UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques
i Informàtica

Treball final del grau de Matemàtiques

A key-exchange system based on imaginary quadratic fields

Gori Camps Tomàs

Director: Dr. Artur Travesa Grau
Barcelona, 20 de juny de 2021

Abstract

The aim of this project is to give an overview of the field of mathematical cryptography through the lenses of asymmetric protocols based on the Discrete Logarithm Problem over imaginary quadratic fields. The mathematical foundation is illustrated with the study of quadratic orders and their class groups, which are the relevant algebraic infrastructure for a Diffie-Hellman-type protocol known as Buchmann-Willams cryptosystem. The relationship between quadratic orders and binary quadratic forms is exploited to develop and explain the computational aspect of cryptography, providing convenient ways of machine computation. The connection between ideals in the maximal and non-maximal orders is the key to developing computationally-efficient cryptographic protocols over quadratic fields. In that sense, the Hühnlein-Jacobson and the Paulus-Takagi cryptosystems are introduced. Finally, the security component of the protocols is analyzed by discussing the Discrete Logarithm Problem and measures to obtain conjectural security.

Resum

L'objectiu del treball és donar una visió a gran escala de la criptografia matemàtica per mitjà de l'estudi de criptosistemes asimètrics basats en el problema del logaritme discret en cossos quadràtics imagniaris. La fonamentació matemàtica s'il·lustra amb l'estudi dels ordres quadràtics i els seus respectius grups de classes: l'infraestructura algebraica que permet definir un criptosistema tipus Diffie-Hellman, conegut com criptosistema de Buchmann-Williams. La relació entre ordres quadràtics i formes binàries quadràtiques permet explicar l'aspecte computacional, tot donant eines de càlcul en el grup de classes. La connexió entre ordres maximals i no maximals és la clau per a construir protocols criptogràfics eficients, entre ells els criptosistemes Hühnlein-Jacobson i Paulus-Takagi. Finalment, es tracta el problema del logaritme discret i formes d'obtenir seguretat conjectural.

2020 Mathematics Subject Classification. Primary 94A60. Secondary 11E16, 11R65, 11T71, 11Y40.

To my tutor Artur Travesa Grau for the continued advice during the project and for his revealing insights on the subject matter. To my friends, and specially to my family, for their relentless support through all these years in University.

Contents

Introduction

Cryptography and public-key cryptosystems are of great importance as security protocols in an Internet-driven society. Some parts of cryptography are founded over the cements of number theory and provide a real world application of mathematically-intensive courses. Many elements play a role in the conception and design of a cryptosystem, including, but not limited to, the mathematical foundation, algorithms and implementation.

In this project, we aim to provide a holistic approach to one type of cryptosystem, in hopes that it will serve as a comprehensive and illustrative example of the field of cryptography. Imaginary quadratic cryptography will serve as motivation to delve in the world of binary quadratic forms and quadratic fields, the relation between them and how mathematical results from the late 18^{th} century evolve during the 19^{th} century to finally give rise to cryptosystems in the 20^{th} century.

Public-key methods appear in a publication for the first time in 1976. Diffie and Hellman, co-authors of the paper, essentially describe a conjecturally one-way function, that is, a function that is easy to calculate but whose inverse is computationally intractable. The Diffie-Hellman key exchange protocol is based on the arithmetic of the multiplicative group of integers modulo a big prime[1]. This group can be replaced by other finite abelian groups. In 1988, Buchmann and Williams introduced a Diffie-Hellman-type protocol based on the class group of imaginary quadratic fields, thus giving birth to the field of quadratic field cryptography.

In the following chapters, we aim to retrace the steps of Buchmann and Williams when creating the cryptosystem. We are confronted with the problem of finding a group that is suitable for cryptographic purposes and we are interested in discussing what properties of the class group of an imaginary quadratic field put it on the spotlight as a candidate. In particular, we will find that the relation between certain ideals in the field and binary quadratic forms is a key ingredient in going back and forth between a number-theory-intensive formulation and a computationally convenient approach. In other words, we will find in the language of binary quadratic forms a way to design and implement efficient algorithms to perform the computations needed in the cryptosystem. Similarly, we will find in the language of groups of ideal classes a formalism on which to discuss the design of said cryptosystem.

Furthermore, we will go one step beyond and discuss more recent updates and modifications to the Buchmann-Willams protocol. In doing so, we will outline what properties of the underlying infrastructure of quadratic fields motivate these changes, while also reinforcing the original idea of working over quadratic fields. In this sense, the Paulus-Takagi cryptosystem will be described as a fast-decryption alternative to the Buchmann-Willams protocol.

The original Buchmann-Willams protocol was inefficient in comparison with other cryptosystems, in the sense that encryption and decryption were more costly and more information needed to be exchanged. In this setting, the updates that we discuss will work towards improving the practicality of the implementation, using once again the properties

[1]Here, "big" is related to computation power. Indeed, with advances in technology, what years back was "big" may now be too small for cryptographic purposes.

of the ideals in an imaginary quadratic field. Indeed, the running times of the protocols need to be taken into account when comparing cryptosystems for actual implementations.

Finally, a major topic in cryptography will be introduced: the security of the cryptosystem. Of course, no matter how interesting a cryptosystem is, it is security that tells apart what is useful for concealed communication and what is merely an interesting group. The Discrete Logarithm Problem and the Factoring Problem will be introduced. The difficulty of solving these problems is the basis for the security of our cryptographic protocols. We will also mention known algorithms that could possibly break the cryprosystem and how we can prevent them from doing so.

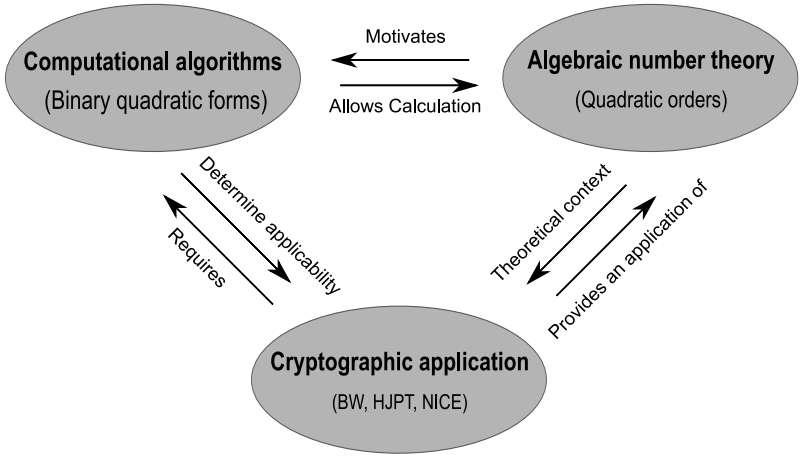

Figure 1: Outline of the content of this work. The main goal, as explained, is to exploit the relationship between the three areas in grey in the context of imaginary quadratic field cryptography.

Chapter 1

Cryptography basics and introduction to the problem

This chapter serves as a recap of the basic aspects of cryptography. The focus of attention is public-key cryptography, since it encompasses the type of protocols that are object of this project. In particular, Diffie-Hellman and ElGamal protocols are introduced and briefly analyzed (cf. Section 1.2). It is from this analysis that the motivation for the rest of the work will become apparent.

1.1 Cryptography

Informally, cryptography may be defined as the study and practice of secure communication in the presence of third parties. Alice and Bob are fictional characters commonly used as placeholders in the discussion of cryptographic protocols; other stereotypical characters are also common. With this agreement, one may say that the main concern of cryptography is to find a way for Alice and Bob to exchange a message in such a way that it cannot be read by a third party, usually named Eve or Mallory.

Nonetheless, a more formal approach is needed in most contexts; as it certainly is in a mathematics project. The definition below [Buc09] is the usual formalization behind the idea of secure communication described above.

Definition 1.1. *A* **cryptosystem** *is a tuple* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *satisfying:*

(i) $\mathcal{P}$ *is a set. It is called the* **plaintext space**. *Its elements are called* **plaintexts**.

(ii) $\mathcal{C}$ *is a set. It is called the* **ciphertext space**. *Its elements are called* **ciphertexts**.

(iii) $\mathcal{K}$ *is a set. It is called the* **key space**. *Its elements are called* **keys**.

(iv) $\mathcal{E} = \{E_k : k \in \mathcal{K}\}$ *is a family of functions* $E_k : \mathcal{P} \longrightarrow \mathcal{C}$. *Its elements are called* **encryption functions**.

(v) $\mathcal{D} = \{D_k : k \in \mathcal{K}\}$ *is family of functions* $D_k : \mathcal{C} \longrightarrow \mathcal{P}$. *Its elements are called* **decryption functions**.

(vi) For each $e \in \mathcal{K}$ there is a $d \in \mathcal{K}$ such that $D_d(E_e(p)) = p$ for all $p \in \mathcal{P}$.

1.1.1 Symmetric and asymmetric cryptosystems

According to the relationship between the encryption and decryption keys, $e \in \mathcal{K}$ and $d \in \mathcal{K}$, respectively, two types of cryptosystems are defined. If the decryption key, is either always equal to or easily obtained from the encryption key, the cryptosystem is said to be ***symmetric***. Otherwise, when the encryption and decryption keys are different and computation of the decryption key from the encryption key is infeasible, the cryptosystem is said to be ***asymmetric***. In a symmetric cryptosystem, the key must be kept secret, whereas in an asymmetric cryptosystem, the encryption key can be made public.

In the case of a symmetric cryptosystems, the secret key e must be known by both ends. Thus, a secure channel is required to exchange such key. On the other hand, in an asymmetric cryptosystem, anyone can encrypt messages using a public encryption key, but only the owner of the private decryption key can decrypt the messages. This is why asymmetric cryptosystems are also called ***public-key cryptosystems***.

Key distribution and management are more elegant and effective in a public-key cryptosystem, for example by using a publicly available directory of encryption keys. When Alice wants to send a message to Bob, all she has to do is get Bob's key from the directory, encrypt the message, and send it. However, in general, symmetric cryptosystems are faster and more convenient. Thus, traditionally, the use of asymmetric cryptosystems is restricted to key exchanges, while the key is used as the private key for a symmetric cryptosystem. With modern computers, however, the interplay between the two types of cryptosystems has somewhat changed: asymmetric cryptosystems can also be used for message exchange and many times, are.

1.1.2 Security

The objective of a cryptographic protocol is to conceal a message in such a way that it may be send through a public (insecure) channel and only understood by the desired recipient. Thus, when discussing any particular cryptosystem, it is of utmost importance to discuss in which ways (if any) someone may intercept the encrypted message and decrypt its original meaning.

In general, the security of any given cryptosystem can not be proved (the only known exception being Vernam's cipher [Buc09]). Instead, it is conjectured, usually in comparison to other cryptosystems. In other words, in most cases, it is only possible to say "a cryptosystem A is more/less/at least as secure than another cryptosystem B". Another important fact is that the security of a cryptosystem is based on known algorithms, it may be the case that a new algorithm is discovered that lets someone break a cryptosystem that was previously thought to be secure.

The security of a cryptosystem is based on difficult problems in some areas of Mathematics, such as number theory. Here, the adjective "difficult" just means that the known algorithms that could potentially break the cryptosystems are computationally unfeasible with current technology: they require too much time to solve if the secret keys are not known.

1.2 Diffie-Hellman and ElGamal

The first example of a cryptographic protocol for a key-exchange through an insecure channel is the Diffie-Hellman protocol, introduced by Whitfield Diffie and Martin Hellman in 1976 [DH76]. Originally, Diffie and Hellman worked with the multiplicative group of integers modulo a prime. However, it is immediate to generalize the protocol to an arbitrary cyclic group. We present this generalized version of the Diffie-Hellman protocol.

The key-exchange is as follows: Alice and Bob publicly agree on a cyclic group G and a generator, g, of the group. Furthermore, they choose private keys a and b, respectively. Then, Alice sends Bob g^a, while Bob sends Alice g^b. This way, both may compute the secret key $g^{ab} = (g^b)^a = (g^a)^b$. For a third party reading the messages, g^{ab} need be computed from g^a, g^b and g in order to acquire the key. The latter computation is known as the ***Diffie-Hellman Problem***. Of course, the difficulty of the problem depends on the infrastructure group. The point is, then, to find a group such that the Diffie-Hellman Problem on that group is computationally unfeasible to solve.

Similarly, ElGamal cryptosystem is an encryption protocol (rather than a key exchange protocol) based on the idea of Diffie-Hellman. This cryptosystem first appeared in 1985 [ElG85]. In the following, we briefly describe the idea behind the protocol. Let Alice choose a cyclic group $G = \langle g \rangle$ of order q and a random integer $x \in \{1, ..., q-1\}$. The public key is $(G, q, g, h := g^x)$ and the integer x is the private key. To send a message to Alice, Bob maps the message M to an element $m \in G$ and computes $s = h^y$, where $y \in \{1, ..., q-1\}$ is randomly selected by Bob himself. The message is encrypted as $(c_1, c_2) = (g^y, m \cdot s)$. To decrypt, Alice uses her secret key to compute s as c_1^x and retrieves the message as $m = c_2 \cdot s^{-1}$.

It is important to keep in mind that there are two different facets to the protocols above: one is mathematical, the other is computational. Indeed, in order to implement the ElGamal protocol, one must know how to interpret a message as an element of the group, as well as being able to operate on the group (Alice and Bob need to be able to efficiently compute inverses and powers in G).

The underlying idea is the same in both protocols, so they may be "cracked" in similar manners. The security problem in both protocols can be traced back to the Discrete Logarithm Problem, described below. It is for this reason that this (and other) protocols are all referred to as Discrete Logarithm Problem-based cryptosystems.

Definition 1.2. *In the notations above, let α be an element in the group G. The* **Discrete Logarithm Problem (DLP)** *is to find a non-negative integer x such that $\alpha = g^x$. We say that x is a discrete logarithm of α to the base g.*

Remark 1.3. *In some texts, the Discrete Logarithm Problem is stated as the problem of finding the* **smallest** *non-negative integer satisfying the condition. However, if x is a discrete logarithm of α then so is $\alpha + n|G|$ for any integer n. Because the solution to the Discrete Logarithm Problem is used to crack the cryptosystem and any discrete logarithm serves that purpose, there is no need to impose restrictions on x.*

Of course, it is obvious that an algorithm to solve the Discrete Logarithm Problem on a group G can also solve the Diffie-Hellman Problem in G. Nonetheless, up to date it

is unclear whether an algorithm to solve Diffie-Hellman Problem could be adapted to efficiently solve discrete logarithms. It is important to realise that solving the Discrete Logarithm Problem is one way to crack the cryptosystem, but there may be other (possibly more efficient) ways.

In short, the original protocols were described on the multiplicative group of residue classes of integers modulo some prime. Computations in said group can be carried out by a computer without many problems. However, it is also possible to change the group G. It is in this context that the motivation for this project arises. Ultimately, we wish to examine why class groups of orders in an imaginary quadratic field are good candidates for the group G. To do so, we must gain insight on the theory of quadratic fields and see how and why we may establish computationally-efficient algorithms to work on these groups.

Chapter 2

Quadratic fields, quadratic orders and class groups

The aim of this chapter is to introduce the relevant algebraic infrastructure necessary to define the class group of an order in a quadratic field. A brief summary of basic results over quadratic fields opens the chapter and serves as the basis to define quadratic orders, which will naturally lead to the notion of class group. Many of the results in the following sections are stated without proof. For detailed proofs, see [Tra20a] and [Tra20b].

Definition 2.1. *A* **quadratic (number) field** *is a field of degree two over the field of the rational numbers,* $\mathbb{Q}$.

Remark 2.2. *In this work, unless explicitly stated, any quadratic field will be embedded in the field of complex numbers. Notice that the set of algebraic complex numbers is an algebraic closure of the quadratic field.*

The first step in discussing quadratic fields is to give a characterization. This is done through the following proposition.

Proposition 2.3. *Let* $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ *be subfields such that* $[K : \mathbb{Q}] = 2$. *Then there is a unique element* $\theta \in K$ *such that* $K = \mathbb{Q}(\theta)$ *and* $d := \theta^2 \in \mathbb{Z}$ *is square-free. Moreover, the polynomial* $f(X) = X^2 - d \in \mathbb{Z}[X]$ *is irreducible in* $\mathbb{Q}[X]$ *and* K *is the splitting field of* $f(X)$.

The basic invariant of a quadratic field $\mathbb{Q}\left(\sqrt{d}\right)$ is its ***fundamental discriminant***, Δ, which is defined as

$$\Delta = \begin{cases} d, & \text{if } d \equiv 1 \pmod 4, \\ 4d, & \text{if } d \equiv 2, 3 \pmod 4. \end{cases} \tag{2.0.1}$$

Remark 2.4. *Notice* $\Delta \equiv 0, 1 \pmod 4$ *and the quadratic field is determined by its discriminant,* $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}(\sqrt{\Delta})$. *Moreover, since we have chosen* d *to be square-free, the case* $d \equiv 0 \pmod 4$ *is not possible.*

2.1 Quadratic algebraic integers

The concept of ring of algebraic integers is introduced in this section. In the same line of thought, a characterization for such ring in the context of quadratic fields is provided.

Definition 2.5. *Let B be a commutative ring and let $A \subseteq B$ be a subring. An element $b \in B$ is said to be integral over A if, and only if, it is the root of a monic polynomial with coefficients in A.*

Proposition 2.6. *In the notation of Definition 2.5, the set of all elements of B that are integral over A is a ring and it is called the* **integral closure of A in B**.

Definition 2.7. *Let K be a number field. The integral closure of $\mathbb{Z}$ in K is called the* **ring of integers** *of K, $\mathcal{O}_K$. The elements in the ring are called* **algebraic integers** *of K.*

Remark 2.8.

- *The algebraic integers in general (without reference to a particular field) are all the elements of $\overline{\mathbb{Q}}$ that are integral over $\mathbb{Z}$, in the sense of Definition 2.5.*
- *When confusion is possible, the elements of $\mathbb{Z}$ will be referred to as "rational integers".*
- *Notice that any algebraic integer is algebraic over the rationals.*

The next logical step in this discussion is to give a characterization of the algebraic integers that lie in a given quadratic field.

Proposition 2.9. *Let $d \neq 0, 1$ be a square-free integer. Then the set of algebraic integers in $K = \mathbb{Q}\left(\sqrt{d}\right)$ can be computed explicitly.*

(i) If $d \equiv 2, 3 \pmod 4$ then $\mathcal{O}_K = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\} = \mathbb{Z}[\sqrt{d}]$.

(ii) If $d \equiv 1 \pmod 4$ then $\mathcal{O}_K = \left\{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a \equiv b \ (mod\ 2)\right\} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Remark 2.10. *In essence, Proposition 2.9 means that the underlying group in the ring of algebraic integers in a quadratic field is a free abelian group of rank two over the integers, which admits a $\mathbb{Z}$-basis $\{1, \delta\}$, where the value of δ is*

$$\delta = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{2.1.1}$$

Equivalently, we may use the discriminant, Δ, to write $\mathcal{O}_K$ in a way that is independent on the residue class of d:

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta + \sqrt{\Delta}}{2}\right]. \tag{2.1.2}$$

Similarly, the group underlying any ideal in the ring of integers is also a free abelian group of rank two.

Proposition 2.11. *The group structure underlying any ideal in the ring of integers is itself a free abelian group of rank 2. Therefore, any ideal also admits a $\mathbb{Z}$-basis.*

The latter has one important consequence that we introduce in the following proposition, which is the quadratic case of a more general result.

Proposition 2.12. *Let K be a quadratic number field and let $\mathcal{O}_K$ be the ring of integers of K. For any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite.*

Definition 2.13. *In the notation of Proposition 2.12, the* **norm** *of the ideal $\mathfrak{a}$ is defined as $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. By the same proposition, the norm of any ideal is finite.*

The first important property of the ring of integers is that it is a Dedekind domain. This important result is summarized in the following proposition, which, again is the quadratic case of a more general result.

Proposition 2.14. *Let $\mathcal{O}_K$ be the ring of integers in a number field K. Then $\mathcal{O}_K$ is a Dedekind domain, which means that:*

(i) $\mathcal{O}_K$ is integrally closed in K. This is, if $\alpha \in K$ satisfies a monic polynomial with equation in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$.

(ii) $\mathcal{O}_K$ is Noetherian. This is, for any tower of ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ there is an integer n such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$.

(iii) Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

2.2 Class group of the ring of integers

Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ be a quadratic field of discriminant Δ. Consider the ring of integers of K, $\mathcal{O}_K$. The objective of this section is to introduce the class group of the ring of integers. There are two main ways in which this may be done. The first one is to define a group structure in the set of ideals and then obtain the class group as a quotient group. The second one is to define a certain equivalence relation in the set of ideals and then introduce the group structure in the quotient set. Both alternatives are equivalent, but there are some subtle considerations which tell them apart. The second alternative is essentially the same procedure we will use to define the class group of binary quadratic forms, because in that context the first alternative is not possible: a group structure can not be induced in the set of forms *per se*. On the other hand, the first alternative shows that in the case of the ideals in the ring of integers, the group structure can be induced in the set of ideals and, consequently, in the set of classes through a quotient group.

Consider the set of non-zero $\mathcal{O}_K$-ideals. In this set, one has the usual product of ideals as the binary operation. However, in order to have inverses the concept of fractional ideal (cf. [Tra20b], [Cox89]) is needed.

Definition 2.15. *Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ be a quadratic field and $\mathcal{O}_K$ the ring of integers of K. A* **fractional ideal** *of $\mathcal{O}_K$ is a nonzero finitely generated $\mathcal{O}_K$-submodule of K.*

Remark 2.16. *The name fractional ideal comes from the fact that any such ideal can be written in the form $\alpha\mathfrak{a}$, where $\alpha \in K$ and $\mathfrak{a}$ is a "regular" (hereafter called "integral" to avoid confusion) ideal of $\mathcal{O}_K$ (cf. Proposition 2.4.4 [Tra20b]).*

For the purposes concerning this work, the essential result is the following theorem.

Theorem 2.17. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field and let $\mathcal{O}_K$ be the ring of integers of K. The set of non-zero fractional ideals of $\mathcal{O}_K$ is a free abelian group. The product of two fractional ideals αI and βJ is $(\alpha\beta)IJ$, the inverse of a fractional ideal I is the ideal $I^{-1} := \{\alpha \in K : \alpha I \subseteq \mathcal{O}_K\}$ and the neutral element is $\mathcal{O}_K$.*

Proof. A more general version of this theorem can be found in Theorem 2.4.5 in [Tra20a]. Also, Exercise 31 of Chapter 3 in [Mar18] summarizes the main points for this proof and describes the relationship between the two points of view introduced at the beginning of this section. □

Definition 2.18. *Denote by I_K the group defined in Theorem 2.17 and by P_K the subgroup of fractional ideals of the form $\alpha\mathcal{O}_K$, where $\alpha \in K^*$, called the subgroup of principal fractional ideals. The* **ideal class group** *of $\mathcal{O}_K$, denoted by $Cl(\mathcal{O}_K)$ is the quotient group I_K/P_K.*

The original Buchmann and Williams key exchange protocol [BW88] is based on the class group of Definition 2.18. However, the theory may be taken a bit further and it is actually useful for our objective to do so. That is why, in the following sections, we introduce the concept of "order".

2.3 Orders in a quadratic field

The aim of this section is to introduce the concept of order in a quadratic field. In general, an order, unlike the ring of integers, is not a Dedekind domain. As a consequence, the ideal theory is more complicated, and we will need to restrict the ideals under consideration. The concept of orders is not needed for the original Buchmann-Williams key exchange protocol. Rather, it will be useful when working towards a generalization of the protocol that is more practical in terms of computation time.

Definition 2.19. *An* **order** *in a quadratic field K is a subset $\mathcal{O} \subset K$ such that $\mathcal{O}$ is a subring of K containing 1, $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module and $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.*

Remark 2.20.

- *The first and third conditions simply mean that the group structure of $\mathcal{O}$ is a free abelian group of rank 2. It is clear that the ring of integers itself is an order.*
- *The first and second conditions imply that any order satisfies $\mathcal{O} \subseteq \mathcal{O}_K$. Thus, we call $\mathcal{O}_K$ the* **maximal order**.
- *By condition number three, K is the field of fractions of $\mathcal{O}$.*
- *Proposition 2.12 can easily be extended to the case of orders, so that the norm of an ideal in an order is also defined as in Definition 2.13.*

Similarly, for ideals in a quadratic order we have the following result, which states that the underlying group structure is also a free abelian group of rank two.

Proposition 2.21. *Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}$. Then $\alpha_1, \alpha_2 \in \mathfrak{a}$ exist such that $\{\alpha_1, \alpha_2\}$ is a $\mathbb{Z}$-basis of the ideal $\mathfrak{a}$.*

Next, we give the essential characterization of orders in a quadratic field.

Proposition 2.22. *Let K be a quadratic field over the rationals. Let $\mathcal{O}$ be an order in K. Then the index $q = [\mathcal{O}_K : \mathcal{O}]$ is finite and $\mathcal{O} = \mathbb{Z} + q\mathcal{O}_K$. Conversely, any set $\mathcal{O} = \mathbb{Z} + q\mathcal{O}_K$ with $q \geq 1$ is an order in K such that $q = [\mathcal{O}_K : \mathcal{O}]$.*

Proof. Since $\mathcal{O}_K$ and $\mathcal{O}$ are free $\mathbb{Z}$-modules of rank 2 and $\mathcal{O} \subseteq \mathcal{O}_K$, the index $q = [\mathcal{O}_K : \mathcal{O}]$ must be finite. Now, since $q\mathcal{O}_K \subset \mathcal{O}$, it is clear that $\mathbb{Z} + q\mathcal{O}_K \subset \mathcal{O}$. It is enough to show that $q = [\mathcal{O}_K : \mathbb{Z} + q\mathcal{O}_K]$. Indeed, in that case $\mathcal{O}_K$ and $\mathbb{Z} + q\mathcal{O}_K$ must be equal because they are free abellian groups. We know that a basis for $\mathcal{O}_K$ is $\{1, \delta\}$, and it follows that $\{1, q\delta\}$ is a basis for $\mathbb{Z} + q\mathcal{O}_K$. The result is now obvious, since the change of basis is given by

$$M = \begin{bmatrix} 1 & 0 \\ 0 & q \end{bmatrix}.$$

Conversely, let $q \geq 1$ then $\mathcal{O} = \mathbb{Z} + q\mathcal{O}_K$ is an order. Indeed, it is a subring of K, it contains $1 \in K$, and it is finitely generated as a $\mathbb{Z}$-module. Furthermore, since $\mathcal{O}_K$ contains a $\mathbb{Q}$-basis $\{a_1, a_2\}$ of K, the ring $\mathcal{O}$ contains the $\mathbb{Q}$-basis $\{qa_1, qa_2\}$. □

Definition 2.23. *Let $\mathcal{O} \subset \mathcal{O}_K$ be an order. The index $[\mathcal{O}_K : \mathcal{O}]$ is called the* **conductor** *of the order $\mathcal{O}$.*

Notice that Proposition 2.22 implies that for any $q \geq 1$ there is a unique order of conductor q in K. Also, the discriminant of an order $\mathcal{O}$ is, by extension of the definition, the discriminant of any $\mathbb{Z}$-basis of the order. We have the following result.

Proposition 2.24. *The discriminant of an order $\mathcal{O}$ of conductor q is $q^2 d_K$, where d_k is the discriminant of the field K.*

Proof. In Proposition 2.9 and in the proof of Proposition 2.22, we saw that $\{1, \delta\}$ and $\{1, q\delta\}$ are $\mathbb{Z}$-basis of $\mathcal{O}_K$ and $\mathcal{O}$, respectively. Therefore the discriminant of $\mathcal{O}$ is $\mathcal{D}(1, q\delta) = q^2\mathcal{D}(1, \delta) = q^2 d_k$. □

The idea behind this last result is that the discriminants of orders in K are exactly the fundamental discriminants multiplied by a square, or, what is the same, the discriminants of binary quadratic forms. Yet another way to state this result is that for any $d \equiv 0, 1 \pmod 4$, we have $d = q^2 d_k$ for a unique $q \geq 1$ and fundamental discriminant d_k. This anticipates that the correspondence between classes of forms and classes ideals in a quadratic field will have to do with the orders of the field (see Section 3.4). Indeed, were we to only consider the maximal order, we could only establish a correspondence with the group of classes of forms of fundamental discriminant.

For any ideal of the maximal order, there is another ideal such that the product of the two is the whole ring, $\mathcal{O}_K$ (*c.f.* Theorem 2.17). We say that any ideal in the maximal order is invertible. This is, however, not true for ideals in an order. It is of interest, then, to establish a criterion to determine when an ideal in an order is invertible.

Definition 2.25. *Let $\mathcal{O}$ be an order in K. An ideal $\mathfrak{a}$ of $\mathcal{O}$ is* **proper** *if, and only if, $\mathcal{O} = \{x \in K : x\mathfrak{a} \subseteq \mathfrak{a}\}$.*

Remark 2.26. *Because $\mathfrak{a}$ is an $\mathcal{O}$-ideal, the inclusion $\mathcal{O} \subseteq \{x \in K : x\mathfrak{a} \subseteq \mathfrak{a}\}$ always holds. Moreover, the definition above generalizes trivially to fractional ideals.*

It is clear that every ideal in the maximal order is proper. Indeed, if $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$, then $\{x \in K : x\mathfrak{a} \subseteq \mathfrak{a}\}$ is an order that contains $\mathcal{O}_K$, so it must be $\mathcal{O}_K$ itself. Definition 2.25 is motivated precisely by this fact. The main result is the following theorem.

Theorem 2.27. *Let $\mathcal{O}$ be an order in K and $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then $\mathfrak{a}$ is invertible in $\mathcal{O}$ if, and only if, it is a proper ideal. Moreover, in that case the inverse is given by $\bar{\mathfrak{a}}/N(\mathfrak{a})$, where $\bar{\mathfrak{a}}$ is the conjugate ideal, that is, the ideal of all Galois conjugates of $\mathfrak{a}$.*

For clarity's sake, a technical lemma is proved before the actual theorem.

Lemma 2.28. *Let $K = \mathbb{Q}(\tau)$ be a quadratic field. Let $p(X) = aX^2 + bX + C \in \mathbb{Z}[X]$ be the minimal polynomial of τ, with $gcd(a, b, c) = 1$. Then $\langle 1, \tau\rangle$ is a proper ideal of the order $\langle 1, a\tau\rangle$.*

Proof. Fist, notice that $a\tau$ is an algebraic integer, because it is the product of the integer a times the algebraic integer τ. Therefore, $\langle 1, a\tau\rangle$ is an order. Similarly, $\langle 1, \tau\rangle$ is an ideal in the order. Let x be an element of K. The condition $x\langle 1, \tau\rangle \subset \langle 1, \tau\rangle$ in the definition of proper ideal is equivalent to $x \cdot 1 \in \langle 1, \tau\rangle$ and $x \cdot \tau \in \langle 1, \tau\rangle$.

The first condition implies that integers m and n exist such that $x = m + n\tau$. Therefore, one has that

$$x\tau = m\tau + n\tau^2 = m\tau + \frac{n}{a}(-b\tau - c) = -\frac{cn}{a} + \left(-\frac{bn}{a} + m\right)\tau.$$

Since $gcd(a, b, c) = 1$, from the above, we get that $x\tau \in \langle 1, \tau\rangle \Leftrightarrow a|n$. Therefore, $\{x \in K : x\langle 1, \tau\rangle \subset \langle 1, \tau\rangle\} = \langle 1, a\tau\rangle$. □

Proof. (Theorem 2.27) First, we prove that an invertible $\mathcal{O}$-ideal $\mathfrak{a}$ is proper. Because $\mathfrak{a}$ is invertible, an $\mathcal{O}$-ideal $\mathfrak{b}$ exists, such that $\mathfrak{ab} = \mathcal{O}$. Let $x \in K$ and $x\mathfrak{a} \subseteq \mathfrak{a}$, then

$$x\mathcal{O} = x(\mathfrak{ab}) = (x\mathfrak{a})\mathfrak{b} \subseteq \mathfrak{ab} = \mathcal{O}.$$

Therefore, $x \in \mathcal{O}$, so that $\mathfrak{a}$ is a proper ideal.

Conversely, suppose that $\{\alpha, \beta\}$ with $\alpha, \beta \in K$ is a $\mathbb{Z}$-basis for the $\mathcal{O}$-ideal $\mathfrak{a}$. Let $\tau = \beta/\alpha$ (this quotient is an element of K). Then we may write $\mathfrak{a} = \alpha\langle 1, \tau\rangle$. Consider the minimal polynomial of τ, $p(X) = aX^2 + bX + c \in \mathbb{Z}[X]$ with $gcd(a, b, c) = 1$ and the order $\langle 1, a\tau\rangle$. Let $\sigma : x \longrightarrow \overline{x}$ be the non-trivial $\mathbb{Q}$-automorphism of K. Since $\overline{\tau}$ is the other root of the minimal polynomial of τ, by Lemma 2.28, it is clear that $\bar{\mathfrak{a}} = \overline{\alpha}\langle 1, \overline{\tau}\rangle$ is an ideal of $\mathcal{O} = \langle 1, a\tau\rangle = \langle 1, a\overline{\tau}\rangle$. We claim that $\mathfrak{a}\bar{\mathfrak{a}} = \frac{N(\alpha)}{a}\mathcal{O}$.

Indeed, we have that $a\mathfrak{a}\bar{\mathfrak{a}} = a\alpha\overline{\alpha}\langle 1, \tau\rangle\langle 1, \overline{\tau}\rangle = N(\alpha)\langle a, a\tau, a\overline{\tau}, a\tau\overline{\tau}\rangle$. Using the Vieta formulas, we have that $\tau + \overline{\tau} = -\frac{b}{a}$ and $\tau\overline{\tau} = \frac{c}{a}$. Thus since $gcd(a, b, c) = 1$, $a\mathfrak{a}\bar{\mathfrak{a}} = N(\alpha)\langle a, a\tau, -b, c\rangle = N(\alpha)\langle 1, a\tau\rangle = N(\alpha)\mathcal{O}$. □

We are now able to define the class group of $\mathcal{O}$, similar to Definition 2.18. It is important to realise that at the level of orders, neither closure nor existence of inverses are guaranteed in general. This is why the notion of proper ideals is crucial, because it solves both issues. Moreover, notice that the situation in the maximal order is easier, since all ideals are proper and closure and inverse are guaranteed.

Definition 2.29. *Suppose $\mathcal{O}$ is an order and denote by $I(\mathcal{O})$ the set of* **proper** *fractional $\mathcal{O}$-ideals. By Theorem 2.27, $I(\mathcal{O})$ is a group under multiplication. Moreover, the principal ideals give a subgroup $P(\mathcal{O}) \subset I(\mathcal{O})$, so that we can consider the ideal class group of $\mathcal{O}$:*

$$Cl(\mathcal{O}) := \frac{I(\mathcal{O})}{P(\mathcal{O})}. \tag{2.3.1}$$

Notice that when $\mathcal{O} = \mathcal{O}_K$, we have the notions of the previous sections.

2.4 Orders prime to the conductor

Determining whether an ideal is proper can be a tedious task. In this section we study ideals prime to the conductor, which will provide an easier characterization of the class group of an order.

Definition 2.30. *Let $\mathcal{O}$ be an order of conductor q in a given quadratic field and let $\mathfrak{a}$ be a non-zero $\mathcal{O}$-ideal. We say that $\mathfrak{a}$ is* **prime to the conductor** *if, and only if, $\mathfrak{a} + q\mathcal{O} = \mathcal{O}$.*

The following result is the key to the relationship. Essentially, it provides a characterization of ideals prime to the conductor in terms of the norm of the ideal. Even more, it also provides a connection to proper (that is, invertible) ideals.

Proposition 2.31. *Let $\mathcal{O}$ be an order of conductor q. Then:*

(i) An $\mathcal{O}$-ideal $\mathfrak{a}$ is coprime to q if, and only if, $gcd\,(N(\mathfrak{a}), q) = 1$.

(ii) Any $\mathcal{O}$-ideal prime to q is proper, that is, invertible.

Proof. (i) Let m_q be the multiplication by q endomorphism in the abelian group $\mathcal{O}/\mathfrak{a}$. Then we have that

$$\mathfrak{a} + q\mathcal{O} = \mathcal{O} \Leftrightarrow m_q \text{ surjective} \Leftrightarrow m_q \text{ isomorphism} \Leftrightarrow gcd([\mathcal{O} : \mathfrak{a}], q) = 1.$$

In the last equivalence, we have used the structure theorem for finite abelian groups. Also notice that $[\mathcal{O} : \mathfrak{a}]$ is, by definition, the norm of $\mathfrak{a}$.

(ii) Let $\beta \in K$ such that $\beta\mathfrak{a} \subseteq \mathfrak{a}$. Then clearly $\beta \in \mathcal{O}_K$, so that $\beta\mathcal{O} = \beta(\mathfrak{a} + q\mathcal{O}) = \beta\alpha + \beta q\mathcal{O} \subseteq \mathfrak{a}q\mathcal{O}_K$. Since $q\mathcal{O}_K \subseteq \mathcal{O}$, we have that $\beta\mathcal{O} \subseteq \mathcal{O}$. That is precisely that $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal. □

Therefore, given an order $\mathcal{O}$ of conductor q, we conclude that the set of $\mathcal{O}$-ideals prime to q is, in fact, a subgroup of $I(\mathcal{O})$. Indeed, notice that the product of ideals prime to q is prime to q because the norm of the product is the product of norms, and is coprime to q. The next proposition shows that we may describe the class group of the order $\mathcal{O}$ solely in terms of ideals prime to the conductor.

Proposition 2.32. *Let $I(\mathcal{O})$ be the group of ideals of the order $\mathcal{O}$, of conductor q and let $P(\mathcal{O})$ be the subgroup of principals ideals. Similarly, let $I(\mathcal{O},q)$ and $P(\mathcal{O},q)$ the group of ideals of the order $\mathcal{O}$ prime to q and the subgroup generated by principal ideals $\alpha\mathcal{O}$ where $\alpha \in \mathcal{O}$ has norm prime to q, respectively. Then there is an isomorphism between $I(\mathcal{O},q)/P(\mathcal{O},q)$ and $C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$.*

Proof. The inclusion map $I(\mathcal{O},q) \longrightarrow C(\mathcal{O})$ is surjective, for there is an ideal prime to the conductor in any class. What's more, the kernel is the set of $I(\mathcal{O},q) \cap P(\mathcal{O})$. Clearly, we have that $P(\mathcal{O},q) \subseteq I(\mathcal{O},q) \cap P(\mathcal{O})$. For the other inclusion, let $\alpha\mathcal{O}$ be in $I(\mathcal{O},q) \cap P(\mathcal{O})$. Then we must have $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$ with α, β ideals prime to q. Let $m = N(\mathfrak{b})$, then we have $m\mathcal{O} = N(\mathfrak{b})\mathcal{O} = \mathfrak{b}\bar{\mathfrak{b}}$, so that $m\mathfrak{b}^{-1} = \bar{\mathfrak{b}}$. Finally, this implies that $m\alpha\mathcal{O} = \mathfrak{a}m\mathfrak{b}^{-1} = \mathfrak{a}\bar{\mathfrak{b}} \subseteq \mathcal{O}$. Therefore, $m\alpha\mathcal{O} \in P(\mathcal{O},q)$ and $\alpha\mathcal{O} = m\alpha\mathcal{O} \cdot (m\mathcal{O})^{-1} \in P(\mathcal{O},q)$. □

We have seen with this proposition that to determine the class group of an order with a certain conductor, we only need the ideals that are prime to that conductor. However, we can take it one step further. We now wish to see how the $\mathcal{O}$-ideals prime to the conductor relate to certain ideals in the maximal order, $\mathcal{O}_K$. First, a definition, which is analogous to Definition 2.30 but for ideals in the maximal order.

Definition 2.33. *Let $\mathcal{O}_K$ be the maximal order in an imaginary quadratic field and let m be a positive integer. We say that an $\mathcal{O}_K$-ideal $\mathfrak{a}$ is* **prime to** *m if, and only if, $\mathfrak{a} + m\mathcal{O}_K = \mathcal{O}_K$.*

With the above definition, we have the next result, which gives the explicit relationship between the ideals in an order and the maximal order.

Theorem 2.34. *Let K be an imaginary quadratic field. Let $\mathcal{O}_K$ be the maximal order in K and let $\mathcal{O}$ be an order of conductor q. Then:*

(i) If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to q, then $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal prime to q of the same norm.

(ii) If $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to q, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal prime to q of the same norm.

(iii) The map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induces an isomorphism, Φ, between the group of $\mathcal{O}$-ideals prime to q and the group of $\mathcal{O}_K$-ideals prime to q. The inverse of this map is given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$

Proof. To prove *(i)*, consider the natural map $i : \mathcal{O}/\mathfrak{a} \cap \mathcal{O} \longrightarrow \mathcal{O}_K/\mathfrak{a}$ given by

$$x(\mathfrak{a} \cap \mathcal{O}) \longmapsto x\mathfrak{a}.$$

Clearly this map is well defined, since for any order we have $\mathcal{O} \subseteq \mathcal{O}_K$. Furthermore, this map is injective, since it is an inclusion map. Because $N(\mathfrak{a})$ is prime to q, by Lagrange's Theorem, it must be that $N(\mathfrak{a} \cap \mathcal{O})$ is prime to q. Indeed, if $d \neq 0,1$ divides $N(\mathfrak{a} \cap \mathcal{O}) = |\mathcal{O}/\mathfrak{a} \cap \mathcal{O}|$, because i is injective, it must also divide $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$, contradicting the fact that $\mathfrak{a}$ is prime to the conductor. Therefore, $\mathfrak{a} \cap \mathcal{O}$ is prime to q.

Moreover, since $\mathfrak{a}$ is prime to the conductor, multiplication by q yields an automorphism of $\mathcal{O}_K/\mathfrak{a}$. Thus, since $q\mathcal{O}_K \subseteq \mathcal{O}$, i must be surjective. As a consequence, $N(\mathfrak{a}) = N(\mathfrak{a} \cap \mathcal{O})$.

Next, we prove *(iii)*. We want to show that $\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a}$ for any $\mathcal{O}$-ideal, $\mathfrak{a}$, prime to q and that $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$ for any $\mathcal{O}_K$-ideal, $\mathfrak{a}$, prime to q.

For the first equality, the inclusion $a \subseteq \mathfrak{a}\mathcal{O}_K \cap \mathcal{O}$ is obvious from the definition of $\mathcal{O}$-ideal. Conversely, we have that

$$\begin{aligned} \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} &= (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\mathcal{O}_K = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{a} + q\mathcal{O}) \\ &\subseteq \mathfrak{a} + q(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) \subseteq \mathfrak{a} + \mathfrak{a}(q\mathcal{O}_K) \subseteq \mathfrak{a} + \mathfrak{a}\mathcal{O} \subseteq \mathfrak{a}. \end{aligned} \tag{2.4.1}$$

For the second equality, the inclusion $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K \subseteq \mathfrak{a}$ is trivial. For the other inclusion, we have that $\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + q\mathcal{O}) \subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + q\mathfrak{a}$. However, since $q\mathfrak{a} \subseteq q\mathcal{O}_K \subseteq \mathcal{O}$, we have the desired inclusion.

Finally, we prove *(ii)*. Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal prime to q. Then we have that $\mathfrak{a}\mathcal{O}_K + q\mathcal{O}_K = (\mathfrak{a} + q\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K$. Therefore $\mathfrak{a}\mathcal{O}_K$ is also prime to q.

The statement about norms, comes from *(iii)* and *(i)*. From *(iii)* we get a bijection on the sets of $\mathcal{O}_K$-ideals and $\mathcal{O}$-ideals. The map $a \longmapsto \mathfrak{a}\mathcal{O}_K$ is multiplicative (this is, $(\mathfrak{a}\mathfrak{b})\mathcal{O}_K = \mathfrak{a}\mathcal{O}_K\mathfrak{b}\mathcal{O}_K$), so that we get an isomorphism between the $\mathcal{O}_K$-ideals prime to q and the $\mathcal{O}$-ideals prime to q. □

At this point, we can describe the group of classes of ideals of $\mathcal{O}$ in terms of the maximal order.

Proposition 2.35. *Let $\mathcal{O}$ be an order of conductor q in an imaginary quadratic field K. Then there are natural isomorphisms*

$$Cl(\mathcal{O}) \simeq I(\mathcal{O}, q)/P(\mathcal{O}, q) \simeq I_K(q)/P_{K,\mathbb{Z}}(q),$$

where $I_K(q)$ is the group of $\mathcal{O}_K$-ideals prime to q and $P_{K,\mathbb{Z}}(q)$ is the subgroup of $I_K(q)$ generated by principal ideals of the form $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}_K$ satisfies that $\alpha \equiv a \pmod{q\mathcal{O}_K}$ for some integer a relatively prime to q.

Proof. See [Cox89] Proposition 7.22. □

The results in the sections about orders will be central in discussing the Hühnlein-Jacobson and Paulus-Takagi variants of the Buchmann-Willams cryptosystem (cf. Section 4.4). In particular, Theorem 2.34 is the key to enable faster decryption times.

Chapter 3

Forms and quadratic fields

At this point, it is worth it to recap the basics of the previous analysis of quadratic fields. Initially, we desired to find a group on which to apply a Diffie-Hellman/ElGamal cryptographic protocol, and we proposed the class group of a quadratic field as a candidate. In the last chapter, we did primarily two things. First, we introduced the class group of a quadratic field and second, we slightly generalized this concept to quadratic orders.

However, we are yet to mention what makes the class group a suitable candidate for our cryptographic purposes. In this chapter we wish to discuss this topic in great detail. We begin by introducing binary quadratic forms and studying their basic properties, the majority of which were introduced by Gauss in his *Disquisitiones arithmeticae* [Gau96], published in 1801. Later on, we will show why computing on ideals or on binary quadratic forms is essentially the same. Certain algorithms are more efficient in the context of quadratic forms, and that is the reason why the class group is a good candidate. In short, in this chapter we delve in the computational aspect of the cryptosystems: we introduce the theoretical framework that relates ideals in a quadratic order and binary quadratic forms.

3.1 Binary quadratic forms

The main concern of this section is to introduce binary quadratic forms and provide a basic characterization of their properties. The results here presented will mostly follow [Bue89] and [Cox89]. First, a couple of useful definitions.

Definition 3.1. *A (binary integral quadratic)* **form** $f(x, y)$ *is a quadratic homogeneous polynomial in two variables with coefficients over the integers.*

$$f(X_1, X_2) := (a, b, c) := aX_1^2 + bX_1X_2 + cX_2^2 \in \mathbb{Z}[X_1, X_2].$$

Definition 3.2. *The* **discriminant** *of a form* (a, b, c) *is defined as* $D = b^2 - 4ac$.

Remark 3.3. *Notice that at the level of discriminant,* (a, b, c) *and* (c, b, a) *are the same form (only the names of variables have changed). However, when we introduce the concept of reduced forms (cf. Definition 3.15) we will see that the above forms are different.*

Definition 3.4. *A form $f(X_1, X_2) = (a, b, c)$ is said to be* **primitive** *if the the greatest common divisor of a, b and c is one, that is, $gcd(a, b, c) = 1$.*

Sometimes, it is convenient to represent binary quadratic forms as matrices. The following definition goes in that direction.

Definition 3.5. *Let $f(X_1, X_2)$ be a form. The* **matrix** *of f is the unique 2×2 symmetric matrix M_f such that*

$$f(X_1, X_2) = \begin{bmatrix} X_1 & X_2 \end{bmatrix} M_f \begin{bmatrix} X_1 \\ X_2 \end{bmatrix}.$$

For a form $f = (a, b, c)$ the matrix M_f can be written explicitly.

$$\begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}.$$

Remark 3.6. *The discriminant of a form is related to the determinant of its matrix by $D(f) = -4 \det(M_f)$.*

The first important result is the characterization of the discriminants of forms. This is the content of Proposition 3.7.

Proposition 3.7. *If (a, b, c) is a form of discriminant $D = d$, then $d \equiv 0, 1 \pmod 4$. Conversely, if $d \equiv 0, 1 \pmod 4$, there is a form g of discriminant d.*

Proof. By Definition 3.1 it is clear that $d = b^2 - 4ac \equiv b^2 \pmod 4$. Therefore, since the only quadratic residues modulo 4 are 0 and 1, it must be that $d \equiv 0, 1 \pmod 4$.

Conversely, if $d \equiv 0, 1 \pmod{mod}\ 4$ consider the form

$$g := \begin{cases} \left(1, 0, -\dfrac{d}{4}\right) & \text{if } d \equiv 0 \pmod 4, \\ \left(1, 1, \dfrac{1-d}{4}\right) & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Clearly, g is a form of discriminant d. This form is called the ***principal form*** of discriminant d. □

Remark 3.8. *As we anticipated, the discriminants of binary quadratic forms are congruent to 0 or 1 modulo 4, so they can be written as a square times a fundamental discriminant, exactly like the discriminants of quadratic orders.*

Next, we advance a result that will be studied later. It is, however, relevant to mention it here because it is the motivation for the next couple of definitions. We wish to briefly introduce composition of forms in the sense of Gauss's ***Disquisitiones arithmeticae*** [Gau96]:

Definition 3.9. *Let $f = a_1X_1^2 + b_1X_1Y_1 + c_1Y_1^2$ and $g = a_2X_2^2 + b_2x_2Y_2 + c_2Y_2^2$ be binary quadratic forms of discriminant D. There is a change of variables*

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_3 & q_4 \end{bmatrix} \begin{bmatrix} X_1X_2 \\ X_1Y_2 \\ Y_1X_2 \\ Y_1Y_2 \end{bmatrix}$$

and integers A, B and C, such that

$$(a_1X_1^2 + b_1X_1Y_1 + c_1Y_1^2)(a_2X_2^2 + b_2x_2Y_2 + c_2Y_2^2) = AX^2 + BXY + CY^2.$$

Moreover, $B^2 - 4AC = D$.

In essence, the composition of forms is not well defined at the level of forms: there is not a unique form satisfying Definition 3.9. For this reason, an equivalence relation is introduced. It is in the set of classes that the group structure is present.

Definition 3.10. *Let $f(X_1, X_2) = (a, b, c)$ be a form. Let σ be an element of $SL_2(\mathbb{Z})$. Then the form $\sigma f(X_1, X_2)$ is defined as $\sigma f(X_1, X_2) = f((X_1, X_2)\sigma)$. In other words, we perform the linear change of variables given by σ. By definition, in the matrix form, we have $M_{\sigma f} = \sigma M_f \sigma^T$.*

Remark 3.11. *The above definition is a group action of $SL_2(\mathbb{Z})$ over the set of (binary integral quadratic) forms, since if f is a form and $\sigma, \tau \in SL_2(\mathbb{Z})$ then*

$$\sigma(\tau f)(X_1, X_2) = (\tau f)((X_1, X_2)\sigma) = f((X_1, X_2)\sigma\tau) = (\sigma\tau)f(X_1, X_2).$$

It is also clear that the action of the identity matrix satisfies $(Idf)(X_1, X_2) = f(X_1, X_2)$.

The group action defined above induces an equivalence relation, namely, two elements are equivalent if, and only if, they belong to the same orbit. We end the section by stating some basic results of equivalent forms.

Proposition 3.12. *Let f and f' be forms. If f and f' are equivalent, they have the same discriminant.*

Proof. If f and f' are equivalent, then there is an element $\sigma \in SL_2(\mathbb{Z})$ such that $f' = \sigma f$. Therefore, we have $D(f') = -4\det(M_{\sigma f}) = -4(\det(\sigma))^2 \det(M_f) = D(f)$. □

Given a form (a, b, c) with discriminant $D < 0$, notice a and c must have the same sign, since it holds that $b^2 - 4ac = D$. However, if D is positive, a and c can be of the same or different sign. This motivates the definition that follows.

Definition 3.13. *Let $f(x, y) = (a, b, c)$ be a form of discriminant $D = b^2 - 4ac$. If $D < 0$ the form is said to be* **definite**. *Moreover, if both a and c are positive, the form is said to be* **positive definite**. *If $D > 0$ the form is said to be* **indefinite**.

Remark 3.14. *The discriminant has another effect on the form. Since $D \equiv b^2 \pmod 4$, it follows that the middle coefficient is even (resp. odd) if, and only if, $D \equiv 0 \pmod 4$ (resp. $D \equiv 1 \pmod 4$).*

3.2 Reduction of positive definite forms

The objective of this section is to find a canonical representative for each equivalence class of primitive positive definite forms defined in the previous section. Moreover, an explicit algorithm exists that lets one compute the representative of any given form. This algorithm is the first example of an efficient algorithm in the context of quadratic forms that can be used in the context of ideals in a quadratic order (see Chapter 4). First the notion of reduced forms is introduced.

Definition 3.15. *A primitive positive definite primitive form (a, b, c) of discriminant D is said to be* **reduced** *if, and only if, $|b| \leq a \leq c$ and if, in addition, when $|b| = a$ or $a = c$, then $b \geq 0$.*

Remark 3.16. *The nice property we want of reduced forms is that there is exactly one in any equivalence class. The additional condition is needed because otherwise (a, b, a) and $(a, -b, a)$ are reduced and equivalent. The same goes for $(a, -a, c)$ and (a, a, c).*

First, some basic results about reduced forms are introduced. Essentially, these are prerequisites before introducing the main result, which loosely states that there is a distinguished representative in every class.

Proposition 3.17. *Let $f = (a, b, c)$ be positive-definite binary quadratic form of discriminant $D = b^2 - 4ac < 0$.*

(i) If f is reduced, then $a \leq \sqrt{\frac{|D|}{3}}$.

(ii) Conversely, if $a < \sqrt{\frac{|D|}{4}}$ and $-a < b \leq a$, then f is reduced.

Proof. First, we prove (i). Since f is reduced, then $|D| = 4ac - b^2 \geq 4a^2 - a^2$. The result follows immediately. Conversely, for (ii), we need to prove that $c \geq a$. This is immediate because $c = \frac{b^2+|D|}{4a} \geq \frac{|D|}{4a} > \frac{a^2}{a} = a$. □

Proposition 3.18. *Let $d \equiv 0, 1 \pmod 4$ be a positive integer. The number of reduced forms of fixed discriminant $D = -d$ is finite.*

Proof. Let $f = (a, b, c)$ be a reduced form with discriminant $-d$. There are finitely many possible values for b. Indeed, since f is reduced $4b^2 \leq 4 \cdot a \cdot c$. By Definition 3.1, it is true that $4ac = b^2 + d$. Substituting in the previous inequality it is clearly seen that $3b^2 \leq d$. Therefore, because b is an integer, it can only take values in the finite set

$$\left\{ n \in \mathbb{Z} : -\sqrt{\frac{d}{3}} \leq n \leq \sqrt{\frac{d}{3}} \right\}.$$

Now, because $b^2 + d = 4ac$, for each possible value of b there are finitely many values of a and c, given by the factorings of $b^2 + d$. □

The important result of this section is that there is exactly one reduced form in every equivalence class of positive definite forms of negative discriminant.

Theorem 3.19. *In every class of quadratic forms of discriminant $D < 0$ there exists exactly one reduced form. In particular, the cardinality of $Cl(D)$ is finite. We call this cardinality, the* **class number** *and denote it by $h(D) := |Cl(D)|$.*

Proof. Consider a given class of quadratic forms satisfying the conditions of the theorem. Since the coefficients are integers, we may choose a form (a, b, c) for which a is minimal. Notice that for any such form $c \geq a$, since $(a, b, c) \sim (c, -b, a)$ (changing (X_1, X_2) into $(X_1, -X_1)$). Let $k = \left\lfloor \frac{a-b}{2a} \right\rfloor$. Then, changing (X_1, X_2) into $(X_1 + k \cdot X_2, X_2)$ gives a form (a', b', c') such that $a' = a$ and $b' \in (-a, a]$. Since a is minimal, we still have $a' \leq c'$, so

the form (a', b', c') is essentially reduced. In the case $c = a$, changing (a', b', c') into the equivalent form $(c', -b', a')$ sets $b \geq 0$, as desired. This proves that there is a reduced form in every class.

Conversely, let (a, b, c) be a reduced form. We claim that a is minimal among all equivalent forms. Indeed, any other a', coprime integers m and n exist such that

$$a' = am^2 + bmn + cn^2 = am^2 + \left(1 + \frac{bn}{am}\right) + cn^2 = am^2 + cn^2\left(1 + \frac{bm}{cn}\right).$$

Since $|b| \leq a \leq c$, it is clear that $a' \leq a$. What is more, the identities above also show that the only forms (a', b', c') equivalent to (a, b, c) such that $a' = a$ are obtained with $m = 1$ and $n = 0$. Therefore, the reduced form is unique.

For the last claim, notice that we have seen that there is a finite number of reduced forms and there is only one reduced form in every class. □

3.3 Class group of binary quadratic forms

The aim of this section is to introduce the class group of binary quadratic forms of a given discriminant. The reason why this group is important is because it is related to the class group of ideals in quadratic orders and provides computationally-convenient methods to perform calculations.

There is one essential difference between the case of binary quadratic forms and the case of ideals. While the set of ideals is a group in itself, the set of binary quadratic forms of a given discriminant is not; the group structure must be defined in the set of classes.

Gauss' definition of composition (Definition 3.9) is not practical since it does not give a way to obtain a composition of two forms. Moreover, it can be seen that the composite forms are not unique. In fact, it was noted by Gauss that if F is a composition, then any form equivalent to F is also a composition (see [Gau96], Fifth Section, 236-239). It was Dirichlet, student of Gauss, that came up with a more practical approach to the composition of binary quadratic forms. Nonetheless, it is important to bear in mind that Dirichlet's composition still does not induce a group structure in the set of forms: the group structure is, yet again, defined in the set of classes. Before giving Dirichlet's definition, some preliminaries are needed.

Definition 3.20. *Let (a, b, c) and (a', b', c') be two forms of the same discriminant. The forms are said to be* **united** *if a, a' and $\frac{b+b'}{2}$ are coprime.*

Remark 3.21. *Notice b and b' have the same parity, because the discriminant of the two forms is the same (cf. Remark 3.14). Therefore, the fraction in the definition is, in fact, an integer. Thus, the greatest common divisor above is well defined.*

Lemma 3.22. *Let (a, b, c) and (a', b', c') be united forms. Forms $(a, B, a'C)$ and (a', B, aC) exist such that $(a, b, c) \sim (a, B, a'C)$ and $(a', b', c') \sim (a', B, aC)$. The integer B is unique modulo $2aa'$.*

Proof. To prove this, it is sufficient to show that we can find a unique B modulo $2aa'$ that

satisfies the following congruences:

$$\begin{cases} B \equiv b \ (mod\ 2a), \\ B \equiv b' \ (mod\ 2a'), \\ B^2 \equiv D \ (mod\ 4aa'). \end{cases}$$

Indeed, in this case, if $B = 2ak + b$ then the transformation

$$M_{\sigma_1 f} = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}$$

takes (a, b, c) to an equivalent form $(a, B, \cdot)$. From the third equivalence and the fact that the new form has discriminant D, we get the third coefficient. The same procedure applies to the second form. A detailed proof of existence and uniqueness of solution can be found in [Cox89], Lemma 3.2. □

The above Lemma 3.22 is used to define Dirichlet's composition of united forms as follows.

Definition 3.23. *Let $f = (a, b, c)$ and $g = (a', b', c')$ be two united binary quadratic forms of discriminant D. Then the* **Dirichlet composition** *of f and g is the form*

$$F(X_1, X_2) := (f \circ g)(X_1, X_2) = \left(aa', B, \frac{B^2 - D}{4aa'}\right) = aa'X_1^2 + BX_2X_1 + \frac{B^2 - D}{4aa'}X_2^2,$$

where B is the integer of Lemma 3.22, which is unique modulo $2aa'$.

Remark 3.24. *It is straightforward to show that the composite is a primitive positive definite form and it is a composition of f and g in the sense of Definition 3.9. Primitiveness follows from the fact that F represents the products $f(x, y)g(z, w)$, where f and g are primitive forms.*

Theorem 3.25. *Let $D \equiv 0, 1 \pmod 4$ be negative. Then Dirichlet composition induces a well defined binary operation on the set of classes of primitive positive defined forms, $Cl(D)$. The identity element of the group is class of the principal form and the inverse of the class with representative (a, b, c) has representative $(a, -b, c)$.*

Proof. Let $f(X_1, X_2) = aX_1^2 + bX_1X_2 + cX_2^2$ and $g(X_1, X_2)$ be primitive positive definite forms. The first objective is to replace g by an equivalent form $a'X_1 + b'X_1X_2 + c'X_2$ such that $gcd(a, a') = 1$ (and, consequently, $gcd(a, a', \frac{b+b'}{2}) = 1$).

The latter can be done in two steps. First, it can be seen that if the form g primitively represents an integer m (this is, coprime integers p and q exist such that $g(p, q) = m$) then g is equivalent to a form $mX_1^2 + b'X_1X_2 + c'X_2^2$. Indeed, if p and q are coprime, then integers r, s exist such that $ps - qr = 1$. Therefore, consider the matrix

$$\sigma = \begin{bmatrix} p & q \\ r & s \end{bmatrix}.$$

The matrix σ is an element of $SL_2(\mathbb{Z})$ and transforms g into a form with m as the first coefficient.

The second step is to prove that a primitive form can primitively represent and integer that is coprime to any chosen number.

This is done as follows. Let m be an integer and consider the prime decomposition of a, c and m. Let P be the product of primes dividing a, b and c, Q the product of primes dividing a and b but not c; R the product of primes dividing c and m but not a and S the product of the remaining primes dividing m. With this definitions $gcd(Q, RS) = 1$ and g represents $aQ^2 + bQRS + (RS)^2$, which is coprime to m.

Thus, by letting $m = a$ and applying the previous results, a form with the desired property can be obtained. The Dirichlet composition, then, is defined for any pair of classes.

To get a group structure we need to show that the binary operation is well defined on the level of classes and that it induced an abelian group structure on the set $Cl(D)$. While this can certainly be done, it is easier to do it after we have established the relationship to the ideal class group. For now, we assume that both are true.

Now, let us show that the identity element is the principal form:

$$g := \begin{cases} \left(1, 0, -\dfrac{D}{4}\right) \ if\ D \equiv 0 \pmod 4, \\ \left(1, 1, \dfrac{1-D}{4}\right) \ if\ D \equiv 1 \pmod 4. \end{cases}$$

Let $f(X_1, X_2) = (a, b, c)$ be any form. Clearly, f and g are united forms and $B = b$ satisfies the conditions in Lemma 3.22, and so the form F from Definition 3.23 is f.

Finally, we prove that given a form $f(X_1, X_2) = (a, b, c)$ its opposite is the form $f'(X_1, X_2) = (a, -b, c)$. To do so, we need to show that the principal form is a composition of f and f'. Notice that f and f' are not united in general, since $gcd(a, a, (b-b)/2) = a$. However, we may obtain a form f'' equivalent to f' by applying the change of variables $(X_1, X_2) \longmapsto (-X_2, X_1)$. We get $f''(X_1, X_2) = (c, b, a)$. We may now apply Dirichlet composition, since $gcd(a, c, (b+b)/2) = gcd(a, c, b) = 1$ (remember that the forms are primitive). Clearly, $B = b$, so that the composition is the form $(ac, b, 1)$. If we show that the latter form reduces to the principal form, by Theorem 3.19, we have that they are equivalent. The reduction can be done as in the proof of the latter theorem. □

3.4 Binary quadratic fields and quadratic forms

At this point it is important to remember that the reason why we introduced binary quadratic forms is to provide computationally-efficient algorithms. Therefore, the next goal must be to justify this claim; to see why working on the class group of binary quadratic forms and on the group of classes of ideals is essentially the same.

Definition 3.26. *Let $f = (a, b, c)$ be a primitive positive definite binary quadratic form of discriminant $D < 0$. The* **root** *of f is the unique complex number τ such that τ lies in the upper-half plane $\mathbb{H}$ and $f(\tau, 1) = 0$. Since f is positive definite, it follows that $\tau = \frac{-b+\sqrt{D}}{2a}$.*

We state a couple results that illustrate why it may be useful to think about roots. In short, there is a nice relationship between forms and roots of said forms.

Proposition 3.27. *A primitive positive-definite form $f = (a, b, c)$ with root τ is reduced if, and only if τ belongs to the region*

$$F = \{z \in \mathbb{H} : |Re(z)| \leq 1/2, |z| \geq 1 \text{ and } Re(z) \geq 0 \text{ if } |Re(z)| = 1/2 or |z| = 1\}. \quad (3.4.1)$$

Remark 3.28. *It is important to remember that the cases $|b| = a$ and $a = c$ we choose the reduced form such that $b \geq 0$.*

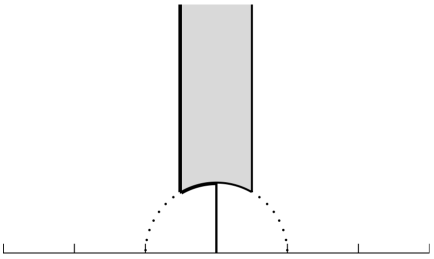

Figure 3.1: The region F of Proposition 3.27 in the upper-half complex plane.

Proposition 3.29. *Every $\tau \in \mathbb{H}$ is $SL_2(\mathbb{Z})$-equivalent to a unique point of F. Moreover, no points in F are roots of equivalent forms.*

Next, we provide the relationship between the group of classes of ideals and the group of classes of quadratic forms. The results in this section are particularly important, since they are the reason that we can even think of establishing cryptographic protocols over imaginary quadratic fields: they are the reason why we can compute on said fields in reasonable times using a computer.

Because we are considering orders (and not just the maximal order $\mathcal{O}_K$), we are able to work with any primitive positive definite form, not only with those of fundamental discriminant. Before the main theorem, we prove a technical lemma.

Lemma 3.30. *Let $f(X_1, X_2)$ and $g(X_1, X_2)$ be forms of discriminant $D < 0$. And let τ, τ' be the roots of f and g in the sense of Definition 3.26. Then the following are equivalent:*

(i) $f(X_1, X_2), g(X_1, X_2)$ *are properly equivalent.*

(ii) $\tau' = \frac{p\tau+q}{r\tau+s}$ *with* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{Z})$.

(iii) $\langle 1, \tau \rangle = \lambda \langle 1, \tau' \rangle$, $\lambda \in K^*$.

Proof. The root of a form f is the solution to $f(X, 1) = 0$ in the upper half plane, $\mathbb{H}$. Thus, the proof of this result is based on the action of $SL_2(\mathbb{Z})$ in $\mathbb{H}$.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} z \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{az+b}{cz+d} \\ 1 \end{bmatrix}$$

The latter action also provides insight into the geometrical interpretation of quadratic forms through their roots. See [Cox89] Theorem 7.7 for details. □

Theorem 3.31. *Let $\mathcal{O}$ be an order of discriminant D in an imaginary quadratic field K. Then:*

(i) If $f(X_1, X_2) = aX_1^2 + bX_1X_2 + cX_2^2$ is a primitive positive definite quadratic form of discriminant D, then $\mathfrak{a}_f = \left\langle a, \frac{-b+\sqrt{D}}{2} \right\rangle$ is a proper ideal of $\mathcal{O}$.

(ii) The map sending $f(X_1, X_2)$ to $\mathfrak{a}_f$ induces an isomorphism between the class group of forms $Cl(D)$ and the ideal class group $Cl(\mathcal{O})$.

(iii) A positive integer m is represented by a form $f(X_1, X_2)$ if, and only if, m is the norm of some ideal in the corresponding ideal class.

Proof. Let $f = aX_1^2 + bX_1X_2 + cX_2^2$ be a primitive positive definite quadratic form of discriminant D. Remember that positive definite implies that the discriminant is negative. Consider the polynomial $f(X, 1) = aX^2 + bX + c$. The roots of $f(X, 1)$ are non-real, because the discriminant is negative. Moreover, there is a unique root, τ, in the complex upper-half plane, which we defined as the *root* of $f(X_1, X_2)$. Moreover, $\tau \in K$. Because $a > 0$, we can obtain τ using the quadratic formula to get $\tau = \frac{-b+\sqrt{D}}{2a}$. With this in mind, we may write $\left\langle a, \frac{-b+\sqrt{D}}{2} \right\rangle = \langle a, a\tau \rangle = a \langle 1, \tau \rangle$.

First we prove *(i)*. By Lemma 2.28, we have that $a \langle 1, \tau \rangle$ is a proper ideal of the order $\mathcal{O} = \langle 1, a\tau \rangle$. Let q be the conductor of $\mathcal{O}$. Then by Proposition 2.24 $D = q^2 d_k$, so we have that

$$a\tau = \frac{-b + \sqrt{D}}{2} = \frac{-b + q\sqrt{d_K}}{2} =$$
$$-\frac{b + qd_K}{2} + q\left(\frac{d_K + \sqrt{d_K}}{2}\right) = -\frac{b + qd_K}{2} + q\delta.$$

Since $D = b^2 - 4ac$, qd_K and b have the same parity, so that $\langle 1, a\tau \rangle = \langle 1, q\delta \rangle$ and it follows that $\langle 1, a\tau \rangle = \mathcal{O}$. In conclusion, $a \langle 1, \tau \rangle$ is a proper ideal of $\mathcal{O}$.

We now prove *(ii)*. Notice that the mapping is well-defined over classes by Lemma 3.30. We need to show that the mapping is a bijection and that it preserves the group structure. First, we use Lemma 3.30 to show that the map $\Psi : C(D) \longrightarrow C(\mathcal{O})$ such that $f(X_1, X_2) \longmapsto a \langle 1, \tau \rangle$ is an injection.

Let $f(X_1, X_2) = (a, b, c)$ and $g(X_1, X_2) = (a', b', c')$ be two forms such that $\Psi(f) = \Psi(g)$. By definition, we have $a \langle 1, \tau \rangle = a' \langle 1, \tau' \rangle$, where τ, τ' are the roots of f and g, respectively. Now, as an element in the field, a is invertible, so that we can write $\langle 1, \tau \rangle = \frac{a'}{a} \langle 1, \tau' \rangle$, with $a'/a \in K^*$) (since f and g are forms, we have $a \neq 0$ and $\mathfrak{a}' \neq 0$). By Lemma 3.30, we have that f and g are properly equivalent, thus being the same class. This proves that Ψ is an injection.

Next, we prove that Ψ is surjective. We need to show that for any ideal $\mathfrak{a} \in \mathcal{O}$, there is a positive definite primitive form of discriminant D, f, such that $\Psi(f) = \mathfrak{a}$. Let, then, $\mathfrak{a}$ be an $\mathcal{O}$-ideal and let $\{\alpha_1, \alpha_2\}$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$, the existence of which is guaranteed by Proposition 2.21. Switching the subscripts if necessary, we may assume without loss of generality that $\tau = \alpha_2/\alpha_1$ lies in the upper half plane (effectively, what we have done here is choose an ordering for the basis). Let $p(X) = aX^2 + bX + c$ be the minimal polynomial of τ, with $gcd(a, b, c) = 1$. Since τ lies in the upper half plane, it must be that $a > 0$. Then, the form $f(X_1, X_2) = aX_1^2 + bX_1X_2 + cX_2^2$ is a primitive, positive defined binary quadratic

form of discriminant D that maps to $a\langle 1, \tau\rangle$. This ideal lies in the class of $\mathfrak{a}$, thus proving surjectivity.

Finally, we need to prove that the mapping is a morphism, that is, that it preserves the group structure. Let $f(X_1, X_2) = (a, b, c)$ and $g(X_1, X_2) = (a', b', c')$ be forms and let $[f], [g] \in Cl(D)$ be their respective classes. We need to show that $\Psi([f] \cdot [g]) = \Psi([f])\Psi([g])$. We may assume, changing the class representative if necessary, that f and g are Dirichlet united forms (as in Definition 3.20). By Lemma 3.22, we may write the composition of f and g as

$$F(X_1, X_2) = f(X_1, X_2) \cdot g(X_1, X_2) = \left(aa', B, \frac{B^2 - D}{4aa'}\right),$$

where B satisfies $B \equiv b \pmod{2a}$, $B \equiv b' \pmod{2a'}$ and $B^2 \equiv D \pmod{4aa'}$. The images of these forms under Φ are, then:

$$\Psi(f) = \left\langle a, \frac{-b + f\sqrt{d_K}}{2} \right\rangle, \ \Psi(g) = \left\langle a', \frac{-b' + f\sqrt{d_K}}{2} \right\rangle,$$
$$\Psi(F) = \left\langle aa', \frac{-B + f\sqrt{d_K}}{2} \right\rangle.$$

Let $\phi = \frac{-B+f\sqrt{d_K}}{2}$. Because $B \equiv b \pmod{2a}$, we compute the image $\Psi(f)$ as

$$\left\langle a, \frac{-b + f\sqrt{d_k}}{2} \right\rangle = \left\langle a, \frac{-B + f\sqrt{d_K}}{2} - na \right\rangle = \langle a, \phi\rangle.$$

Similarly, $\Psi(g) = \langle a', \phi\rangle$ and $\Psi(F) = \langle aa', \phi\rangle$. We proceed to show that $\langle aa', \phi\rangle = \langle a, \phi\rangle \langle a', \phi\rangle$. Indeed, we know that $\phi^2 \equiv -B\phi \pmod{aa'}$ (because $B^2 \equiv D \pmod{4aa'}$). Therefore, we have that $\langle a, \phi\rangle \langle a', \phi\rangle = \langle aa', a\phi, a'\phi, \phi^2\rangle = \langle aa', a\phi, a'\phi, -B\phi\rangle$. Since a, a' and B are coprime (this is immediate from $gcd(a, a', (b + b')/2) = 1$), it must be that

$$\langle aa', a\phi, a'\phi, -B\phi\rangle = \langle aa', \phi\rangle.$$

Finally, we prove *(iii)*. Let m be represented by $f(X_1, X_2)$, then we may write $m = d^2a$, with a represented by a primitive form and d is the greatest common divisor of the coefficients of f. We may assume that $f = (a, b, c)$ so that it maps to $\mathfrak{a} = a\langle 1, \tau\rangle$, with $N(\mathfrak{a}) = a$. Then the ideal $d\mathfrak{a}$ has norm $m = d^2a$.

Conversely, let $\mathfrak{a}$ be an ideal of norm m. We may write $\mathfrak{a}$ in the form $\alpha\langle 1, \tau\rangle$, where $\mathcal{I}m(\tau) > 0$, $a\tau^2 + b\tau + c = 0$, $a > 0$ and $gcd(a, b, c) = 1$. Then, the form $f(X_1, X_2) = aX_1^2 + bX_1X_2 + cX_2^2$ maps to the class of $\mathfrak{a}$. The only thing left to prove is that f represents m. Since $\alpha\langle 1, \tau\rangle \subset \langle 1, \alpha\tau\rangle$, we can find integers p, q, r, s such that $\alpha = p + q\alpha\tau$ and $\alpha\tau = r + s\alpha\tau$.

Therefore, we can write $(p + q\alpha\tau)\tau = r + s\alpha\tau$. Since $a\tau^2 + b\tau + c = 0$, comparing the coefficients in the latter expression, it must be that $p = as + bq$. Thus,

$$m = \frac{N(\alpha)}{a} = as^2 + bsq + cq^2.$$

This concludes the proof. □

As we have just seen, there is an isomorphism between $Cl(D)$ and $Cl(\mathcal{O})$. However, we are yet to present the inverse of the homomorphism Ψ. This is the content of the next proposition.

Proposition 3.32. *Let $\mathcal{O}$ be the order in an imaginary quadratic field K of conductor $q \geq 1$. Let $\mathfrak{a}$ be a proper (that is, invertible) $\mathcal{O}$-ideal. Let $\{\alpha, \beta\}$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$ such that $\mathcal{I}m(\beta/\alpha) > 0$. Then the form*

$$f_{\mathfrak{a}}(X_1, X_2) = \frac{N(\alpha X_1 - \beta X_2)}{N(\mathfrak{a})} \tag{3.4.2}$$

is a primitive binary integral quadratic form of discriminant $D = q^2 d_K$, with $d_K < 0$. Moreover, at the level of classes, the mapping sending $\mathfrak{a}$ to $f_{\mathfrak{a}}(X_1, X_2)$ is the inverse of the map in Theorem 3.31.

Proof. We first show that $f_{\mathfrak{a}}(X_1, X_2)$ is a binary quadratic form. Direct calculation of the numerator yields $N(\alpha X_1 - \beta X_2) = \alpha\bar{\alpha}X_1^2 - \left(\alpha\bar{\beta} + \bar{\alpha}\beta\right) X_1X_2 + \beta\bar{\beta}X_2^2$.

The coefficients of $N(\alpha X_1 - \beta X_2)$ are, respectively $N(\alpha)$, $Tr(\alpha\bar{\beta})$ and $N(\beta)$, all of them belonging to $\mathfrak{a}\bar{\mathfrak{a}}$. By Theorem 2.27, we know that $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$, so that $a, b, c \in \mathcal{O}$ exist such that $N(\alpha) = aN(\mathfrak{a})$, $N(\beta) = bN(\mathfrak{a})$ and $Tr(\alpha\bar{\beta}) = cN(\mathfrak{a})$. Even more, since α, β and $\alpha\bar{\beta}$ are all algebraic integers, their norms are rational integers. Therefore, we have that $a, b, c \in \mathcal{O} \cap \mathbb{Q} \subseteq \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, so the form is integral.

Computation of the discriminant of the form is trivial from the explicit form of the numerator and the equality $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$ from Theorem 2.27.

$$\frac{(\alpha\bar{\beta} + \bar{\alpha}\beta)^2 - 4\alpha\bar{\alpha}\beta\bar{\beta}}{N(\mathfrak{a})^2} = \frac{(\alpha\bar{\beta} - \bar{\alpha}\beta)^2}{N(\mathfrak{a})^2} = q^2 d_k,$$

where in the last step we used the fact that $q^2 d_k \cdot N(\mathfrak{a})^2 = Disc(\alpha, \beta)$.

To prove that the form is primitive, it is enough to show to that there is an element $a \in \mathfrak{a}$ such that $N(a)/N(\mathfrak{a})$ is coprime to q. Indeed, if $p|a, b, c$, then $p|q^2 d_k$. Since d_k is square-free it must be that $p|q$. But now, $f_{\mathfrak{a}}$ represents $N(a)/N(\mathfrak{a})$, so that we have $p|N(a)/N(\mathfrak{a})$, contradicting the coprimality of q and $N(a)/N(\mathfrak{a})$. The initial claim follows from the fact that an ideal coprime to the conductor exists in every class.

Next, we prove that the morphism is well-defined at the level of classes. This is immediate from Lemma 3.30, because equivalent ideals are related by a principal ideal. Similarly, we can show that different basis for an ideal satisfying the condition on the imaginary part yield equivalent forms.

To end with, we show that the map Φ sending $\mathfrak{a}$ to $f_{\mathfrak{a}}$ is the inverse of the map in Theorem 3.31. Let Ψ be the map in the latter theorem and let $f = (a, b, c)$ be a positive definite form. Then $\Psi(f)$ is the ideal

$$\left\langle a, \frac{-b + \sqrt{D}}{2} \right\rangle.$$

The image $\Phi(\Psi(f))$ can be easily computed. After some simple algebraic manipulations, the expression for $\Phi(\Psi(f))$ is

$$\frac{N\left(aX_1 - \frac{-b+\sqrt{D}}{2}X_2\right)}{N(\mathfrak{a})} = \frac{a^2X_1^2 + abX_1X_2 + acX_2^2}{N(\mathfrak{a})}.$$

Finally, we compute the norm of the ideal as

$$N(\mathfrak{a})^2 = \frac{Disc\left(a, \frac{-b+\sqrt{D}}{2}\right)^2}{D} = a^2,$$

where $Disc\left(a, \frac{-b+\sqrt{D}}{2}\right)$ is the discriminant of the basis, computed as the square of determinant of the matrix of Galois embeddings. Therefore, we have seen that $\Phi \circ \Psi = Id_{Cl(D)}$ and we know from Theorem 3.31 that Ψ is a bijection, so that Ψ^{-1} must be Φ. This concludes the proof. □

Remark 3.33. *Notice that the condition $\mathcal{I}m(\beta/\alpha) > 0$ imposes an ordering of the basis. This was anticipated in the proof of Theorem 3.31.*

Chapter 4

Computing in the ideal class group

As we have seen, there is a nice relationship between the ideal class group of a quadratic order and the class group of binary quadratic forms of a certain discriminant. We anticipated earlier that this relationship is the main reason why imaginary quadratic field cryptography is interesting. In the following sections, we take advantage of it to give algorithms that will allow Alice and Bob to work on the ideal class group.

The idea is to use Theorem 3.31 to translate from the language of ideals to that of binary quadratic forms. Algorithms on forms have been thoroughly studied and optimized, so they provide efficient ways of computation.

While computer implementation is not the main goal of the project, it may be of interest to see how such implementation may be done. For convenience, the algorithms are presented in an Appendix A.

The first algorithm we discuss in detail is the form reduction. Given a binary quadratic form, we wish to find a reduced form (cf. Definition 3.15) that is equivalent to the initial form. Later, we will focus on the composition of forms. The objective is to be able to operate in the group of classes of forms.

4.1 Message Embedding

To work on the class group for cryptographic purposes means to think of messages as elements in that group. Yet, in practice, messages are typically written in plain language (for example, in English). It is therefore necessary to find a way to embed a message in an ideal. This is the content of this section.

Let $\mathcal{O}$ be a quadratic order of discriminant Δ_q and let $\mathcal{O}_K$ be the maximal order containing $\mathcal{O}$, with discriminant Δ. The first step is to translate the message into an integer. This is simple, since letters on a computer are (mostly) in ASCII format, which is in binary. Therefore, one can simply concatenate the letters an then interpret the resulting binary as an integer.

Example 4.1. *To illustrate the previous point, take the message "Hello"*[1]*. The ASCII encoding for*

[1]This step is case-sensitive, so it is relevant that the first letter of message is in caps.

each of the letters is as follows.

$$H = 1001000_b,\ e = 1100101_b,\ l = 1101100_b,\ o = 1101111_b.$$

Thus, we can write the message as

$$Hello = 1001000110010111011001101100111011111_b$$

and interpret it as an integer by thinking in the decimal form

$$1001000110010111011001101100111011111_b = 19540948591_d.$$

In the cryptosystems discussed in this paper the message has to be split in sub-messages, since there are restrictions on the size of the message (when encoded as an integer). In particular, for our cryptosystems, we require that the message integer m satisfies $m \leq \sqrt{\Delta/4} \leq \sqrt{\Delta_q/4}$. This way, we ensure that the message ideal is reduced, by Proposition 3.17. Additionally, in practice, the messages are usually filled with random characters in certain positions (known by the interlocutors) so as to difficult decryption by comparing ciphered texts.

Once the message has been converted into an integer of the desired size, which we hereafter call m, we proceed to the embedding. The naïve way of proceeding is to associate the message m to the ideal (m, b_m), where b_m is a square root of the discriminant modulo $4m$. However, computation of b_m can be quite inefficient when m is not a prime number. While there are other alternative ways of remedying this situation, we choose a technique called ***distance embedding***. In essence, we compute the prime number closest to m, p and store the message as a pair $\big((p, b_p), d\big)$, where b_p is a square root of the discriminant modulo $4m$ and $d = p - m$ is the signed distance[2] between p and m. In this case, b_p can be computed using Shanks' RESSOL algorithm [Sha73].

4.2 Reduction algorithm

The reduction algorithm is presented in Appendix A. The number of steps (as a characterization of the running time) is discussed in Proposition 4.3, the proof of which requires Lemma 4.2.

The reduction algorithm is simply the proof of Theorem 3.19 presented in a more convenient and ready-to-implement format. The corresponding Algorithm 3 presented in Appendix A is extracted from [Coh93].

In the following results we study the complexity of the reduction algorithm. Precisely, the number of steps needed to reduce any given binary quadratic form is presented.

Lemma 4.2. *Let $f = (a, b, c)$ be a primitive positive-definite of discriminant $D < 0$, such that $-a \leq b \leq a$ and $a < \sqrt{|D|}$. Then either (a, b, c) is reduced or the form (c, r, s) where $-b = 2cq + r$ with $-c < r \leq c$ obtained by one reduction step is reduced.*

Proof. If (a, b, c) is reduced we are done. Suppose that (a, b, c) is not reduced. In that case, either (i) $a > c$ or (ii) $a = c$ and $b < 0$, because we are assuming $-a < b \leq a$. In the second case, (ii), after one reduction step we get $(a, -b, a)$, which is reduced.

[2] In some cases, the prime p is chosen to be bigger than m, so that this distance is positive.

The first case is more complicated. Assume $a > c$. If $a \geq 2c$, then $c < \sqrt{|D|/4}$, so that (c, r, s) is reduced. If $-c < -b \leq c$, then it must be $q = 0$, so that $(c, r, s) = (c, -b, a)$ is reduced. Therefore, we only need to consider the case $c < a < 2c$ and $-b \leq -c$ or $-b > c$. Since $|b| \leq a$, it follows that in the Euclidean division of $-b$ by $2c$ we must have that $q = \pm 1$. Thus, we have that $s = a - bq + cq^2 = a \mp b + c \geq c$ ($|b| \leq a$). Then wither $s = c$ or the form is reduced. In the case $s = c$ it must be that $a = \pm b$ and $b > 0$, $q = -1$ and $r = 2c - b \geq 0$. Therefore (c, r, s) is also reduced in this case. □

With this lemma, we may now compute the running time (expressed as number of bit operations) of the reduction algorithm.

Proposition 4.3. *The number of Euclidean steps in Algorithm 3 is at most equal to*

$$2 + \left\lceil lg\left(\frac{a}{\sqrt{|D|}}\right)\right\rceil, \tag{4.2.1}$$

where lg is the base 2 logarithm.

Proof. Let f be a form. Assume that at the beginning of Step 3 in Algorithm 3 we have $f = (a, b, c)$. If $a > \sqrt{|D|}$, we have that

$$c = \frac{b^2 + |D|}{4a} \leq \frac{a^2 + a^2}{4a} = \frac{a}{2}.$$

In Step 3, a and c are exchanged and a decreases by a factor of at least 2. Therefore, after at most $\left\lceil lg\left(\frac{a}{\sqrt{|D|}}\right)\right\rceil$ we obtain at the beginning of Step 3 a form with $a < \sqrt{|D|}$. Then, Lemma 4.2 completes the proof. □

Therefore, the reduction algorithm, Algorithm 3, is linear on the number of binary digits of the quotient $a/\sqrt{|D|}$. Since the discriminant is related to the coefficients of the binary quadratic form as $D = b^2 - 4ac$, we expect a to be of the order of $\sqrt{|D|}$. As a consequence, the reduction algorithm is fast, even for large discriminants.

4.3 Composition algorithm

To be able to work in the ideal class group, we need a way to perform the group operation in a reasonable time. The most powerful version of the composition algorithm is a pair of algorithms known as NUCOMP and NUDUPL and it is due to Shanks and Atkins.

The NUCOMP algorithm computes the unique reduced composite of two given binary quadratic forms of discriminant D. The main point is that the forms to be composed are partially reduced before the composition step, thus lowering the size of operands from $\mathcal{O}(D)$ to $\mathcal{O}(D^{1/2})$ in most cases or to $\mathcal{O}(D^{3/4})$ in the worst case [JP02].

It is important to keep in mind that NUCOMP and NUDUPL algorithms are written in the language of binary quadratic forms. To compute products in the ideal class group, one has to use Theorem 3.31 to go from classes of ideals to binary quadratic forms and vice versa.

It is important to realise that NUDUPL, Algorithm 7, does not output any arbitrary power, but just the square of a given form. In order to compute arbitrary powers efficiently, it is used in conjunction with ***binary exponentiation techniques*** [Coh93]. In general, given a group G and an element $g \in G$, we wish to compute g^n for some integer n. As the name suggests, the idea is to use the binary representation of the exponent, $n = \sum_i \epsilon_i 2^i$, with $\epsilon_i \in \{0,1\}\ \forall i$. In that case, we can compute the n-th power of g as $g^n = \prod_{\epsilon_i} \left(g^{2^i}\right)$. The exact algorithm can be found in [Coh93]. When performing the algorithm, we need to compute the even powers of g up to $g^{\lfloor log_2(n) \rfloor}$ and then multiply them. In total, we need $2 \cdot \lfloor log_2(|n|) \rfloor + 1$ operations. Thus, the algorithm is linear in the size of the exponent, so that the limiting factor is the implementation of the group operation.

As suggested by [JP02], the running time of NUCOMP is significantly shorter than the usual composition (that is, without intermediate partial reduction steps). Needless to say, run times depend on the computer, so giving the run times obtained in a 2002 machine is essentially pointless. However, the ratio of run times of both algorithms is of interest. For a discriminant with 1024 binary digits, [JP02] reports that, in average, NUCOMP is approximately 1.65 times faster, whereas for a discriminant with 2048 binary digits, NUCOMP is almost two times faster.

As expected, when the discriminant is larger, the NUCOMP and NUDUPL algorithms become significantly more efficient. Of course, this is highly desirable, since the protocols that we describe later require large discriminants, or else they would be too easy to crack. Thus, when implementing the form composition for the protocols, it is preferable to use a combination of NUCOMP and NUDUPL, rather than the basic composition algorithm.

4.4 Switching algorithms

The Hühnlein-Jacobson and Paulus-Takagi cryptosystems are variants of the original Buchmann-Williams protocol that aspire to practical implementation. The key to overcome practical shortcomings is Theorem 2.34. Indeed, switching back and forth between maximal and non-maximal orders enables much faster decryption times.

The goal of this section is to "translate" the isomorphism in Theorem 2.34 to class groups. This is not straightforward, since the relationship above is defined between the groups of ideals prime to the conductor in $\mathcal{O}_f$ and $\mathcal{O}_K$, respectively; but not on the class groups. Nonetheless, since the presented cryptosystems are based on class groups, it is convenient to have a similar result.

Given $\mathfrak{a}, \mathfrak{b}$ two $\mathcal{O}_f$-ideals prime to f such that $\mathfrak{a} \sim \mathfrak{b}$, it is not true in general that $\Phi^{-1}(\mathfrak{a}) \sim \Phi^{-1}(\mathfrak{b})$. The converse, however, does hold [HJPT98].

Lemma 4.4. *Let $\mathfrak{a}, \mathfrak{b}$ be $\mathcal{O}_q$-ideals prime to q such that $\mathfrak{a} \sim \mathfrak{b}$. Then $\Phi(\mathfrak{a}) \sim \Phi(\mathfrak{b})$.*

We will see that under certain conditions, one can establish an isomorphism in class groups. First, let us assume that the conductor, q, is a prime number such that $\sqrt{\frac{|\Delta|}{3}} < q$. By Lemma 2.31 and by Proposition 3.17 we have that all reduced ideals in $Cl(\Delta)$ are prime to q. Moreover, as seen in Proposition 2.35, only ideals prime to the conductor are needed to describe the class group of $\mathcal{O}_q$. Consequently, we may identify each class of ideals to the

unique reduced ideal then define the following map, which is based on the isomorphism Φ of Theorem 2.34.

$$\begin{aligned} \phi : Cl(\Delta_q) &\longrightarrow Cl(\Delta) \\ \mathfrak{a} &\longmapsto Red_\Delta(\Phi(\mathfrak{a})) = Red_\Delta(\mathfrak{a}\mathcal{O}_K). \end{aligned} \tag{4.4.1}$$

This map is well defined, by Lemma 4.4, but it is not an isomorphism, for it is not injective. The next goal is to describe an "inverse" map for ϕ. To that end, we will need to add an additional restriction. We summarize the process in two lemmas:

Lemma 4.5. *Let $\mathfrak{a} = (a, b)$ be a reduced ideal in $\mathcal{O}_q$, prime to q, where q is a prime integer. If $a \leq \sqrt{\frac{|\Delta|}{4}}$, then $\mathcal{A} = \Phi(\mathcal{A})$ is also reduced in $\mathcal{O}_K$.*

Proof. By Theorem 2.34, we know that $\mathcal{A}$ and $\mathfrak{a}$ have the same norm. Moreover, the norm of $\mathfrak{a}$ is equal to a, so that $N(\mathcal{A}) \leq \sqrt{\frac{|\Delta|}{4}}$. By Proposition 3.17, the latter implies that $\mathcal{A}$ is reduced in $\mathcal{O}_K$. □

Lemma 4.6. *Let $\mathcal{A}$ be a reduced ideal in $\mathcal{O}_K$ prime to q. Then $\mathfrak{a} = \Phi^{-1}(\mathcal{A})$ is reduced in $\mathcal{O}_q$.*

Proof. Since $\mathcal{A}$ is reduced, then its norm is upper-bounded by $\sqrt{\frac{|\Delta|}{3}}$. By Theorem 2.34 and for $q > 1$ we have that $N(\mathfrak{a}) = N(\mathcal{A}) \leq \sqrt{|\Delta|/3} < \sqrt{|q^2\Delta|/4}$. Thus, $\mathfrak{a}$ is reduced. □

Therefore, by Theorem 2.34 and the two lemmas above, there is a one-to-one correspondence between the reduced ideals in $Cl(\Delta_q)$ and $Cl(\Delta)$ whose norms are smaller than $\sqrt{\frac{|\Delta|}{4}}$.

Remark 4.7. *Even though it may be seen in various ways, what is essential in this discussion is that the isomorphism in Theorem 2.34 does not work well on the level of classes. The map*

$$\phi : Cl(\Delta_q) \longrightarrow Cl(\Delta)$$

is surjective. Therefore, by the Isomorphism Theorem of Groups an isomorphism exists such that

$$\frac{Cl(\Delta_q)}{Ker(\phi)} \cong Cl(\Delta)$$

Thus, there is an ambiguity in the definition of the inverse of ϕ, in other words, given an element $\mathfrak{a}$ in $Cl(\Delta_q)$ all elements of the form $\mathfrak{ab}$ with $\mathfrak{b} \in Ker(\phi)$ have the same image, so that there is a $|Ker(\phi)|$-fold ambiguity in the definition of the inverse. To solve this problem, we distinguish a certain ideal using the concept of norm. If we choose a primitive ideal in I_{Δ_q} with norm smaller than $\sqrt{\frac{|\Delta|}{4}}$ then both $\mathfrak{a}$ and its image by Φ are reduced. Then $\phi(\mathfrak{a}) \cap \mathcal{O}_q$ is reduced, so we can compute a distinguished inverse of ϕ.

Consequently, one may think of classes in a class group as the unique reduced form in the class, essentially choosing a canonical representative for each class. Therefore we may think of the map ϕ in (4.4.1) as sending a reduced ideal in $Cl(\Delta_q)$ to a reduced ideal in $Cl(\Delta)$.

For any ideal (a, b) in $Cl(\Delta_q)$, $\phi((a, b))$ may be computed in quadratic time [PT98]. That is, the complexity of the algorithm is $O((\log \sqrt{|\Delta|})^2)$. See Algorithm 4 in Appendix A.

The inverse of the map ϕ is easy to compute [PT98]. Indeed, given a reduced ideal $(A, B) \in Cl(\Delta_q)$ with norm smaller that $\sqrt{|\Delta|/4}$, then

$$\phi((A, qB \pmod{2a})) = (A, B).$$

This algorithm requires is also of quadratic complexity in the square root of the discriminant. See Algorithm 5 in Appendix A.

Chapter 5

The Buchmann-Williams protocols and variants

The aim of this chapter is to discuss the practical application of previous results. First, we introduce the Buchmann-Williams key exchange protocol and cryptosystem [BW88]. As mentioned, the protocols are based on a Diffie-Hellman key-exchange protocol using the class group of the maximal order of an imaginary quadratic field.

To solve the inefficient decryption of the original Buchmann-Willams, we introduce two variants; the Hühnlein-Jacobson and Paulus-Takagi cryptosystems. The latter is the most efficient variant, with quadratic decryption time [PT98]. On the other hand, the Hühnlein-Jacobson cryptosystem, the generalization of Buchmann-Willams to non-maximal orders, is a middle step in the road to practicality [HJPT98]. The idea is that we may use Theorem 2.34 and the algorithms in Section 4.4 to achieve faster decryption times.

5.1 The Buchmann-Williams protocols

The Buchmann-Willams key-exchange protocol uses the class group of the ring of integers (that is, the maximal order) in an imaginary quadratic field as infrastructure. It is in this context that the mathematical formalism discussed in the previous chapters will prove useful. The general idea will be to use Theorem 3.31 to translate the language of ideals to the language of forms, in which we have efficient computation tools, namely the reduction algorithm and NUCOMP/NUDUPL composition algorithms. See Chapter 4 and Appendix A for descriptions of the used algorithms.

Public Elements : A negative discriminant $\Delta < 0$, an imaginary quadratic field $K = \mathbb{Q}\left(\sqrt{\Delta}\right)$, and an ideal $\mathfrak{a}$ in $\mathcal{O}_K$.

Private Elements: A random integer x to be chosen and kept private by Alice and another random integer y to be chosen and kept private by Bob.

1 **[Communication initiation by Alice]**
Alice computes the unique reduced ideal, $\mathfrak{b}$, in the class of $\mathfrak{a}^x$.
Alice sends the ideal $\mathfrak{b}$ to Bob.

2 **[Bob's response]**
Bob computes the unique reduced ideal in the class of $\mathfrak{a}^y$. Let $\mathfrak{c}$ be this ideal.
Bob sends $\mathfrak{c}$ to Alice.

3 **[Computations]**
Alice computes the unique reduced ideal in the class of c^x. Call it I_1.
Bob computes the unique reduced ideal in the class of b^y. Call it I_2.

4 **[Key establishment]**
We have that $I_1 \sim c^x \sim (a^y)^x = (a^x)^y \sim b^y \sim I_2$.
$I_1 = I_2$ is the unique reduced ideal in the class of $(\mathfrak{a}^x)^y$.
Thus, $N(I_1) = N(I_2)$, so it can be used as secret key.

Algorithm 1: Original Buchmann-Williams key exchange protocol based on ideal class group of imaginary quadratic fields. It allows Alice and Bob to share a common key via an insecure communication channel.

The key exchange described in Algorithm 1 can be slightly modified to accommodate a public-key cryptosystem. The result is an ElGamal-type encryption and decryption scheme. The details of these modifications are presented in Algorithm 2.

Public Elements : A negative discriminant $\Delta < 0$, an imaginary quadratic field $K = \mathbb{Q}\left(\sqrt{\Delta}\right)$, an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ and a public directory with Bob's public key $\mathfrak{c} = \mathfrak{a}^y$.

Private Elements: A random integer x to be chosen and kept private by Alice, Bob's private key, y, and Alice's message m, encoded as an element of $\mathbb{Z}$.

1 **[Communication initiation by Alice]**
Alice chooses a random integer x and computes the unique reduced ideal in the class of $\mathfrak{c}^x$. Let I_1 be this ideal. Notice that $\mathfrak{c}$ is obtained from a public directory.
Alice sends Bob the message encrypted as $(M + \alpha, \mathfrak{b})$, where α is the integer norm of I_1, b is the unique reduced ideal in the class of $\mathfrak{a}^x$ and M is the first block of the message, m, with $M < \alpha$.

2 **[Bob's response]**
To find M, Bob needs α.
Bob computes α by finding the reduced ideal in the class of $\mathfrak{b}^y$.
Notice that y is only known to Bob: it is his private key.

Algorithm 2: Original Buchmann-Williams (BW) asymmetric cryptosystem based on ideal class group of imaginary quadratic fields. It allows Alice to send Bob a private message through an insecure channel.

5.1.1 Security

To crack the Buchmann-Willams cryptosystem, one may attempt to solve the Discrete Logarithm Problem (cf. Definition 1.2) in the ideal class group. The most efficient algorithms to solve this task are Hafner and McCurley's algorithm ([HM89], [Coh93]) and its variants. Without getting into specifics, the take-away is that they are used to compute the structure of the class group as a finite abelian group in subexponential complexity. Afterwards, one can solve the Discrete Logarithm Problem as in Proposition 5.1.

Proposition 5.1. *Let $Cl(\Delta)$ be the ideal class group of the ring of integers of a quadratic field. By the structure theorem of finite abellian groups, assume that $Cl(\Delta)$ can be written as*

$$Cl(\Delta) \cong \bigotimes_{i=1}^{l} C(m_i),$$

where $C(m_i)$ are cyclic subgroups of order m_i. Then, solving the Discrete Logarithm Problem in $Cl(\Delta)$ is equivalent to solving a system of simultaneous congruences.

Proof. Let g_i be a generator of the cyclic group $C(m_i)$. To solve the Discrete Logarithm Problem, given $\mathfrak{a}, \mathfrak{b} \in Cl(\Delta)$, we have to find an integer x such that $\mathfrak{a} = \mathfrak{b}^x$. First we compute the representations

$$\mathfrak{a} \sim (g_i^{a_i})_{i\in\{1,\dots,l\}} \text{ and } \mathfrak{b} \sim (g_i^{b_i})_{i\in\{1,\dots,l\}}$$

of $\mathfrak{a}$ and $\mathfrak{b}$ over the generators. Then, the Discrete Logarithm Problem can be rewritten as finding x such that $(g_i^{a_i}) \sim (g_i^{xb_i})$.

The integer x can be found by solving the system of simultaneous congruences $a_i \equiv xb_i \pmod{m_i}$ for $1 \leq i \leq l$ using the Chinese remainder theorem. Moreover, if the system has no solution, there is no solution to the Discrete Logarithm Problem either. □

It is important to realise that the representation of the class group only has to be computed once if the discriminant doesn't change. In this scenario, once the structure is known, the computation of the Discrete Logarithm Problem is more efficient. This result gives and idea of the size of the discriminant needed for a Buchmann-Willams protocol.

5.2 The Hühnlein-Jacobson Cryptosystem

The major concern with Buchmann-Willams protocol is implementation efficiency. Indeed, the size of the discriminants needed for conjectural security is too large to work efficiently with the algorithms in Chapter 4. A first step toward a practical implementation was taken by D. Hühnlein, M. J. Jacobson Jr. and others in 1998 [HJPT98]. We will refer to their cryptosystem as Hühnlein-Jacobson or HJPT (the initials of the authors).

The idea of Hühnlein-Jacobson is to generalise the Buchmann-Willams protocol by introducing non-maximal orders (cf. Definition 2.19). Non-maximal orders are harder to manage because, unlike the maximal order, they are not Dedekind domains. Thus, we must ensure that the ideals we work with are prime to the conductor (cf. Definition 2.30), since these are the ideals that are useful for computations. The factorization of the discriminant of the order can be used to go back and forth between the class group of the non-maximal order and the class group of the maximal order, using Theorem 2.34 and the results in Section 4.4. This speeds up the decryption process while not hindering the security of the cryptosystem.

The first step to setup the cryptosystem is to choose an imaginary quadratic field and

an order of said field. To do so, we select a large[1] prime p and let:

$$\Delta = \begin{cases} -p, & \text{if } p \equiv 3 \pmod 4, \\ -4p, & \text{otherwise.} \end{cases} \tag{5.2.1}$$

This way, Δ is a negative fundamental discriminant, that is, the discriminant of the imaginary quadratic field $\mathbb{Q}\left(\sqrt{\Delta}\right)$. Next, we choose another large prime q, that will be the conductor of the order, and we compute its discriminant: $\Delta_q = q^2\Delta$. The reason why we want the conductor to be a prime is because we ensure that we can work with ideals prime to the conductor (see Proposition 2.31). Because we want to identify each class with the reduced form, we demand $\sqrt{|\Delta|} < q$, so that every reduced ideal is prime to q [HJPT98]. Moreover, because of Proposition 2.35, we only need the well-behaved ideals prime to the conductor to describe the class group.

After the order has been selected, we choose an $\mathcal{O}_q$-ideal that will serve as the base ideal. To that end, let g be another large prime such that the Kronecker symbol is $\left(\frac{\Delta_q}{g}\right) = +1$. This last condition simply means that the discriminant Δ_q is a square modulo $4g$ or, since 4 is a square, modulo g. With this, we have found a binary quadratic form of discriminant Δ_q; equivalently, using Theorem 3.31, an ideal in $\mathcal{O}_q$. Explicitly, if b_g is the square root of Δ_q, then the base ideal is $\mathfrak{g} = \left(g, b_g\right)$. By switching the sign of b_g if necessary, we may assume that $\mathcal{I}m(b_g/g) = \mathcal{I}m(b_g) \geq 0$. Thus, Proposition 3.32 can be used to translate into the language of forms to compute.

Finally, we need to compute the public and private keys. We choose an integer a such that $2 \leq a \leq \lfloor\sqrt{|\Delta_q|}\rfloor$, this will be the private key. The public key will be the reduced ideal $\mathfrak{a}$ in the class of $\mathfrak{g}^a$.

We now turn our attention to the encryption and decryption of a message in the Hühnlein-Jacobson cryptosystem. Both are based on the ElGamal protocol. First, encryption is discussed. The message is encrypted as a pair of reduced $\mathcal{O}_q$-ideals, (η_1, η_2), where $\eta_1 = \mathfrak{g}^k$ and $\eta_2 = \mathfrak{m}\mathfrak{a}^k$. Of course, $\mathfrak{m}$ is the message ideal, that has been created using the embedding technique in Section 4.1. Additionally, we require that $N(\mathfrak{m}) < \sqrt{|\Delta|/4}$ in order to be able to decrypt. Indeed, as we will discuss, the decryption is performed in the maximal order, and thus we must ensure that the corresponding ideal in that order is reduced. Notice that the latter follows from Lemma 4.5 and because the pre-image is a reduced ideal. Moreover, the encryption process is performed with reduced ideals in the non-maximal order, $\mathcal{O}_q$.

The decryption process is also similar to ElGamal decryption, but it is performed in the maximal order $\mathcal{O}_K$, where the coefficients are smaller, and thus easier to manage. It is based on the following proposition.

Proposition 5.2. *Let $\mathcal{O}_q$ be the order of conductor q. Let $\mathfrak{a}$ be an $\mathcal{O}_q$-ideal prime to q. Then $\Phi(\mathfrak{a})^x \sim \Phi(\mathfrak{a}^x)$, for any integer x.*

To perform the decryption process, we use the isomorphism from Theorem 2.34 to compute $H_1 = \Phi(\eta_1), H_2 = \Phi(\eta_2)$, which are the maximal-order ideals equivalent to

[1] The size of the parameters is related to the security, see Section 5.4.

η_1 and η_2, respectively. We may compute compute the original message by $\Phi^{-1}(\mathcal{M}) = \Phi^{-1}\left(H_2(H_1)^a\right)^{-1}$.

Proof. (Correctness of decryption process) By definition of $\eta_2 = \mathfrak{m}\mathfrak{a}^k$ we have that

$$H_2 = \Phi(\mathfrak{m}\mathfrak{a}^k) = \Phi(\mathfrak{m})\Phi(\mathfrak{a}^k) \sim \Phi(m)\Phi(\mathfrak{a})^k.$$

In the last step, we have used Proposition 5.2. Similarly, by definition of $\eta_2 = \mathfrak{g}^k$, we have that

$$H_1^a = \Phi(\mathfrak{g}^k)^a \sim \Phi(\mathfrak{g})^{ka} \sim \Phi(\mathfrak{g}^a)^k \sim \Phi(\mathfrak{a})^k.$$

Again, in the chain of equivalences, we have used Proposition 5.2 and the fact that $\mathfrak{a}$ is the (unique) reduced ideal in the class of $\mathfrak{g}^a$, which is how we defined $\mathfrak{a}$ in the setup of the cryptosystem. Therefore, for the message ideal, we must have the following for the message in the maximal order:

$$\mathcal{M} \sim \Phi(m)\Phi(\mathfrak{a})^k(\Phi(\mathfrak{a})^k)^{-1} \sim \Phi(\mathfrak{m}).$$

Since we have chosen $N(\mathfrak{m}) \leq \sqrt{\frac{|\Delta|}{4}}$, we can uniquely decrypt $\Phi^{-1}(\mathcal{M}) = \mathfrak{m}$. □

In practice, this idea is an important improvement over the Buchmann-Willams cryptosystem. Indeed, as seen in Proposition 2.24 and Proposition 2.22, the discriminant of the non-maximal order is bigger than that of the maximal order by a factor q^2 (remember that q is a large prime) and the coefficients of the elements in the order with respect to a basis are also larger by a factor q. Since the decryption process is carried out in the maximal order, the coefficients are smaller and consequently, the computation time is reduced.

5.3 Paulus-Takagi Cryptosystem

It has been seen that Theorem 2.34 may be used to speed up the decryption process in the Buchmann-Willams cryptosystem, giving rise to the Hühnlein-Jacobson cryptosystem. However, there is no essential difference between these two cryptosystems: both are ElGamal-type protocols, with cubic decryption time. In the following, we will examine another way to apply Theorem 2.34 to create a cryptosystem with quadratic decryption time. We will refer to this cryptosystem as Paulus-Takagi or *New Ideal Coset Encryption* (NICE for short). While still a Discrete Logarithm Problem cryptosystem, it is different from the Buchmann-Willams and the Hühnlein-Jacobson, since the decryption is no longer based on the ElGamal decryption scheme.

We first present a rough approximation to the Paulus-Takagi cryptosystem, using two finite abellian groups G and H. We will particularize this idea in the context of class groups of quadratic fields in Section 5.3.1.

Let, G and H be the above groups. Consider a surjective map $\pi : G \longrightarrow H$ and suppose there is a well-defined bijective map $\varphi : H \longrightarrow U \subseteq G$ such that for any element $h \in H$, $\pi(\varphi(h)) = h$. Moreover, let $k \in Ker(\pi)$. If one can embed a message as en element of U, it may be encrypted by multiplying by a random power of k, k^r. Then the cyphertext is $c = m \cdot k^r$ and it can be decrypted simply by computing $\varphi(\pi(c))$.

5.3.1 Paulus-Takagi cryptosystem over a quadratic order

In this section, we discuss the implementation of the Paulus-Takagi cryptosystem over the infrastructure of class groups of quadratic orders. This discussion is extracted from the original article [PT98].

First, the key generation. Generate two random primes $p, q > 4$ such that $p \equiv 3 \pmod 4$ and $\sqrt{p/3} < q$. As discussed in Remark 4.7, this condition guarantees that all ideals in $Cl(\Delta)$ are prime to q. Let $\Delta = -p$ and $\Delta_q = q^2\Delta$. Then Δ is a fundamental discriminant, so that it makes sense to consider the class group $Cl(\Delta)$ of the maximal order in the imaginary quadratic field of discriminant Δ. Similarly, consider the non-maximal order $\mathcal{O}_q$ of conductor q Sin $\mathrm{Q}(\sqrt{\Delta})$. The class group of this order will be denoted by $Cl(\Delta_q)$.

Let l_1 and l_2 be the bit lengths of $\lfloor\sqrt{|\Delta|/4}\rfloor$ and $q - \left(\frac{\Delta}{q}\right)$, respectively. Consider the map $\phi : Cl(\Delta_q) \longrightarrow Cl(\Delta)$ defined in (4.4.1). Let $\mathfrak{p} \in Ker(\phi)$. The publicly available parameters are (p, Δ_q, l_1, l_2). The secret keys are (Δ, q), and must be kept private.

The message is embedded in a reduced ideal $\mathfrak{m}$ in $Cl(\Delta_q)$. We impose a restriction on the size of the ideal by demanding $\log_2(N(\mathfrak{m})) < l_1$. The restriction on the size is, again, because we want to identify each class with the reduced element in that class. Next, randomly choose an integer with $l_2 - 1$ bits, r. This size restriction is convenient, since l_2 is precisely the size of the kernel. Then the cyphertext is $\mathfrak{c} = Red_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$. This encryption process is of cubic time, namely $O((\log_2(\sqrt{(}\Delta_q)))^3)$, because the exponentiation step is the most costly; it is as complex as the encryption in Buchmann-Willams and Hühnlein-Jacobson.

The secret keys (Δ, q) are used to decrypt. First, the cyphertext ideal is taken to the maximal order, using the results in Section 4.4. We denote $\mathfrak{C}$ the image $\phi(\mathfrak{c})$. This can be done using quadratic complexity. Second, the message ideal $\mathfrak{m}$ may be recovered by computing the inverse of $\mathfrak{C}$. Again, this may be done with quadratic complexity.

5.4 Security of Hühnlein-Jacobson and Paulus-Takagi

Both Hühnlein-Jacobson and Paulus-Takagi allow for faster decryption times than the original Buchmann-Willams. However, there is the possibility that security of the cryptosystems is compromised by this same fact. In this section, we analyze the security of Hühnlein-Jacobson and Paulus-Takagi.

The classical approach to crack both cryptosystems is to examine the Discrete Logarithm Problem. Since the conductor, q, is not known by any third parties, the Discrete Logarithm Problem must be solved in the non maximal order. Alternatively, an attacker may try to find the conductor, q. Of course, once the conductor is known, the cryptosystems are no longer safe, since they both rely on switching from non-maximal to maximal order.

In Theorem 5.3, we prove that braking the Hühnlein-Jacobson cryptosystem by solving the Discrete Logarithm Problem in the maximal order is as hard as factoring the non-fundamental discriminant Δ_q.

Theorem 5.3. *Suppose an algorithm is known that can solve the Discrete Logarithm Problem in the class group of the maximal order, $Cl(\mathcal{O}_K)$. To break the Hühnlein-Jacobson cryptosystem is computationally equivalent to finding a factorization $\Delta_q = q^2\Delta$ for the discriminant of the non-maximal order.*

Proof. An outline of the proof may be found in the original paper describing the Hühnlein-Jacobson cryptosystem [HJPT98]. Our goal here is to comment on that sketch. A common approach to breaking the Hühnlein-Jacobson cryptosystem, as mentioned, is to try to solve the Discrete Logarithm Problem in the class group of the non-maximal order, $Cl(\mathcal{O})$. This is thought to be a difficult task (albeit the exact difficulty is not know). We want to see that going to the maximal order to solve the Discrete Logarithm Problem is not an easy alternative to break the cryptosystem.

Suppose there exists an algorithm that can compute the message ideal, $\mathfrak{m}$. This would allow us to solve the Discrete Logarithm Problem in $Cl(\mathcal{O})$. Indeed, from the encrypted message, we may obtain $\mathfrak{g}^k = \eta_1$ and $\mathfrak{a}^k = \mathfrak{m}^{-1}\eta_2$ and the ideals $\mathfrak{g}$ and $\mathfrak{a}$ are public. As proposed by Shanks and discussed in the Buchmann-Willams original article [BW88], such a solution to the Discrete Logarithm Problem is likely to yield a factorization of Δ_q in the desired form.

Conversely, assume that we are able to factor $\Delta_q = q^2\Delta$, then we may use the conductor and the isomorphism from Theorem 2.34 to translate the problem to the maximal order, where we are assuming that we know how to solve the Discrete Logarithm Problem. □

Similarly, in Theorem 5.4 we show that an algorithm to switch between non-maximal and maximal orders without the conductor is, in a sense, a factorization algorithm.

Theorem 5.4. *Let $\mathfrak{a} = (a, b)$ be an $\mathcal{O}$-ideal prime to the conductor. Assume that there is an algorithm AL that computes $\mathcal{U} = \phi(\mathfrak{a}) = (A, B)$ without knowledge of the conductor, q. Then AL can be used to factorize Δ_q in polynomial time.*

Proof. The relation between ideals $\mathfrak{a}$ and $\mathcal{U}$ is that $a = A$ and $B \equiv bq^{-1} \pmod{a}$. Therefore, since $1 = gcd(B, a) = gcd(b, a)$, we can compute $q \equiv bB^{-1}$.

We may take advantage of this idea by creating prime ideals (p_i, b_{p_i}), which can be generated in polynomial time [PT98]. Then we can recover the conductor q solving the obtained system of congruences by using the Chinese Remainder Theorem. Moreover, we can check whether we obtain the right conductor by verifying that $\Delta_q = q^2\Delta$. □

Remark 5.5. *In the Paulus-Takagi protocol, we use an element of $Ker(\phi)$ as the public key. It could be the case that said element could help factor the discriminant, Δ_q. It is discussed in [PT98] that the latter is unlikely. Although it is not proven, it is conjectured that knowledge of the public key does not help factor Δ_q.*

We have shown that the security of both Paulus-Takagi and Hühnlein-Jacobson can be compromised in two main ways: solving the Discrete Logarithm Problem in the non-maximal order or factoring the non-fundamental discriminant. Next we discuss whether these problems can or can not be solved. It turns out that algorithms to solve them do exist, but their efficiency is related to the size (that may be expressed in number of bits) of the parameters: the discriminants Δ_q, Δ and the conductor q. In this sense, the security

of the cryptosystem is based on computational power: the mathematical solution to the problem is known, it is the computation time that limits its applicability. In other words, there may come a time when this (and others) cryptographic protocols are no longer secure due to the improvement in computer power and computation time.

In 5.1.1 we have discussed how to approach the Discrete Logarithm Problem in a class group. For this reason, in what follows we concentrate on the factorization of the non-fundamental discriminant, Δ_q. Essentially, we need a discriminant Δ_q large enough such that it is not feasible to either factorize it as $\Delta_q = q^2\Delta$ or solve the Discrete Logarithm Problem in the class group of the order of discriminant Δ_q. To date, the most efficient factorization methods are the General Number Field Sieve and the Elliptic Curve Method. Instead, we are only interested in the fact that their conjectured running times impose approximate lower bounds for the HJPT parameter sizes [HJPT98]. In particular, a discriminant Δ_q with more than 513 binary digits makes factorization with the number field sieve unlikely. Similarly, for discriminants $\Delta, q > 2^{170}$ the elliptic curve algorithm is not likely to be able to factor Δ_q. It is important to remember that after factorization of Δ_q, one has to solve the Discrete Logarithm Problem in the class group of the ring of integers. Therefore, choosing $\Delta > 2^{216}$ may provide an extra layer of security.

Last but not least, it is worth mentioning that selecting the fundamental discriminant and the conductor to be prime numbers also has an impact on security. Needless to say, the original reason why we chose them to be prime numbers was to ensure that all ideals were prime to the conductor. However, it turns out that attempting to factorize a discriminant $\Delta_F = F^2\Delta$ for a non-prime F may be easier because F has smaller factors.

The main take-away is that performing the decryption process in the maximal order (as opposed to the non-maximal order) considerably reduces execution time in the Hühnlein-Jacobson cryptosystem [HJPT98]. In the case of Paulus-Takagi the decryption process is even faster, because the complexity of the decryption process is now quadratic [PT98]. Notice the BW protocol in this context means that the decryption is performed in the non-maximal order as an ElGamal decryption.

Summary and conclusions

Since the publishing of Diffie and Hellman's key exchange protocol over the multiplicative group of integers modulo a prime, many variants have emerged that adapt the Diffie-Hellman protocol to other groups. Appearing published for the first time in 1988, quadratic field cryptography implements a Diffie-Hellman key exchange over the ideal class group of an imaginary quadratic field. In this work, we analyzed the fundamentals of imaginary quadratic fields and their application to cryptography.

Buchmann and Williams' original key exchange was the first key-exchange protocol based on the class group of an imaginary quadratic field. We discussed the mathematical background behind the scheme, introducing the notion of ring of integers, orders and class groups. Moreover, we gave tools to enable machine computation in the ideal class group by relating it to the group of classes of binary quadratic forms. Exploiting this last relationship enables us to use well-studied algorithms on forms. In that sense, we introduced the NUCOMP/NUDUPL composition and form reduction algorithms.

While the latter protocol serves as a great example to introduce the field of mathematical cryptography, implementation inefficiency and long run times severely hinder its applicability. It is for this reason that we presented a more efficient variant: the Paulus-Takagi cryptosystem, with quadratic decryption time. To introduce the latter, we first generalized the idea of the Buchmann-Willams protocol to non-maximal quadratic orders, giving rise to the Hühnlein-Jacobson cryptosystem; a first step towards practical implementation. Both Paulus-Takagi and Hühnlein-Jacobson rely on switching between maximal and non-maximal orders to achieve faster decryption times. There is, however one important difference between the two. Hühnlein-Jacobson enables faster decryption times by making the coefficients smaller, but at its core it is still an ElGamal decryption scheme, with a cubic exponentiation step. On the other hand, the decryption in the Paulus-Takagi cryptosystem is radically different, since it does not require an exponentiation step.

Last, but not least, we studied the security of all three protocols: Buchmann-Willams, Hühnlein-Jacobson and Paulus-Takagi. As Diffie-Hellman protocols, the central topic in security is the Discrete Logarithm Problem. In particular, Hafner and McCurley's algorithm (and its variants) allow computations of discrete logarithms through finding the group structure as a finite abellian group. We also argued that Hühnlein-Jacobson and Paulus-Takagi are susceptible to attacks that factor the discriminant of the non-maximal order. Namely, the General Number Field Sieve and the Elliptic Curve Method are the best factoring algorithms. Consequently, lower bounds for the sizes of the parameters are determined by both types of algorithms.

The objective of the project was to give an overview of the world of cryptography through the lenses of quadratic field cryptography. This analysis opens the door to a future in-depth analysis of the practical implementation of the cryptosystems and the corresponding attacks.

Appendix A

Algorithms

We present the algorithms described in Chapter 4. They are all presented in a ready-to-implement format, following [Coh93].

Input: A primitive positive-definite binary quadratic form $f = (a, b, c)$ with discriminant $D < 0$.
Output: The unique reduced form equivalent to f.

1 **[Initialize]**
If $-a < b \leq a$ go to Step 3.

2 **[Euclidean Step]**
Let $b = 2aq + r$ with $0 \leq r < 2a$ be the euclidean division of b by $2a$.
If $r > a$, set $r \leftarrow r - 2a$ and $q \leftarrow q + 1$.
Set $c \leftarrow c - \frac{(b+r)q}{2}$ and $b \leftarrow r$

3 **[Finished?]**
If $a > c$ set $b \leftarrow -b$, exchange a and c and go to Step 2.
Otherwise, if $a = c$ and $b < 0$, set $b \leftarrow -b$ and output (a, b, c)

Algorithm 3: Form reduction algorithm from [Coh93].

Input : The discriminant of the non-maximal order, Δ_q, the fundamental discriminant Δ, the conductor q and a reduced ideal $\mathfrak{a} = (a, b) \in Cl(\Delta_q)$.
Output: A reduced ideal $\mathcal{U} \in Cl(\Delta)$ such that $\phi(\mathfrak{a}) = \mathcal{U} = (A, B)$.

1
$A \leftarrow a$
$b \leftarrow \Delta_q \pmod 2$

2
Solve $1 = \mu q + \lambda a$ for $\mu, \lambda \in \mathbb{Z}$ using Euclid's extended algorithm

3
$B \leftarrow b\mu + ab\lambda \pmod{2a}$

4
$\mathcal{U} = (A, B) \leftarrow Red_\Delta(A, B)$

Algorithm 4: Computation of the image of a class by ϕ in Remark 4.7.

Input : A reduced ideal $\mathcal{A} = (A, B) \in Cl(\Delta)$ such that $N(\mathcal{A}) < \sqrt{\frac{|\Delta|}{4}}$, the conductor q.
Output: A reduced ideal $\mathfrak{a} \in Cl(\Delta_q)$ such that $\phi^{-1}(\mathcal{A}) = \mathfrak{a} = (a, b)$.

1
$a \leftarrow A$
$b \leftarrow Bq \pmod{2a}$

Algorithm 5: Computation of the inverse of the map ϕ.

Input: Integers a and b. The constant $L = \lfloor |D/4|^{1/4} \rfloor$.
1 **[Initialize]**
Set $v \leftarrow 0$, $d \leftarrow a$, $v_2 \leftarrow 1$, $v_3 \leftarrow b$ and $z \leftarrow 0$.
2 **[Finished?]**
If $|v_3| > L$ go to step 3. Otherwise, if z is odd, set $v_2 \leftarrow -v_2$ and $v_3 \leftarrow -v_3$. Terminate the sub algorithm.
3 **[Euclidean Step]**
Let $q = \lfloor d/v_3 \rfloor$ and $t_3 \leftarrow d \pmod{v_3}$.
Set $t_2 \leftarrow v - qv_2$, $v \leftarrow v_2$, $d \leftarrow v_3$, $v_2 \leftarrow t_2$, $v_3 \leftarrow t_3$ $z \leftarrow z + 1$.
Go to step 2.

Algorithm 6: PARTEUCL algorithm from [Coh93].

Input: A primitive positive definite form $f = (a, b, c)$ of discriminant D and the constant $L = \lfloor |D/4|^{1/4} \rfloor$.
Output: The square of the form f, $f_2 := f := (a_2, b_2, c_2)$.
1 **[Euclidean step]**
Use Euclid's extended algorithm to find a triple (u, v, d_1) such that $ub + va = d_1 = gcd(a, b)$.
Set $A \leftarrow a/d_1$, $B \leftarrow b/d_1$, $C \leftarrow -cu \pmod{A}$, $C_1 \leftarrow A - C$. If $C_1 < C$, set $C \leftarrow -C_1$.
2 **[Partial reduction]**
Execute sub-algorithm PARTEUCL(A,C).
3 **[Special case]**
If $z = 0$, set $g \leftarrow (Bv_3 + c)/d$, $a_2 \leftarrow d^2$, $c_2 \leftarrow v_3^2$, $b_2 \leftarrow b + (d + v_3)^2 - a_2 - c_2$ and $c_2 = c_2 + gd_1$.
Reduce the form $f = a_2, b_2, c_2$. Output the result and terminate.
4 **[Final Computations]**
Set $e \leftarrow (cv + Bd)/A$, $g \leftarrow (ev_2 - B)/v$ (Both divisions are exact and the case $v = 0$ has been considered above). Set $b_2 \leftarrow ev_2 + vg$.
If $d_1 > 1$, set $b_2 \leftarrow d_1 b_2$, $v \leftarrow d_1 v$ and $v_2 \leftarrow d_1 v_2$.
Finally, in order, set $a_2 \leftarrow d^2$, $c_2 \leftarrow v_3^2$, $b_2 \leftarrow b_2 + (d + v_3)^2 - a_2 - c_2$, $a_2 \leftarrow a_2 + ev$, $c_2 \leftarrow c_2 + gv_2$.
Reduce the form $f_2 = (a_2, b_2, c_2)$, output the result and terminate.

Algorithm 7: NUDUPL algorithm. Based on Daniel Shanks

Input: $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_s, b_2, c_2)$ primitive positive definite forms of the same discriminant, D. The constant $L = \lfloor |D/4|^{1/4} \rfloor$.

Output: The unique reduced form $f_3 = (a_3, b_3, c_3)$ in the class of the composition of f_1 and f_2.

1 **[Initialize]**
If $a_1 < a_2$ exchange f_1 and f_2. Set $s \leftarrow (b_1 + b_2)/2$ and $n \leftarrow b_2 - s$

2 **[First Euclidean step]**
Use Euclid's extended algorithm to compute u, v, d such that $ua_2 + va_1 = d = gcd(a_1, a_2)$
If $d = 1$, set $A \leftarrow -un$, $d_1 \leftarrow d$ and go to step 5 [Special case]
If $d \neq 1$ but $d|s$, set $A \leftarrow -un$, $d_1 \leftarrow d$, $a_1 \leftarrow a_1/d_1$, $a_2 \leftarrow a_2/d_1$, $s \leftarrow s/d_1$ and go to step 5 [Special Case]

3 **[Second Euclidean step]**
(In this step $d \nmid s$, since the other cases have been considered separately) Using Euclid's extended algorithm, compute $u_1, v_1 and d_1$ such that $u_1 s + v_1 d = d_1 = gcd(s, d)$
If $d_1 > 1$, set $a_1 \leftarrow a_1/d_1$, $a_2 \leftarrow a_2/d_1$, $s \leftarrow s/d_1$ and $d \leftarrow d/d_1$

4 **[Reduction Initialization]**
Compute $l \leftarrow -u_1(uc_1 + vc_2) \pmod{d}$ by first reducing c_1 and $c_2 \pmod{d}$, doing the operation, and then reducing again
Set $A \leftarrow -u(n/d) + l(a_1/d)$

5 **[Partial reduction]**
Set $A \leftarrow A \pmod{a_1}$, $A_1 \leftarrow a_1 - A$ and if $A_1 < A$ set $A \leftarrow A_1$
Execute PARTEUCL(a_1,A

6 **[Special case]**
If $z = 0$, set $Q_1 \leftarrow a_2 v_3$, $Q_2 \leftarrow Q_1 + n$, $f \leftarrow Q_2/d$, $g \leftarrow (sd + c_2)/d$, $a_3 \leftarrow da_2$, $c_3 \leftarrow v_3 d + g d_1$, $b_3 \leftarrow 2Q_1 + b_2$
Reduce the form $f_3 = (a_3, b_3, c_3)$, output f_3 and terminate

7 **[Final computations]**
Set $b \leftarrow (a_2 d + nv)/a_1$, $Q_1 \leftarrow bv_3$, $Q_3 \leftarrow Q_1 + n$, $f \leftarrow Q_2/d$, $e \leftarrow (sd + c_2 v)/a_1$, $Q_3 \leftarrow ev_2$, $Q_4 \leftarrow Q_3 - s$, $g \leftarrow Q_4/v$ and if $d > 1$, set $v_2 \leftarrow d_1 v_2$, $v \leftarrow d_1 v$
Set $a_3 = db + ev$, $c_3 = v_3 f + g v_2$ and $b_3 \leftarrow Q_1 + Q_2 + d_1(Q_3 + Q_4)$
Reduce the form $f_3 = (a_3, b_3, c_3)$
Output f_3 and terminate

Algorithm 8: NUCOMP algorithm. Computes the reduced form in the class of the composition of two given forms.

References

[Buc09] Johannes A. Buchmann. *Introduction to cryptography*. Springer-Verlacht, 2009.

[Bue89] Duncan A. Buell. *Binary quadratic forms: classical theory and modern computations*. Springer-Verlag, New York Inc., 1989.

[BW88] Johannes Buchmann and H. C. Williams. A key-exchange system based on imaginary quadratic fields. *Journal of Cryptology*, pages 107–118, 1988.

[Coh93] Henri Cohen. *Course in computational algebraic number theory*. Springer-Verlag Berlin Heidelberg, 1993.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons Inc., 1989.

[DH76] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Transactions on information theory*, 22:644–654, 1976.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In George Robert Blakley and David Chaum, editors, *Advances in Cryptology*, pages 10–18, Berlin, Heidelberg, 1985. Springer Berlin Heidelberg.

[Gau96] Carl Friedrich Gauss. *Disquisicions Aritmètiques*. Institut d'Estudis Catalans, Barcelona, 1996. Traducció i pròleg de Griselda Pascual Xufré.

[HJPT98] Detlef Hühnlein, Michael Jacobson, Jr, Sachar Paulus, and Tsuyoshi Takagi. A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption. In *Lectures on Computer Science*, volume 1403, pages 294–307, 05 1998.

[HM89] James L. Hafner and Kevin S. McCurley. A rigurous subexponential algorithm for computation of class groups. *Journal of the American Mathematical Society*, pages 937–850, 1989.

[JP02] Michael Jacobson, Jr and Alfred Poorten. Computational aspects of nucomp. In *Lecture Notes in Computer Science*, pages 120–133, 06 2002.

[Mar18] Daniel A. Marcus. *Number fields*. Springer International Publishing AG, 2018.

[PT98] Sachar Paulus and Tsuyoshi Takagi. A new public-key cryptosystem over a quadratic order with quadratic decryption time. *Journal of Cryptology*, 13:263–272, 1998.

[Sha73] Daniel Shanks. Five number-theoretic algorithms. In *Proceedings of the Second Manitoba Conference on Numerical Mathematics*, pages 51–70, 1973.

[Tra20a] Artur Travesa. *Equacions algebraiques*. Universitat de Barcelona, 2020. Available in pdf format at `https://travesa.cat/`.

[Tra20b] Artur Travesa. *Teoria de Nombres*. Universitat de Barcelona, 2020. Available in pdf format at `https://travesa.cat/`.