Linearly Homomorphic Encryption from DDH

Guilhem Castagnos, Fabien Laguillaumie

Linearly Homomorphic Encryption from DDH

Guilhem Castagnos[1], Fabien Laguillaumie[2]

[1] Institut de Mathématiques de Bordeaux UMR 5251, Université de Bordeaux
351, cours de la Libération, 33405 Talence cedex, France
guilhem.castagnos@math.u-bordeaux.fr
[2] Université Claude Bernard Lyon 1
CNRS/ENSL/INRIA/UCBL LIP
Laboratoire de l'Informatique du Parallélisme
46 Allée d'Italie, 69364 Lyon, France
fabien.laguillaumie@ens-lyon.fr

Abstract. We design a linearly homomorphic encryption scheme whose security relies on the hardness of the decisional Diffie-Hellman problem. Our approach requires some special features of the underlying group. In particular, its order is unknown and it contains a subgroup in which the discrete logarithm problem is tractable. Therefore, our instantiation holds in the class group of a non maximal order of an imaginary quadratic field. Its algebraic structure makes it possible to obtain such a linearly homomorphic scheme whose message space is the whole set of integers modulo a prime p and which supports an unbounded number of additions modulo p from the ciphertexts. A notable difference with previous works is that, for the first time, the security does not depend on the hardness of the factorization of integers. As a consequence, under some conditions, the prime p can be scaled to fit the application needs.

Keywords: Linearly Homomorphic Encryption, Orders of Quadratic Fields, Diffie-Hellman Assumptions

1 Introduction

Encryption protocols insure confidentiality during information transmission. They are the heart of any communication architecture. Their security has been formally defined for long, and many efficient encryption schemes fulfill the strongest security requirement, namely the indistinguishability of ciphertexts under an adaptive chosen message attack. Roughly speaking, it means that an attacker will learn not even a single bit of a message, given its encryption, even if he has access to a decryption oracle.

Paradoxically, a widely deployed kind of encryption scheme has an "algebraic" property which precludes it to reach this highest level of security. It is called *homomorphic*, because an operation on the ciphertexts translates into an operation on the underlying plaintexts. It is well-known that such protocols cannot reach the highest level of security, even though, this homomorphic property is actually very important for many applications, like e-voting for instance. Indeed, an *additively* homomorphic encryption makes it possible to obtain an encryption of the sum of all the ballots (which consists in 0 or 1 in the case of a 2-choice referendum for instance) from their encryption, so that a single decryption will reveal the result of the election, saving a lot of computational resources

which would have been necessary to decrypt all the ciphertexts one by one. Linearly homomorphic encryption schemes have attracted a lot of attention because of their potential applications. A tremendous breakthrough related to homomorphic encryption was Gentry's theoretical construction of a *fully* homomorphic encryption scheme [Gen09], which actually allows to evaluate any function on messages given their ciphertexts.

Currently, no linearly homomorphic encryption scheme is secure under a discrete logarithm related assumption. This theoretical question has been open for thirty years. In this paper, we provide the first construction of such a scheme.

Related Work. The story of homomorphic encryption begins with the first probabilistic encryption scheme, which was also homomorphic, by Goldwasser and Micali from [GM84], improved by Benaloh in his thesis [Ben88], then by Naccache and Stern in [NS98] and Okamoto and Uchiyama [OU98]. One of the most achieved system was actually designed by Paillier [Pai99]. Its semantic security relies on the decisional composite residuosity assumption. Paillier's scheme has then been generalized by Damgård and Jurik [DJ01], allowing to encrypt larger messages. This family of practical linearly homomorphic schemes is still growing with the recent work of Joye and Libert [JL13]. The security of these schemes is based on the problem of factoring RSA integers (including the elliptic curve variant of Paillier [Gal02]).

To design a linearly homomorphic encryption based on the Discrete Logarithm problem (DL), a folklore solution consists in encoding the message in the exponent of an Elgamal encryption, *i.e.*, in encrypting m as $(g^r, h^r g^m)$ where g is a generator of a cyclic group $G = \langle g \rangle$ and $h = g^x$ is the public key. Unfortunately, to decrypt, one has to recover m from g^m and as the DL problem in G must be intractable, m has to be small enough to ensure a fast decryption. As a result, only a logarithmic number of additions is possible. There have been some attempts to reach a fully additive homomorphy based on the DL problem, with a variant of Elgamal modulo p^2 ([CPP06]) or with messages encoded as a small smooth number ([CC07]); both solutions still have a partial homomorphy. In [W+11], the map $m \mapsto g_0^m \mod p_0$ is used with the plain Elgamal, where p_0 is a prime such that $p_0 - 1$ is smooth and g_0 is a primitive root modulo p_0. Unfortunately, although not clearly stated, this scheme only supports a limited number of additions, and it is not semantically secure as the set of encoded messages does not belong to a proper subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$ where the Decisional Diffie-Hellman assumption (DDH) holds.

A full solution has been proposed by Bresson *et al.* in [BCP03]. However, their scheme is not only based on the DL problem but also on the factorization problem. It is less efficient than [Pai99] but has an additional property: it has a double trapdoor. The idea is to use the same setting as Paillier: In $(\mathbf{Z}/N^2\mathbf{Z})^\times$, the DL problem in basis $f = 1 + N$ is easy. Bresson *et al.* use an Elgamal encryption of the message m as $(g^r, f^m \cdot h^r)$ modulo N^2, where N is an RSA integer.

To our knowledge, designing a linearly homomorphic scheme based on the sole hardness of the DL problem is an open problem, as stated in [CPP06]. Some other schemes allow more homomorphic operations, like [BGN05] or [CL12]. As already mentioned, a fully homomorphic encryption (FHE) scheme appeared in 2009 [Gen09]. Its security relies on hard problems related to lattices. The latest developments of FHE [BV14] are

getting more and more efficient and might become operational soon for applications that need a complex treatment over ciphertexts. Meanwhile, for applications that need only to add ciphertexts, protocols that rely on "classical" algorithmic assumptions are still more competitive, in particular in terms of compactness.

Our Contributions. Our contribution has both a theoretical and a practical impact. On one hand, we propose a linearly homomorphic encryption scheme whose security relies on the hardness of the decisional Diffie-Hellman problem. In particular it is the first time that the security of such a scheme does not depend on the hardness of the factorization of integers. On the other hand, we provide an efficient implementation within some specific group, namely the class group of orders in imaginary quadratic fields.

The design of our scheme is somehow similar to the one of [BCP03]. We use a group $G = \langle g \rangle$ such that the DDH assumption holds in G and such that there exists a subgroup $\langle f \rangle$ of G where the DL problem is easy (called a DDH group with an easy DL subgroup). Then the core of the protocol is an Elgamal encryption of the message m as $(g^r, f^m \cdot h^r)$ for a random r. In our case, the message space will be $(\mathbf{Z}/p\mathbf{Z})^*$, where p is a prime. Compared to some other linearly homomorphic schemes, ours allows some flexibility as p can be chosen (with some restrictions) independently from the security parameter.

To reach this unnatural feature without involving the factorization problem, we had to use the particular algebraic structure of class groups of imaginary quadratic fields, which have some specificities which seem hard to find in other groups. We designed a method to compute a group of unknown[3] order (to insure the hardness of a partial discrete logarithm assumption) which contains an easy DL subgroup (of known order). The interest of class group of orders in imaginary (or real) quadratic fields in cryptography decreased after critical attacks by Castagnos *et al.* [CL09,CJLN09] on some specific cryptosystems such as NICE [HPT99,PT00] and its real variant [JSW08]. These attacks will not apply in our setting. Indeed, these attacks recover the secret key by exposing the factorization of the discriminant of the field, thanks to the structure of the kernel of the surjection between the class group of a non maximal order to the class group of the maximal order. In our case, the factorization of the discriminant will be public and we will use constructively the ideas of [CL09]: the subgroup with an easy DL will be precisely the kernel of this surjection. The security of our scheme is proved to rely only on the hardness of the DDH problem in the class group of a non maximal order and on the hardness of computing class numbers. Several systems that adapt either Diffie-Hellman or Elgamal in class groups are already based on the DL problem and the DDH assumption in class groups of maximal order ([BW88,BDW90,SP05,BH01,BV07]) of discriminant Δ_K. The current best known algorithms to solve these problems have a sub-exponential complexity of complexity $L_{|\Delta_K|}(1/2, o(1))$ (cf. [BJS10]). It means that the factorization problem (or the discrete logarithm problem in a finite field) can be solved asymptotically *faster* than the discrete logarithm in the class group.[4] Moreover,

[3] Using groups of unknown order in cryptography has already been done [Bre00,CHN99,DF02]

[4] Note that it is well known (see [HM00] for instance) that computing the class number of a quadratic field of discriminant Δ allows to factor Δ . However for our scheme, the factorization of the discrim-

arithmetic operations in class groups are very efficient, since the reduction and composition of quadratic forms have a quadratic time complexity (and even quasi linear using fast arithmetic).

As a result, our scheme is very competitive. With a straightforward implementation and using an underlying arithmetics very favorable to [Pai99,BCP03], it compares very well with these linearly homomorphic protocols. With a similar level of security, it is faster than [BCP03] with a 2048 bits modulus, and the decryption process is faster than Paillier's for a 3072 bits modulus.

A very nice application of our protocol is that it can be used directly in Catalano and Fiore's linearly homomorphic encryption transformation to evaluate degree-2 computations on ciphertexts [CF14]. Their technique requires the message space to be a public ring in which it is possible to sample elements uniformly at random. Our scheme has this feature naturally, contrary to some of the other additively homomorphic schemes. It is therefore a very competitive candidate in 2-server delegation of computation over encrypted data (see [CF14] for more details).

The rest of the paper is organized as follows. In Section 2, we formalize the notion of DDH *Group with an Easy* DL *Subgroup*, give reductions between related problems and propose a generic construction of a linearly homomorphic encryption scheme which relies on such group, and prove its security. Sections 3 and 4 present our instantiation in class groups. We give benchmarks and comparisons before concluding. Background on linearly homomorphic encryption can be found in Appendix A. Background on class groups of imaginary quadratic fields and their use for DL based cryptography are given in Appendix B.

2 DDH Group with an Easy DL Subgroup

In this section, we introduce and formalize the concept of a group in which the decisional Diffie-Hellman problem is hard, whereas it contains a subgroup in which the discrete logarithm problem is easy. This problem has already been used to design cryptosystems, including, for instance, Bresson *et al.*'s encryption scheme [BCP03]. It will be adjusted to build our new encryption protocol.

2.1 Definitions and Reductions

Definition 1. *We define a* DDH group with an easy DL subgroup *as a pair of algorithms* $(\mathsf{Gen}, \mathsf{Solve})$. *The* Gen *algorithm is a group generator which takes as input two parameters* λ *and* μ *and outputs a tuple* (B, n, p, s, g, f, G, F). *The integers* B, n, p *and* s *are such that* s *is a* λ*-bit integer,* p *is a* μ*-bit integer,* $\gcd(p, s) = 1$, $n = p \cdot s$ *and* B *is an upper bound for* s. *The set* $(G, \cdot)$ *is a cyclic group of order* n *generated by* g, *and* $F \subset G$ *is the subgroup of* G *of order* p *and* f *is a generator of* F. *The upper bound* B *is chosen such that the distribution induced by* $\{g^r, r \xleftarrow{\$} \{0, \ldots, Bp-1\}\}$ *is statistically indistinguishable from*

inant Δ will be public or Δ will be a prime, so we will not rely on the hardness of the factorization problem.

the uniform distribution on G. We assume that the canonical surjection $\pi : G \to G/F$ is efficiently computable from the description of G, H and p and that given an element $h \in G/F$ one can efficiently lift h in G, i.e., *compute an element $h_\ell \in \pi^{-1}(h)$.*

We suppose moreover that:

1. *The* DL *problem is easy in F. The* Solve *algorithm is a deterministic polynomial time algorithm that solves the discrete logarithm problem in F:*

$$\Pr\big[x = x^\star : (B, n, p, s, g, f, G, F) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, 1^\mu), x \xleftarrow{\$} \mathbf{Z}/p\mathbf{Z}, X = f^x, \\ x^\star \leftarrow \mathsf{Solve}(B, p, g, f, G, F, X)\big] = 1$$

2. *The* DDH *problem is hard in G even with access to the* Solve *algorithm:*

$$\Big|\Pr\big[b = b^\star : (B, n, p, s, g, f, G, F) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, 1^\mu), x, y, z \xleftarrow{\$} \mathbf{Z}/n\mathbf{Z}, X = g^x, Y = g^y, \\ b \xleftarrow{\$} \{0,1\}, Z_0 = g^z, Z_1 = g^{xy}, b^\star \xleftarrow{\$} \mathcal{A}(B, p, g, f, G, F, X, Y, Z_b, \mathsf{Solve}(.))\big] - \frac{1}{2}\Big|$$

is negligible for all probabilistic polynomial time attacker $\mathcal{A}$.

The bound B for the order s in Definition 1 can be chosen as $B = 2^{2\lambda}$. Indeed, according to Lemma 4 in Appendix C, the statistical distance of $\{g^r, r \xleftarrow{\$} \{0, \ldots, Bp-1\}\}$ to the uniform distribution is upper bounded by $n/(4pB) = s/2^{2\lambda+2} \leqslant 2^{-\lambda-2}$ which a negligible function of λ.

It is fundamental to note that in this definition, the order n of the group G is *not* an input of the adversary or of the Solve algorithm: Only the bound Bp is implicitly given. Indeed, if n or s were efficiently computable from the description of G, a DDH group with an easy DL subgroup would not exist since it would be possible to partially compute discrete logarithms. More formally, let us define the following partial discrete logarithm problem initially introduced by Paillier in [Pai99], in the context of the group $(\mathbf{Z}/N^2\mathbf{Z})^\times$.

Definition 2 (Partial Discrete Logarithm (PDL) Problem). *Let* (Gen, Solve) *be a* DDH *group with an easy* DL *subgroup. Let $(B, n, p, s, g, f, G, F) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, 1^\mu)$, $x \xleftarrow{\$} \mathbf{Z}/n\mathbf{Z}, X = g^x$. The* Partial Discrete Logarithm Problem *consists in computing x modulo p; given (B, p, g, f, G, F, X) and access to the* Solve *algorithm.*

Lemma 1. *Let* (Gen, Solve) *be a* DDH *group with an easy* DL *subgroup and let the tuple (B, n, p, s, g, f, G, F) be an output of $\mathsf{Gen}(1^\lambda, 1^\mu)$. The knowledge of n makes the* PDL *problem easy.*

Proof. If an adversary is given an instance (B, p, g, f, G, F, X) of the PDL problem, as well as n, he can compute $s = n/p$ and then for all $h \in G$, h^s lies in F. The adversary can run the Solve algorithm with g^s as input to find $\alpha \in \mathbf{Z}/p\mathbf{Z}$ such that $g^s = f^\alpha$. Note that $\alpha \not\equiv 0 \pmod p$ as g has order n. Thanks to another run of the Solve algorithm with X^s as input, the adversary obtains $\beta \in \mathbf{Z}/p\mathbf{Z}$ such that $X^s = g^{sx} = f^\beta$. Eventually, he computes $x \equiv \beta\alpha^{-1} \pmod p$. □

Lemma 2. *Let G be a* DDH *group with an easy* DL *subgroup. The* DDH *problem in G reduces to the* PDL *problem.*

Proof. Let $(B, p, g, f, G, F, X, Y, Z)$ be an instance of the DDH problem in G. Three queries to the PDL oracle respectively on (B, p, g, f, G, F, X), (B, p, g, f, G, F, Y) and (B, p, g, f, G, F, Z), gives the adversary x, y and z modulo p. His answer to the DDH instance will be 1 if and only if $xy \equiv z \pmod{p}$. Indeed, if (X, Y, Z) is a true DDH triple then $xy \equiv z \pmod{n}$ and he always finds the right answer. Conversely, if (X, Y, Z) is not a DDH triple, $xy \not\equiv z \pmod{n}$, and then the adversary fails to correctly responds if $xy \equiv z \pmod{p}$. But this happens with probability $1/p$. As a result, we have sketched a probabilistic polynomial time adversary against DDH with a non negligible advantage equals to $\frac{1}{2}(1 - \frac{1}{p})$. □

Remark 1. Combining Lemmas 1 and 2 we get that as previously mentioned, with the notation of Definition 1, if n is easily computable from the description of G, then the DDH problem in G is easy so, G can not be a DDH group with an easy DL subgroup.

The following problem was introduced in [BCP03] in $(\mathbf{Z}/N^2\mathbf{Z})^\times$. It is a variant of the computational Diffie-Hellman problem, that we adapt to our general context.

Definition 3 (Lift Diffie-Hellman (LDH) Problem). *Let* $(\mathsf{Gen}, \mathsf{Solve})$ *be a* DDH *group with an easy* DL *subgroup. Let* $(B, n, p, s, g, f, G, F) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, 1^\mu)$. *Let* $x, y \xleftarrow{\$} \mathbf{Z}/n\mathbf{Z}, X = g^x, Y = g^y$ *and* $Z = g^{xy}$ *and* $\pi : G \to G/F$ *be the canonical surjection. The* Lift Discrete Logarithm Problem *consists in computing Z, given the tuple* $(B, p, g, f, G, F, X, Y, \pi(Z))$ *and access to the* Solve *algorithm.*

In the following theorem we prove that this problem is equivalent to the PDL problem. Curiously only one implication was proved in [BCP03].

Theorem 1. *In a* DDH *group with an easy* DL *subgroup, the* LDH *and* PDL *are equivalent.*

Proof. In all the proof, we implicitly set $s = n/p$ and $\alpha \in (\mathbf{Z}/p\mathbf{Z})^\times$ such that $g^s = f^\alpha$ and denote $\beta \equiv \alpha^{-1} \pmod{p}$. Let us first prove that the PDL problem reduces to the LDH problem, which is a direct generalization of the proof of [BCP03, Theorem 10]. Let (B, p, g, f, G, F, X) be a PDL challenge and let denote $X = g^x$ where $x = x_1 + x_2 p$ with $x_1 = x \mod p$. The adversary draws $r_1 \xleftarrow{\$} \{0, \ldots, B-1\}$, $r_2 \xleftarrow{\$} \{0, \ldots, p-1\}$ and sets $Y = g^{r_1} f^{r_2}$. Note that $Y = g^{r_1 + s\beta r_2}$. Let us prove that the random variable Y is statistically indistinguishable from the uniform distribution in G.

The distance between Y and the uniform distribution in G is the same than the distance between $Y' = r_1 + s\beta r_2 \mod n$ with r_1 uniformly drawn in $\{0, \ldots, B-1\}$ and r_2 independently uniformly drawn in $\{0, \ldots, p-1\}$ and the uniform distribution in $\{0, \ldots, n-1\}$. Let y be an element of $\{0, \ldots, n-1\}$, we denote $y = y_1 + y_2 s$ with $y_1 \in \{0, \ldots, s-1\}$ and $y_2 \in \{0, \ldots, p-1\}$ the euclidean division of y by s. We have

$$\Pr[Y' = y] = \Pr[Y' = y_1 + y_2 s] = \Pr[r_1 + s\beta r_2 \equiv y_1 + y_2 s \pmod{n}] =$$

$$\Pr[r_1 \equiv y_1 \pmod{s}] \Pr[r_2\beta \equiv y_2 \pmod{p}] = \Pr[r_1 \equiv y_1 \pmod{s}]/p$$

as $\beta \not\equiv 0 \pmod{p}$. Now let $B = qs + r$ with $0 \leqslant r < s$ be the euclidean division of B by s. We proceed as in the proof of Lemma 4 in Appendix C. For $y_1 < r$, $\Pr[r_1 \equiv y_1 \pmod{s}] = (q+1)/B > \frac{1}{s}$ and for $y_1 \geqslant r$, $\Pr[r_1 \equiv y_1 \pmod{s}] = q/B \leqslant \frac{1}{s}$. Eventually,

$$\Delta(X, Y) = r\left(\frac{q+1}{Bp} - \frac{1}{n}\right) = \frac{r(s-r)}{Bn} = \frac{r(n-pr)}{pBn} \leqslant \frac{r(n-r)}{pBn}.$$

This last quantity is the statistical distance of $\{g^r, r \xleftarrow{\$} \{0, \ldots, Bp-1\}\}$ to the uniform distribution in G which is suppose to be negligible. This proves that Y is statistically indistinguishable from the uniform distribution in G.

The adversary then compute $Z' = \pi(X^{r_1}) = \pi(X^{r_1 + s\beta r_2})$ and queries the LDH oracle with $(B, p, g, f, G, F, X, Y, Z')$. The oracle provides with non negligible probability

$$Z = X^{r_1+s\beta r_2} = X^{r_1}(g^x)^{s\beta r_2} = X^{r_1} g^{(x_1+x_2p)(s\beta r_2)} = X^{r_1} g^{x_1 s\beta r_2} = X^{r_1} f^{x_1 r_2}.$$

Then, $Z/X^{r_1} = f^{x_1 r_2}$ and running the Solve algorithm on this value gives $x_1 r_2 \pmod{p}$ to the adversary from which he can get x_1, the answer to the PDL instance.

Now, let us prove that the LDH problem reduces to the PDL problem. Let us consider $X = g^x, Y = g^y$, $Z = g^{xy}$ for random x and y, such that the LDH challenge writes as $(B, p, g, f, G, F, X, Y, Z' = \pi(Z))$. The adversary makes two queries to the PDL oracle relative to X and Y, from which he obtains $x \pmod{p}$ and $y \pmod{p}$. The adversary draws $r_1 \xleftarrow{\$} \{0, \ldots B-1\}$ and $r_2 \xleftarrow{\$} \{0, \ldots, p-1\}$ and sets $U = g^{r_1} f^{r_2}$, which is as before statistically indistinguishable from the uniform distribution in G. The adversary queries the PDL oracle with U, which gives $r_1 + s\beta r_2 \pmod{p}$ as $U = g^{r_1+s\beta r_2}$. From this answer, the adversary can compute $s\beta \pmod{p}$. From the definition of a DDH group with an easy DL subgroup, the adversary can compute $Z'_\ell \in \pi^{-1}(Z')$. He then draws $r \xleftarrow{\$} \mathbf{Z}/p\mathbf{Z}$ and computes $V = f^r Z'_\ell$. The random variable V is uniformly distributed in G. As $\pi(V) = Z' = \pi(Z)$, there exists $\gamma \in \mathbf{Z}/p\mathbf{Z}$ such that $V = f^\gamma Z = g^{s\beta\gamma + xy}$. From a last call to the PDL oracle, the adversary can get $s\beta\gamma + xy \pmod{p}$ from which he can compute γ since $\gcd(s\beta, p) = 1$. Eventually, the adversary deduces Z from $V = f^\gamma Z$. □

We now further analyze the relations between the problems in G/F and G. We first give a lemma that shows that we can define a morphism in order to lift the elements from G/F to G.

Lemma 3. *Let $(B, n, p, s, g, f, G, F) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, 1^\mu)$ where $(\mathsf{Gen}, \mathsf{Solve})$ is a DDH group with an easy DL subgroup. Denote $\pi : G \to G/F$ the canonical surjection. The map $\psi : G/F \to G$ s.t. $h \mapsto h_\ell^p$, where $h_\ell \in \pi^{-1}(h)$, is an effective injective morphism.*

Proof. First ψ is well defined: if $h_\ell^{(1)}, h_\ell^{(2)} \in \pi^{-1}(h)$ are two distinct pre-images of h then there exists an element $f^r \in F$ such that $h_\ell^{(1)} = f^r h_\ell^{(2)}$, and $(h_\ell^{(1)})^p = (h_\ell^{(2)})^p$ as F is of order p. Moreover it is easy to see that ψ is a morphism. Consider h in G/F

such that $\psi(h) = h_\ell^p = 1$ in G, with $h_\ell \in \pi^{-1}(h)$. Applying π gives $\pi(h_\ell)^p = h^p = 1$. As G/F is of order s prime to p then $h = 1$, so the map is injective. Eventually, ψ is efficiently computable as computing h_ℓ is easy by definition of a DDH group with an easy DL subgroup. □

Theorem 2. *Let* $(B, n, p, s, g, f, G, F) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, 1^\mu)$ *where* $(\mathsf{Gen}, \mathsf{Solve})$ *is a* DDH *group with an easy* DL *subgroup. The* DL *problem in* G/F *reduces to the* DL *problem in* G.

Proof. Consider a DL problem instance in G/F: Let $h = g^x$ where g is a generator of G/F of order s and $x \xleftarrow{\$} \mathbf{Z}/s\mathbf{Z}$. The adversary chooses $r, r' \xleftarrow{\$} (\mathbf{Z}/p\mathbf{Z})^\times$ and computes $g_\ell = \psi(g)f^r$ and $h_\ell = \psi(h)f^{r'}$ where the map ψ is defined in Lemma 3. The element $\psi(g)$ has order s as ψ is injective and f^r has order p. As $\gcd(p, s) = 1$, g_ℓ has order ps and is a generator of G. Moreover, G can be viewed as the direct product $\psi(G/F) \times F$. The element h is uniformly distributed in G/F, $f^{r'}$ is uniformly distributed in F so $h_\ell = \psi(h)f^{r'}$ is uniformly distributed in G. As a consequence, an oracle for the DL problem in G gives x_ℓ such that $g_\ell^{x_\ell} = h_\ell$ to the adversary with a non negligible advantage. He then has $g_\ell^{x_\ell} = \psi(g)^{x_\ell} f^{rx_\ell} = h_\ell = \psi(h)f^{r'}$. By the uniqueness of the decomposition of an element of G in a product of an element of $\psi(G/F)$ and an element of F, and because ψ is injective, we must have $g^{x_\ell} = h$ and therefore $x_\ell \equiv x \pmod{s}$. □

Unfortunately, it seems unlikely that a similar reduction of the DDH problem in G/F to the DDH problem in G exists. Indeed, a DDH challenge in G/F can be lifted into $\psi(G/F) \subset G$. But $G = \psi(G/F) \times F$, so the reduction has to fill the $F-$part to keep the DDH challenge's form. This seems impossible with a non-negligeable advantage.

2.2 Examples

Let G be the group of quadratic residues modulo N^2 where $N = (2p'+1)(2q'+1)$ is the product of two safe primes. In this case, the order of G is $Np'q'$. The subgroup H of order N of G is generated by $1+N$, and since $(1+N)^k \equiv 1 + kN \pmod{N^2}$, the DL problem is easy in H (cf. [Pai99]). If the factorization of N is known, then DDH problem in G can not be hard (cf. Remark 1). This inspired [BCP03, Theorem 4] where the factorization acts as a second trapdoor to an Elgamal-like protocol in G. A generalization of this protocol is given in the next subsection.

Now, let G be the group of quadratic residues modulo p^2 where $p = 2p' + 1$ is a safe prime. In this case, the DL problem is easy in the subgroup of order p generated by $1+p$. The order of G is pp' and it can not be hidden from the description of G (*i.e.*, the integer p^2). As a result, the PDL and DDH problems are easy. In [CPP06], the partial logarithm of an element is called the *class* of an element. They define a variant of the DDH problem, namely the *Decision Class Diffie-Hellman problem*, which is believed to be intractable in such a group G. From that problem, [CPP06] derived a modification of Elgamal which, unfortunately, is *partially* homomorphic: it only supports the addition of a constant.

2.3 A Generic Linearly Homomorphic Encryption Scheme

From a DDH group with an easy DL subgroup, we can devise generically a linearly homomorphic encryption scheme. An Elgamal type scheme is used in G, with plaintext message $m \in \mathbf{Z}/p\mathbf{Z}$ mapped to $f^m \in F$. The resulted scheme is linearly homomorphic. Thanks to the Solve algorithm, the decryption does not need a complex DL computation. We depict this scheme in Fig. 1. Note that the outputs n and s of Gen are not used in the algorithms.

Algorithm $\mathsf{KeyGen}(1^\lambda)$

1. $(B, n, p, s, g, f, G, F) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, 1^\mu)$
2. Pick[a] $x \xleftarrow{\$} \{0, \ldots, Bp-1\}$ and set $h \leftarrow g^x$
3. Set $pk \leftarrow (B, p, g, h, f)$ and $sk \leftarrow x$.
4. Return (pk, sk)

Algorithm $\mathsf{Encrypt}(1^\lambda, pk, m)$

1. Pick $r \xleftarrow{\$} \{0, \ldots, Bp-1\}$
2. Compute $c_1 \leftarrow g^r$
3. Compute $c_2 \leftarrow f^m h^r$
4. Return (c_1, c_2)

[a] As n will be unknown in the sequel, x is picked at random in $\{0, \ldots, Bp-1\}$

Algorithm $\mathsf{Decrypt}(1^\lambda, pk, sk, (c_1, c_2))$

1. Compute $M \leftarrow c_2/c_1^x$
2. $m \leftarrow \mathsf{Solve}(p, g, f, G, F, M)$
3. Return m

Algorithm $\mathsf{EvalSum}(1^\lambda, pk, (c_1, c_2), (c_1', c_2'))$

1. Compute $c_1'' \leftarrow c_1 c_1'$ and $c_2'' \leftarrow c_2 c_2'$
2. Pick $r \xleftarrow{\$} \{0, \ldots, Bp-1\}$
3. Return $(c_1'' g^r, c_2'' h^r)$

Algorithm $\mathsf{EvalScal}(1^\lambda, pk, (c_1, c_2), \alpha)$

1. Compute $c_1' \leftarrow c_1^\alpha$ and $c_2' \leftarrow c_2^\alpha$
2. Pick $r \xleftarrow{\$} \{0, \ldots, Bp-1\}$
3. Return $(c_1' g^r, c_2' h^r)$

Fig. 1. A generic linearly homomorphic encryption scheme

Let us prove the homomorphic property of the scheme. Let us consider an output of the EvalSum algorithm on an input corresponding to encryptions of m and m'. Due to Elgamal's multiplicativity, the first line of the decryption algorithm applied on this output gives $M = f^m f^{m'} = f^{m+m' \mod p}$ as f as multiplicative order p. As a consequence, the decryption process indeed returns $m+m' \mod p$, and the EvalSum algorithm gives a random encryption of $m+m' \pmod p$ (in the sense that it has the same output distribution than the encryption algorithm on the input $m+m' \pmod p$). The same argument works for the EvalScal algorithm, with any scalar $\alpha \in \mathbf{Z}/p\mathbf{Z}$.

2.4 Security

The total break of our scheme ($\mathsf{tb}-\mathsf{cpa}$ attack) consists in finding x from (B, p, g, g^x, f), *i.e.*, in computing a discrete logarithm in G. From Theorem 2, this is harder than computing a discrete logarithm in G/F.

Theorem 3. *The scheme described in Fig. 1 is one-way under chosen plaintext attack ($\mathsf{ow}-\mathsf{cpa}$) if and only if the Lift Diffie-Hellman (LDH) problem is hard (so if and only if the partial discrete logarithm problem (PDL) is hard).*

Proof. From the equivalence of Theorem 1, it suffices to prove the equivalence between the $\mathsf{ow}-\mathsf{cpa}$ security and the hardness of the LDH problem. Let us consider $(c_1, c_2) = (g^r, f^m h^r)$, a ciphertext with the public key $h = g^x$. Then as $\pi(c_2) = \pi(h^r) = \pi(g^{xr})$, the triplet $(h, c_1, \pi(c_2))$ is an LDH challenge. Given a LDH oracle, we obtain $Z = g^{xr} = h^r$ and recover m by running Solve on c_2/Z.

Conversely let $(X, Y, Z') = (g^x, g^y, \pi(Z))$ be an LDH challenge with $Z = g^{xy}$. From this triplet, one can set X as public key and construct the ciphertext $(c_1, c_2) = (Y, f^r Z'_\ell)$ where $Z'_\ell \in \pi^{-1}(Z')$ and r is a random element of $\mathbf{Z}/p\mathbf{Z}$. As $\pi(c_2) = Z' = \pi(Z)$, one as $c_2 = f^m Z$ for an element $m \in \mathbf{Z}/p\mathbf{Z}$. As a result, (c_1, c_2) is a correct ciphertext of m, and a decryption oracle would respond m from which we can compute c_2/f^m and recover Z.

Theorem 4. *The scheme described in Fig. 1 is semantically secure under chosen plaintext attacks (*$\mathsf{ind}-\mathsf{cpa}$*) if and only the decisional Diffie-Hellman problem is hard in* G.

Proof. Let's construct a reduction $\mathcal{R}$ that solve the DDH assumption using an efficient $\mathsf{ind}-\mathsf{cpa}$ adversary $\mathcal{A}$. $\mathcal{R}$ takes as input a DDH instance $(B, p, g, f, G, F, X, Y, Z)$ and sets $pk = (B, p, g, X, f)$. When $\mathcal{A}$ requests an encryption of one of his choice of challenge messages m_0 and m_1, $\mathcal{R}$ flips a bit b encrypts m_b as $(Y, f^{m_b} Z)$ and sends this ciphertext as its answer to $\mathcal{A}$. If Z was not a random element, this ciphertext would be indistinguishable from a true encryption of m_b because of the choice of the bound B, and $\mathcal{A}$ will correctly answer with its (non-negligeable) advantage ϵ. Otherwise, the encryption is independent of the message and $\mathcal{A}$'s advantage to distinguish is $1/2$. Therefore, the reduction returns one if and only $\mathcal{A}$ correctly guessed b and has advantage $\epsilon/2$ to solve the DDH assumption. □

3 A Linearly Homomorphic Encryption from DDH

We prove that, somewhat like in Paillier's encryption scheme [Pai99] within $\mathbf{Z}/N^2\mathbf{Z}$, a subgroup with an easy discrete logarithm problem exists in class groups of imaginary quadratic fields, and it allows to design a new linearly homomorphic encryption scheme. We refer the reader to Appendix B for background on class groups of imaginary quadratic fields and their use in Discrete Logarithm based cryptography.

3.1 A Subgroup with an Easy DL Problem

The next proposition, inspired by [CL09, Theorem 2], establish the existence of a subgroup of a class group of an imaginary quadratic fields where the DL problem is easy.

Proposition 1. *Let* Δ_K *be a fundamental discriminant with* $\Delta_K \equiv 1 \pmod 4$ *of the form* $\Delta_K = -pq$ *where* p *is an odd prime and* q *a non-negative integer prime to* p *such that* $q > 4p$. *Let* $\mathfrak{f} = (p^2, p)$ *be an ideal of* $\mathcal{O}_{\Delta_p}$, *the order of discriminant* $\Delta_p = \Delta_K p^2$. *Denote by* $f = [\mathfrak{f}]$ *the class of* $\mathfrak{f}$ *in* $C(\mathcal{O}_{\Delta_p})$. *For* $m \in \{1, \ldots, p-1\}$, $\mathsf{Red}(f^m) = (p^2, L(m)p)$ *where* $L(m)$ *is the odd integer in* $[-p, p]$ *such that* $L(m) \equiv 1/m \pmod p$. *Moreover,* f *is a generator of the subgroup of order* p *of* $C(\mathcal{O}_{\Delta_p})$.

Proof. We consider the surjection $\bar{\varphi}_p : C(\mathcal{O}_{\Delta_p}) \longrightarrow C(\mathcal{O}_{\Delta_K})$. From [CL09, Lemma 1] and [Cox99, Proposition 7.22 and Theorem 7.24], the kernel of $\bar{\varphi}_p$ is isomorphic to $(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K})^\times/(\mathbf{Z}/p\mathbf{Z})^\times$. As $p \mid \Delta_K$, the group $(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K})^\times$ is isomorphic to $(\mathbf{F}_p[X]/(X^2))^\times$. This group contains $p(p-1)$ elements of the form $a+b\sqrt{\Delta_K}$ where $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ and $b \in \mathbf{Z}/p\mathbf{Z}$. Now let us consider the quotient group $(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K})^\times/(\mathbf{Z}/p\mathbf{Z})^\times$ where $[x] = [y]$ with $x, y \in (\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K})^\times$ if and only if there exists $\lambda \in (\mathbf{Z}/p\mathbf{Z})^\times$ such that $x = \lambda y$. This quotient is cyclic of order p and a system of representatives is $[1]$ and $[a+\sqrt{\Delta_K}]$ where a is an element of $(\mathbf{Z}/p\mathbf{Z})^\times$. Let $g = [1+\sqrt{\Delta_K}]$, one has $g^m = [1+m\sqrt{\Delta_K}] = [L(m)+\sqrt{\Delta_K}]$ for all $m \in \{1, \ldots, p-1\}$ and $g^p = [1]$.

Let $\alpha_m = \frac{L(m)+\sqrt{\Delta_K}}{2} \in \mathcal{O}_{\Delta_K}$. Then α_m is a representative of the class g^m. The element g^m maps to the class $[\varphi_p^{-1}(\alpha_m\mathcal{O}_{\Delta_K})]$ of the kernel of $\bar{\varphi}_p$. From [BTW95, Proposition 2.9], one can see that $\alpha_m\mathcal{O}_{\Delta_K} = (N(\alpha_m), -L(m) \mod 2N(\alpha_m))$ where the remainder is computed from the centered euclidean division. Now,

$$\varphi_p^{-1}(\alpha_m\mathcal{O}_{\Delta_K}) = (N(\alpha_m), -L(m)p \mod 2N(\alpha_m)).$$

As $N(\alpha_m) = \frac{L(m)^2-\Delta_K}{4}$ and $q > 4p$, it follows that $p^2 < N(\alpha_m)$ and that $-L(m)p \mod 2N(\alpha_m) = -L(m)p$. As a consequence, this ideal $\varphi_p^{-1}(\alpha_m\mathcal{O}_{\Delta_K})$ corresponds to the quadratic form $\left(\frac{L(m)^2-\Delta_K}{4}, -L(m)p, p^2\right)$, of discriminant Δ_p. Moreover this form is equivalent to the form $(p^2, L(m)p, \frac{L(m)^2-\Delta_K}{4})$ which corresponds to the ideal $(p^2, L(m)p)$. Eventually, this ideal of $\mathcal{O}_{\Delta_p}$ is reduced as $|L(m)p| < p^2 < \sqrt{|\Delta_p|}/2$, where the second inequality holds because $q > 4p$. Consequently, if $\mathfrak{t} = (p^2, p)$, then $[\mathfrak{t}]$ generates the kernel of $\bar{\varphi}_p$ as $[\mathfrak{t}] = [\varphi_p^{-1}(\alpha_1\mathcal{O}_{\Delta_K})]$. Moreover, $[\mathfrak{t}]^m = [\varphi^{-1}(\alpha_m\mathcal{O}_{\Delta_K})]$ so $\mathsf{Red}([\mathfrak{t}]^m) = (p^2, L(m)p)$, for $m \in \{1, \ldots, p-1\}$. □

We devise, in Fig. 2, a new DDH group with an easy DL subgroup in class groups of imaginary quadratic fields, by assuming the difficulty of the DDH problem. In the Gen algorithm, we first construct a fundamental discriminant $\Delta_K = -pq$ such that the 2-Sylow subgroup of $C(\Delta_K)$ is of order 2 (cf. Appendix B.3). Then, using [HJPT98, Subsection 3.1]'s method, we construct an ideal $\mathfrak{r}$ of $\mathcal{O}_{\Delta_K}$ of norm r, where r is a prime satisfying $\left(\frac{\Delta_K}{r}\right) = 1$. We then assume, as in the previous implementations of Elgamal (cf. Appendix B.4) that the class $[\mathfrak{r}^2]$ will be of order s, an integer of the same order of magnitude than the odd part, $h(\Delta_K)/2$. Due to our choice of p and q, pq is 2λ-bit integer, and as s is close to $\sqrt{|\Delta_K|}$ (cf. Appendix B.3), it will be a λ-bit integer.

If $\mu > 80$, following the Cohen-Lenstra heuristics, the probability that p divides $h(\Delta_K)$ and s is negligible. Therefore, we can assume that $\gcd(p, h(\Delta_K)) = 1$. We consider the non-maximal order $\mathcal{O}_{\Delta_p}$ of discriminant $p^2\Delta_K$ as in Proposition 1. The fact that $\lambda \geqslant \mu + 2$ ensures that $q > 4p$. As a result, the subgroup F generated by f gives an easy DL subgroup. The morphism $\bar{\varphi}_p$ defined in Appendix B.1 plays the role of the surjection π between $C(\mathcal{O}_{\Delta_p})$ and $C(\mathcal{O}_{\Delta_p})/F \simeq C(\mathcal{O}_{\Delta_K})$, which is computable in polynomial time, knowing p (cf. [HJPT98, Algorithm 3]). Moreover, still with the knowledge of p, it is possible to lift elements of $C(\mathcal{O}_{\Delta_K})$ in $C(\mathcal{O}_{\Delta_p})$, using [HPT99, Algorithm 2]. We can then apply the injective morphism of Lemma 3 on $[\mathfrak{r}^2]$ to get a class of $C(\Delta_p)$ with the

same order s and multiply this class by f^k where $k \xleftarrow{\$} \{1, p-1\}$. As $\gcd(p,s) = 1$ the result, g is of order ps (this procedure to get an element of order ps was also used in the proof of Theorem 2). Note that g is still a square of $C(\Delta_p)$: as the map of Lemma 3 is a morphism, the lift of $[\mathfrak{r}^2]$ gives a square of $C(\Delta_p)$. Moreover, F is a subgroup of the squares: $f = (f^{2^{-1} \bmod p})^2$ as p is odd. As a consequence, g is a square as it is a product of two squares.

Eventually, we take $B = \lceil |\Delta_K|^{3/4} \rceil$. According to Lemma 4 in Appendix C, the statistical distance of $\{g^r, r \xleftarrow{\$} \{0, \ldots, Bp-1\}\}$ to the uniform distribution is upper bounded by $ps/(4pB) = s/(4\lceil |\Delta_K|^{3/4} \rceil)$. By Equation 1 in Appendix B.3 , this is less than $\frac{\log |\Delta_K|}{4\pi \lceil |\Delta_K|^{1/4} \rceil} \in \tilde{\mathcal{O}}(2^{-\lambda/2})$ which is a negligible function of λ. As a consequence, the distribution $\{g^r, r \xleftarrow{\$} \{0, \ldots, Bp-1\}\}$ is statistically indistinguishable from the uniform distribution in $G = \langle g \rangle$. In practice, for performance issue, one can take a better bound for B, for example $B = 2^{80} \lceil \log(|\Delta_K|) |\Delta_K|^{1/2}/(4\pi) \rceil$, which makes the statistical distance less than 2^{-80}.

Algorithm $\mathsf{Gen}(1^\lambda, 1^\mu)$

1. Assume $\lambda \geqslant \mu + 2$
2. Pick p a random μ-bits prime and q a random $(2\lambda - \mu)$ prime such that $pq \equiv -1 \pmod 4$ and $(p/q) = -1$.
3. Set $\Delta_K \leftarrow -pq$ and $\Delta_p \leftarrow p^2 \Delta_K$.
4. Set $f \leftarrow [(p^2, p)]$ in $C(\Delta_p)$ and $F = \langle f \rangle$
5. Let r be a small prime, with $r \neq p$ and $\left(\frac{\Delta_K}{r}\right) = 1$ and set $\mathfrak{r}$ an ideal lying above r.
6. Let $k \xleftarrow{\$} \{1, p-1\}$ and set $g \leftarrow [\varphi_p^{-1}(\mathfrak{r}^2)]^p f^k$ in $C(\Delta_p)$ and $G \leftarrow \langle g \rangle$
7. Let $B \leftarrow \lceil |\Delta_K|^{3/4} \rceil$
8. Return $(B, \emptyset, p, \emptyset, g, f, G, F)$

Algorithm $\mathsf{Solve}(B, p, g, f, G, F, X)$

1. Parse $\mathsf{Red}(X)$ as $(p^2, \tilde{x}p)$
2. If fails return $\perp$
3. Else return $\tilde{x}^{-1} \pmod p$

Fig. 2. A new DDH Group with an Easy DL Subgroup

3.2 The new protocol

The DDH group with an easy DL subgroup of Fig. 2 gives rise to a linearly homomorphic encryption scheme in quadratic fields, using the generic construction of Fig. 1. Compared to previous solutions based on a similar construction ([BCP03]), this scheme is only based on the difficulty of the discrete logarithm in G, and does not rely on the difficulty of factorization.

In practice, the best attack against the scheme consists in retrieving the private key, *i.e.*, in computing a discrete logarithm. As said in Appendix B.3, the problems of computing discrete logarithm in $C(\mathcal{O}_{\Delta_K})$ and computing $h(\mathcal{O}_{\Delta_K})$ have similar complexity. Given oracle for both problems, one can compute discrete logarithm in $C(\mathcal{O}_{\Delta_p})$ and

totally break the scheme. Indeed, if $s = h(\mathcal{O}_{\Delta_K})$, given g and $h = g^x$, we can compute $\bar{\varphi}_p(g)$ and $\bar{\varphi}_p(h) = \bar{\varphi}_p(g)^{x \bmod s}$. The oracle for discrete logarithm in $C(\mathcal{O}_{\Delta_K})$ gives $x \bmod s$. Furthermore, as shown in Lemma 1, if s is known the PDL problem is easy, so one can compute $x \bmod p$ and we get x as $\gcd(p, s) = 1$ with the Chinese remainder theorem. Moreover, finding $h(\mathcal{O}_{\Delta_K})$ or the multiplicative order of g can be sufficient: knowing $s = h(\mathcal{O}_{\Delta_K})$ breaks the PDL problem (cf. Lemma 1) and the one wayness of the scheme by Theorem 3.

4 Extensions

4.1 Removing the Condition on the Relative Size of p and q

To have a polynomial Solve algorithm, we impose that $q > 4p$, in order that the reduced elements of $\langle f \rangle$ are the ideals of norm p^2. If we want a large message space, for example 2048 bits (as for the cryptosystem of Paillier or the scheme of [BCP03] with a 2048 bit RSA integer), this means that p has 2048 bits, so $|\Delta_p| = p^3 q > 4p^4$ has more than 8194 bits and $|\Delta_K| = pq > 4p^2$ has more than 4098 bits. Therefore we loose our advantage over factoring based schemes, as we only need a discriminant Δ_K of 1348 bits to have the same security than a 2048 bit RSA integer (cf. Appendix B.3).

For example, suppose that we work with $\Delta_K = -p$. In the order $\mathcal{O}_{\Delta_p}$ of discriminant $\Delta_p = p^2 \Delta_K = -p^3$, the ideals of norm p^2 are no longer reduced. However, we can still have a polynomial time algorithm to solve the discrete logarithm in $\langle f \rangle$ where $f = [(p^2, p)]$. From the proof of Proposition 1, f still generate the subgroup of order p, and for $k \in \{1, \ldots, p-1\}$, the class f^k still contains a non reduced ideal $(p^2, L(k)p)$ where $L(k)$ is defined as in Proposition 1. We can use the main result of [CL09] constructively to find this non reduced ideal that will disclose the discrete logarithm k given the reduced element of the class f^k. The idea is to lift this reduced element in a class group of a suborder where the ideals of norm p^2 are reduced. Let $\Delta_{p^2} = p^4 \Delta_K$. For $p > 4$, we have $p^2 < \sqrt{|\Delta_{p^2}|}/2$ so the ideals of norm p^2 are reduced. We lift an element of $\mathcal{O}_{\Delta_p}$ in $\mathcal{O}_{\Delta_{p^2}}$ by computing $[\varphi_p^{-1}(\cdot)]^p$ on a representative ideal prime to p (we can use [HJPT98, Algorithm 1] to find an ideal prime to p in a given class). This map is injective, so applied on f we get a class f_ℓ of order p in $C(\mathcal{O}_{\Delta_{p^2}})$. Moreover, this class is in the kernel of the map $\bar{\varphi}_{p^2}$ from $C(\mathcal{O}_{\Delta_{p^2}})$ to $C(\mathcal{O}_{\Delta_K})$, and an easy generalization of Proposition 1 shows that the subgroup of $C(\mathcal{O}_{\Delta_{p^2}})$ generated by f_ℓ is also generated by $[(p^2, p)]$. As a result, if $h = f^x$ in $C(\mathcal{O}_{\Delta_p})$, we have $h_\ell = [\varphi_p^{-1}([h])]^p = ([\varphi_p^{-1}([f])]^p)^x = f_\ell^x$ and x can be computed as $x = y/z$ where y is the discrete logarithm of h_ℓ in basis $[(p^2, p)]$ and y is the discrete logarithm of f_ℓ in basis $[(p^2, p)]$. Both logarithms can be computed as in $C(\mathcal{O}_{\Delta_p})$.

This variant can also work with $\Delta_K = -pq$ and $q < 4p$, so p can be chosen independently from the security level, with the restriction that p must have at least 80 bits.

4.2 A Faster Variant

We can change the KeyGen algorithm as follows: g is now in the class group of the maximal order (*i. e.*, g is the class of $\mathfrak{r}^2$) and we set $h = g^x$ where x is the secret key and the computation is done in $C(\mathcal{O}_{\Delta_K})$. Let us denote by $\psi : C(\mathcal{O}_{\Delta_K}) \to C(\mathcal{O}_{\Delta_p})$ the injective morphism of Lemma 3, that computes $[\varphi_p^{-1}(\cdot)]^p$ on a representative ideal prime to p.

To encrypt $m \in \mathbf{Z}/p\mathbf{Z}$, we compute $c_1 = g^r$ and $c_2 = f^m\psi(h^r)$ in $C(\mathcal{O}_{\Delta_p})$. To decrypt, we first compute c_1^x and lift it, by computing $c_1' = \psi(c_1^x)$ in $C(\mathcal{O}_{\Delta_p})$. Then we retrieve $f^m = c_2/c_1'$. This variant can be viewed as a mix of an Elgamal cryptosystem in $C(\mathcal{O}_{\Delta_K})$ (lifted in $C(\mathcal{O}_{\Delta_p})$ by applying ψ) and of a cryptosystem based on the subgroup decomposition problem using the direct product between $\psi(\langle g\rangle)$ and $\langle f\rangle$. The advantage of this variant is that ciphertexts are smaller (c_1 is in $C(\mathcal{O}_{\Delta_K})$ instead of $C(\mathcal{O}_{\Delta_p})$) and that computations are faster: encryption performs two exponentiations in $C(\mathcal{O}_{\Delta_K})$ instead of $C(\mathcal{O}_{\Delta_p})$ and one lift (which computational cost is essentially the exponentiation to the power p). Decryption similarly involves one exponentiation in $C(\mathcal{O}_{\Delta_K})$ instead of $C(\mathcal{O}_{\Delta_p})$ and a lift. However, the semantic security is now based on a non standard problem. Let g be a generator of a subgroup of $C(\mathcal{O}_{\Delta_K})$ of order s. After having chosen m, the adversary is asked to distinguished the following distributions : $\{(g^x, g^y, \psi(g^{xy})), x, y \xleftarrow{\$} \mathbf{Z}/s\mathbf{Z}\}$ and $\{(g^x, g^y, \psi(g^{xy})f^m), x, y \xleftarrow{\$} \mathbf{Z}/s\mathbf{Z}\}$. The total break is equivalent to the DL problem in $C(\mathcal{O}_{\Delta_K})$.

5 Performances and Comparisons.

We now compare the efficiency of our cryptosystem with some other linearly homomorphic encryptions schemes, namely the system of Paillier and the one from [BCP03]. The security of the Paillier cryptosystem is based on the factorization problem of RSA integers, while [BCP03] is based on both the factorization and the DL problems. For our scheme, the best attack consists in computing DL in $C(\mathcal{O}_{\Delta_K})$ or in computing $h(\mathcal{O}_{\Delta_K})$ and both problems have similar complexity.

As said in Appendix B.3, in [BJS10], the Discrete Logarithm problem with a discriminant Δ_K of 1348 (resp. 1828 bits) is estimated as hard as factoring a 2048 (resp. 3072 bits) RSA integer n. In Fig. 1, we give the timings in ms of the time to perform an encryption and decryption for the three schemes. Concerning Paillier, for encryption and decryption, the main operation is an exponentiation of the form $x^k \mod n^2$ where k has the same bit length as n. Concerning [BCP03], which has an Elgamal structure, two exponentiations of the form $x^k \mod n^2$ with k an integer of the same bit length as n^2 are used for encryption and one for decryption. Our scheme has also this structure with two exponentiations for encryption and one for decryption. Decryption also involves an inversion modulo p. The exponentiations are made in $C(\mathcal{O}_{\Delta_p})$ with $\Delta_p = p^2\Delta_K$. The size of the exponent is bounded by Bp where we have seen that B can be chosen roughly of the bit size of $\sqrt{\Delta_K}$ plus 80 bits. For a same security level, our scheme is thus more efficient for a small p.

The timings where performed with Sage 6.3 on a standard laptop with a straightforward implementation. The exponentiation in class group uses a PARI/GP function (qfbnupow). We must stress that *this function is far less optimized than the exponentiation in* $\mathbf{Z}/n\mathbf{Z}$*, so there is a huge bias in favor of BCP and Paillier.* A more optimized implementation would give much better results for our system. Nevertheless, we see that for a 2048 bits modulus, our cryptosystem is already faster than the protocol from [BCP03]. Moreover, for stronger securities, our system will be faster, as asymptotically, the factorization algorithms have complexity $L(1/3, \cdot)$ whereas the algorithms for class groups of quadratic fields have complexity $L(1/2, \cdot)$. Moreover the multiplication modulo n and the composition of quadratic forms have both quasi linear complexity [Sch91]. As shown in Table 1, already with a 3072 bits modulus our cryptosystem is competitive: faster than Paillier for decryption. For a very high security level (7680 bits modulus), our system would be twice as fast as Paillier for encryption, for messages of 512 bits. We also give timings of our faster variant of Subsection 4.2. For a same security level, this variant becomes more interesting when the message space grows. In Table 1, we see that even with a naive implementation, our system is competitive for message space up to 256 bits (resp. 912 bits) for 2048 bits security (resp. for 3072 bits security).

Note that a medium size message space can be sufficient for applications. For example, our system may be used as in [CGS97] to design a voting scheme. For a yes/no pool, a voter encrypts 0 (resp. 1) to vote no (resp. to vote yes). By combining all the ciphertexts, the election manager would get an encryption of the sum of the vote modulo p. Decryption allows to decide the result if the number of voters ℓ satisfies $\ell < p$. So a 80-bit p is largely sufficient as $2^{80} \approx 10^{24}$. With Elgamal, in [CGS97], the discrete logarithm in decryption involves a baby-step giant-step computation of time $\mathcal{O}(\sqrt{\ell})$ (so a very low number of voters can be handled) whereas a single inversion modulo p is needed for our scheme. For a multi-candidate election system with m candidates and ℓ voters, one votes for the i^{th} candidate by encrypting ℓ^i. The tally is decrypted with a decomposition in base ℓ, so we must have $\ell^m < p$. With a 256 bit integer p, we can have for example 2^{16} voters and 16 candidates, which is the good order of magnitude for real life elections, for which there are around a thousand registered voters by polling stations.

6 Conclusion

We proposed the first linearly homomorphic encryption whose security relies on a sole Diffie-Hellman-like assumption. Our construction crucially uses the algebraic properties of the class group of a non maximal order of an imaginary quadratic field. They make it possible to avoid the factorization assumption and to have $\mathbf{Z}/p\mathbf{Z}$ as the set of messages. Other improvements than those we presented are possible: we can gain efficiency using the Chinese Remainder Theorem using discriminant of the form $\Delta_K = -(\prod_{i=1}^{n} p_i)q$, and generalizing *à la* Damgård and Jurik (cf. [DJ01]), with discriminants of the form $\Delta_{p^t} = p^{2t}\Delta_K$, with $\Delta_K = -pq$ and $t \geqslant 1$ to enlarge the message space to $\mathbf{Z}/p^t\mathbf{Z}$ without losing the homomorphic property. A non-trivial adaptation may also be possible with

Cryptosystem	Parameter	Message Space	Encryption (ms)	Decryption (ms)
Paillier	2048 bits modulus	2048 bits	**28**	**28**
BCP03	2048 bits modulus	2048 bits	107	54
New Proposal	1348 bits Δ_K	80 bits	93	49
Variant Subsec. 4.2	1348 bits Δ_K	80 bits	82	45
Variant Subsec. 4.2	1348 bits Δ_K	256 bits	105	68
Paillier	3072 bits modulus	3072 bits	**109**	109
BCP03	3072 bits modulus	3072 bits	427	214
New Proposal	1828 bits Δ_K	80 bits	179	91
Variant Subsec. 4.2	1828 bits Δ_K	80 bits	145	**78**
Variant Subsec. 4.2	1828 bits Δ_K	512 bits	226	159
Variant Subsec. 4.2	1828 bits Δ_K	912 bits	340	271

Table 1. Efficiency Comparison of Linearly Homomorphic Encryption Schemes

real quadratic fields. Experiments show that our protocol is competitive with existing ones.

Acknowledgement: This work has been supported in part by ERC Starting Grant ERC-2013-StG-335086-LATTAC and by the financial support from the French State, managed by the French National Research Agency (ANR) in the frame of the "Investments for the future" Programme IdEx Bordeaux (ANR-10-IDEX-03-02), Cluster of excellence CPU.

References

[BCP03] E. Bresson, D. Catalano and D. Pointcheval. *A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications*. Proc. of Asiacrypt'03, Springer LNCS Vol. 2894, 37–54 (2003)

[BDW90] J. Buchmann, S. Düllmann and H. C. Williams. *On the Complexity and Efficiency of a New Key Exchange System*. Proc. of Eurocrypt'89, Springer LNCS Vol. 434, 597–616 (1990)

[Ben88] J. C. Benaloh. *Verifiable Secret-Ballot Elections*. PhD thesis, Yale University (1988)

[BGN05] D. Boneh, E.-J. Goh and K. Nissim. *Evaluating 2-DNF Formulas on Ciphertexts*. Proc. of TCC'05, Springer LNCS Vol. 3378, 325–341 (2005)

[BH01] J. Buchmann and S. Hamdy. *A survey on IQ-cryptography*, Public-Key Cryptography and Computational Number Theory, de Gruyter, Berlin, 1–15, (2001)

[BJS10] J.-F. Biasse, M. J. Jacobson Jr. and A. K. Silvester. *Security Estimates for Quadratic Field Based Cryptosystems*. Proc. of ACISP'10, Springer LNCS Vol. 6168, 233–247 (2010)

[Bre00] R. P. Brent. *Public Key Cryptography with a Group of Unknown Order*. Technical Report, Oxford University (2000)

[BTW95] J. Buchmann, C. Thiel and H. C. Williams. *Short Representation of Quadratic Integers*. Proc. of CANT'92, Math. Appl. 325, Kluwer Academic Press, 159–185 (1995)

[BV07] J. Buchmann and U. Vollmer. *Binary Quadratic Forms. An Algorithmic Approach*. Springer (2007)

[BV14] Z. Brakerski and V. Vaikuntanathan. *Efficient Fully Homomorphic Encryption from (Standard) LWE*, SIAM J. Comput., 43(2), 831–871 (2014)

[BW88] J. Buchmann and H. C. Williams. *A Key-Exchange System Based on Imaginary Quadratic Fields.* J. Cryptology, 1(2), 107–118 (1988)

[CC07] G. Castagnos, B. Chevallier-Mames. *Towards a DL-based Additively Homomorphic Encryption Scheme.* Proc. of ISC 2007, Springer LNCS Vol. 4779, 362–375 (2007)

[CF14] D. Catalano and D. Fiore. *Boosting Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data.* Cryptology ePrint Archive, report 2014/813, http://eprint.iacr.org/2014/813 (2014)

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. In *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118. Springer-Verlag, 1997.

[CJLN09] G. Castagnos, A. Joux, F.Laguillaumie and P. Q. Nguyen. *Factoring pq^2 with Quadratic Forms: Nice Cryptanalyses.* Proc. of Asiacrypt'09, Springer LNCS Vol. 5912, 469–486 (2009)

[CL09] G. Castagnos and F. Laguillaumie. *On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis.* Proc. of Eurocrypt'09, Springer LNCS Vol. 5479, 260–277 (2009)

[CL12] G. Castagnos and F. Laguillaumie. *Homomorphic Encryption for Multiplications and Pairing Evaluation.* Proc. of SCN 2012, Springer LNCS Vol. 7485, 374–392 (2012)

[CPP06] B. Chevallier-Mames, P. Paillier, D. Pointcheval. *Encoding-free Elgamal Encryption without Random Oracles.* Proc. of PKC 2006, Springer LNCS Vol. 3958, 91–104 (2006)

[CHN99] J.-S. Coron, H. Handschuh and D. Naccache. *ECC: Do We Need to Count?* Proc. of Asiacrypt 1999, Springer LNCS Vol. 1716, 122–134 (1999)

[Coh00] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer (2000).

[Cox99] D. A. Cox. *Primes of the form $x^2 + ny^2$.* John Wiley & Sons (1999)

[DF02] I. Damgård and E. Fujisaki. *A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order.* Proc. of Asiacrypt'02, Springer LNCS Vol. 2501, 125–142 (2002)

[DJ01] I. Damgård and M. J. Jurik. *A Generalisation, a Simplification and some Applications of Paillier's Probabilistic Public-Key System*, Proc. of PKC' 01, Springer LNCS Vol. 1992, 119–136 (2001)

[Gal02] S. D. Galbraith. *Elliptic Curve Paillier Schemes.* J. Cryptology, Vol. 15(2), 129–138 (2002)

[Gen09] C. Gentry. *Fully homomorphic encryption using ideal lattices.* Proc. of STOC 2009, ACM, 169–178 (2009)

[GM84] S. Goldwasser and S. Micali. *Probabilistic Encryption.* JCSS, Vol. 28(2), 270–299 (1984)

[HJPT98] D. Hühnlein, M. Jacobson, Jr., S. Paulus and T. Takagi. *A Cryptosystem Based on Non-Maximal Imaginary Quadratic Orders with Fast Decryption.* Proc. of Eurocrypt'98, Springer LNCS Vol. 1403, 294–307 (1998)

[HM00] S. Hamdy and B. Möller. *Security of Cryptosystems Based on Class Groups of Imaginary Quadratic Orders.* Proc. of Asiacrypt'00, Springer LNCS Vol. 1976, 234–247 (2000)

[HPT99] M. Hartmann, S. Paulus and T. Takagi. *NICE - New Ideal Coset Encryption.* Proc. of CHES'99, Springer LNCS Vol. 1717, 328–339 (1999)

[Jac00] M. J. Jacobson Jr. *Computing discrete logarithms in quadratic orders.* J. Cryptology, Vol. 13, 473–492 (2000)

[Jac04] M. J. Jacobson Jr. *The Security of Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders*, Proc. of ACISP'04, Springer LNCS Vol. 3108, 149–156 (2004)

[JJ00] É. Jaulmes and A. Joux. *A NICE Cryptanalysis.* Proc. of Eurocrypt'00, Springer LNCS Vol. 1807, 382–391 (2000)

[JL13] M. Joye and B. Libert. *Efficient Cryptosystems from 2^k-th Power Residue Symbols*, Proc. of Eurocrypt 2013, Springer LNCS Vol. 7881, 76–92 (2013)

[JSW08] M. J. Jacobson Jr., R. Scheidler and D. Weimer. *An Adaptation of the NICE Cryptosystem to Real Quadratic Orders.* Proc. of Africacrypt'08, Springer LNCS Vol. 5023, 191–208 (2008)

[Kap78] P. Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique.* J. Math. Soc. Japan, 25(4), 547–733 (1976)

[KM03] H. Kim and S. Moon. *Public-key cryptosystems based on class semigroups of imaginary quadratic non-maximal orders*, Proc. of ACISP'03, Springer LNCS Vol. 2727, 488–497 (2003)

[NS98] D. Naccache and J. Stern. *A New Public Key Cryptosystem Based on Higher Residues.* Proc. of ACM CCS'98, 546–560 (1998)

[OU98] T. Okamoto and S. Uchiyama. *A New Public-Key Cryptosystem as Secure as Factoring.* Proc. of Eurocrypt'98, Springer LNCS Vol. 1403, 308–318 (1998)

[Pai99] P. Paillier. *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes.* Proc. of Eurocrypt'99, Springer LNCS Vol. 1592, 223–238 (1999)

[PT00] S. Paulus and T. Takagi. *A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time.* J. Cryptology, 13(2), 263–272 (2000)

[SP05] D. Schielzeth and M. E. Pohst. *On Real Quadratic Number Fields Suitable for Cryptography.* Experiment. Math. 14(2), 189–197 (2005)

[Sch91] A. Schönhage. *Fast reduction and composition of binary quadratic forms.* Proc. of ISSAC'91, ACM, 128–133 (1991)

[W+11] L. Wang, L. Wang, Y. Pan, Z. Zhang, Y. Yang. *Discrete Logarithm Based Additively Homomorphic Encryption and Secure Data Aggregation.* Information Sciences, Vol. 181(16), 3308–3322 (2011)

A Public-key Encryption: Definitions

Encryption Scheme: Definition. Let λ be an integer. An encryption scheme is a tuple of algorithms $\Pi = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$. The probabilistic polynomial-time key generation algorithm KeyGen takes a security parameter λ in unary as input and returns a pair (pk, sk) of public key and the matching secret key. The probabilistic polynomial-time encryption algorithm $\mathsf{Encrypt}$ takes a security parameter, a public key pk and a message m as inputs, and outputs a ciphertext c. The deterministic polynomial-time $\mathsf{Decrypt}$ decryption algorithm takes a security parameter, a secret key sk and a ciphertext c and returns either a message m or the symbol $\perp$ which indicates the invalidity of the ciphertext. The scheme must be *correct*, which means that for all security parameters λ, and for all messages m, if $(pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$ then $\mathsf{Decrypt}(1^\lambda, sk, \mathsf{Encrypt}(1^\lambda, pk, m)) = m$ with probability (taken on all internal random coins and random choices).

Encryption Scheme: Security. The *total break* of an encryption scheme is declared if an attacker can recover the secret key from (at least) the public key. Therefore any probabilistic polynomial-time Turing machine $\mathcal{B}$ must have a success in recovering the public key arbitrarily small, where the *success* is defined, for an integer λ, as the probability $\Pr\left[(pk, sk) \leftarrow \Pi.\mathsf{KeyGen}(1^\lambda) : \mathcal{B}(pk) = sk\right]$.

The intuitive security notion expected from an encryption scheme is the *one-wayness*, which means that, given only the public data, an adversary cannot recover the message corresponding to a given ciphertext. More precisely, any probabilistic polynomial-time Turing machine $\mathcal{A}$ (the *attacker*) has a success in inverting the encryption algorithm arbitrarily small, where the *success* is defined, for an integer λ, as the probability $\Pr\left[(pk, sk) \leftarrow \Pi.\mathsf{KeyGen}(1^\lambda) : \mathcal{A}(pk, \Pi.\mathsf{Encrypt}(1^\lambda, sk, m)) = m\right]$.

The previous definition supposes that the attacker has no more information that the public key : the attacker is said to do a *chosen-plaintext attack* (since he can produce the ciphertext of message of his choice). If he has access to a decryption oracle, the attack is said be a *chosen-ciphertext attack*.

An encryption scheme must indeed reach a stronger notion of security : it must have *semantic security* (aka *indistinguishability*). This means that an attacker is computationally unable to distinguish between two messages, chosen by himself, which one has been encrypted, with a probability significantly better than one half. The *indistinguishability game* is formally defined as:

$$\boxed{\text{Experiment } \mathbf{Exp}_{\Pi}^{\mathsf{ind\text{-}atk}}(\mathcal{A})}$$
$(pk, sk) \leftarrow \Pi.\mathsf{KeyGen}(1^\lambda)$
$(m_0, m_1, s) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$b^\star \xleftarrow{\$} \{0,1\}$
$c^\star \leftarrow \Pi.\mathsf{Encrypt}(pk, m_{b^\star})$
$b \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(s, c^\star)$
Return 1 if $b = b^\star$ and 0 otherwise

with

- $\mathsf{atk} = \mathsf{cpa}$ and
  - $\mathcal{O}_1 = \emptyset$
  - $\mathcal{O}_2 = \emptyset$
- $\mathsf{atk} = \mathsf{cca1}$ and
  - $\mathcal{O}_1 = \Pi.\mathsf{Decrypt}(\mathsf{params}, sk, \cdot)$
  - $\mathcal{O}_2 = \emptyset$
- $\mathsf{atk} = \mathsf{cca2}$ and
  - $\mathcal{O}_1 = \Pi.\mathsf{Decrypt}(\mathsf{params}, sk, \cdot)$
  - $\mathcal{O}_2 = \Pi.\mathsf{Decrypt}(\mathsf{params}, sk, \cdot)$

where the adversary $\mathcal{A}$ is modelled as a 2-stage PPTM $(\mathcal{A}_1, \mathcal{A}_2)$. The *advantage* of the attacker is then defined as

$$\mathsf{Adv}_{\Pi}^{\mathsf{ind\text{-}atk}}(\mathcal{A}) = \left| \Pr\left(\mathbf{Exp}_{\Pi}^{\mathsf{ind\text{-}atk}}(\mathcal{A}) = 1\right) - \frac{1}{2} \right|.$$

Linearly Homomorphic Encryption Let suppose that the set of plaintexts $\mathcal{M}$ (resp. the set of ciphertexts $\mathcal{C}$) is equipped with an additive (resp. a multiplicative) group structure. An encryption scheme Π is said to be *homomorphic* if $\forall \lambda \in \mathbf{N}$, $\forall (pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$, $\forall m_1, m_2 \in \mathcal{M}$, if $c_1 \leftarrow \mathsf{Encrypt}(pk, m_1)$ and $c_2 \leftarrow \mathsf{Encrypt}(pk, m_2)$, then the product $c_1 c_2$ is a valid encryption of $m_1 + m_2$. The exponentiation of a ciphertext c_1 to a power α is as well a valid encryption of αm_1. The formal definition of a linearly homomorphic encryption includes two algorithms $\mathsf{EvalSum}$ and $\mathsf{EvalScal}$ that fulfills the corresponding correctness property.

Of course, to achieve semantic security $\Pi.\mathsf{Encrypt}$ has to be probabilistic, but even though, the highest level of indistinguishability an homomorphic encryption scheme can achieve is indeed $\mathsf{ind} - \mathsf{cca1}$. As a matter of fact, an attacker will always win the $\mathsf{cca2}$ game by querying, in the second phase, for instance $c^\star \cdot \mathsf{Encrypt}(pk, 0)$ to the decryption oracle: this one will answer with $m_{b^\star} + 0 = m_{b^\star}$.

B Background on Imaginary Quadratic Fields

B.1 Imaginary Quadratic Fields and Class Group

Let $D < 0$ be a squarefree integer and consider the quadratic imaginary field $K = \mathbf{Q}(\sqrt{D})$. The *fundamental discriminant* Δ_K of K is defined as $\Delta_K = D$ if $D \equiv 1 \pmod 4$ and $\Delta_K = 4D$ otherwise. An *order* $\mathcal{O}$ in K is a subset of K such that $\mathcal{O}$ is a subring of K containing 1 and $\mathcal{O}$ is a free $\mathbf{Z}$-module of rank 2. The ring $\mathcal{O}_{\Delta_K}$ of algebraic integers in K is the *maximal* order of K. It can be written as $\mathbf{Z} + \omega_K \mathbf{Z}$, where $\omega_K = \frac{1}{2}(\Delta_K + \sqrt{\Delta_K})$. If we set $f = [\mathcal{O}_{\Delta_K} : \mathcal{O}]$ the *finite* index of any order $\mathcal{O}$ in $\mathcal{O}_{\Delta_K}$,

then $\mathcal{O} = \mathbf{Z} + f\omega_K\mathbf{Z}$. The integer f is called the *conductor* of $\mathcal{O}$. The discriminant of $\mathcal{O}$ is then $\Delta_f = f^2\Delta_K$. Now, let $\mathcal{O}_\Delta$ be an order of discriminant Δ and $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_\Delta$, its norm is $\mathrm{N}(\mathfrak{a}) = |\mathcal{O}_\Delta/\mathfrak{a}|$. A *fractional* ideal is a subset $\mathfrak{a} \subset K$ such that $d\mathfrak{a}$ is an ideal of $\mathcal{O}_\Delta$ for $d \in \mathbf{N}$. A fractional ideal $\mathfrak{a}$ is said to be *invertible* if there exists an another fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}_\Delta$. The *ideal class group* of $\mathcal{O}_\Delta$ is $C(\mathcal{O}_\Delta) = I(\mathcal{O}_\Delta)/P(\mathcal{O}_\Delta)$, where $I(\mathcal{O}_\Delta)$ is the group of invertible fractional ideals of $\mathcal{O}_\Delta$ and $P(\mathcal{O}_\Delta)$ the subgroup consisting of principal ideals. Its cardinality is the *class number* of $\mathcal{O}_\Delta$ denoted by $h(\mathcal{O}_\Delta)$. The group $\mathcal{O}_\Delta^\star$ of units in $\mathcal{O}_\Delta$ is equal to $\{\pm 1\}$ for all $\Delta < 0$, except when Δ is equal to -3 and -4 ($\mathcal{O}_{-3}^\star$ and $\mathcal{O}_{-4}^\star$ are respectively the group of sixth and fourth roots of unity)

A nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$, $\mathfrak{a}$ is said to be *prime to* f if $\mathfrak{a} + f\mathcal{O}_\Delta = \mathcal{O}_\Delta$. We denote by $I(\mathcal{O}_\Delta, f)$ the subgroup of $I(\mathcal{O}_\Delta)$ of ideals prime to f. The map $\varphi_f : I(\mathcal{O}_{\Delta_f}, f) \to I(\mathcal{O}_{\Delta_K}, f)$, $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_K}$ is an isomorphism. This map induces a surjection $\bar{\varphi}_f : C(\mathcal{O}_{\Delta_f}) \twoheadrightarrow C(\mathcal{O}_{\Delta_K})$. In our settings, we will use a prime conductor $f = p$ and consider $\Delta_p = p^2\Delta_K$, for a fundamental discriminant Δ_K divisible by p. The order of the kernel of $\bar{\varphi}_p$ is then given by the classical *analytic class number formula* (see for instance [BV07]): $\frac{h(\mathcal{O}_{\Delta_p})}{h(\mathcal{O}_{\Delta_K})} = p$ if $\Delta_K < -4$.

B.2 Representation of the Classes

Working with ideals modulo the equivalence relation of the class group is essentially equivalent to work with binary quadratic forms modulo $\mathsf{SL}_2(\mathbf{Z})$ (cf. Section 5.2 of [Coh00]). Every (primitive) ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ can be written as $\mathfrak{a} = \left(a\mathbf{Z} + \frac{-b+\sqrt{\Delta}}{2}\mathbf{Z}\right)$ with $a \in \mathbf{N}$ and $b \in \mathbf{Z}$ such that $b^2 \equiv \Delta \pmod{4a}$, and denoted by (a, b) for short. The norm of such an ideal is then a. This notation also represents the binary quadratic form $ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta$. This representation of the ideal is unique if the form is normal: $-a < b \leqslant a$.

An ideal is reduced if it is normal, and $a \leqslant c$, and $b \geqslant 0$ for $a = c$. Note that in every class of $\mathcal{O}_\Delta$-ideals there exists exactly one reduced ideal. We note $\mathsf{Red}(\mathfrak{a})$ the unique reduced ideal equivalent to an ideal $\mathfrak{a}$, or $\mathsf{Red}([\mathfrak{a}])$ the unique reduced ideal in the class $[\mathfrak{a}]$. From the theory of quadratic forms, we can efficiently compute $\mathsf{Red}(\mathfrak{a})$ given $\mathfrak{a}$. The algorithm, which is due to Gauss, is described in [Coh00, Algorithm 5.4.2 p. 243] and is called Red in this paper. In general, instead of working with classes, we will work with reduced ideals. The product of ideals is also efficiently computable with the composition of quadratic forms algorithm, see [Coh00, Algorithm 5.4.7 p. 243]. These two algorithms have quadratic complexity (and even quasi linear using fast arithmetic).

A crucial fact for our purpose is described in [Coh00, Lemma 5.3.4] and [BV07, Lemma 6.5.1]: a normal ideal $\mathfrak{a} = (a, b)$ with $|a| < \sqrt{|\Delta|}/2$ is reduced.

B.3 Class Number Computation and DL Problem

In 2000, Jacobson has described an index-calculus method to solve the discrete logarithm problem in class group of imaginary quadratic field of discriminant Δ_K [Jac00]. Various

improvements have been proposed to this algorithm: In [BJS10], it is conjecture that a state of the art implementation has conjectured complexity $L_{|\Delta_K|}[1/2, o(1)]$. Moreover, the best known algorithm to compute class numbers of fundamental discriminant are again index-calculus method with the same complexity.

In [HM00], Hamdy and Möller discuss the selection of a discriminant Δ_K such that the discrete logarithm problem in $C(\mathcal{O}_{\Delta_K})$ is as hard as in finite fields: It is advised to construct a fundamental discriminant Δ_K and to minimize to 2-Sylow subgroup of the class group. In our case, by construction Δ_K will be the product of two odd primes. If we take $\Delta_K = -pq$ with p and q such that $p \equiv -q \pmod 4$ then Δ_K is a fundamental discriminant. Moreover the 2-Sylow subgroup will be isomorphic to $\mathbf{Z}/2\mathbf{Z}$ if we choose p and q such that $(p/q) = (q/p) = -1$ (cf. [Kap78, p. 598]). In that case, we will work with the odd part, which is the group of squares of $C(\mathcal{O}_{\Delta_K})$.

Following the Cohen-Lenstra heuristics, cf. [Coh00, Chapter 5.10.1], the probability that the odd part of the class group is cyclic is 97.757% and the probability that an odd prime r divides $h(\mathcal{O}_{\Delta_K})$ is approximately $1/r + 1/r^2$. As a result, we can not guarantee that the order of the odd part is not divisible by small primes. Nevertheless, as indicated in [HM00], this does not lead to a weakness on the discrete logarithm problem, as there is no efficient algorithm to compute $h(\mathcal{O}_{\Delta_K})$ or odd multiples or factors of $h(\mathcal{O}_{\Delta_K})$, hence an adaptation of the Pohlig-Hellman Algorithm is not possible.

On average, $h(\mathcal{O}_{\Delta_K})$ is in the order of $\sqrt{|\Delta_K|}$, see [Coh00, Theorem 4.9.15 (Brauer-Siegel)]. Moreover (cf. [Coh00, p. 295]),

$$h(\Delta_K) < \frac{1}{\pi} \log |\Delta_K| \sqrt{|\Delta_K|}. \tag{1}$$

To conclude, following [HM00], if Δ_K is taken large enough, generic methods to compute discrete logarithm such as Pollard $\lambda-$method are slower than the index-calculus algorithms. Thus, since index-calculus algorithms for solving the discrete logarithm problem are asymptotically much slower than index-calculus algorithms to solve the integer factorization problem, the discriminant can be taken smaller than RSA modulus. In [BJS10], the discrete logarithm problem with a discriminant of 1348 bits (resp. 1828 bits) is estimated as hard as factoring a 2048 bits (resp. 3072 bits) RSA integer.

B.4 Elgamal Cryptosystem Adaptations in Class Group

In [BW88], Buchmann and Williams proposed an adaptation of the Diffie-Hellman key exchange in imaginary quadratic fields and briefly described an adaptation of the Elgamal cryptosystem in the same setting. Efficient implementations of these cryptosystems are discussed in [BDW90,SP05,BH01] and [BV07]. At a high level, the key generation process of these adaptations of Elgamal can be sketched as follows:

- Generate Δ_K a fundamental negative discriminant, such that $|\Delta_K|$ is large enough to thwart the computation of discrete logarithm (cf. previous subsection) ;
- choose g a class of $C(\mathcal{O}_{\Delta_K})$ of even order (from the discussion of the previous subsection, the order of g will be close to $h(\Delta_K) \approx \sqrt{|\Delta_K|}$ with high probability) ;

– the private key is $x \xleftarrow{\$} \{0, \ldots, \lfloor\sqrt{|\Delta_K|}\rfloor\}$ and the public key is (g, h), where $h = g^x$.

To implement Elgamal, it remains the problem of the embedding of a message. In [BW88], an integer m is encrypted as $(g^r, m + N(h^r))$ where $N(h^r)$ denotes the norm of the reduced ideal of the class h^r. As a result, the scheme is not based on the traditional DDH assumption.

Another solution is given in [SP05, Section 2]. An integer message $m \leq \sqrt{|\Delta|}/2$ is mapped to the class M of an ideal above p where p is the first prime with $p > m$ such that Δ is a quadratic residue modulo p. If $d = m - p$, the message m is encrypted as (g^r, Mh^r, d): The distance d seems to be public, in order to recover m from M. This can be a problem for semantic security: the first stage adversary can choose two messages m_0, m_1 such that $d_0 \neq d_1$ and easily win the indistinguishability game with probability one by recognizing the message thanks to the distance.

In [BH01], a "hashed" version is used, a bit-string m is encrypted as $(g^r, m \oplus H(h^r))$ where H is a cryptographic hash function. In [BV07], an adaptation of DHIES is described.

An variant of the Elgamal cryptosystem in a non maximal order of discriminant $\Delta_q = q^2\Delta_K$ is presented in [HJPT98]. A traditional setup of Elgamal is done in $C(\mathcal{O}_{\Delta_q})$, $h = g^x$. A ciphertext is (g^r, mh^r) in $C(\mathcal{O}_{\Delta_q})$ where m is an ideal of norm smaller than $\sqrt{\Delta_K}/2$. To decrypt, the ciphertext is moved in the maximal order with the trapdoor q where a traditional decryption is made to recover the message in $C(\mathcal{O}_{\Delta_K})$. Eventually, the message is lifted back in $C(\mathcal{O}_{\Delta_q})$. This variant can be seen as an Elgamal with a CRT decryption procedure: its advantage is that most of the decryption computation is done in $C(\mathcal{O}_{\Delta_K})$ and Δ_K can be chosen relatively small (big enough such the factorization of Δ_q is intractable, the discrete logarithm problem can be easy in $C(\mathcal{O}_{\Delta_K})$). The problem of the embedding of the plaintext in an ideal is not addressed in this paper. A chosen-ciphertext attack against this cryptosystem has been proposed in [JJ00].

In [KM03], an adaptation of the Diffie-Hellman key exchange and of the Elgamal cryptosystem are given using class semigroup of an imaginary non-maximal quadratic order. Unfortunately a cryptanalysis of this proposal has been presented in [Jac04].

A final important remark on the adaptation of the Elgamal cryptosystem is that it is necessary to work in the group of squares, *i. e.*, the *principal genus*. We didn't find this remark in previous works: in the whole class group, the DDH problem is easy. Indeed, it is well known that in $(\mathbf{Z}/p\mathbf{Z})^\times$, one can compute Legendre symbols and defeats the DDH assumption. As a consequence, it is necessary to work in the group of squares. In a class group, for example if the discriminant $\Delta = -\prod_{i=1}^{k} p_i$ is odd and the p_i are distinct primes numbers, we can associate to a class the value of the generic characters, the Legendre symbols (r, p_i) for i from 1 to k where r is an integer represented by the class (see [Cox99] for details on genus theory). It is easy to see that the previous attack in $(\mathbf{Z}/p\mathbf{Z})^\times$ can be adapted in class groups with the computation of the generic characters. As a result, it is necessary to work in the group of squares, which is the principal genus (cf. [Cox99, Theorem 3.15]), *i. e.*, the set of classes such that the generic characters all equal 1.

C Uniform Sampling in a Cyclic Group

Let us first recall some well known facts on the statistical distance of two discrete random variables.

Let X and Y two discrete random variables with values in Ω. The statistical distance between X and Y is defined as $\Delta(X,Y) = \sup_{A\subseteq\Omega} |\Pr[X \in A] - \Pr[Y \in A]|$.

Note that $\Pr[X \in \bar{A}] - \Pr[Y \in \bar{A}] = 1 - \Pr[X \in A] - 1 + \Pr[Y \in A] = \Pr[Y \in A] - \Pr[X \in A]$. So we can restrict to subsets A such that the difference is positive. Moreover, in order to maximize the difference, we can let $A = \{\omega \in \Omega, \Pr[X = \omega] > \Pr[Y = \omega]\}$. So

$$\Delta(X,Y) = \sum_{\omega\in A} \Pr[X = \omega] - \Pr[Y = \omega].$$

Now as

$$\Delta(X,Y) = \Delta(Y,X) = \Pr[Y \in \bar{A}] - \Pr[X \in \bar{A}] = \sum_{\omega\in\bar{A}} \Pr[Y = \omega] - \Pr[X = \omega],$$

we have

$$2\Delta(X,Y) = \sum_{\omega\in\Omega} |\Pr[X = \omega] - \Pr[Y = \omega]|, \text{ so } \Delta(X,Y) = \frac{1}{2}\sum_{\omega\in\Omega} |\Pr[X = \omega] - \Pr[Y = \omega]|.$$

Lemma 4. *Let G be a cyclic group of order n, generated by g. Consider the random variable X with values in G with uniform distribution: $\Pr[X = h] = \frac{1}{n}$ for all h in G, and Y the random variable with values in G defined as follows. Draw y in $\{0,\ldots,B-1\}$ from the uniform distribution with $B \geqslant n$, and $Y = g^y$. Let $r = B \mod n$. Then, $\Delta(X,Y) = \frac{r(n-r)}{nB} \leqslant \frac{n}{4B}$.*

Proof. Let X' the random variable with values in $\{0,\ldots,n-1\}$ with uniform distribution and Y' defined by $Y' = (y \mod n)$ where y is drawn in $\{0,\ldots,B-1\}$ with uniform distribution. Clearly, $\Delta(X,Y) = \Delta(X',Y')$. Let $B = qn + r$ with $0 \leqslant r < n$ be the euclidean division of B by n. For $c \in \{0,\ldots,r-1\}$, $\Pr[Y' = c] = (q+1)/B > \frac{1}{n}$ as $(q+1)n > B$. For $c \in \{r,\ldots,n-1\}$, $\Pr[Y' = c] = q/B \leqslant 1/n$. So for $A = \{0,\ldots,r-1\}$, we have

$$\Delta(X,Y) = \Delta(X',Y') = \sum_{c\in A} \Pr[Y' = c] - \Pr[X' = c] = r\left(\frac{q+1}{B} - \frac{1}{n}\right).$$

Using the fact that $q = \frac{B-r}{n}$, this simplifies to $\Delta(X,Y) = \frac{r(n-r)}{nB}$. Moreover as $r(n-r) \leqslant n^2/4$,

$$\Delta(X,Y) \leqslant \frac{n}{4B}.$$

□