Numéro National de Thèse : TODO

THÈSE DE DOCTORAT DE L'UNIVERSITÉ DE LYON
opérée au sein de
l'École Normale Supérieure de Lyon

École Doctorale N°512
École Doctorale en Informatique et Mathématiques de Lyon

Spécialité de doctorat : Informatique

Soutenue publiquement le 01/12/2023, par :
Paul Fermé

Fancy english title

Titre français fancy

Devant le jury composé de :

Valjean Jean, Associate Professor, Università di Catania (Italie)	Rapporteur
Valjeanne Jeanne, Assistant Professor, I.I.T. Madras (Inde)	Examinatrice
Fawzi Omar, Directeur de Recherche, Inria et ENS de Lyon	Directeur de thèse

Dédicace,
peut-être…

Résumé

Dans cette thèse, nous étudions...

Abstract

In this thesis, we study...

Remerciements/Acknowledgements

Je tiens tout d'abord à remercier mon directeur de thèse Omar Fawzi, qui m'a accompagné durant toute la durée de ma thèse et m'a gratifié de sa présence et de sa disponibilité tout au long de cette aventure.

I would also like to thank... english

Ma famille ?

Je tenais aussi à remercier mes amis...

Contents

List of Symbols

General Notations

to	TO
do	DO

Usual sets

$\mathbb{N}$	the set of nonnegative integers
$\mathbb{R}$	the set of real numbers
$[k]$	the set of integers from 1 to k, ie. $\{1, \ldots, k\}$

Résumé substantiel en Français

Intro

Section 1

Resumé section 1

Sous-section 1

Résumé sous-section 1

Chapter 1

Introduction

In the last fifty years, the use of cryptography has shifted from military and commercial secrets to a broader public. For instance, the Enigma machine had a design for military purposes, and another one for companies (Enigma A26). As of today, about 60% of the first million most visited websites propose encrypted and authenticated communications (via `https`), and so are most of the communications channels used by electronic devices (like *Wifi Protected Access*).

At the same time, the growth of exchanged data and the sensitivity of transferred information make the urge of protecting these data efficiently even more critical. While we are reaching the Moore's law barrier, other threats exist against nowadays' cryptosystems. For instance, the existence of a quantum computer with sufficient memory [Sho99] would break most of real-world cryptographic designs, which mostly rely on modular arithmetic assumptions. In this context, it is crucial to design cryptographic schemes that are believed to be quantum-resistant.

To address this problem, *post-quantum cryptography* arose in the early 2000s. The different candidates rely on several mathematical objects, such as lattices, error-correcting codes, systems of multivariate polynomials, etc. Recently, the National Institute of Standards and Technology (or *NIST*) organized a competition to evaluate different post-quantum schemes for encryption and signatures [NIS17]. In this competition, 82 protocols have been proposed out of which: 28 were lattice-based, 24 were code-based, 13 were multi-variate based, 4 were hash-based and the 13 left were categorized as "other".

Though, real-world cryptography mainly aims at designing digital signatures and encryption schemes, as illustrated by the NIST competition. Meanwhile, ongoing research in cryptology proposes different solutions to address more specific problems, such as the design of electronic-cash systems[1] [CFN88], which are the digital analogue of real money. Coins are delivered by a central authority (the bank) and spendings remain untraceable. In case of misbehavior (such as double-spending), the identity of the cheater is revealed.

Cryptographic constructions should additionally verify some security requirements. For instance, an encryption scheme has to hide a message in the presence of an eavesdropper, or even an active adversary who can alter some messages. To guarantee these requirements, cryptographers provide security proofs in the sense of precise security models. A security

[1] Which is not to be confused with cryptocurrency…

proof mainly states that a given cryptographic scheme is secure if some problems are hard.

At last but not least, the importance of privacy and data protection has been a hot topic in the last years, as reflected by the development of the general data protection regulation law in 2016, which is implemented since may 25th. Hence, it is appealing to have privacy-preserving cryptographic constructions which would ideally resist the advent of a quantum computer. Nevertheless, the design of such protocols crucially relies on "zero-knowledge proofs". These are 2-party protocols between a prover and a verifier where the prover should convince the verifier of a statement without leaking any piece of information about this statement. In the context of post-quantum cryptography, such proofs systems are still limited in power or costly in terms of time, memory and communication consumptions.

1.1 Privacy-Preserving Cryptography

In this context, 'privacy-preserving' refers to the ability of a primitive to provide some functionalities while holding sensitive information private. An example of such primitives are *anonymous credentials* [Cha85, CL01]. Informally, this primitive allows users to prove themselves to some verifiers without telling their identity, nor the pattern of their authentications. To realize this, this system involves one (or more) credential issuer(s) and a set of users who have their own secret keys and pseudonyms that are bound to their secret. Users can dynamically obtain credentials from an issuer that only knows users' pseudonyms and obliviously sign users' secret key as well as a set of attributes. Later on, users can make themselves know to verifiers under a different pseudonym and demonstrate possession of a certification from the issuer, without revealing neither the signature nor the secret key. This primitive thus allows a user to authenticate to a system (e.g., in anonymous access control) while retaining its anonymity. In addition, the system is guaranteed that users indeed possess a valid credential.

Interests in privacy-based cryptography date back to the beginning of public-key cryptography [Rab81, Cha82, GM82, Cha85]. A reason for that could be the similarities between the motivations of cryptography and the requirements of privacy protection. Additionally, cryptographers' work in this field may have direct consequences in term of services that could be developed in the real-world. Indeed, having a practical anonymous credential scheme will enable its use for access control in a way that limits security flaws. Whereas, nowadays' implementations are based on more elementary building blocks, like signatures, whose manipulations may lead to different security holes [VP17].

Similarly, *advanced primitives* often involve simpler building blocks in their design. The difference lies in that provable security conveys security guarantees for the construction. As explained before, these proofs make the security of a set of schemes rely on hardness assumptions. Thus, the security relies on the validity of those assumptions, which are independently studied by cryptanalysts. Hence, security is guaranteed by the study of those assumptions. For example, the security analysis of multilinear maps in [CHL$^+$15] made obsolete a large amount of candidates at this time. This example reflects the importance of relying on well-studied and simple assumptions as we will explain in **??**.

In the context of this thesis, the developed cryptographic schemes rely on lattices and bilinear maps over cyclic groups. Lattice-based cryptography is used to step towards post-quantum cryptography, while the latter proves useful in the design of practical schemes.

The details of these two structures are given in **??**.

1.1.1 Zero-Knowledge Proofs

As explained before, zero-knowledge proofs are a basic building block for privacy-preserving cryptography. They require completeness, soundness and zero-knowledge properties. Completeness captures the correctness of the protocol if everyone is honest. In the case of a dishonest prover, soundness asks the probability that the verifier is convinced to be negligible. On the contrary, if the verifier is cheating, the zero-knowledge property guarantees that the prover's secret remains hidden.

In the case of identification schemes, the nature of the secret remains simple and solutions exist under multiple assumptions [Sch96, Ste96, KTX08, Lyu08]. For more complex statements, such as proving correct computation, a gap appears between post-quantum schemes and modular arithmetic-based schemes. In the case of pairing-based cryptography, there exist non-interactive zero-knowledge proofs which can prove a large variety of statements [GOS06, GS08] without idealized assumptions. Such proofs are still missing in the context of post-quantum cryptography so far.

In the lattice world, there are two main families of proof systems: Schnorr-like proofs [Sch96, Lyu09] and Stern-like proofs [Ste96], named after their respective authors. The first family works on some structured lattices. Exploiting this structure allows for more compact proofs, while the expressiveness of statements is quite restricted. The second kind of proofs is combinatorial and works on the representation of lattice elements (as matrix and vectors). By nature, these proofs are quite expensive in term of communication complexity. However, they can be used to prove a wide variety of statements as we will explain in more details along this thesis and especially in **??**. More generally, zero-knowledge proofs are detailed in **??**.

1.1.2 Signatures with Efficient Protocols

To enable privacy-preserving functionalities, a possible avenue is to couple zero-knowledge proofs with signature schemes. One of such signatures are *signatures with efficient protocols*. This primitive extends the functionalities of ordinary digital signature schemes in two ways: (i) It provides a protocol to allow a signer to obliviously sign a hidden message and (ii) Users are able to prove knowledge of a hidden message-signature pair in a zero-knowledge fashion.

These two properties turn out to be extremely useful when it comes designing efficient anonymity-related protocols such as anonymous credentials or e-cash. The design of effective signatures with efficient protocols is thus important for privacy-preserving cryptography.

In this thesis, we provide two of these signature schemes. One of them, described in **??**, based on pairings, shifts the [LPY15] signature scheme to an idealized but practically acceptable model, aiming at efficiency. The other, described in **??**, adapts a variant of Boyen's signature [Boy10, BHJ+15] along with the Kawachi-Tanaka-Xagawa commitment scheme [KTX08] to provide a lattice-based signature schemes that is compatible with Stern-like proofs. This scheme has also been relaxed in the context of adaptive oblivious

transfer where, in some places, it is only required to have random-message security instead of security against chosen-message security as described in **??**.

1.2 Pairings and Lattices

In this thesis, the proposed constructions rely on the assumed hardness of assumptions over pairing-friendly groups and lattices. These two objects have widely been used in cryptography since the early 2000s [SOK00, Reg05]. Even since, they attracted much attention from cryptographers, leading to multiple constructions in advanced cryptography (as in [Jou00, BBS04, BN06, GS08, LYJP14, LPQ17] for pairings, and [GPV08, ABB10, BV11, GSW13, dPLNS17] for lattices).

1.2.1 Pairing-Based Cryptography

A pairing is a bilinear map from two cyclic source groups to a target group. This bilinear property takes advantage of a rich structure to groups that are compatible with such a map. It is then not surprising to see the variety of schemes that stems from pairing-based cryptography. In the context of privacy-based cryptography, an important breakthrough was the introduction of Groth-Sahai proofs [GOS06, GS08] that allow proving in a non-interactive zero-knowledge fashion a large class of statements in the standard model. For instance, Groth-Sahai proofs have been used in group signatures and anonymous-credential schemes [Gro07, BCKL08, BCC$^+$09], or e-cash systems in the standard model [BCKL09].

In this thesis, however, our pairing-based constructions focus on practicality. Thus, they are instantiated in the random oracle model, where Schnorr's proof are made non-interactive through the Fiat-Shamir transform when the statement to prove is simple enough.

A recent line of work in cryptanalysis of bilinear maps [KB16, MSS17, BD18] led to a change in the panorama of practical pairing-based cryptography. This affects us in the sense that security parameter has to be increased in order to achieve the same security level.

Nevertheless, pairing-based cryptography offers a nice tradeoff between its capabilities and efficiency. As an example, we can cite the work of Döttling and Garg [DG17b], who closed the problem of providing an identity-based encryption scheme which only relies on the Diffie-Hellman assumption (it is construction on cyclic groups that does not need pairings, as defined in Definition 3.11). While their construction relies on a simpler mathematical object, it does not reach the efficiency of pairing-based ones [BB04].

1.2.2 Lattice-Based Cryptography

From an algebraic point of view, a lattice is a discrete subgroup of $\mathbb{R}^n$, which leads to a simple additive structure. The core difference with number-theoretic cryptography, such as discrete-logarithm-based cryptography, is the existence of the geometrical structure of the lattice. From this geometry rises some problems that are believed to withstand quantum computers. Despite this apparently simple structure, some advanced primitives are only known, as of today, to be possible under lattice assumptions, such as fully-homomorphic encryption [Gen09, BV11, GSW13].

The versatility of lattice-based cryptography is enabled by the existence of lattice trapdoors [GPV08, CHKP10, MP12], as we explain in **??**. Informally, the knowledge of a short

basis for a lattice allows sampling short vectors, which is believed to be hard without such a short basis. Furthermore, knowing a short basis for the lattice $\{\mathbf{v} \in \mathbb{Z}^m \mid \mathbf{Az} = 0 \bmod q\}$ described by matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ makes it possible to generate a short basis for a related lattice described by $[\mathbf{A} \mid \mathbf{B}] \in \mathbb{Z}_q^{n \times m'}$. An application for this property is Boyen's signature scheme [Boy10]. In this scheme, a signature for message m is a short vector in the orthogonal lattice of the matrix $\mathbf{A}_m = [\mathbf{A} \mid \mathbf{B}_m]$, where $\mathbf{B}_m$ is publicly computable. Hence, knowing a trapdoor for $\mathbf{A}$ makes the computation of this short vector possible, and the message is bound to the description of the lattice $\mathbf{A}_m$.

Still, the use of lattice trapdoors comes at a price, as it significantly decreases the efficiency of cryptographic designs that use them [Lyu12, LLNW16]. Given that we provide the first lattice-based construction for the scheme we present, we focused on designing provably-secure scheme under well-studied assumptions.

1.3 Our Results

In this thesis, we present several cryptographic constructions that preserve privacy. These constructions are the result of both improvements we made in the use of zero-knowledge proofs and the ability to prove the security of our constructions under standard assumptions. We believe that these advances on zero-knowledge proofs are of independent interest and that the given schemes are a step towards quantum-secure privacy-preserving cryptography. In the following, we detail four contributions that are developed in this thesis. These results are taken from four published articles: [LMPY16, LLM+16a, LLM+16b, LLM+17].

1.3.1 Dynamic Group Signatures and Anonymous Credentials

In **??**, we present two primitives: dynamic group signatures and anonymous credentials. We already described the behavior of anonymous credential in Section 1.1. As for dynamic group signatures, they are a primitive that allows a group of users to authenticate messages on behalf of the group while remaining anonymous inside this group. The users still remain accountable for their actions, as another authority knows a secret information that gives it the ability to lift anonymity of misbehaving users.

By itself, this primitive can be used to provide anonymous authentications while providing accountability (which is not the case with anonymous credentials). For instance, in the Internet of things, such as smart cars, it is important to provide authenticated communication channels as well as anonymity. For car communications, if exchanged data may not be sensitive by themselves, the identity of the driver could be. We can imagine a scenario where some burglars eavesdrop a specific car to know whenever a house is empty.

In this thesis, we present in **??** pairing-based group signatures that aims at efficiency while relying on simple assumptions. The resulting scheme shows competitive signature size with other schemes that rely on more ad-hoc assumptions, and its practicality is supported by an implementation. This scheme is presented in [LMPY16], which is joint work with Benoît Libert, Thomas Peters and Moti Yung presented at AsiaCCS'16.

?? presents the first *dynamic* group signature scheme relying on lattice assumptions. This has been made possible by adapting Stern-like proofs to properly interact with a signature scheme: a variant of Boyen's signature [Boy10, BHJ+15]. It results in a *signature with efficient protocols* that is of independent interest. Later, it has been adapted in the design

dynamic group encryption [LLM+16b] and adaptive oblivious transfer [LLM+17]. This work is described in [LLM+16a], made with Benoît Libert, San Ling, Khoa Nguyen and Huaxiong Wang and presented at Asiacrypt'16.

1.3.2 Group Encryption

Group encryption schemes [KTY07] are the encryption analogue of group signatures. In this setting, a user is willing to send a message to a group member, while keeping the recipient of the message hidden inside the group. In order to keep user accountable for their actions, an opening authority is further empowered with some secret information allowing it to un-anonymize ciphertexts.

More formally, a group signature scheme is a primitive allowing the sender to generate publicly verifiable proofs that: (1) The ciphertext is well-formed and intended to some registered group member who will be able to decrypt; (2) The opening authority will be able to identify the receiver if necessary; (3) The plaintext satisfies certain properties, such as being a witness for some public relation. In the model of Kiayias, Tsiounis and Yung [KTY07], the message secrecy and anonymity properties are required to withstand active adversaries, which are granted access to decryption oracles in all security definitions.

A natural application is to allow a firewall to filter all incoming encrypted emails except those intended for some certified organization members and the content of which is additionally guaranteed to satisfy certain requirements, like the absence of malware. Furthermore, group encryption schemes are motivated by privacy applications such as anonymous trusted third parties, key recovery mechanisms or oblivious retriever storage system. In cloud storage services, group encryption enables privacy-preserving asynchronous transfers of encrypted datasets. Namely, it allows users to archive encrypted datasets on remote servers while convincing those servers that the data is indeed intended to some anonymous certified client who has a valid account to the storage provider. In case of suspicions on the archive's content, a judge should be able do identify the recipient of the archive.

To tackle the problem of designing lattice-based group encryption, we needed to handle "quadratic relations". Indeed, lattice-based zero-knowledge proof systems were able to handle only relations where witnesses are multiplied by a public value. Let us recall that, in Learning-With-Errors schemes, an encryption have the form $\mathbf{A} \cdot \mathbf{s} + \mathbf{e} + \mathbf{m}\lceil \frac{q}{2} \rceil \bmod q$, where $\mathbf{A}$ is the recipient public-key. As group encryption requires this public-key $\mathbf{A}$ to be private, a way to achieve this is to have a zero-knowledge proof system which handles relations where the witness is multiplied with a private matrix.

We address this issue introducing new technique to handle this kind of relations. These techniques, based on a *divide-and-conquer* strategy, are described in **??**, as well as the construction of the group encryption scheme proven fully-secure in the standard model. This work have been presented at Asiacrypt'16 [LLM+16b] and have been done with Benoît Libert, San Ling, Khoa Nguyen and Huaxiong Wang.

1.3.3 Adaptive Oblivious Transfer

Oblivious transfer is a primitive coined by Rabin [Rab81] and later extended by Even, Goldreich and Lempel [EGL85]. It involves a server with a database of messages indexed

from 1 to N and a receiver with a secret index $\rho \in \{1, \ldots, N\}$. The protocol allows the receiver to retrieve the ρ-th message from the database without letting it infer anything on his choice. Furthermore, the receiver only obtains the ρ-th message and learns nothing about the other messages.

In its adaptive flavor [NP99], oblivious transfer allows the receiver to interact k times with the server to obtain k messages in such a way that, each request may depend on the previously retrieved messages.

From a theoretical point of view, oblivious transfer is known to be a *complete building block* for cryptography in the sense that, if it can be realized, then any secure multiparty computation can be. In its adaptive variant, oblivious transfer has applications in privacy-preserving access to sensitive databases (such as medical records or financial data) stored in an encrypted form on a remote server.

In its basic form, (adaptive) oblivious transfer does not restrict in any way the population of users who can obtain specific records. In many sensitive databases (e.g., DNA samples or patients' medical history), however, not all users should be able to access the whole database. It is thus crucial to protect the access to certain entries conditioned on the receiver holding suitable credentials delivered by authorities. At the same time, privacy protection requires that authorized users should be able to query database records while leaking as little as possible about their interests or activities.

These requirements are handled by endowing oblivious transfer with access control, as stated by Camenish, Dubovitskaya and Neven [CDN09]. In this variant, each database record is protected by a different access control policy. Based on their attributes, users can obtain credentials from pre-determined authorities, which entitle them to anonymously retrieve database records of which the access policy accepts their certified attributes. During the transfer phase, the user demonstrates, in a zero-knowledge manner, possession of an attribute string compatible with the policy of a record in the database, as well as a credential for this attribute. The only information that the database holder eventually learns is that some user retrieved some record which he was authorized to obtain.

To achieve this, an important property is the expressiveness of such access policies. In other words, the system should be able to handle complex attribute policies while keeping time and memory consumption reasonable[2]. In this thesis, we propose in **??** a zero-knowledge protocol to efficiently handle any access policy that can be described with a logarithmic-depth boolean circuit, also known as $\mathsf{NC1}$, based on lattices. In the context of adaptive oblivious transfer with access control, most of the schemes (based on pairing assumptions) manage to handle the case of conjunctions under reasonable assumptions [CDN09, CDNZ11, ACDN13]. Under strong assumptions, however, the case of $\mathsf{NC1}$ can be taken care of [ZAW+10].

This joint work with Benoît Libert, San Ling, Khoa Nguyen and Huaxiong Wang was presented at Asiacrypt'17 [LLM+17].

[2] Here, "*reasonable*" means (probabilistic) polynomial time.

Part I

Background

Chapter 2

Chapter 1 Background

Provable security is a subfield of cryptography where constructions are proven secure with respect to a security model. To illustrate this notion, let us take the example of public-key encryption schemes. This primitive consists in three algorithms: *key generation*, *encryption* and *decryption*. These algorithms acts according to their names. Naturally, the question of "how to define the security of this set of algorithms" arises. To answer this question, we have to define the power of the adversary, and its goal. In cryptography, many approaches have been used to define this (random oracle model, universal composability (UC) [Can01]…) which give rise to stronger security guarantees. If one aims at the strongest security for its construction, there are known impossibility results in strong models. For instance, in the UC model, it is impossible to realize two-party computation [Yao86] without trusted setup [CKL06], while it is possible in the plain model [LP07].

In this chapter, we will focus on the computational complexity elements we need to define properly the security models we will use in this thesis. Then we will define these security models.

2.1 Security Reductions

Provable security provides constructions for which security is guaranteed by a security proof, or *security reduction*. The name "reduction" comes from computational complexity. In this field of computer science, research focuses on defining equivalence classes for problems or hierarchical relations between them, based on the necessary amount of resources to solve them. In order to define lower bounds for the complexity of some problems, a classical approach is to provide a construction that goes from an instance of a problem A to an instance of problem B such that, if a solution of B is found, then so is a solution of A. This amounts to saying that problem B is at least as hard as problem A up to the complexity of the transformation. For instance, Cook has shown that satisfiability of Boolean formulas is at least as hard as every problem in NP [Coo71] up to a polynomial-time transformation.

Let us now define more formally the notions of reduction and computability using the computational model of Turing machines.

Definition 2.1 (Turing Machine)**.** A k-tape Turing Machine (TM) is described by a triple $M = (\Gamma, Q, \delta)$ containing:

- A finite set Γ, called the *tape alphabet*, which contains symbols that the TM uses in its tapes. In particular, Γ contains a *blank symbol* "$\square$", and "$\triangleright$" that denotes the beginning of a tape.

- A finite set Q called the *states* of the TM. It contains special states q_{start}, q_{halt}, called respectively the *initial state* and the *halt state*.

- A function $\delta : (Q \backslash \{q_{halt}\}) \times \Gamma^{k-1} \to Q \times \Gamma^{k-1} \times \{\leftarrow, \downarrow, \rightarrow\}^k$, called the *transition function*, that describes the behavior of the internal state of the machine and the TM heads.
  Namely, $\delta(q, a_1, \ldots, a_{k-1}) = (r, b_2, \ldots, b_k, m_1, \ldots, m_k)$ means that upon reading symbols $(a_1, \ldots, a_{k-1})$ on tapes 1 to $k-1$ (where the first tape is the input tape, and the k-th tape is the output tape) on state q, the TM will move to state r, write $b_2, \ldots, b_k$ on tapes 2 to k and move its heads as dictated by $m_1, \ldots, m_k$.

A TM M is said to *compute* a function $f : \Sigma^\star \to \Gamma^\star$ if, for any finite input $x \in \Sigma^\star$ on tape T_1, blank tapes $T_2, \ldots, T_k$ with a beginning symbol $\triangleright$ and initial state q_{start}, M halts in a finite number of steps with $f(x)$ written on its output tape T_k.

A TM M is said to *recognize* a language $L \subseteq \Sigma^\star$ if, on a finite input $x \in \Sigma^\star$ written on its input tape T_1, blank tapes $T_2, \ldots, T_k$ with a beginning symbol $\triangleright$ and initial state q_{start}, the machine M eventually ends on the state q_{halt} with 1 written on its output tape if and only if $x \in L$.

A TM M is said to run in $T(n)$-time if, on any input x, it eventually stops within $T(|x|)$ steps.

A TM M is said to run in $S(n)$-space if, on any input x, it eventually stops after having written at most $S(|x|)$ memory cells in its working tapes.

Turing machines are a computational model that proved useful in complexity theory as it is convenient to evaluate the running time of a Turing machine, which amounts to bounding the number of steps the machine can take. Similarly, the working tapes works analogously to the memory of a program, and then counting the number of cells the machine uses is equivalent to evaluating the amount of memory the program requires.

From these considerations, it is possible to describe the time and space complexity of a program from the definition of Turing machines. In our context, we will work with Turing machines that run in polynomial-time and space, as polynomials benefit from good stability properties (sum, product, composition, …).

Definition 2.2 (P [Rab60])**.** The class P describes the set of languages that can be recognized by a Turing machine running in time $T(n) = \mathcal{O}(\mathsf{poly}(n))$.

In theoretical computer science, the class P is often considered as the set of "easy" problems. These problems are considered easy in the sense that the growth of the cost to solve them is asymptotically negligible in front of other functions such as exponential. In this context, it is reasonable to consider the computational power of an adversary as polynomial (or quasi-polynomial) in time and space. As cryptographic algorithms are not deterministic, we also have to consider the probabilistic version of the computation model.

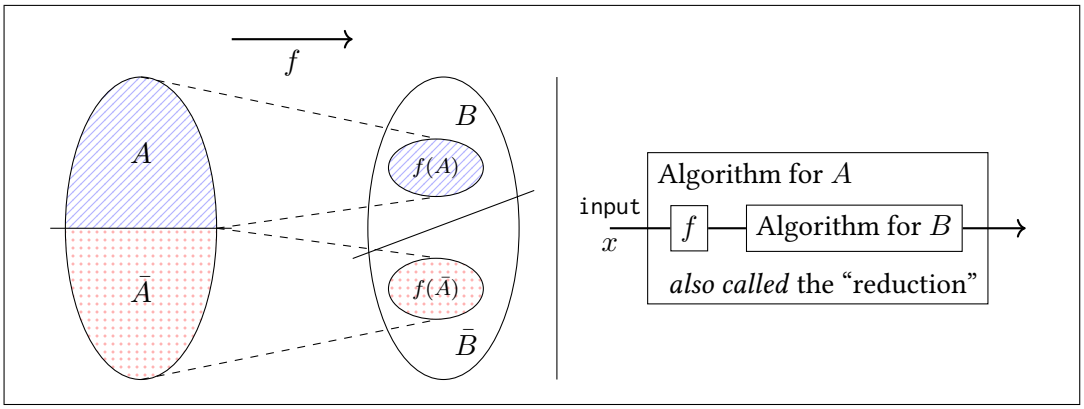


Figure 2.1 – Illustration of a polynomial-time reduction from A to B [AB09, Fig. 2.1].

Definition 2.3 (Probabilistic Turing machine)**.** A *probabilistic Turing machine* is a Turing machine with two different transition functions δ_0 and δ_1 where, at each step, a random coin is tossed to pick δ_0 or δ_1 with probability $1/2$ independently of all the previous choices.

The machine only outputs `accept` and `reject` depending on the content of the output tape at the end of the execution. We denote by $M(x)$ the random variable corresponding to the value M writes on its output tape at the end of its execution.

Definition 2.4 (PP [Gil77])**.** The class PP describes the set of languages $L \subseteq \Sigma^\star$ that a Turing machine M recognizes such that the TM M stops in time $\mathsf{poly}(|x|)$ on every input x and

$$\begin{cases} \Pr[M(x) = 1 \mid x \in L] > \frac{1}{2} \\ \Pr[M(x) = 0 \mid x \notin L] \leq \frac{1}{2} \end{cases}.$$

In the following PPT stands for "probabilistic polynomial time".

We defined complexity classes that corresponds to natural sets of programs that are of interest to us. In order to work with them, we will define the principle of polynomial time reduction.

Definition 2.5 (Polynomial time reduction)**.** A language $A \subseteq \{0,1\}^\star$ is *polynomial-time reducible to* a language $B \subseteq \{0,1\}^\star$, denoted by $A \preceq_P B$, if there is a *polynomial-time computable* function $f : \{0,1\}^\star \to \{0,1\}^\star$ such that for every $x \in \{0,1\}^\star$, $x \in A$ if and only if $f(x) \in B$.

In other words, a polynomial reduction from A to B is the description of a polynomial time algorithm (also called "*the reduction*"), that uses an algorithm for B in a black-box manner to solve A. This is illustrated in Figure 3.1.

To write down that a TM has black-box access to a TM M^O that computes function O, we sometimes use the *oracle* terminology.

Definition 2.6 (Oracle machine)**.** A Turing Machine M is said to have *oracle access* to a function $O(\cdot)$ if it has access to the result of $O(x)$ for any input x of its choice in constant time. We denote the output of M on input x with oracle O by $M^O(x)$.

We can notice that P and PP are both closed under polynomial-time reduction. Namely, if a problem is easier than another problem in P (resp. PP), then the former problem is also in P (resp. PP).

Until know, we mainly focus on the running time of the algorithms. In cryptology, it is also important to consider the success probability of algorithms: an attack is successful if the probability that it succeeds is noticeable.

Definition 2.7 (Landau notations)**.** Let f, g be two functions from $\mathbb{N}$ to $\mathbb{R}$. Let us define the so-called *Landau notations* to asymptotically compare functions.

f **is bounded by** g**:** $f(x) = \mathcal{O}(g(x))$ if there exists a constant $k > 0$ such that $|f(n)| \leq k \cdot |g(n)|$ eventually.

f **is not dominated by** g**:** $f(x) = \Omega(g(x))$ if there exists a constant $k > 0$ such that $|f(n)| \geq k \cdot |g(n)|$ eventually.

f **is bounded by** g **from above and below:** $f(x) = \Theta(g(x))$ if $f(x) = \mathcal{O}(g(x))$ and $f(x) = \Omega(g(x))$.

g **dominates** f**:** $f(x) = o(g(x))$ if for any $k > 0$, $f(n) \geq k \cdot |g(n)|$ eventually.

f **dominates** g**:** $f(x) = \omega(g(x))$ if for any $k > 0$, $|f(n)| > k \cdot |g(n)|$ eventually.

Definition 2.8 (Negligible, noticeable, overwhelming probability)**.** Let $f : \mathbb{N} \to [0, 1]$ be a function. The function f is said to be *negligible* if $f(n) = n^{-\omega(1)}$, and this is written $f(n) = \mathsf{negl}(n)$.
Non-negligible functions are also called *noticeable* functions.
Finally, if $f = 1 - \mathsf{negl}(n)$, f is said to be *overwhelming*.

Now, we have to define two more notions to be able to work on security proofs. Namely, the *security notions* and the *hardness assumptions*. The former are the statements we need to prove, and the latter are the hypotheses on which we rely.

The details of the hardness assumptions we use are given in **??**. Nevertheless, some notions are common to these and are evoked here.

The confidence one can put in a hardness assumption depends on many criteria. First of all, a weaker assumption is preferred to a stronger one. To illustrate this, let us consider the two following assumptions:

Definition 2.9 (Discrete logarithm)**.** The *discrete algorithm problem* is defined as follows. Let $(\mathbb{G}, \cdot)$ be a cyclic group of order p. Given $g, h \in \mathbb{G}$, the goal is to find the integer $a \in \mathbb{Z}_p$ such that: $g^a = h$.

The *discrete logarithm assumption* is the intractability of this problem for any PPT algorithm with noticeable probability.

Definition 2.10 (Indistinguishability)**.** Let D_0 and D_1 be two probabilistic distributions and par be public parameters. Let us define the following experiments $\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},0}$ and $\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},1}$ for any algorithm $\mathcal{D}$:

$\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},b}(\lambda)$

$x \hookleftarrow D_b$

$b' \leftarrow \mathcal{D}(1^\lambda, \mathsf{par}, x)$

return b'

The advantage of an adversary $\mathcal{D}$ for this game is defined as

$$\mathrm{Adv}^{\mathrm{Dist}}_{\mathcal{D}}(\lambda) \triangleq \left|\Pr\left[\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},1}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},0}(\lambda) = 1\right]\right|.$$

A PPT algorithm which has a noticeable advantage for the above experiments is called a *distinguisher* between D_0 and D_1.

Two distributions D_0 and D_1 are *computationally indistinguishable* if there does not exist any PPT distinguisher between those two distributions.

Definition 2.11 (Decisional Diffie-Hellman)**.** Let $\mathbb{G}$ be a cyclic group of order p. The *decisional Diffie-Hellman* (DDH) distribution is

$$\mathsf{D}_{\mathsf{DDH}} \triangleq \{(g, g^a, g^b, g^{ab}) \mid g \hookleftarrow \mathcal{U}(\mathbb{G}), a, b \hookleftarrow \mathcal{U}(\mathbb{Z}_p)\}.$$

The *DDH assumption* states that the distributions $\mathsf{D}_{\mathsf{DDH}}$ and $\mathcal{U}(\mathbb{G}^4)$ are computationally indistinguishable given the public parameter $\mathbb{G}$ (the description of the group).

The discrete logarithm assumption is implied by the decisional Diffie-Hellman assumption for instance. This is why it is preferable to work with the discrete logarithm assumption when it is possible. For instance, there is no security proofs for the El Gamal encryption scheme from DLP.

Another criterion to evaluate the security of an assumption is to look if the assumption is "simple to state" or not. This observation is buttressed by the statement of [KL07, p.25]: "*... there is a general preference for assumptions that are simpler to state, since such assumptions are easier to study and to refute.*".

Indeed, it is complicated to evaluate the security of an assumption as q-Strong Diffie-Hellman assumptions defined as follows.

Definition 2.12 (q-Strong Diffie-Hellman assumption [BB04, BBS04])**.** In a cyclic group $\mathbb{G}$, the *q-Strong Diffie-Hellman* (q-SDH) problem is, given $g, g^a, g^{a^2}, \ldots, g^{a^q}$, compute the element $g^{a^{q+1}}$.

The security of this assumption inherently depends on the parameter q of the assumption. Cheon additionally showed that, for large values of q, this assumption is no more trustworthy [Che06]. These parameterized assumptions are called *q-type assumptions*. There also exist other kinds of non-static assumptions, such as interactive assumptions. An example can be the "1-*more-DL*" assumption. Given oracle access to n discrete logarithm queries (n is not known in advance), the 1-more-DL problem is to solve a $n+1$-th discrete logarithm. These non-interactive assumptions are furthermore *non-falsifiable* according to the definition of Naor [Nao03]. Non-interactive and constant-size assumptions are sometimes called "*standard*".

The next important aspect of a security proof is the model in which it takes place. This is the purpose of the next section.

2.2 Random-Oracle Model and Standard Model

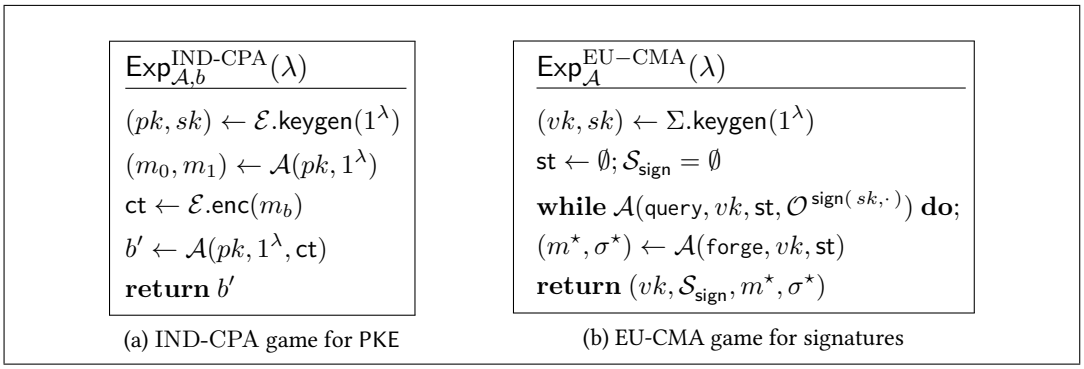
Security proofs should preferably stand in the *standard model* of computation, where no idealization is assumed on behalf of the building blocks. In this model, no implicit assumptions are assumed.

For instance, cryptographic hash functions enjoy several different associated security notions [KL07]. On of the weakest is the collision resistance, that states that it is intractable to find two strings that map to the same digest. A stronger notion is the second pre-image resistance, that states that given $x \in \{0,1\}^\star$, it is not possible for a PPT algorithm to find an $\tilde{x} \in \{0,1\}^\star$ such that $h(x) = h(\tilde{x})$. Similarly to what we saw in the previous section about DDH and DLP, we can see that collision resistance implies second pre-image resistance. Indeed, if there is an attacker against second pre-image, then one can choose a string $x \in \{0,1\}^\star$ and obtains from this attacker another string $\tilde{x} \neq x \in \{0,1\}^\star$ such that $h(x) = h(\tilde{x})$. Hence, a hash function that is collision resistant is also second pre-image resistant.

The *random oracle model* [FS86, BR93], or ROM, is an idealized security model where hash functions are assumed to behave as a truly random function. This implies collision resistance (if the codomain of the hash function is large enough) and other security notions related to hash functions. In this model, hash functions are modeled as oracles in the view of the adversary. These oracles are controlled by the reduction, meaning that the reduction can program the hash function as it likes as long as the responses look random and independent. Moreover, the reduction has access to the conversation between the adversary and the random oracle. It thus eventually knows all inputs for which the adversary chose to evaluate the function.

We can notice that this computation model is unrealistic [CGH98]. Let us construct a *counter-example*. Let Σ be a secure signature scheme, and let Σ_y be the scheme that returns $\Sigma(m)$ as a signature if and only if $h(0) \neq y$ and 0 as a signature otherwise. In the ROM h behaves as a random function. Hence, the probability that $h(0) = y$ is negligible with respect to the security parameter for any fixed y. On the other hand, it appears that when h is instantiated with a real-world hash function, then $\Sigma_{h(0)}$ is the null function, and therefore completely insecure as a signature scheme. □

In this context, one may wonder why is the ROM still used in cryptographic proofs [LMPY16, LLM+16a]. One reason is that some constructions are not known to exist yet from the standard model. For instance, non-interactive zero-knowledge (NIZK) proofs for all NP languages is not known to follow solely from lattice assumptions [Ste96, Lyu08]. NIZK proofs form an elementary building block for privacy-based cryptography. In the lattice setting, we do not have much better options that using random oracles [LLM+16a]. Another reason to use the ROM in cryptography, is because it enables much more efficient constructions and we have no example of a failure in the random oracle methodology for a natural cryptographic construction [BR93]. The example we built earlier is artificial, and in practice there is no known attacks against the ROM for a natural scheme used in real-life applications. Thus, for practical purposes, constructions in the ROM are usually more



(a) IND-CPA game for PKE

(b) EU-CMA game for signatures

Figure 2.2 – Some security games examples.

efficient. For instance, the scheme we present in **??** adapts the construction of dynamic group signature in the standard model from Libert, Peters and Yung [LPY15] to the ROM. Doing this transform reduces the signature size from 32 elements in $\mathbb{G}$, 14 elements in $\widehat{\mathbb{G}}$ and *one* scalar in the standard model [LPY15, App. J] down to 7 elements in $\mathbb{G}$ and 3 scalars in the ROM.

We now have defined the context we are working on and the base tools that allows security proofs. The following section explains how to define the security of a cryptographic primitive.

2.3 Security Games and Simulation-Based Security

In order to define security properties, a common manner is to define security *games* (or *experiments*) [GM82, Sho06].

Two examples of security game are given in Figure 3.2: to formalize the notions of *indistinguishability under chosen-plaintext attacks* (IND-CPA) for public-key encryption (PKE) schemes and *existential unforgeability under chosen message attacks* (EU-CMA) for signature schemes.

IND-CPA security is modeled by an *indistinguishability* game, meaning that the goal for the adversary $\mathcal{A}$ against this game is to distinguish between two messages from different distributions. To model this, for any adversary $\mathcal{A}$, we define a notion of *advantage* for the IND-CPA game as

$$\mathrm{Adv}^{\text{IND-CPA}}_{\mathcal{A}}(\lambda) \triangleq \left|\Pr\left[\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},1}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},0}(\lambda) = 1\right]\right|.$$

We say that a PKE scheme is IND-CPA if, for any PPT $\mathcal{A}$, the advantage of $\mathcal{A}$ in the IND-CPA game is negligible with respect to λ.

This definition of advantages models that the adversary is unable to distinguish whether the ciphertext ct comes from the experiment $\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},0}$ or the experiment $\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},1}$. As a consequence, the adversary cannot get a single bit of information about the ciphertext.

This kind of definition is also useful to model anonymity. For instance in **??**, the definition of anonymity for group signatures is defined in a similar fashion (**??**).

To handle indistinguishability between distributions, it is useful to quantify the distance between two distributions. In this context, we define the statistical distance as follows.

Definition 2.13 (Statistical Distance)**.** Let P and Q be two distributions. The *statistical distance* $\Delta(P, Q)$ between P and Q is defined as

$$\Delta(P, Q) \triangleq \frac{1}{2} \sum_{x \in \mathrm{Supp}(P) \cup \mathrm{Supp}(Q)} |P(x) - Q(x)|.$$

Two distributions are *statistically close* if their statistical distance is negligible with respect to the security parameter. It is worth noticing that if two distributions are statistically close, then the advantage of an adversary in distinguishing between them is negligible.

Notation. $P \approx_s Q$ means that P is *statistically close* to Q.

Another interesting metric, that will be used in the security proof of is the Rényi Divergence:

Definition 2.14 (Rényi divergence)**.** For any two discrete distributions P and Q such that $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$, and $a \in]1, +\infty[$, we define the *Rényi divergence* of order a by:

$$R_a(P||Q) = \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{\frac{1}{a-1}}.$$

We define the Rényi divergences of orders 1 and $+\infty$ as:

$$R_1(P||Q) = \exp\left(\sum_{x \in \mathrm{Supp}(P)} P(x) \log \frac{P(x)}{Q(x)} \right) \text{ and } R_\infty(P||Q) = \max_{x \in \mathrm{Supp}(P)} \frac{P(x)}{Q(x)}.$$

The divergence R_1 is the (exponential) of the Kullback-Leibler divergence.

Bai, Langlois, Lepoint, Stehlé and Steinfeld [BLL+15] observed that the Rényi Divergence has a property similar to the *triangular inequality* with respect to multiplication, and can be useful in the context of unforgeability game as we will explain it in the following paragraph. Prest further presented multiple uses of the Rényi Divergence in [Pre17].

We notice that security definitions for signature scheme are not indistinguishability-based experiments, but search experiments (i.e., the adversary has to output a string rather than distinguishing between two experiments by outputting a single bit). The goal of the adversary is not to distinguish between two distributions, but to forge a new signature from what it learns via signature queries.

Those signature queries are handled by an oracle $\mathcal{O}^{\mathsf{sign}(\,sk,\cdot\,)}$, which on input m returns the signature $\sigma = \Sigma.\mathsf{sign}(sk, m)$ and adds σ to $\mathcal{S}_{\mathsf{sign}}$. The initialization of these sets and the oracle's behavior may be omitted in the rest of this thesis for the sake of readability.

For EU-CMA, the advantage of an adversary $\mathcal{A}$ is defined as

$$\mathrm{Adv}^{\text{EU-CMA}}_{\mathcal{A}}(\lambda) \triangleq \Pr\left[\Sigma.\mathsf{verif}(vk, m^\star, \sigma^\star) = \top \ \wedge \ \sigma^\star \notin \mathcal{S}_{\mathsf{sign}} \right].$$

A signature scheme is considered unforgeable under chosen message attacks if, for any PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible with respect to λ.

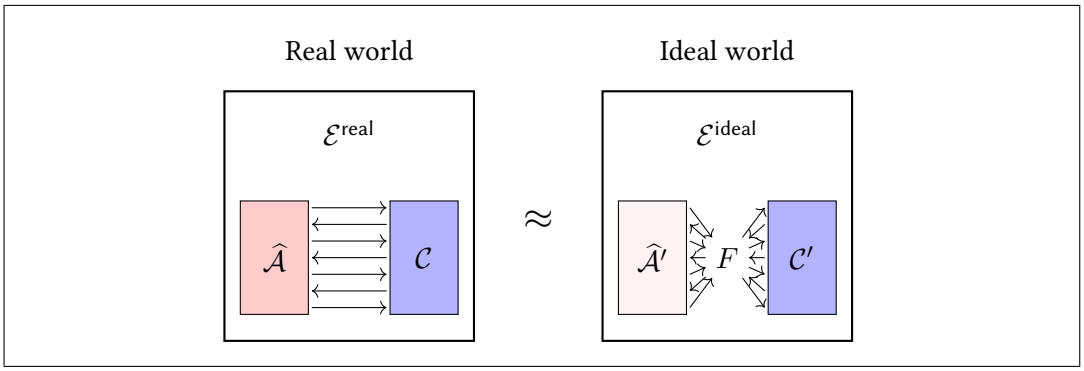


Figure 2.3 – Simulation-based cryptography.

This means that, within reasonable expected time[1], no adversary can create a new valid signature without the signing key (sk). This kind of definitions are often used in the case of authentication primitives. In our example of group signatures in Part **??**, the *security against misidentification attacks* (or *traceability*) experiment follows the same structure. This security notion illustrates that no collusion between malicious users and the group authority can create valid signatures that open on an honest user, or do not open to a valid registered user.

The security definition of IND-CPA is defined via an indistinguishability experiment. The first security definition for PKE was nevertheless a simulation-based definition [GM82]. In this context, instead of distinguishing between two messages, the goal is to distinguish between two different environments. In the following, we will use the *Real world*/*Ideal world* paradigm [Can01] to describe those different environments. Namely, for PKE, it means that, for any PPT adversary $\widehat{\mathcal{A}}$ – in the *Real world* – that, interacts with a challenger $\mathcal{C}$, there exists a PPT *simulator* $\widehat{\mathcal{A}}'$ – in the *Ideal world* – that interacts with the same challenger $\mathcal{C}'$ with the difference that the functionality F is replaced by a trusted third party in the *Ideal word*.

In other words, it means that the information that $\widehat{\mathcal{A}}$ obtains from its interaction with the challenger $\mathcal{C}$ does not allow $\mathcal{A}$ to lean any more information than it does via black-box access to the functionality.

In the context of PKE, the functionality is the access to the public key pk as described in Line 2 of $\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},b}(\lambda)$. Therefore, the existence of a simulator $\widehat{\mathcal{A}}$ that does not use pk shows that $\mathcal{A}$ does not learn anything from pk.

For PKE, the simulation-based definition for chosen-plaintext security is equivalent to the indistinguishability security [Gol04, Se. 5.2.3], even if the two security definitions are conceptually different. As indistinguishability-based model are often easier to work with, they are more commonly used to prove security of PKE schemes. For other primitives, such as Oblivious Transfer (OT) described in **??**, the simulation-based definitions are strictly stronger than indistinguishability definitions [NP99]. Therefore, it is preferable to have security proofs of the strongest *possible* definitions in theoretical cryptography.

Even though, the question of which security model is the strongest remains a complex one, as it depends on many parameters: the answer mainly depends on the manner the scheme

[1]Reasonable time may have multiple definitions, in the context of theoretical cryptography, we assume that quasi-polynomial time is the upper bound of reasonable.

will be used as well as the adversarial model. For example, we know from the work of Canetti and Fischlin [CF01] that it is impossible to construct a UC-secure bit commitment scheme[2] in the plain model, while the design of such a primitive is possible assuming a *trusted setup*. In the *trusted setup* model or *common reference string* (CRS) model, all the participants are assumed to have access to a common string $\mathsf{crs} \in \{0,1\}^\star$ that is drawn from some specific distribution D_{crs}.

[2]The definition of a commitment scheme is given in **??**. To put it short, it is the digital equivalent of a safe.

Part II

Part 2

Chapter 3

Chapter 1 Part 2

Provable security is a subfield of cryptography where constructions are proven secure with respect to a security model. To illustrate this notion, let us take the example of public-key encryption schemes. This primitive consists in three algorithms: *key generation*, *encryption* and *decryption*. These algorithms acts according to their names. Naturally, the question of "how to define the security of this set of algorithms" arises. To answer this question, we have to define the power of the adversary, and its goal. In cryptography, many approaches have been used to define this (random oracle model, universal composability (UC) [Can01]…) which give rise to stronger security guarantees. If one aims at the strongest security for its construction, there are known impossibility results in strong models. For instance, in the UC model, it is impossible to realize two-party computation [Yao86] without trusted setup [CKL06], while it is possible in the plain model [LP07].

In this chapter, we will focus on the computational complexity elements we need to define properly the security models we will use in this thesis. Then we will define these security models.

3.1 Security Reductions

Provable security provides constructions for which security is guaranteed by a security proof, or *security reduction*. The name "reduction" comes from computational complexity. In this field of computer science, research focuses on defining equivalence classes for problems or hierarchical relations between them, based on the necessary amount of resources to solve them. In order to define lower bounds for the complexity of some problems, a classical approach is to provide a construction that goes from an instance of a problem A to an instance of problem B such that, if a solution of B is found, then so is a solution of A. This amounts to saying that problem B is at least as hard as problem A up to the complexity of the transformation. For instance, Cook has shown that satisfiability of Boolean formulas is at least as hard as every problem in NP [Coo71] up to a polynomial-time transformation.

Let us now define more formally the notions of reduction and computability using the computational model of Turing machines.

Definition 3.1 (Turing Machine)**.** A k-tape Turing Machine (TM) is described by a triple $M = (\Gamma, Q, \delta)$ containing:

- A finite set Γ, called the *tape alphabet*, which contains symbols that the TM uses in its tapes. In particular, Γ contains a *blank symbol* "$\square$", and "$\triangleright$" that denotes the beginning of a tape.

- A finite set Q called the *states* of the TM. It contains special states q_{start}, q_{halt}, called respectively the *initial state* and the *halt state*.

- A function $\delta : (Q \backslash \{q_{halt}\}) \times \Gamma^{k-1} \to Q \times \Gamma^{k-1} \times \{\leftarrow, \downarrow, \rightarrow\}^k$, called the *transition function*, that describes the behavior of the internal state of the machine and the TM heads.
  Namely, $\delta(q, a_1, \ldots, a_{k-1}) = (r, b_2, \ldots, b_k, m_1, \ldots, m_k)$ means that upon reading symbols $(a_1, \ldots, a_{k-1})$ on tapes 1 to $k-1$ (where the first tape is the input tape, and the k-th tape is the output tape) on state q, the TM will move to state r, write $b_2, \ldots, b_k$ on tapes 2 to k and move its heads as dictated by $m_1, \ldots, m_k$.

A TM M is said to *compute* a function $f : \Sigma^\star \to \Gamma^\star$ if, for any finite input $x \in \Sigma^\star$ on tape T_1, blank tapes $T_2, \ldots, T_k$ with a beginning symbol $\triangleright$ and initial state q_{start}, M halts in a finite number of steps with $f(x)$ written on its output tape T_k.

A TM M is said to *recognize* a language $L \subseteq \Sigma^\star$ if, on a finite input $x \in \Sigma^\star$ written on its input tape T_1, blank tapes $T_2, \ldots, T_k$ with a beginning symbol $\triangleright$ and initial state q_{start}, the machine M eventually ends on the state q_{halt} with 1 written on its output tape if and only if $x \in L$.

A TM M is said to run in $T(n)$-time if, on any input x, it eventually stops within $T(|x|)$ steps.

A TM M is said to run in $S(n)$-space if, on any input x, it eventually stops after having written at most $S(|x|)$ memory cells in its working tapes.

Turing machines are a computational model that proved useful in complexity theory as it is convenient to evaluate the running time of a Turing machine, which amounts to bounding the number of steps the machine can take. Similarly, the working tapes works analogously to the memory of a program, and then counting the number of cells the machine uses is equivalent to evaluating the amount of memory the program requires.

From these considerations, it is possible to describe the time and space complexity of a program from the definition of Turing machines. In our context, we will work with Turing machines that run in polynomial-time and space, as polynomials benefit from good stability properties (sum, product, composition, …).

Definition 3.2 (P [Rab60])**.** The class P describes the set of languages that can be recognized by a Turing machine running in time $T(n) = \mathcal{O}(\mathsf{poly}(n))$.

In theoretical computer science, the class P is often considered as the set of "easy" problems. These problems are considered easy in the sense that the growth of the cost to solve them is asymptotically negligible in front of other functions such as exponential. In this context, it is reasonable to consider the computational power of an adversary as polynomial (or quasi-polynomial) in time and space. As cryptographic algorithms are not deterministic, we also have to consider the probabilistic version of the computation model.

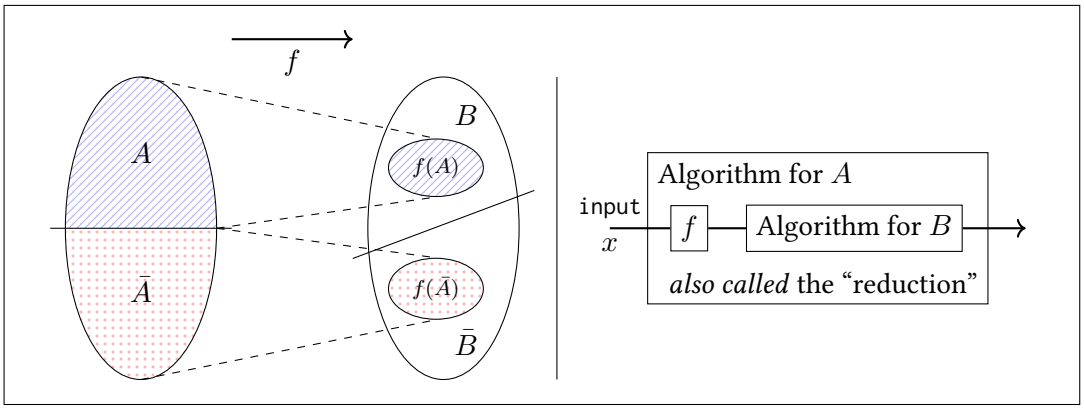


Figure 3.1 – Illustration of a polynomial-time reduction from A to B [AB09, Fig. 2.1].

Definition 3.3 (Probabilistic Turing machine)**.** A *probabilistic Turing machine* is a Turing machine with two different transition functions δ_0 and δ_1 where, at each step, a random coin is tossed to pick δ_0 or δ_1 with probability $1/2$ independently of all the previous choices.

The machine only outputs `accept` and `reject` depending on the content of the output tape at the end of the execution. We denote by $M(x)$ the random variable corresponding to the value M writes on its output tape at the end of its execution.

Definition 3.4 (PP [Gil77])**.** The class PP describes the set of languages $L \subseteq \Sigma^\star$ that a Turing machine M recognizes such that the TM M stops in time $\mathsf{poly}(|x|)$ on every input x and

$$\begin{cases} \Pr\left[M(x) = 1 \mid x \in L\right] > \frac{1}{2} \\ \Pr\left[M(x) = 0 \mid x \notin L\right] \leq \frac{1}{2} \end{cases}.$$

In the following PPT stands for "probabilistic polynomial time".

We defined complexity classes that corresponds to natural sets of programs that are of interest to us. In order to work with them, we will define the principle of polynomial time reduction.

Definition 3.5 (Polynomial time reduction)**.** A language $A \subseteq \{0,1\}^\star$ is *polynomial-time reducible to* a language $B \subseteq \{0,1\}^\star$, denoted by $A \preceq_P B$, if there is a *polynomial-time computable* function $f : \{0,1\}^\star \to \{0,1\}^\star$ such that for every $x \in \{0,1\}^\star$, $x \in A$ if and only if $f(x) \in B$.

In other words, a polynomial reduction from A to B is the description of a polynomial time algorithm (also called "*the reduction*"), that uses an algorithm for B in a black-box manner to solve A. This is illustrated in Figure 3.1.

To write down that a TM has black-box access to a TM M^O that computes function O, we sometimes use the *oracle* terminology.

Definition 3.6 (Oracle machine)**.** A Turing Machine M is said to have *oracle access* to a function $O(\cdot)$ if it has access to the result of $O(x)$ for any input x of its choice in constant time. We denote the output of M on input x with oracle O by $M^O(x)$.

We can notice that P and PP are both closed under polynomial-time reduction. Namely, if a problem is easier than another problem in P (resp. PP), then the former problem is also in P (resp. PP).

Until know, we mainly focus on the running time of the algorithms. In cryptology, it is also important to consider the success probability of algorithms: an attack is successful if the probability that it succeeds is noticeable.

Definition 3.7 (Landau notations)**.** Let f, g be two functions from $\mathbb{N}$ to $\mathbb{R}$. Let us define the so-called *Landau notations* to asymptotically compare functions.

f **is bounded by** g**:** $f(x) = \mathcal{O}(g(x))$ if there exists a constant $k > 0$ such that $|f(n)| \leq k \cdot |g(n)|$ eventually.

f **is not dominated by** g**:** $f(x) = \Omega(g(x))$ if there exists a constant $k > 0$ such that $|f(n)| \geq k \cdot |g(n)|$ eventually.

f **is bounded by** g **from above and below:** $f(x) = \Theta(g(x))$ if $f(x) = \mathcal{O}(g(x))$ and $f(x) = \Omega(g(x))$.

g **dominates** f**:** $f(x) = o(g(x))$ if for any $k > 0$, $f(n) \geq k \cdot |g(n)|$ eventually.

f **dominates** g**:** $f(x) = \omega(g(x))$ if for any $k > 0$, $|f(n)| > k \cdot |g(n)|$ eventually.

Definition 3.8 (Negligible, noticeable, overwhelming probability)**.** Let $f : \mathbb{N} \to [0, 1]$ be a function. The function f is said to be *negligible* if $f(n) = n^{-\omega(1)}$, and this is written $f(n) = \mathsf{negl}(n)$.
Non-negligible functions are also called *noticeable* functions.
Finally, if $f = 1 - \mathsf{negl}(n)$, f is said to be *overwhelming*.

Now, we have to define two more notions to be able to work on security proofs. Namely, the *security notions* and the *hardness assumptions*. The former are the statements we need to prove, and the latter are the hypotheses on which we rely.

The details of the hardness assumptions we use are given in **??**. Nevertheless, some notions are common to these and are evoked here.

The confidence one can put in a hardness assumption depends on many criteria. First of all, a weaker assumption is preferred to a stronger one. To illustrate this, let us consider the two following assumptions:

Definition 3.9 (Discrete logarithm)**.** The *discrete algorithm problem* is defined as follows. Let $(\mathbb{G}, \cdot)$ be a cyclic group of order p. Given $g, h \in \mathbb{G}$, the goal is to find the integer $a \in \mathbb{Z}_p$ such that: $g^a = h$.

The *discrete logarithm assumption* is the intractability of this problem for any PPT algorithm with noticeable probability.

Definition 3.10 (Indistinguishability)**.** Let D_0 and D_1 be two probabilistic distributions and par be public parameters. Let us define the following experiments $\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},0}$ and $\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},1}$ for any algorithm $\mathcal{D}$:

$\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},b}(\lambda)$

$x \hookleftarrow D_b$

$b' \leftarrow \mathcal{D}(1^\lambda, \mathsf{par}, x)$

return b'

The advantage of an adversary $\mathcal{D}$ for this game is defined as

$$\mathrm{Adv}^{\mathrm{Dist}}_{\mathcal{D}}(\lambda) \triangleq \left|\Pr\left[\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},1}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathrm{Dist}}_{\mathcal{D},0}(\lambda) = 1\right]\right|.$$

A PPT algorithm which has a noticeable advantage for the above experiments is called a *distinguisher* between D_0 and D_1.

Two distributions D_0 and D_1 are *computationally indistinguishable* if there does not exist any PPT distinguisher between those two distributions.

Definition 3.11 (Decisional Diffie-Hellman)**.** Let $\mathbb{G}$ be a cyclic group of order p. The *decisional Diffie-Hellman* (DDH) distribution is

$$\mathsf{D}_{\mathsf{DDH}} \triangleq \{(g, g^a, g^b, g^{ab}) \mid g \hookleftarrow \mathcal{U}(\mathbb{G}), a, b \hookleftarrow \mathcal{U}(\mathbb{Z}_p)\}.$$

The *DDH assumption* states that the distributions $\mathsf{D}_{\mathsf{DDH}}$ and $\mathcal{U}(\mathbb{G}^4)$ are computationally indistinguishable given the public parameter $\mathbb{G}$ (the description of the group).

The discrete logarithm assumption is implied by the decisional Diffie-Hellman assumption for instance. This is why it is preferable to work with the discrete logarithm assumption when it is possible. For instance, there is no security proofs for the El Gamal encryption scheme from DLP.

Another criterion to evaluate the security of an assumption is to look if the assumption is "simple to state" or not. This observation is buttressed by the statement of [KL07, p.25]: "*... there is a general preference for assumptions that are simpler to state, since such assumptions are easier to study and to refute.*".

Indeed, it is complicated to evaluate the security of an assumption as q-Strong Diffie-Hellman assumptions defined as follows.

Definition 3.12 (q-Strong Diffie-Hellman assumption [BB04, BBS04])**.** In a cyclic group $\mathbb{G}$, the *q-Strong Diffie-Hellman* (q-SDH) problem is, given $g, g^a, g^{a^2}, \ldots, g^{a^q}$, compute the element $g^{a^{q+1}}$.

The security of this assumption inherently depends on the parameter q of the assumption. Cheon additionally showed that, for large values of q, this assumption is no more trustworthy [Che06]. These parameterized assumptions are called *q-type assumptions*. There also exist other kinds of non-static assumptions, such as interactive assumptions. An example can be the "1-*more-DL*" assumption. Given oracle access to n discrete logarithm queries (n is not known in advance), the 1-more-DL problem is to solve a $n+1$-th discrete logarithm. These non-interactive assumptions are furthermore *non-falsifiable* according to the definition of Naor [Nao03]. Non-interactive and constant-size assumptions are sometimes called "*standard*".

The next important aspect of a security proof is the model in which it takes place. This is the purpose of the next section.

3.2 Random-Oracle Model and Standard Model

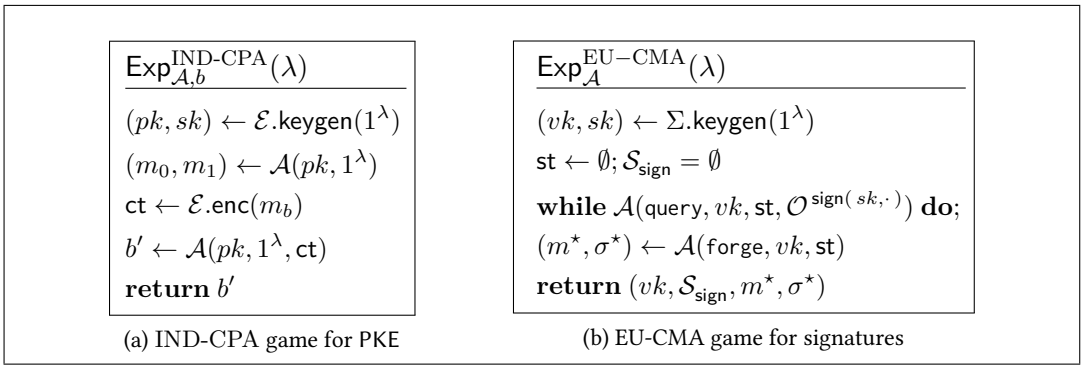
Security proofs should preferably stand in the *standard model* of computation, where no idealization is assumed on behalf of the building blocks. In this model, no implicit assumptions are assumed.

For instance, cryptographic hash functions enjoy several different associated security notions [KL07]. On of the weakest is the collision resistance, that states that it is intractable to find two strings that map to the same digest. A stronger notion is the second pre-image resistance, that states that given $x \in \{0,1\}^\star$, it is not possible for a PPT algorithm to find an $\tilde{x} \in \{0,1\}^\star$ such that $h(x) = h(\tilde{x})$. Similarly to what we saw in the previous section about DDH and DLP, we can see that collision resistance implies second pre-image resistance. Indeed, if there is an attacker against second pre-image, then one can choose a string $x \in \{0,1\}^\star$ and obtains from this attacker another string $\tilde{x} \neq x \in \{0,1\}^\star$ such that $h(x) = h(\tilde{x})$. Hence, a hash function that is collision resistant is also second pre-image resistant.

The *random oracle model* [FS86, BR93], or ROM, is an idealized security model where hash functions are assumed to behave as a truly random function. This implies collision resistance (if the codomain of the hash function is large enough) and other security notions related to hash functions. In this model, hash functions are modeled as oracles in the view of the adversary. These oracles are controlled by the reduction, meaning that the reduction can program the hash function as it likes as long as the responses look random and independent. Moreover, the reduction has access to the conversation between the adversary and the random oracle. It thus eventually knows all inputs for which the adversary chose to evaluate the function.

We can notice that this computation model is unrealistic [CGH98]. Let us construct a *counter-example*. Let Σ be a secure signature scheme, and let Σ_y be the scheme that returns $\Sigma(m)$ as a signature if and only if $h(0) \neq y$ and 0 as a signature otherwise. In the ROM h behaves as a random function. Hence, the probability that $h(0) = y$ is negligible with respect to the security parameter for any fixed y. On the other hand, it appears that when h is instantiated with a real-world hash function, then $\Sigma_{h(0)}$ is the null function, and therefore completely insecure as a signature scheme. □

In this context, one may wonder why is the ROM still used in cryptographic proofs [LMPY16, LLM+16a]. One reason is that some constructions are not known to exist yet from the standard model. For instance, non-interactive zero-knowledge (NIZK) proofs for all NP languages is not known to follow solely from lattice assumptions [Ste96, Lyu08]. NIZK proofs form an elementary building block for privacy-based cryptography. In the lattice setting, we do not have much better options that using random oracles [LLM+16a]. Another reason to use the ROM in cryptography, is because it enables much more efficient constructions and we have no example of a failure in the random oracle methodology for a natural cryptographic construction [BR93]. The example we built earlier is artificial, and in practice there is no known attacks against the ROM for a natural scheme used in real-life applications. Thus, for practical purposes, constructions in the ROM are usually more



(a) IND-CPA game for PKE

(b) EU-CMA game for signatures

Figure 3.2 – Some security games examples.

efficient. For instance, the scheme we present in **??** adapts the construction of dynamic group signature in the standard model from Libert, Peters and Yung [LPY15] to the ROM. Doing this transform reduces the signature size from 32 elements in $\mathbb{G}$, 14 elements in $\widehat{\mathbb{G}}$ and *one* scalar in the standard model [LPY15, App. J] down to 7 elements in $\mathbb{G}$ and 3 scalars in the ROM.

We now have defined the context we are working on and the base tools that allows security proofs. The following section explains how to define the security of a cryptographic primitive.

3.3 Security Games and Simulation-Based Security

In order to define security properties, a common manner is to define security *games* (or *experiments*) [GM82, Sho06].

Two examples of security game are given in Figure 3.2: to formalize the notions of *indistinguishability under chosen-plaintext attacks* (IND-CPA) for public-key encryption (PKE) schemes and *existential unforgeability under chosen message attacks* (EU-CMA) for signature schemes.

IND-CPA security is modeled by an *indistinguishability* game, meaning that the goal for the adversary $\mathcal{A}$ against this game is to distinguish between two messages from different distributions. To model this, for any adversary $\mathcal{A}$, we define a notion of *advantage* for the IND-CPA game as

$$\mathrm{Adv}^{\text{IND-CPA}}_{\mathcal{A}}(\lambda) \triangleq \left|\Pr\left[\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},1}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},0}(\lambda) = 1\right]\right|.$$

We say that a PKE scheme is IND-CPA if, for any PPT $\mathcal{A}$, the advantage of $\mathcal{A}$ in the IND-CPA game is negligible with respect to λ.

This definition of advantages models that the adversary is unable to distinguish whether the ciphertext ct comes from the experiment $\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},0}$ or the experiment $\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},1}$. As a consequence, the adversary cannot get a single bit of information about the ciphertext.

This kind of definition is also useful to model anonymity. For instance in **??**, the definition of anonymity for group signatures is defined in a similar fashion (**??**).

To handle indistinguishability between distributions, it is useful to quantify the distance between two distributions. In this context, we define the statistical distance as follows.

Definition 3.13 (Statistical Distance)**.** Let P and Q be two distributions. The *statistical distance* $\Delta(P, Q)$ between P and Q is defined as

$$\Delta(P, Q) \triangleq \frac{1}{2} \sum_{x \in \mathrm{Supp}(P) \cup \mathrm{Supp}(Q)} |P(x) - Q(x)|.$$

Two distributions are *statistically close* if their statistical distance is negligible with respect to the security parameter. It is worth noticing that if two distributions are statistically close, then the advantage of an adversary in distinguishing between them is negligible.

Notation. $P \approx_s Q$ means that P is *statistically close* to Q.

Another interesting metric, that will be used in the security proof of is the Rényi Divergence:

Definition 3.14 (Rényi divergence)**.** For any two discrete distributions P and Q such that $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$, and $a \in]1, +\infty[$, we define the *Rényi divergence* of order a by:

$$R_a(P||Q) = \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{\frac{1}{a-1}}.$$

We define the Rényi divergences of orders 1 and $+\infty$ as:

$$R_1(P||Q) = \exp\left(\sum_{x \in \mathrm{Supp}(P)} P(x) \log \frac{P(x)}{Q(x)} \right) \text{ and } R_\infty(P||Q) = \max_{x \in \mathrm{Supp}(P)} \frac{P(x)}{Q(x)}.$$

The divergence R_1 is the (exponential) of the Kullback-Leibler divergence.

Bai, Langlois, Lepoint, Stehlé and Steinfeld [BLL+15] observed that the Rényi Divergence has a property similar to the *triangular inequality* with respect to multiplication, and can be useful in the context of unforgeability game as we will explain it in the following paragraph. Prest further presented multiple uses of the Rényi Divergence in [Pre17].

We notice that security definitions for signature scheme are not indistinguishability-based experiments, but search experiments (i.e., the adversary has to output a string rather than distinguishing between two experiments by outputting a single bit). The goal of the adversary is not to distinguish between two distributions, but to forge a new signature from what it learns via signature queries.

Those signature queries are handled by an oracle $\mathcal{O}^{\mathsf{sign}(\,sk,\cdot\,)}$, which on input m returns the signature $\sigma = \Sigma.\mathsf{sign}(sk, m)$ and adds σ to $\mathcal{S}_{\mathsf{sign}}$. The initialization of these sets and the oracle's behavior may be omitted in the rest of this thesis for the sake of readability.

For EU-CMA, the advantage of an adversary $\mathcal{A}$ is defined as

$$\mathrm{Adv}^{\text{EU-CMA}}_{\mathcal{A}}(\lambda) \triangleq \Pr\left[\Sigma.\mathsf{verif}(vk, m^\star, \sigma^\star) = \top \ \wedge \ \sigma^\star \notin \mathcal{S}_{\mathsf{sign}} \right].$$

A signature scheme is considered unforgeable under chosen message attacks if, for any PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible with respect to λ.

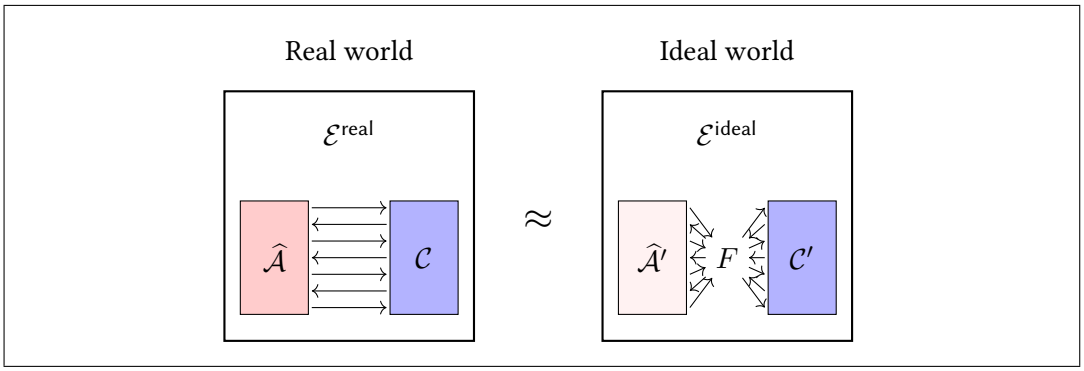


Figure 3.3 – Simulation-based cryptography.

This means that, within reasonable expected time[1], no adversary can create a new valid signature without the signing key (sk). This kind of definitions are often used in the case of authentication primitives. In our example of group signatures in Part **??**, the *security against misidentification attacks* (or *traceability*) experiment follows the same structure. This security notion illustrates that no collusion between malicious users and the group authority can create valid signatures that open on an honest user, or do not open to a valid registered user.

The security definition of IND-CPA is defined via an indistinguishability experiment. The first security definition for PKE was nevertheless a simulation-based definition [GM82]. In this context, instead of distinguishing between two messages, the goal is to distinguish between two different environments. In the following, we will use the *Real world*/*Ideal world* paradigm [Can01] to describe those different environments. Namely, for PKE, it means that, for any PPT adversary $\widehat{\mathcal{A}}$ – in the *Real world* – that, interacts with a challenger $\mathcal{C}$, there exists a PPT *simulator* $\widehat{\mathcal{A}}'$ – in the *Ideal world* – that interacts with the same challenger $\mathcal{C}'$ with the difference that the functionality F is replaced by a trusted third party in the *Ideal word*.

In other words, it means that the information that $\widehat{\mathcal{A}}$ obtains from its interaction with the challenger $\mathcal{C}$ does not allow $\mathcal{A}$ to lean any more information than it does via black-box access to the functionality.

In the context of PKE, the functionality is the access to the public key pk as described in Line 2 of $\mathsf{Exp}^{\text{IND-CPA}}_{\mathcal{A},b}(\lambda)$. Therefore, the existence of a simulator $\widehat{\mathcal{A}}$ that does not use pk shows that $\mathcal{A}$ does not learn anything from pk.

For PKE, the simulation-based definition for chosen-plaintext security is equivalent to the indistinguishability security [Gol04, Se. 5.2.3], even if the two security definitions are conceptually different. As indistinguishability-based model are often easier to work with, they are more commonly used to prove security of PKE schemes. For other primitives, such as Oblivious Transfer (OT) described in **??**, the simulation-based definitions are strictly stronger than indistinguishability definitions [NP99]. Therefore, it is preferable to have security proofs of the strongest *possible* definitions in theoretical cryptography.

Even though, the question of which security model is the strongest remains a complex one, as it depends on many parameters: the answer mainly depends on the manner the scheme

[1]Reasonable time may have multiple definitions, in the context of theoretical cryptography, we assume that quasi-polynomial time is the upper bound of reasonable.

will be used as well as the adversarial model. For example, we know from the work of Canetti and Fischlin [CF01] that it is impossible to construct a UC-secure bit commitment scheme[2] in the plain model, while the design of such a primitive is possible assuming a *trusted setup*. In the *trusted setup* model or *common reference string* (CRS) model, all the participants are assumed to have access to a common string $\mathsf{crs} \in \{0,1\}^\star$ that is drawn from some specific distribution D_{crs}.

[2]The definition of a commitment scheme is given in **??**. To put it short, it is the digital equivalent of a safe.

Conclusion

In this thesis, we presented new cryptographic schemes that rely on lattice or pairing assumptions. These contributions focus on the design and the analysis of new cryptographic schemes that target privacy-preserving applications.

In pairing-based cryptography, we proposed a practical dynamic group signature scheme, whose security relies on well-understood assumptions in the random oracle. It relies on widely used assumptions with simple and constant-size descriptions which have been studied for more than ten years. This work is also supported by an implementation in `C`.

The results in the lattice setting gave rise to three realizations of fundamental primitives that were missing in the landscape of lattice-based privacy-preserving cryptography. Even if these schemes suffer from a lack of efficiency due to their novelty, we do believe that they take one step towards a quantum-secure privacy-friendly world.

On the road, improvements have been made in the state of the art of zero-knowledge proofs in the lattice setting by providing building blocks that, we believe, are of independent interest. For example, our signature with efficient protocols has already been used to design a privacy-preserving lattice-based e-cash system [LLNW17].

All these works are proven to satisfy strong security models under simple assumptions. This provides a breeding ground for new theoretical constructions.

Open Problems

The path of providing new cryptographic primitives and proving them secure is full of pitfalls. The most obvious question that stems from this work is how to tackle the trade-offs we made in the design of those primitives. In particular, the specific question naturally arise:

Question 1. *Is it possible to build a fully-simulatable adaptive oblivious transfer (even without access control) secure under* LWE *with polynomially large modulus?*

In other words, is it possible to avoid the use of noise flooding to guarantee receiver-security in the adaptive oblivious transfer scheme of **??**. In our current protocol, this issue arises from the use of Regev's encryption scheme, where we need to prevent the noise distribution from leaking the receiver's index. However, while a finer analysis of the noise in GSW

ciphertexts [GSW13] seems promising to achieve this at reasonable cost [BdPMW16], it is not sufficient in our setting because it would leak the norm of the noise vector of ciphertexts. Then, another difficulty is to have zero-knowledge proofs compatible with the access control and the encryption components.

Question 2. *Can we construct provably-secure adaptive oblivious transfer schemes in the universal composability model?*

Our adaptive oblivious transfer scheme relies on zero-knowledge proofs to hedge against malicious adversaries. The security proofs take advantage of the fact that the proofs can be rewound to extract a witness (as described in **??**). The Peikert-Vaikuntanathan-Waters [PVW08] construction, based on dual-mode encryption, achieves 1-out-of-2 composable oblivious transfer (which can be generalized to 1-out-of-2^t OT), without relying on zero-knowledge proofs, but it does not imply OT with adaptive queries (i.e., where each index ρ_i may depend on messages received in previous transfers). Actually, the use of ZK proofs is not ruled out in this setting, as shown by the pairing-based construction of Green and Hohenberger [GH08]. However, this protocol uses the trapdoor extractability of Groth-Sahai proofs [GS08] to achieve straight-line extraction. It is not known to be possible in the lattice setting.

Question 3. *Can we obtain a more efficient compact e-cash system from lattice assumptions?*

Another privacy-preserving primitive is compact e-cash [Cha82, Cha83, CHL05]. As explained in the introduction, it is the digital equivalent of real-life money. A body of research followed its introduction [CFN88, OO91, CP92, FY93, Oka95, Tsi97], and the first compact realization was given by Camenisch, Hohenberger and Lysyanskaya [CHL05] (here, "compact" means that the complexity of coin transfers is at most logarithmic in the value of withdrawn wallets). Before the work of Libert, Ling, Nguyen and Wang [LLNW17], all compact constructions were based on traditional number-theoretic techniques. This construction still suffers from efficiency issues akin to the problem we met in this thesis. It is thus interesting to improve the efficiency of this scheme and obtain viable constructions of anonymous e-cash from post-quantum assumptions.

Zero-Knowledge Proofs

Question 4. *Can we provide NIZK proofs in the standard model for all NP languages while relying on the standard* LWE *assumption only?*

Extending the work of Groth, Ostrovsky and Sahai [GOS06] to the lattice setting would be a breakthrough result for lattice-based cryptography in general. This question remains open for more than 10 years [PV08]. A recent line of work makes steps forward in this direction [KW18, RSS18], but they rely on primitives that do not exist yet [RSS18] (NIZK proofs for a variant of the bounded decoding distance problem) or assume pre-processing [KW18].

The Stern-like proof systems we studied in this thesis, despite being flexible enough to prove a large variety of statements, suffer from the stiffness of being combinatorial. The choice of permutations used to ensure the zero-knowledge property (and thus witness-indistinguishability) is quite strict, and forces the challenge space to be ternary. This turns out to be a real bottleneck in the efficiency of such proof systems.

Question 5. *Can we get negligible soundness error in one shot for expressive statements in the post-quantum setting?*

This question can be restated as "can we combine the expressiveness of Stern-like proofs with the efficiency of Schnorr-like proof with rejection sampling?". For Stern-like protocols, decreasing the soundness error from $2/3$ to $1/2$ would already be an interesting improvements with a direct impact on the efficiency of all lattice-based schemes presented in this thesis. Recall that the *soundness error* is the probability that a cheating prover convinces an honest verifier of a false statement. As long as it is noticeably different from 1, it is possible to make the soundness error negligible by repeating the protocol a sufficient number of times. Likewise, isogeny-based proof systems [JDF11, GPS17] suffer from similar issues as the challenge space is small (binary). The $2/3$ soundness error is also present in [IKOS07], which is a technique to obtain zero-knowledge proofs relying on secure multi-party computation. With this technique, however, the size of the proof is proportional to the size of the circuit describing the relation we want to prove (which is not the case with Stern-like protocols). Thus, the question of having efficient post-quantum zero-knowledge proofs for expressive statements is a difficult question and remains open as of today.

Cryptographic Constructions

Question 6. *Can we construct more efficient lattice-based signature schemes compatible with zero-knowledge proofs?*

In the general lattice setting, the most efficient signature schemes require at least as many matrices as the length ℓ of the random tag used in the signature (like the scheme in **??**). This cost has direct impact on the efficiency and public-key size of schemes or protocols that use them: in our group signatures of **??**, for example, ℓ is logarithmic in the maximal number of members the group can accept N_{gs}. In ideal lattices, it is possible to reduce this cost to a vector of size ℓ [DM14]. In the group signature scheme of [LNWX18], which is based on ideal lattice problems, they use this property to allow an exponential number of group members to join the group, and thus propose a "constant-size" group signature scheme. The method used to construct this group signature is essentially the same as in **??**, where matrices are hidden in the ring structure of the ideal lattice [LS14]. In the construction of [LNWX18], the dependency on $\log N_{\mathsf{gs}}$ is actually hidden in the dimension of the ring. As these signatures are a fundamental building block for privacy-preserving cryptography, any improvement on them has a direct impact on the primitives or protocols that use them as a building block.

Question 7. *Can we obtain more efficient lattice-based one-time signatures in general lattices?*

In our group signature and group encryption schemes (in **??** and **??** respectively), signature and ciphertext contain a public key for a one-time signature scheme. One efficiency issue is that, in lattice-based one-time signatures [LM08, Moh11], the public-key contains a full matrix, that is part of the signature/ciphertext. Therefore, this matrix significantly increase the size of the signature/ciphertext. As security requirements for one-time signature are weaker than those of full-fledged signatures (namely, the adversary has access to only one signature per public key), we can hope for more efficient constructions of one-time signatures based on general lattices where, the public-key is smaller that a full-matrix.

As we explained in the introduction, advanced cryptography from lattices often suffers from the use of lattice trapdoors. Thus, a natural question may be:

Question 8. *Does an efficient trapdoor-free (H)IBE exist?*

In the group encryption scheme of **??**, for instance, trapdoors are used for two distinct purposes. They are used to build a secure public-key encryption scheme under adaptive chosen-ciphertext attacks and a signature scheme. These primitives are both induced by identity-based encryption: the Canetti-Halevi-Katz transform generically turns an IBE into a IND-CCA2 PKE [CHK04], and signatures are directly implied by IND-CPA-secure IBE [BF01, BLS01]. Actually, a recent construction due to Brakerski, Lombardi, Segev and Vaikuntanathan [BLSV18] (inspired by [DG17a]) gives a candidate which relies on garbled circuits, and is fairly inefficient compared to IBE schemes with trapdoors. Even the question of a trapdoor-less IND-CCA2 public key encryption still does not have a satisfactory solution. The construction of Peikert and Waters [PW08] is trapdoor-free, but remains very expensive.

Bibliography

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 1st edition, 2009. Citations: § 13 and 25

[ABB10] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *Eurocrypt*, volume 6110 of *LNCS*, pages 553–572. Springer, 2010. Citations: § 4

[ACDN13] Masayuki Abe, Jan Camenisch, Maria Dubovitskaya, and Ryo Nishimaki. Universally composable adaptive oblivious transfer (with access control) from standard assumptions. In *ACM Workshop on Digital Identity Management*, pages 1–12, 2013. doi:10.1145/2517881.2517883. Citations: § 7

[BB04] D. Boneh and X. Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In *Eurocrypt*, volume 3027 of *LNCS*, pages 223–238. Springer, 2004. Citations: § 4, 15, and 27

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *Crypto*, volume 3152 of *LNCS*, pages 41–55. Springer, 2004. Citations: § 4, 15, and 27

[BCC+09] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable Proofs and Delegatable Anonymous Credentials. In *Crypto*, volume 5677 of *LNCS*, pages 108–125. Springer, 2009. Citations: § 4

[BCKL08] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. P-signatures and Noninteractive Anonymous Credentials. In *TCC*, number 4948 in LNCS, pages 356–374. Springer, 2008. Citations: § 4

[BCKL09] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. Compact E-Cash and Simulatable VRFs Revisited. In *Pairing*, volume 5671 of *LNCS*, pages 114–131. Springer, 2009. Citations: § 4

[BD18] Razvan Barbulescu and Sylvain Duquesne. Updating Key Size Estimations for Pairings. *Journal of Cryptology*, pages 1–39, 2018. doi:10.1007/s00145-018-9280-5. Citations: § 4

[BdPMW16] F. Bourse, R. del Pino, M. Minelli, and H Wee. FHE Circuit Privacy Almost for Free. In *Crypto*, number 9815 in LNCS, pages 62–89, 2016. Citations: § 34

[BF01] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, *Crypto*, pages 213–229. Springer, 2001. Citations: § 36

[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, 2015. Citations: § 3 and 5

[BLL+15] Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence

rather than the statistical distance. In *Asiacrypt*, volume 9452 of *LNCS*. Springer, 2015. Citations: § 18 and 30

[BLS01] Dan Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *Asiacrypt*, LNCS, pages 514–532. Springer, 2001. Citations: § 36

[BLSV18] Zvika Brakerski, Alex Lombardi, Gil Segev, and Vinod Vaikuntanathan. Anonymous IBE, Leakage Resilience and Circular Security from New Assumptions. In *Eurocrypt*, LNCS, pages 535–564. Springer, 2018. Citations: § 36

[BN06] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography*, pages 319–331. Springer, 2006. Citations: § 4

[Boy10] Xavier Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In *PKC*, volume 6056 of *LNCS*, pages 499–517. Springer, 2010. Citations: § 3 and 5

[BR93] Mihir Bellare and Phillip Rogaway. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols. In *CCS*. ACM, 1993. URL: http://doi.acm.org/10.1145/168588.168596, doi:10.1145/168588.168596. Citations: § 16 and 28

[BV11] Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *FOCS*, pages 97–106, 2011. Citations: § 4

[Can01] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS*, pages 136–145, 2001. Citations: § 11, 19, 23, and 31

[CDN09] J. Camenisch, M. Dubovitskaya, and G. Neven. Oblivious transfer with access control. In *ACM-CCS*, pages 131–140, 2009. Citations: § 7

[CDNZ11] J. Camenisch, M. Dubovitskaya, G. Neven, and G. Zaverucha. Oblivious transfer with hidden access control policies. In *PKC'11*, volume 6571 of *LNCS*, pages 192–209, 2011. Citations: § 7

[CF01] Ran Canetti and Marc Fischlin. Universally composable commitments. In *Crypto*, pages 19–40. Springer, 2001. Citations: § 20 and 32

[CFN88] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Crypto*, volume 403 of *LNCS*, pages 319–327, 1988. Citations: § 1 and 34

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. In *STOC*, volume 45. ACM, 1998. URL: http://doi.acm.org/10.1145/1008731.1008734, doi:10.1145/1008731.1008734. Citations: § 16 and 28

[Cha82] D. Chaum. Blind signatures for untraceable payments. In *Crypto*, LNCS, pages 199–203, 1982. Citations: § 2 and 34

[Cha83] D. Chaum. Blind signature system. In *Crypto*, LNCS, page 153, 1983. Citations: § 34

[Cha85] David Chaum. Security without Identification: Transactions System to Make Big Brother Obsolete. 28(10):1030–1044, 1985. Citations: § 2

[Che06] Jung Hee Cheon. Security analysis of the strong diffie-hellman problem. In *Eurocrypt*, volume 4004 of *LNCS*. Springer, 2006. Citations: § 15 and 27

[CHK04] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-Ciphertext Security from Identity-Based Encryption. In *Eurocrypt*, LNCS, pages 207–222. Springer, 2004. Citations: § 36

[CHKP10] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In *Eurocrypt*, volume 6110 of *LNCS*, pages 523–552. Springer, 2010. Citations: § 4

[CHL05] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In *Eurocrypt*, number 3494 in LNCS, pages 302–321. Springer, 2005. Citations: § 34

[CHL+15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the Multilinear Map over the Integers. In *Eurocrypt*, 2015. Citations: § 2

[CKL06] Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. *Journal of Cryptology*, 19(2):135–167, 2006. doi:10.1007/s00145-005-0419-9. Citations: § 11 and 23

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Eurocrypt*, number 2045 in LNCS, pages 93–118. Springer, 2001. Citations: § 2

[Coo71] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, pages 151–158. ACM, 1971. URL: http://doi.acm.org/10.1145/800157.805047, doi:10.1145/800157.805047. Citations: § 11 and 23

[CP92] D. Chaum and T. Pedersen. Transferred Cash Grows in Size. In *Eurocrypt*, volume 658 of *LNCS*, pages 390–407, 1992. Citations: § 34

[DG17a] Nico Döttling and Sanjam Garg. From Selective IBE to Full IBE and Selective HIBE. In *TCC*, LNCS, pages 372–408. Springer, 2017. Citations: § 36

[DG17b] Nico Döttling and Sanjam Garg. Identity-Based Encryption from the Diffie-Hellman Assumption. In *Crypto*, volume 10401 of *LNCS*, pages 537–569. Springer, 2017. Citations: § 4

[DM14] Léo Ducas and Daniele Micciancio. Improved Short Lattice Signatures in the Standard Model. In *Crypto*, LNCS, pages 335–352. Springer, 2014. Citations: § 35

[dPLNS17] Rafa l del Pino, Vadim Lyubashevsky, Gregory Neven, and Gregory Seiler. Practical Quantum-Safe Voting from Lattices. In *CCS*, 2017. Citations: § 4

[EGL85] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. 28(6):637–647, 1985. Citations: § 6

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *Crypto*, pages 186–194. Springer, 1986. Citations: § 16 and 28

[FY93] M. Franklin and M. Yung. Secure and efficient off-line digital money. In *ICALP*, volume 700 of *LNCS*, pages 265–276. Springer, 1993. Citations: § 34

[Gen09] C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, pages 169–178. ACM, 2009. Citations: § 4

[GH08] Matthew Green and Susan Hohenberger. Universally Composable Adaptive Oblivious Transfer. In *Asiacrypt*, number 5350 in LNCS, pages 179–197. Springer, 2008. Citations: § 34

[Gil77] John Gill. Computational Complexity of Probabilistic Turing Machines. *SIAM J. on Computing*, 6(4):675–695, 1977. arXiv:https://doi.org/10.1137/0206049, doi:10.1137/0206049. Citations: § 13 and 25

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *STOC*, pages 365–377. ACM, 1982. Citations: § 2, 17, 19, 29, and 31

[Gol04] Oded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, 2004. Citations: § 19 and 31

[GOS06] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect Non-interactive Zero Knowledge for NP. In *Eurocrypt*, 2006. Citations: § 3, 4, and 34

[GPS17] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. In *Asiacrypt*, LNCS, pages 3–33. Springer, 2017. Citations: § 35

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206. ACM, 2008. Citations: § 4

[Gro07] J. Groth. Fully anonymous group signatures without random oracles. In *Asiacrypt*, volume 4833 of *LNCS*, pages 164–180. Springer, 2007. Citations: § 4

[GS08] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *Eurocrypt*, volume 4965 of *LNCS*, pages 415–432. Springer, 2008. Citations: § 3, 4, and 34

[GSW13] C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Crypto*, number 8042 in LNCS, pages 75–92, 2013. Citations: § 4 and 34

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from Secure Multiparty Computation. In *STOC*, pages 21–30. ACM, 2007. URL: http://doi.acm.org/10.1145/1250790.1250794, doi:10.1145/1250790.1250794. Citations: § 35

[JDF11] David Jao and Luca De Feo. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In *PQCrypto*, LNCS, pages 19–34. Springer, 2011. Citations: § 35

[Jou00] Antoine Joux. A one round protocol for tripartite diffie–hellman. In Wieb Bosma, editor, *Algorithmic Number Theory*, pages 385–393. Springer, 2000. Citations: § 4

[KB16] Taechan Kim and Razvan Barbulescu. Extended tower number field sieve: A new complexity for the medium prime case. In Matthew Robshaw and Jonathan Katz, editors, *Crypto*, pages 543–571. Springer, 2016. Citations: § 4

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007. Citations: § 15, 16, 27, and 28

[KTX08] A. Kawachi, K. Tanaka, and K. Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In *Asiacrypt*, volume 5350 of *LNCS*, pages 372–389. Springer, 2008. Citations: § 3

[KTY07] Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung. Group encryption. In *Asiacrypt*, number 4833 in LNCS, pages 181–199. Springer, 2007. Citations: § 6

[KW18] Sam Kim and David J. Wu. Multi-Theorem Preprocessing NIZKs from Lattices. In *Crypto*, LNCS, page To appear. Springen, 2018. Citations: § 34

[LLM+16a] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In *Asiacrypt*, 2016. URL: http://ia.cr/2016/101. Citations: § 5, 6, 16, and 28

[LLM+16b] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Zero-knowledge arguments for matrix-vector relations and lattice-based group encryption. In *Asiacrypt*, 2016. URL: https://ia.cr/2016/879. Citations: § 5 and 6

[LLM+17] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Adaptive oblivious transfer with access control from lattice assumptions. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Asiacrypt*, pages 533–563. Springer, 2017. Citations: § 5, 6, and 7

[LLNW16] B. Libert, S. Ling, K. Nguyen, and H. Wang. Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-size Ring Signatures and Group Signatures Without Trapdoors. In *Eurocrypt*, volume 9666 of *LNCS*, pages 1–31. Springer, 2016. Citations: § 5

[LLNW17] Beno t Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash. In *Asiacrypt*, LNCS, pages 304–335. Springer, 2017. Citations: § 33 and 34

[LM08] Vadim Lyubashevsky and Daniele Micciancio. Asymptotically Efficient Lattice-Based Digital Signatures. In *TCC*, LNCS, pages 37–54. Springer, 2008. Citations: § 35

[LMPY16] Benoît Libert, Fabrice Mouhartem, Thomas Peters, and Moti Yung. Practical "signatures with efficient protocols" from simple assumptions. In *AsiaCCS*, pages 511–522. ACM, 2016. URL: http://doi.acm.org/10.1145/2897845.2897898, doi:10.1145/2897845.2897898. Citations: § 5, 16, and 28

[LNWX18] San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu. Constant-Size Group Signatures from Lattices. In *PKC*, LNCS, pages 58–88. Springer, 2018. Citations: § 35

[LP07] Yehuda Lindell and Benny Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. In Moni Naor, editor, *Eurocrypt*, pages 52–78. Springer, 2007. Citations: § 11 and 23

[LPQ17] Benoît Libert, Thomas Peters, and Chen Qian. Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts. In *PKC*, volume 10174 of *LNCS*, pages 247–276. Springer, 2017. Citations: § 4

[LPY15] Benoît Libert, Thomas Peters, and Moti Yung. Short group signatures via structure-preserving signatures: Standard model security from simple assumptions. In *Crypto*, volume 9216 of *LNCS*, pages 296–316. Springer, 2015. Citations: § 3, 17, and 29

[LS14] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 2014. Citations: § 35

[LYJP14] Benoît Libert, Moti Yung, Marc Joye, and Thomas Peters. Traceable group encryption. In *PKC 2014*, volume 8383 of *LNCS*, pages 592–610. Springer, 2014. doi:10.1007/978-3-642-54631-0_34. Citations: § 4

[Lyu08] Vadim Lyubashevsky. Lattice-based identification schemes secure under active attacks. In *PKC*, volume 4939 of *LNCS*, pages 162–179. Springer, 2008. Citations: § 3, 16, and 28

[Lyu09] Vadim Lyubashevsky. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. In *Asiacrypt*, pages 598–616. Springer, 2009. Citations: § 3

[Lyu12] V. Lyubashevsky. Lattice signatures without trapdoors. In *Eurocrypt*, volume 7237 of *LNCS*. Springer, 2012. Citations: § 5

[Moh11] Payman Mohassel. One-Time Signatures and Chameleon Hash Functions. In *SAC*, LCNS, pages 302–319. Springer, 2011. Citations: § 35

[MP12] D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Eurocrypt*, volume 7237 of *LNCS*, pages 700–718. Springer, 2012. Citations: § 4

[MSS17] Alfred Menezes, Palash Sarkar, and Shashank Singh. Challenges with Assessing the Impact of NFS Advances on the Security of Pairing-Based Cryptography. In Raphaël C.-W. Phan and Moti Yung, editors, *Paradigms in Cryptology – Mycrypt. Malicious and Exploratory Cryptology*, pages 83–108. Springer, 2017. Citations: § 4

[Nao03] Moni Naor. On cryptographic assumptions and challenges. In Springer, editor, *Crypto*, pages 96–109, 2003. Citations: § 15 and 27

[NIS17] NIST. NIST post-quantum competition. Round 1., 2017. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions. Citations: § 1

[NP99] M. Naor and B. Pinkas. Oblivious transfer with adaptive queries. In *Crypto*, volume 1666 of *LNCS*, pages 573–590, 1999. Citations: § 7, 19, and 31

[Oka95] T. Okamoto. An efficient divisible electronic cash scheme. In *Crypto*, volume 963 of *LNCS*, pages 438–451. Springer, 1995. Citations: § 34

[OO91] K. Ohta and T. Okamoto. Universal electronic cash. In *Crypto*, volume 576 of *LNCS*, pages 324–337. Springer, 1991. Citations: § 34

[Pre17] Thomas Prest. Sharper Bounds in Lattice-Based Cryptography Using the Rényi Divergence. In *Asiacrypt*, LNCS, pages 347–374o. Springer, 2017. Citations: § 18 and 30

[PV08] C. Peikert and V. Vaikuntanathan. Non-interactive statistical zero-knowledge proofs for lattice problems. In *Crypto*, volume 5157 of *LNCS*, pages 536–553. Springer, 2008. Citations: § 34

[PVW08] C. Peikert, V. Vaikuntanathan, and B. Waters. A framework for efficient and composable oblivious transfer. In *Crypto*, volume 5157 of *LNCS*, pages 554–571, 2008. Citations: § 34

[PW08] Chris Peikert and Brent Waters. Lossy Trapdoor Functions and Their Applications. In *STOC*, pages 187–196. ACM, 2008. Citations: § 36

[Rab60] Michael Oser Rabin. Degree of difficulty of computing a function and a partial ordering of recursive sets. Technical Report 2, Hebrew University of Jerusalem, 1960. Citations: § 12 and 24

[Rab81] M. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981. Citations: § 2 and 6

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pages 84–93. ACM, 2005. Citations: § 4

[RSS18] Ron D. Rothblum, Adam Sealfon, and Katerina Sotiraki. Towards Non-Interactive Zero-Knowledge for NP from LWE. iacr ePrint Report, 2018. https://eprint.iacr.org/2018/240. Citations: § 34

[Sch96] Claus Peter Schnorr. Security of 2^t-Root Identification and Signatures. In *Crypto*, LNCS, pages 143–156. Springer, 1996. Citations: § 3

[Sho99] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999. Citations: § 1

[Sho06] Victor Shoup. Sequences of Games: A Tool for Taming Complexity in Security Proofs. Tutorial. http://www.shoup.net/papers/games.pdf, January 2006. Citations: § 17 and 29

[SOK00] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems Based on Pairings. In *Symposium on Cryptography and Information Security*, pages 26–28, 2000. Citations: § 4

[Ste96] Jacques Stern. A new paradigm for public key identification. 42(6):1757–1768, 1996. Citations: § 3, 16, and 28

[Tsi97] Y. Tsiounis. *Efficient Electronic Cash: New Notions and Techniques*. PhD thesis, 1997. Citations: § 34

[VP17] Mathy Vanhoef and Frank Piessens. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In *CCS*, pages 1313–1328. ACM, 2017. Citations: § 2

[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets. In *FOCS*, 1986. Citations: § 11 and 23

[ZAW+10] Y. Zhang, M.-H. Au, D. Wong, Q. Huang, N. Mamoulis, D. Cheung, and S.-M. Yiu. Oblivious transfer with access control: Realizing disjunction without duplication. In *Pairing*, number 6847 in LNCS, pages 96–115, 2010. Citations: § 7

List of Figures

List of Tables