré. Achieving optimal anonymity in transferable e-cash with a judge. In Abderrahmane Nitaj and David Pointcheval, editors, *AFRICACRYPT 11*, volume 6737 of *LNCS*, pages 206–223. Springer, Heidelberg, July 2011.

[BCFK15] Foteini Baldimtsi, Melissa Chase, Georg Fuchsbauer, and Markulf Kohlweiss. Anonymous transferable E-cash. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 101–124. Springer, Heidelberg, March / April 2015.

[BCK+14] Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 551–572. Springer, Heidelberg, December 2014.

[BCKL08] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. P-signatures and noninteractive anonymous credentials. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 356–374. Springer, Heidelberg, March 2008.

[BCN18] Cecilia Boschini, Jan Camenisch, and Gregory Neven. Relaxed lattice-based signatures with short zero-knowledge proofs. In Liqun Chen, Mark Manulis, and Steve Schneider, editors, *ISC 2018*, volume 11060 of *LNCS*, pages 3–22. Springer, Heidelberg, September 2018.

[Ben06] Josh Benaloh. Simple verifiable elections. In *2006 USENIX/ACCURATE Electronic Voting Technology Workshop, EVT'06, Vancouver, BC, Canada, August 1, 2006*, 2006.

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *20th ACM STOC*, pages 103–112. ACM Press, May 1988.

[BG12] Stephanie Bayer and Jens Groth. Efficient zero-knowledge argument for correctness of a shuffle. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 263–280. Springer, Heidelberg, April 2012.

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In Joe Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 325–341. Springer, Heidelberg, February 2005.

[BHJ+15] Florian Böhl, Dennis Hofheinz, Tibor Jager, Jessica Koch, and Christoph Striecks. Confined guessing: New signatures from standard assumptions. *Journal of Cryptology*, 28(1):176–208, January 2015.

[BHJL17] Fabrice Benhamouda, Javier Herranz, Marc Joye, and Benoît Libert. Efficient cryptosystems from 2^k-th power residue symbols. *Journal of Cryptology*, 30(2):519–549, April 2017.

[BKLP15] Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. Efficient zero-knowledge proofs for commitments from learning with errors over rings. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *ESORICS 2015, Part I*, volume 9326 of *LNCS*, pages 305–325. Springer, Heidelberg, September 2015.

[BLMR13] Dan Boneh, Kevin Lewi, Hart William Montgomery, and Ananth Raghunathan. Key homomorphic PRFs and their applications. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 410–428. Springer, Heidelberg, August 2013.

[BMW03] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 614–629. Springer, Heidelberg, May 2003.

[Bou00] Fabrice Boudot. Efficient proofs that a committed number lies in an interval. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 431–444. Springer, Heidelberg, May 2000.

[Boy10] Xavier Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 499–517. Springer, Heidelberg, May 2010.

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 719–737. Springer, Heidelberg, April 2012.

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In Alfred Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 136–153. Springer, Heidelberg, February 2005.

[BW06] Xavier Boyen and Brent Waters. Compact group signatures without random oracles. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 427–444. Springer, Heidelberg, May / June 2006.

[BW13] Dan Boneh and Brent Waters. Constrained pseudorandom functions and their applications. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 280–300. Springer, Heidelberg, December 2013.

[CCs08] Jan Camenisch, Rafik Chaabouni, and abhi shelat. Efficient protocols for set membership and range proofs. In Josef Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 234–252. Springer, Heidelberg, December 2008.

[CDS94] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In Yvo Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 174–187. Springer, Heidelberg, August 1994.

[CFN90] David Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In Shafi Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 319–327. Springer, Heidelberg, August 1990.

[CFSY96] Ronald Cramer, Matthew K. Franklin, Berry Schoenmakers, and Moti Yung. Multi-autority secret-ballot elections with linear work. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 72–83. Springer, Heidelberg, May 1996.

[CG07] Sébastien Canard and Aline Gouget. Divisible e-cash systems can be truly anonymous. In Moni Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 482–497. Springer, Heidelberg, May 2007.

[CG08a] Jan Camenisch and Thomas Groß. Efficient attributes for anonymous credentials. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM CCS 2008*, pages 345–356. ACM Press, October 2008.

[CG08b] Sébastien Canard and Aline Gouget. Anonymity in transferable e-cash. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, *ACNS 08*, volume 5037 of *LNCS*, pages 207–223. Springer, Heidelberg, June 2008.

[CG10] Sébastien Canard and Aline Gouget. Multiple denominations in e-cash with compact transaction data. In Radu Sion, editor, *FC 2010*, volume 6052 of *LNCS*, pages 82–97. Springer, Heidelberg, January 2010.

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. A homomorphic LWE based e-voting scheme. In *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, pages 245–265, 2016.

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 103–118. Springer, Heidelberg, May 1997.

[CGT06] Sébastien Canard, Matthieu Gaud, and Jacques Traoré. Defeating malicious servers in a blind signatures based voting system. In Giovanni Di Crescenzo and Avi Rubin, editors, *FC 2006*, volume 4107 of *LNCS*, pages 148–153. Springer, Heidelberg, February / March 2006.

[CGT08] Sébastien Canard, Aline Gouget, and Jacques Traoré. Improvement of efficiency in (unconditional) anonymous transferable e-cash. In Gene Tsudik, editor, *FC 2008*, volume 5143 of *LNCS*, pages 202–214. Springer, Heidelberg, January 2008.

[Cha81] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, 1981.

[Cha82] David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *CRYPTO'82*, pages 199–203. Plenum Press, New York, USA, 1982.

[Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044, 1985.

[CHL05] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 302–321. Springer, Heidelberg, May 2005.

[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`.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 93–118. Springer, Heidelberg, May 2001.

[CL02] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 61–76. Springer, Heidelberg, August 2002.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 56–72. Springer, Heidelberg, August 2004.

[CL11] Sébastien Canard and Roch Lescuyer. Anonymous credentials from (indexed) aggregate signatures. In *Workshop on Digital Identity Management DIM'11*, pages 53–62. ACM, 2011.

[CL13] Sébastien Canard and Roch Lescuyer. Protecting privacy by sanitizing personal data: a new approach to anonymous credentials. In Kefei Chen, Qi Xie, Weidong Qiu, Ninghui Li, and Wen-Guey Tzeng, editors, *ASIACCS 13*, pages 381–392. ACM Press, May 2013.

[CMM17] Núria Costa, Ramiro Martínez, and Paz Morillo. Proof of a shuffle for lattice-based cryptography. In *Secure IT Systems - 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8-10, 2017, Proceedings*, pages 280–296, 2017.

[CNR12] Jan Camenisch, Gregory Neven, and Markus Rückert. Fully anonymous attribute tokens from lattices. In Ivan Visconti and Roberto De Prisco, editors, *SCN 12*, volume 7485 of *LNCS*, pages 57–75. Springer, Heidelberg, September 2012.

[CP93] David Chaum and Torben P. Pedersen. Transferred cash grows in size. In Rainer A. Rueppel, editor, *EUROCRYPT'92*, volume 658 of *LNCS*, pages 390–407. Springer, Heidelberg, May 1993.

[CPST15a] Sébastien Canard, David Pointcheval, Olivier Sanders, and Jacques Traoré. Divisible E-cash made practical. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 77–100. Springer, Heidelberg, March / April 2015.

[CPST15b] Sébastien Canard, David Pointcheval, Olivier Sanders, and Jacques Traoré. Scalable divisible E-cash. In Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors, *ACNS 15*, volume 9092 of *LNCS*, pages 287–306. Springer, Heidelberg, June 2015.

[CSST06] Sébastien Canard, Berry Schoenmakers, Martijn Stam, and Jacques Traoré. List signature schemes. *Discrete Applied Mathematics*, 154(2):189–201, 2006.

[Cv91] David Chaum and Eugène van Heyst. Group signatures. In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 257–265. Springer, Heidelberg, April 1991.

[dLNS17] Rafaël del Pino, Vadim Lyubashevsky, Gregory Neven, and Gregor Seiler. Practical quantum-safe voting from lattices. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 1565–1581. ACM Press, October / November 2017.

[dLS18] Rafaël del Pino, Vadim Lyubashevsky, and Gregor Seiler. Lattice-based group signatures and zero-knowledge proofs of automorphism stability. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 574–591. ACM Press, October 2018.

[DP06] Cécile Delerablée and David Pointcheval. Dynamic fully anonymous short group signatures. In Phong Q. Nguyen, editor, *Progress in Cryptology - VIETCRYPT 06*, volume 4341 of *LNCS*, pages 193–210. Springer, Heidelberg, September 2006.

[DP16] Léo Ducas and Thomas Prest. Fast fourier orthogonalization. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2016, Waterloo, ON, Canada, July 19-22, 2016*, pages 191–198. ACM, 2016.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[FO97] Eiichiro Fujisaki and Tatsuaki Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In Burton S. Kaliski Jr., editor, *CRYPTO'97*, volume 1294 of *LNCS*, pages 16–30. Springer, Heidelberg, August 1997.

[FPV09] Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Transferable constant-size fair e-cash. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *CANS 09*, volume 5888 of *LNCS*, pages 226–247. Springer, Heidelberg, December 2009.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Heidelberg, August 1987.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 169–178. ACM Press, May / June 2009.

[GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). In *25th FOCS*, pages 464–479. IEEE Computer Society Press, October 1984.

[GGPR13] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct NIZKs without PCPs. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 626–645. Springer, Heidelberg, May 2013.

[GI08] Jens Groth and Yuval Ishai. Sub-linear zero-knowledge argument for correctness of a shuffle. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 379–396. Springer, Heidelberg, April 2008.

[GKV10] S. Dov Gordon, Jonathan Katz, and Vinod Vaikuntanathan. A group signature scheme from lattice assumptions. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 395–412. Springer, Heidelberg, December 2010.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[GMNO18] Rosario Gennaro, Michele Minelli, Anca Nitulescu, and Michele Orrù. Lattice-based zk-snarks from square span programs. *IACR Cryptology ePrint Archive*, 2018:275, 2018.

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In *17th ACM STOC*, pages 291–304. ACM Press, May 1985.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

[Gro07] Jens Groth. Fully anonymous group signatures without random oracles. In Kaoru Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 164–180. Springer, Heidelberg, December 2007.

[Gro11] Jens Groth. Efficient zero-knowledge arguments from two-tiered homomorphic commitments. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 431–448. Springer, Heidelberg, December 2011.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, April 2008.

[GS17] Kristian Gjøsteen and Martin Strand. A roadmap to fully homomorphic elections: Stronger security, better verifiability. In *Financial Cryptography and Data Security - FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers*, pages 404–418, 2017.

[IL13] Malika Izabachène and Benoît Libert. Divisible E-cash in the standard model. In Michel Abdalla and Tanja Lange, editors, *PAIRING 2012*, volume 7708 of *LNCS*, pages 314–332. Springer, Heidelberg, May 2013.

[JJR02] Markus Jakobsson, Ari Juels, and Ronald L. Rivest. Making mix nets robust for electronic voting by randomized partial checking. In *Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, USA, August 5-9, 2002*, pages 339–353, 2002.

[JKPT12] Abhishek Jain, Stephan Krenn, Krzysztof Pietrzak, and Aris Tentes. Commitments and efficient zero-knowledge proofs from learning parity with noise. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 663–680. Springer, Heidelberg, December 2012.

[KKLA01] Kwangjo Kim, Jinho Kim, Byoungcheon Lee, and Gookwhan Ahn. Experimental design of worldwide internet voting system using pki. 2001.

[KY06] Aggelos Kiayias and Moti Yung. Secure scalable group signature with dynamic joins and separable authorities. *IJSN*, 1(1/2):24–45, 2006.

[LLLS13] Fabien Laguillaumie, Adeline Langlois, Benoît Libert, and Damien Stehlé. Lattice-based group signatures with logarithmic signature size. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 41–61. Springer, Heidelberg, December 2013.

[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 Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 373–403. Springer, Heidelberg, December 2016.

[LLNW16] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 1–31. Springer, Heidelberg, May 2016.

[LLNW17] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based PRFs and applications to E-cash. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part III*, volume 10626 of *LNCS*, pages 304–335. Springer, Heidelberg, December 2017.

[LLNW18] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Lattice-based zero-knowledge arguments for integer relations. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 700–732. Springer, Heidelberg, August 2018.

[LNSW13] San Ling, Khoa Nguyen, Damien Stehlé, and Huaxiong Wang. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013*, volume 7778 of *LNCS*, pages 107–124. Springer, Heidelberg, February / March 2013.

[LNW15] San Ling, Khoa Nguyen, and Huaxiong Wang. Group signatures from lattices: Simpler, tighter, shorter, ring-based. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 427–449. Springer, Heidelberg, March / April 2015.

[LS18] Vadim Lyubashevsky and Gregor Seiler. Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 204–224. Springer, Heidelberg, April / May 2018.

[Lyu08] Vadim Lyubashevsky. Lattice-based identification schemes secure under active attacks. In Ronald Cramer, editor, *PKC 2008*, volume 4939 of *LNCS*, pages 162–179. Springer, Heidelberg, March 2008.

[Lyu09] Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, Heidelberg, December 2009.

[MMS16] Víctor Mateu, Josep M. Miret, and Francesc Sebé. A hybrid approach to vector-based homomorphic tallying remote voting. *Int. J. Inf. Sec.*, 15(2):211–221, 2016.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[NZZ15] Phong Q. Nguyen, Jiang Zhang, and Zhenfeng Zhang. Simpler efficient group signatures from lattices. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 401–426. Springer, Heidelberg, March / April 2015.

[OMA+99] Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto. An improvement on a practical secret voting scheme. In Masahiro Mambo and Yuliang Zheng, editors, *ISW'99*, volume 1729 of *LNCS*, pages 225–234. Springer, Heidelberg, November 1999.

[OO92] Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 324–337. Springer, Heidelberg, August 1992.

[Pai99] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 223–238. Springer, Heidelberg, May 1999.

[PFH+17] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice-based compact signatures over ntru. 2017.

[PS96] David Pointcheval and Jacques Stern. Provably secure blind signature schemes. In Kwangjo Kim and Tsutomu Matsumoto, editors, *ASIACRYPT'96*, volume 1163 of *LNCS*, pages 252–265. Springer, Heidelberg, November 1996.

[PS00] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, June 2000.

[PS16] David Pointcheval and Olivier Sanders. Short randomizable signatures. In Kazue Sako, editor, *CT-RSA 2016*, volume 9610 of *LNCS*, pages 111–126. Springer, Heidelberg, February / March 2016.

[PST17] David Pointcheval, Olivier Sanders, and Jacques Traoré. Cut down the tree to achieve constant complexity in divisible E-cash. In Serge Fehr, editor, *PKC 2017, Part I*, volume 10174 of *LNCS*, pages 61–90. Springer, Heidelberg, March 2017.

[PV08] Chris Peikert and Vinod Vaikuntanathan. Noninteractive statistical zero-knowledge proofs for lattice problems. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 536–553. Springer, Heidelberg, August 2008.

[Rüc10] Markus Rückert. Lattice-based blind signatures. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 413–430. Springer, Heidelberg, December 2010.

[SK95] Kazue Sako and Joe Kilian. Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 393–403. Springer, Heidelberg, May 1995.

[SPC95] Markus Stadler, Jean-Marc Piveteau, and Jan Camenisch. Fair blind signatures. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 209–219. Springer, Heidelberg, May 1995.

[Ste96] Jacques Stern. A new paradigm for public key identification. *IEEE Trans. Information Theory*, 42(6):1757–1768, 1996.

[TCG] TCG. Trusted computing group.

[Wik09] Douglas Wikström. A commitment-consistent proof of a shuffle. In Colin Boyd and Juan Manuel González Nieto, editors, *ACISP 09*, volume 5594 of *LNCS*, pages 407–421. Springer, Heidelberg, July 2009.

[XXW13] Xiang Xie, Rui Xue, and Minqian Wang. Zero knowledge proofs from ring-LWE. In Michel Abdalla, Cristina Nita-Rotaru, and Ricardo Dahab, editors, *CANS 13*, volume 8257 of *LNCS*, pages 57–73. Springer, Heidelberg, November 2013.

[ZJZ+18] Pingyuan Zhang, Han Jiang, Zhihua Zheng, Peichu Hu, and Qiuliang Xu. A new post-quantum blind signature from lattice assumptions. *IEEE Access*, 6:27251–27258, 2018.