On the rough order assumption in imaginary quadratic number fields

Antonio Sanso

Ethereum Foundation

Abstract. In this paper, we investigate the rough order assumption (RO_C) introduced by Braun, Damgård, and Orlandi at CRYPTO 23, which posits that class groups of imaginary quadratic fields with no small prime factors in their order are computationally indistinguishable from general class groups. We present a novel attack that challenges the validity of this assumption by leveraging properties of Mordell curves over the rational numbers. Specifically, we demonstrate that if the rank of the Mordell curve E_{-16D} is at least 2, it contradicts the rough order assumption. Our attack deterministically breaks the RO_C assumption for discriminants of a special form, assuming the parity conjecture holds and certain conditions are met. Additionally, for both special and generic cases, our results suggest that the presence of nontrivial 3-torsion elements in class groups can undermine the RO_C assumption. Although our findings are concrete for specific cases, the generic scenario relies on heuristic arguments related to the Birch and Swinnerton-Dyer (BSD) conjecture, a significant and widely believed conjecture in number theory. Attacks against 2-torsion elements in class groups are already well known, but our work introduces a distinct approach targeting 3-torsion elements. These attacks are fundamentally different in nature, and both have relatively straightforward countermeasures, though they do not generalize to higher torsions. While these results do not entirely invalidate the RO_C assumption, they highlight the need for further exploration of its underlying assumptions, especially in the context of specific torsion structures within class groups.

1 Introduction

Cryptography based on class groups of imaginary quadratic orders (IQ cryptography, IQC) is a fascinating area pioneered by Buchmann and Williams in their seminal work [8]. Initially, IQC did not find immediate real-world applications, leading to a period of limited exploration. However, this changed when Lipmaa proposed utilizing the unknown order property of class groups of imaginary quadratic fields to construct secure accumulators without a trusted setup [25]. Recently, the unknown order property has gained prominence as a foundation for various cryptographic primitives, including Verifiable Delay Functions (VDF) [34,30], cryptographic accumulators [4], vector commitments tailored for blockchain applications, and polynomial commitments used in zero-knowledge proofs [9].

Alongside the primary exploration of *maximal orders* in cryptography, significant progress has also been made in analyzing cryptographic schemes based on *non-maximal orders*. For instance, at EUROCRYPT 2009, Castagnos and Laguillaumie [14] achieved a major breakthrough by presenting a polynomial-time chosen-plaintext total break of the NICE family of cryptosystems [24,28,29]. This work not only marked a significant advancement in the field but also introduced a constructive technique that influenced subsequent research. Continuing their innovative contributions, Castagnos and Laguillaumie introduced a novel linearly homomorphic encryption scheme in CT-RSA 2015 [15], operating within the class group of a *non-maximal order of an imaginary quadratic field*. Further advancing this research, at ASIACRYPT 2018, Castagnos, Laguillaumie, and Tucker addressed practical challenges in secure inner product functional encryption modulo p, exploring schemes based on standard assumptions like DDH and Learning with Errors (LWE) [16]. In CRYPTO 2019, Castagnos, Catalano, Laguillaumie, Savasta, and Tucker focused on distributed variants of the ECDSA digital signature standard, introducing a method for achieving simulation-based security without relying on non-standard interactive assumptions [12,13]. Finally, in CRYPTO 2022, Abram, Damgård, Orlandi, and Scholl presented a group-theoretic framework for secure computation tools, unifying approaches based on number-theoretic assumptions such as DDH, Decision Composite Residuosity (DCR), and Quadratic Residuosity (QR) [1].

In this paper, we study the *rough order assumption* (RO_C) introduced by Braun, Damgård, and Orlandi [6]. This assumption has been utilized in subsequent works [5,11], which assert that class groups with no small prime factors in their order are hard to distinguish from general class groups.

Our Contribution In this paper, we make the following contributions to the study of cryptographic schemes based on imaginary quadratic fields and the rough order assumption (RO_C):

- We introduce a novel attack on the RO_C assumption. Our attack deterministically invalidates the assumption for discriminants of a special form, provided the parity conjecture holds and certain conditions are met. Specifically, by applying Proposition 2 from [20], we demonstrate that if the Mordell curve E_{-16D} has rank at least 2, it reveals the presence of nontrivial 3-torsion elements in the class groups, thus contradicting the RO_C assumption for these specific discriminants. For generic cases, while our attack still suggests that nontrivial 3-torsion elements could undermine the RO_C assumption, the results are based on heuristic arguments related to the Birch and Swinnerton-Dyer (BSD) conjecture. This conjecture, though widely believed, introduces some uncertainty in the generic scenario.
- We discuss the broader implications of our findings for cryptographic schemes that rely on the RO_C assumption. Our results highlight potential vulnerabilities and emphasize the need for re-evaluating and possibly strengthening cryptographic assumptions or exploring alternative approaches to maintain robust security guarantees.

Outline This paper is organized as follows. Subsection 1.1 covers essential properties and notations related to elliptic curves, imaginary quadratic orders, quadratic fields, and related algebraic structures. This foundational material is crucial for understanding the theoretical aspects of our work.

In Subsection 1.2, we describe the framework introduced by Castagnos and Laguillaumie, focusing on the algorithm `CLGen` and its implications for cryptographic applications. We also present and define the *unknown order assumption* and the *rough order assumption* (RO_C).

Following this, in Section 2, we present our attack on the rough order assumption. This Section details our attack strategy, utilizing Proposition 2 from [20]. We formally state and prove a theorem demonstrating how a high rank of the Mordell curve E_{-16D} can break the RO_C assumption.

In Section 3, we include computational methods and strategies for determining the rank of Mordell curves, providing a bridge between theory and practical application. Section 4 examines the impact of our attack on papers that rely on the rough order assumption. This analysis provides context for our contributions and situates our work within the broader research landscape.

We conclude by summarizing our findings, discussing the implications for cryptographic schemes based on class groups, and suggesting possible directions for future research.

1.1 Preliminaries

In this Subsection, we discuss properties and notations related to elliptic curves and imaginary quadratic orders. For detailed information on elliptic curves, refer to [33,32]. For comprehensive details on quadratic orders, see [18].

Elliptic curves are smooth projective algebraic curves of genus one with a specified point at infinity, denoted by $\mathcal{O}_E$. These curves can be expressed in the long Weierstraß form, where $\mathcal{O}_E$ serves as the (only) point at infinity. Often, the curve is presented using an affine equation without explicitly mentioning $\mathcal{O}_E$. An elliptic curve is equipped with a natural group law, with $\mathcal{O}_E$ serving as the identity element. The set of rational points on the curve E over a field F is denoted by $E(F)$.

In this work, we primarily focus on elliptic curves where F is the field of rational numbers $\mathbb{Q}$, specifically the Mordell curve $E_k : y^2 = x^3 + k$, where k is an integer. This curve is a key example of an elliptic curve over $\mathbb{Q}$ and is central to our study. Additionally, we occasionally consider elliptic curves over finite fields $\mathbb{F}_p$ in the context of the Birch and Swinnerton-Dyer (BSD) conjecture [3] and the Mestre–Nagao heuristics [26,27].

The **rank** of an elliptic curve E over $\mathbb{Q}$ is defined as follows. By the Mordell-Weil theorem, the group of rational points on E, denoted $E(\mathbb{Q})$, is a finitely generated abelian group. Therefore, it can be written as:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

where:

– r is the **rank** of the elliptic curve E, which corresponds to the number of independent generators of the infinite part,
– T is the **torsion subgroup**, consisting of points of finite order.

Thus, the rank r represents the number of independent rational points of infinite order on the elliptic curve.

Switching focus to quadratic fields, a *quadratic* field K is a subfield of the complex numbers $\mathbb{C}$ with degree 2 over $\mathbb{Q}$. This field can be uniquely expressed as $\mathbb{Q}(\sqrt{n})$, where n is a square-free integer distinct from 1 and 0. The *fundamental discriminant* Δ_K is defined as n if $n \equiv 1 \pmod 4$ and $4n$ otherwise.

An *order* $\mathcal{O}_K$ in K is a subset of K that forms a subring of K, containing 1, and serving as a free $\mathbb{Z}$-module of rank 2. The ring of integers $\mathcal{O}_{\Delta_K}$ in K is the *maximal order*, which contains all other orders of K. It can be represented as $\mathbb{Z} + \frac{1}{2}(\Delta_K + \sqrt{\Delta_K})\mathbb{Z}$. If $\mathcal{O}_K$ is an order in K with finite index f in $\mathcal{O}_{\Delta_K}$, then $\mathcal{O}_K$ can be expressed as $\mathbb{Z} + f\frac{1}{2}(\Delta_K + \sqrt{\Delta_K})\mathbb{Z} = \mathbb{Z} + f\mathcal{O}_{\Delta_K}$. The integer f is known as the *conductor* of $\mathcal{O}_K$.

The discriminant of the order $\mathcal{O}_K$ can be written as $\Delta_f = f^2\Delta_K$. When referring to a specific *non-maximal order* denoted as $\mathcal{O}_{\Delta_f}$, we classify it accordingly. The standard representation of a $\mathcal{O}_\Delta$-ideal, for a discriminant Δ, is

$$\mathfrak{a} = q\left(a\mathbb{Z} + \frac{-b + \sqrt{\Delta}}{2}\mathbb{Z}\right)$$

where $q \in \mathbb{Z}$, $a \in \mathbb{N}$, and $b \in \mathbb{Z}$ such that $b^2 \equiv \Delta \pmod{4a}$. An ideal is called *primitive* if $q = 1$. If $-a < b \leq a$, this expression is uniquely defined, and we denote a primitive ideal by (a, b). This also corresponds to the positive definite binary quadratic form $ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta$. A form $ax^2 + bxy + cy^2$ is *primitive* if its coefficients a, b, and c are relatively prime.

The *class group* of an order $\mathcal{O}$, denoted $\mathrm{cl}(\mathcal{O})$, is the quotient of the group of fractional ideals by the subgroup of principal ideals within $\mathcal{O}$. It measures the failure of unique factorization in the ring of integers of $\mathcal{O}$. Formally, the class group $\mathrm{cl}(\mathcal{O})$ is defined as

$$\mathrm{cl}(\mathcal{O}) = \frac{\mathrm{Ideal}(\mathcal{O})}{\mathrm{Principal}(\mathcal{O})},$$

where $\mathrm{Ideal}(\mathcal{O})$ denotes the group of fractional ideals in $\mathcal{O}$ and $\mathrm{Principal}(\mathcal{O})$ denotes the subgroup of principal ideals.

The *class number* $h_\mathcal{O}$ of $\mathcal{O}$ is the order of its class group. It quantifies the number of distinct ideal classes in $\mathrm{cl}(\mathcal{O})$. Formally,

$$h_\mathcal{O} = |\mathrm{cl}(\mathcal{O})|,$$

where $|\cdot|$ denotes the order of the group. The class number provides insight into the arithmetic properties of the order, with a larger class number indicating a greater failure of unique factorization.

In general, the specific structure of $\mathrm{cl}(\mathcal{O})$ as an abelian group remains largely unknown. For example, even determining the order of $\mathrm{cl}(\mathcal{O})$ is already a highly

non-trivial problem [23]. However, a notable exception is the 2-torsion subgroup of $\mathrm{cl}(\mathcal{O})$; *genus theory* [18][I.§3] provides a very explicit description of $\mathrm{cl}(\mathcal{O})[2] \cong \mathrm{cl}(\mathcal{O})/\mathrm{cl}(\mathcal{O})^2$ by introducing a set of characters $\chi_i : \mathrm{cl}(\mathcal{O}) \to \{\pm 1\}$, where $\mathrm{cl}(\mathcal{O})^2$ is recovered as the intersection of the kernels of these characters. The characters χ_i correspond to the prime factors m_i of the discriminant $\Delta_{\mathcal{O}}$ (with the prime 2 requiring special treatment), and they can be computed in polynomial time with respect to the size of m_i.

The 2-torsion subgroup $\mathrm{cl}(\mathcal{O})[2]$ is trivial if and only if $\Delta_{\mathcal{O}} = -q$ or $\Delta_{\mathcal{O}} = -4q$, where q is a prime satisfying $q \equiv 3 \pmod 4$.

1.2 The CL Framework for Unknown Order Group

The framework was first introduced by Castagnos and Laguillaumie [15] and later refined in [16,12,13], which specifies two algorithms, `CLGen` and `CLSolve`. For the purposes of this paper, we are interested only in the former, so we will describe only this algorithm.

`CLGen`, takes as input the security parameter 1^λ and a prime $q \geq 2^\lambda$, and outputs a set of public parameters $\mathtt{pp}_{\mathtt{cl}} = (q, \bar{s}, f, g_q, \hat{G}, F; \rho)$, which describe a class group, where ρ is the randomness used by `CLGen`. In this tuple, the group of squares $\hat{G}$ contains a cyclic subgroup $G \subseteq \hat{G}$, which factors as the direct product $G = G_q \times F \subseteq \hat{G}$, where $F = \langle f \rangle$ is the unique subgroup of order q, and $G_q = \langle g_q \rangle$ is the subgroup of qth powers.

The order of G_q is unknown, but it is known that an upper bound $\bar{s}$ exists such that $\bar{s} > |G_q|$. The class group associated with G_q has odd order, and computing its order is believed to be difficult when $|q|$ is large. For a discussion on the choice of cryptographic parameters related to such groups, see [7].

The Cohen-Lenstra heuristics [17] suggest that for imaginary quadratic number fields:

- approximately 97.6% of the time, the odd part of the class group is cyclic,
- the frequency $f(d)$ of fundamental discriminants for which the order of the class group is divisible by d is approximately:
  - $f(3) = 44\%$,
  - $f(5) = 24\%$,
  - $f(7) = 16\%$.

These heuristics indicate that while the class group is often cyclic, it frequently contains elements of small odd order. The challenge remains in determining how difficult it is to find such elements, if they exist. This leads to the formal definition of the Unknown Order Assumption (`ORD`):

Definition 1 (Unknown Order Assumption). *Let λ be the security parameter, $q \geq 2^\lambda$ a prime, and A a PPT algorithm. The experiment generates public parameters*

$$\mathtt{pp}_{\mathtt{cl}} := (q, \bar{s}, f, g_q, \hat{G}, F; \rho) \leftarrow \mathtt{CLGen}(1^\lambda, q; \rho)$$

and runs $A(\mathtt{pp}_{\mathtt{cl}})$. We say that A solves the unknown order (ORD) problem if it outputs a group element $h \in (\hat{G} \setminus F)$ and an integer $e \neq 0$ such that $h^e = 1$. We

define the advantage $Adv_A^{ORD}(\lambda)$ *as the success probability. The ORD assumption holds if* $Adv_A^{ORD}(\lambda)$ *is negligible in* λ *for all PPT A.*

Additionally, in [6], Braun, Damgård, and Orlandi introduced the rough order assumption. This new security assumption states that discriminants for class groups with rough order are indistinguishable from those in general. Currently, the topic is not well-explored. Below, we present the original definition of the rough order assumption as introduced by Braun, Damgård, and Orlandi [6]:

Definition 2 (Rough Order Assumption). *Let* λ *be a security parameter,* $q \geq 2^\lambda$ *a prime,* $C \in \mathbb{N}$*, and A be a PPT algorithm. Define* D_C^{rough} *to be the uniform distribution over the set* $\{\rho \in \{0,1\}^\lambda \mid (q, \bar{s}, f, g_q, \hat{G}, F; \rho) \leftarrow \texttt{CLGen}(1^\lambda, q; \rho) \wedge \forall \text{ prime } p < C : p \nmid ord(\hat{G})\}$*, We say A solves the C-rough order (*RO_C*) problem if its advantage*

$$Adv_A^{RO_C}(\lambda) := \left|\Pr\left[1 \leftarrow A(1^\lambda, \rho_0) \mid \rho_0 \in_R \{0,1\}^\lambda\right] - \Pr\left[1 \leftarrow A(1^\lambda, \rho_1) \mid \rho_1 \leftarrow D_C^{rough}\right]\right|$$

is non-negligible. We say the RO_C *assumption holds if* $Adv_A^{RO_C}(\lambda) \leq negl(\lambda)$ *for all PPT A.*

The definition above posits that class groups sampled under normal conditions are indistinguishable from those sampled with a C-rough order, where a C-rough order is defined as having no prime factors smaller than C. Note that the `CLGen` algorithm avoids certain discriminants to circumvent attacks related to the 2-torsion subgroup of the class group, as $\mathrm{cl}(\mathcal{O})[2]$ is trivial if and only if $\Delta_\mathcal{O} = -q$ or $\Delta_\mathcal{O} = -4q$, where q is a prime such that $q \equiv 3 \pmod 4$. By ensuring that q is not of this form, `CLGen` avoids potential vulnerabilities associated with the 2-torsion subgroup as described by genus theory.

2 Attack on the rough order assumption

In this section, we challenge the validity of the rough order assumption and present an efficient attack on the corresponding computational problem. Our attack reduces the problem to one involving the computation or approximation of the rank of a Mordell curve $E_k : y^2 = x^3 + k$ over the rational numbers. The main tool for our attack is Proposition 2 from [20], which we reproduce below with the necessary adaptations.

Proposition 1. *Suppose the positive integer* D *is squarefree, congruent to* 3 $\pmod 4$*, and is neither a multiple of* 3 *nor equal to* 1*. Then the rank of* E_{-16D} *is at most the sum of* 1 *and the* 3*-ranks of the class groups of* $\mathbb{Q}(\sqrt{-D})$ *and* $\mathbb{Q}(\sqrt{3D})$*.*

We now present our main Theorem, which is derived specifically for this paper. The Theorem builds on the aforementioned proposition and demonstrates that the rough order assumption RO_C can be invalidated under certain conditions.

Theorem 1 (informal). *Let D be a positive integer that is squarefree, congruent to* 3 (mod 4)*, and neither a multiple of* 3 *nor equal to* 1*. Suppose the rank of the Mordell curve $E_{-16D} : y^2 = x^3 - 16D$ over $\mathbb{Q}$ is at least 2. Then this contradicts the rough order assumption RO_C for some sufficiently large C, because the 3-torsion subgroup of $E_{-16D}(\mathbb{Q})$ cannot be trivial.*

Proof. Consider the Mordell curve $E_{-16D} : y^2 = x^3 - 16D$ over $\mathbb{Q}$. According to the proposition, if D is squarefree, congruent to 3 (mod 4), and is neither a multiple of 3 nor equal to 1, then the rank of E_{-16D} is at most the sum of 1 and the 3-ranks of the class groups of $\mathbb{Q}(\sqrt{-D})$ and $\mathbb{Q}(\sqrt{3D})$.

Assume, for the sake of contradiction, that the rank of E_{-16D} is at least 2. This implies that the sum of the 3-ranks of the class groups of $\mathbb{Q}(\sqrt{-D})$ and $\mathbb{Q}(\sqrt{3D})$ must be at least 1. In other words, at least one of these class groups must have a nontrivial 3-torsion element.

Now, by the Scholz reflection Theorem [31], the 3-rank of the class group of $\mathbb{Q}(\sqrt{-D})$ is either equal to or one greater than the 3-rank of the class group of $\mathbb{Q}(\sqrt{3D})$ (since D is assumed to be a negative fundamental discriminant and not equal to -3).

Thus, if the 3-rank of the class group of $\mathbb{Q}(\sqrt{3D})$ is non-zero, the 3-rank of the class group of $\mathbb{Q}(\sqrt{-D})$ must also be non-zero, and vice versa. This implies that both class groups contain nontrivial 3-torsion elements.

However, the rough order assumption RO_C asserts that for a sufficiently large C, the class group should have no prime factors smaller than C, including 3. The existence of nontrivial 3-torsion elements directly contradicts this assumption.

Therefore, if the rank of E_{-16D} is at least 2, this would break the rough order assumption RO_C by implying the presence of nontrivial 3-torsion in the class group. This contradiction invalidates the rough order assumption under these conditions. □

Finding the rank of a Mordell curve E_k with a large coefficient $k = -16D$ (where D is a large integer with more than 1000 bits) is a challenging task [19][Section 15.5]. In the next Section, we show how to overcome this challenge for special discriminants and how to tackle the general case using some heuristic methods.

3 Heuristic Insights on the Rank of Elliptic Curves

In addressing the challenge of determining whether a Mordell curve $E_k : y^2 = x^3 + k$ has rank at least 2, especially when dealing with large coefficients, we face significant computational obstacles. In this Subsection, we present heuristic insights that offer valuable evidence regarding the rank of elliptic curves. These insights help us navigate the difficulties associated with verifying the expected rank for curves with coefficients k larger than 1000 bits, which are critical for real-world cryptographic applications.

We begin by identifying a family of discriminants where we have developed a fully working attack, enabling us to effectively assess the rank in these specific

cases. This approach provides a robust methodology for dealing with particular instances. We then extend our focus to the general case, applying heuristic methods to gain a better understanding of the curve's rank and to potentially overcome some of the computational limitations inherent in this process.

3.1 Special discriminants

It is well known that the rough order assumption can be compromised for discriminants with specific forms. These discriminants exhibit particular structural properties that make them vulnerable to certain attacks, thus providing a clear path to undermining the rough order assumption in these cases.

In [2], Belabas, Kleinjung, Sanso, and Wesolowski illustrate that there are specific choices of discriminants for which the *low order assumption* [10, Definition 1] does not hold. These discriminants are associated with special forms defined in Theorems 1 and 2, and Corollary 1 of their paper. Breaking the low order assumption involves finding an element μ in a finite group G and an integer $d < 2^\lambda$ such that $\mu \neq 1_G$ and $\mu^d = 1_G$, where 1_G denotes the identity element of G. Since the low order assumption is a weaker condition compared to the rough order assumption, a violation of the low order assumption implies that the rough order assumption is also invalidated.

By leveraging techniques from [22], we identify special discriminants of the form $D = \frac{3}{4}z^2 \pm 4$, where our Theorem 1 effectively demonstrates how to break the rough order assumption (but not the low order assumption). We show below how these techniques can be applied to achieve this result. The formulae (11) derived in [22][Subsection 6.1] reveal a correlation between the coefficient k and a point $P(x, y)$ in E_k. We report them here:

$$x = z^2 + a, \quad k = -a^2\left(\frac{3}{4}z^2 + a\right), \quad y = z\left(z^2 + \frac{3}{2}a\right)$$

Choosing $a = \pm 4$ yields a Mordell curve E_{-16D} (compatible with Theorem 1) for discriminants of the form $D = \frac{3}{4}z^2 \pm 4$.

We can rewrite the curve as $E_z : y^2 = x^3 + (-12z^2 + 64)$, and the 3-isogenous curve as $y^2 = x^3 + (324z^2 - 1728)$. This construction represents a well-known family of elliptic curves with a generic rank of 1. As z varies, we expect the rank of E_z to be 1, 2, or greater than 2, with probabilities of 50%, 50%, and 0%, respectively. This expectation parallels the behavior of random elliptic curves, where the rank is typically 0, 1, or greater than 1, with the same probabilities. The rationale is that the rank should be even or odd with equal probability.

We use the **parity conjecture** to guide the decision in Algorithm 1 on whether the rough order assumption (RO_C) breaks for a given discriminant of the form $D = \frac{3}{4}z^2 \pm 4$. The parity conjecture helps us predict the parity (odd or even) of the rank of the corresponding elliptic curve E_{-16D}. According to the parity conjecture, the algebraic rank of an elliptic curve and its analytic rank have the same parity, meaning both are either even or odd. By computing the global root number w_E, we determine the parity of the rank of E_{-16D}. If the

rank is predicted to be **even** for this family of elliptic curves, it indicates that the rough order assumption (RO_C) is broken, according to Theorem 1. Conversely, if the rank is predicted to be **odd**, the rough order assumption (RO_C) is more likely to hold. However, it is important to note that this method may miss detecting violations of the rough order assumption (RO_C) when the rank is **odd and greater than 1**. Nevertheless, such cases are expected to occur infrequently, as ranks greater than 1 are highly uncommon in practice.

Computing the Parity for the Mordell Curve For a Mordell curve $E_k : y^2 = x^3 + k$, the parity of the rank is closely related to the **global root number** w_E. The global root number is the product of **local root numbers** at various primes p, including the prime at infinity, and provides an indicator of the parity of the analytic rank. Specifically:

$$w_E = (-1)^{\text{analytic rank}(E_k)}$$

If $w_E = -1$, the analytic rank is odd, and by the parity conjecture, the algebraic rank is also odd. Conversely, if $w_E = +1$, both ranks are even.

To compute the global root number for the Mordell curve E_k, we must:

- Compute the local root number w_∞ at the infinite prime.
- Compute the local root numbers $w_{E,p}$ for all primes p that divide the discriminant Δ_E of the elliptic curve E_k.
- The product of these local root numbers will give the global root number w_E.

For a Mordell curve E_k, the local root number at infinity w_∞ is determined by the sign of the leading term in the equation. Since the Mordell curve $E_k : y^2 = x^3 + k$ has a positive cubic term x^3, the root number at infinity is always:

$$w_\infty = -1$$

For each prime p, the local root number $w_{E,p}$ depends on the reduction type of the curve at that prime. Mordell curves of the form $E_k : y^2 = x^3 + k$ have bad reduction at primes dividing k and at $p = 2$ and $p = 3$, and good reduction otherwise. For a Mordell curve, the local root number at a prime p is computed as follows:

- If $p \nmid \Delta_E$ (i.e., p does not divide the discriminant Δ_E), the curve has good reduction at p, and the local root number $w_{E,p}$ is:

$$w_{E,p} = +1$$

- If $p \mid \Delta_E$ (i.e., p divides the discriminant Δ_E), the curve has bad reduction at p, and we compute $w_{E,p}$ based on the residue of Δ_E modulo p. Specifically:
  - If $p = 2$, the local root number $w_{E,2}$ depends on the behavior of the curve at 2, which can be determined from the 2-adic valuation of Δ_E and the reduction type.

- If $p \geq 3$, the local root number $w_{E,p}$ is determined by the quadratic residue $\Delta_E \pmod p$. If Δ_E is a quadratic residue modulo p, then $w_{E,p} = +1$. If Δ_E is not a quadratic residue modulo p, then $w_{E,p} = -1$.

Finally, the global root number w_E is computed as:

$$w_E = w_\infty \prod_{p|\Delta_E} w_{E,p}$$

If $w_E = -1$, the rank is odd (and likely $r = 1$). If $w_E = +1$, the rank is even (and likely $r = 2$).

Algorithm 1: Check the rough order assumption for special discriminants of the form $D = -\frac{3}{4}z^2 \pm 4$

Input : Discriminant $D = -\frac{3}{4}z^2 \pm 4$
Output: True if RO_C is invalidated, False otherwise

```
Compute the Mordell curve E_{16D} from the discriminant D;
Compute global root number w_E ;
if w_E == +1 then
    return True
else
    return False
```

Thus, the decision in the algorithm is based on whether the computed heuristic score suggests a break in the rough order assumption RO_C, guided by the rank parity obtained from the global root number. If the rank is even, we can be certain that the rough order assumption RO_C does not hold, as Theorem 1 indicates that such cases lead to deviations from the expected behavior. According to the parity conjecture, the rank of an elliptic curve is expected to be either even or odd with equal probability.

Complexity of Computing the Global Root Number For a Mordell curve $E_k : y^2 = x^3 + k$ where $k = -16D$ and D is a prime number, the computation of the global root number w_E involves a few straightforward steps. The discriminant Δ_E of the curve is $-110592D^2$, and the prime factors are 2, 3, and D.

Since D is a prime, the factorization of Δ_E is trivial and requires constant time, $\mathcal{O}(1)$. Calculating the local root numbers $w_{E,2}$, $w_{E,3}$, and $w_{E,D}$ involves evaluating the reduction types at these primes. These computations are typically performed in constant time, $\mathcal{O}(1)$, since they involve modular arithmetic and standard evaluations for local root numbers. Finally, multiplying the local root numbers to determine the global root number w_E also takes constant time, $\mathcal{O}(1)$.

Therefore, the overall complexity of computing the global root number for E_k in this case is $\mathcal{O}(1)$, indicating that the computation is highly efficient and independent of the size of the prime D.

3.2 General Case

For the specific Mordell curve E_{-16D} considered in this paper, its rank provides a lower bound on the 3-rank of the class group. While the rank of this curve is frequently 0 or 1, the Cohen-Lenstra heuristics [17] and numerical evidence indicate that the 3-rank of the associated class group can occasionally be at least 2, although this happens only with limited probability. Consequently, the lower bound derived from the rank generally does not pose a significant challenge to the *rough order assumption*, though potential exceptions cannot be entirely ruled out. The exact frequency of curves with rank 2 or higher is uncertain, but such curves do exist, and their proportion is expected to diminish as $|D| < N$ increases. While finding such curves at random for large D remains difficult, it is not impossible, particularly with the use of heuristic methods.

One standard approach for estimating the rank of elliptic curves is the Mestre–Nagao method, which is informed by the Birch and Swinnerton-Dyer conjecture [3]. According to this conjecture, curves that exhibit a notably large number of points modulo p for most primes p tend to have many rational points as well. The method constructs a score $S(k, B)$ based on the number of points $N_p(E_k)$ on $E_k(\mathbb{F}_p)$ for all primes $p \leq B$, where E_k has good reduction. This score helps estimate the rank of the curve by identifying rational points on E_k for values of k within a search range where $S(k, B)$ exceeds a certain threshold. Originally proposed by Mestre [26] to find elliptic curves with high Mordell–Weil rank, this technique was later refined by Nagao [27] and has been useful in the search for curves with higher ranks.

$$S(k, B) = \sum_{\substack{p<B \\ \text{where } E_k \text{ has good reduction at } p}} \log\left(\frac{N_p(E_k)}{p}\right),$$

where $\exp(-S(k, B))$ represents the partial product. According to the Birch and Swinnerton-Dyer conjecture, if E_k has a high rank, these partial products should approach zero quickly, leading to a large value for $S(k, B)$.

Although higher ranks (i.e., $r > 1$) remain rare, especially for Mordell curves, the parity conjecture provides a useful heuristic for predicting whether a curve has rank 0 or 1. However, applying the Mestre–Nagao method, particularly for Mordell curves with large coefficients k (e.g., greater than 1000 bits), becomes computationally infeasible, especially in contexts relevant to cryptographic applications. For real-world use, the method has limitations in reliably identifying curves with ranks $r \geq 2$, and the rank 0 problem remains unsolved in number theory.

In our case, excluding curves with rank 0 provides enough information to evaluate the *rough order assumption* (RO_C). By using the **parity conjecture** along with the Mestre–Nagao heuristic, it is possible to predict whether the rank of E_{-16D} is even or odd. If the rank is predicted to be even, the rough order assumption (RO_C) may be violated, as outlined in Theorem 1. Conversely, if the rank is odd, the assumption is more likely to hold.

While the Mestre–Nagao score remains a useful heuristic tool, it should be applied cautiously in this context, as it is not always reliable for detecting curves with higher ranks. This limitation highlights the need for further refinement in both theoretical and practical methods for evaluating the rough order assumption (RO_C), particularly in cryptographic applications.

3.3 Attack Implementation

We implemented the attack using SageMath to demonstrate both the correctness of the algorithm and its feasibility. The code for all algorithms and experiments is available at:

`https://anonymous.4open.science/r/rough-order-sage-CC18`

This code provides a comprehensive framework for evaluating the rank of Mordell curves, implementing methods for both special discriminants and the generic case, as described in the Subsections above. This flexibility allows for easy experimentation with different parameters and facilitates further research in this area.

4 Attacks on the Papers and Countermeasures

This section explores vulnerabilities in papers that rely on rough order assumptions, including the original works introducing these assumptions [6,5,11], in the context of our attack. We analyze key weaknesses in these papers and discuss potential countermeasures to mitigate the risks posed by the attack.

The primary assumption in these papers is that class group orders behave similarly to random integers with respect to the sizes of their prime factors. Specifically, this assumption implies that a significant fraction of class groups will have C-rough order, where C is a threshold value. The value C determines the minimum size of prime factors considered "large," meaning that prime factors smaller than C are considered "small." The parameter B represents a bound related to the size or complexity of the class group. If C is small relative to B, then it is expected that many class groups will have prime factors larger than C.

However, when considering our attack on the 3-torsion, this assumption introduces vulnerabilities. Specifically, our attack exploits the presence of small prime factors in the class group order, with a particular focus on the 3-torsion. Since the assumption that class group orders are C-rough is directly undermined by this attack, the 3-torsion behavior in the class group structure provides an exploitable weakness in cryptographic protocols relying on rough order assumptions.

Secure Threshold Cryptography Based on Class Groups [6] Assuming the rough order assumption holds, the paper significantly simplifies zero-knowledge protocols and their security proofs. It enables a much cleaner design and analysis of zero-knowledge protocols compared to using more complex assumptions, such as the strong root assumption. The rough order assumption is primarily used in theoretical proofs, and nothing in practical implementations depends on the specifics of the challenger used in these proofs. For the Multi-Party Computation (MPC) protocol discussed in the paper, the required soundness property is met if an adversarially generated ciphertext is proven to be well-formed and the plaintext can be extracted from the proof. This requirement is weaker than full knowledge soundness, which would also necessitate extracting the ciphertext's randomness. Thus, the assumption that class groups with rough order are indistinguishable from general class groups is sufficient for ensuring soundness in this context. However, if the rough order assumption fails—such as when a distinguisher with an advantage close to 1 is found—it could expose practical vulnerabilities. While the rough order assumption facilitates a cleaner theoretical framework, practical implementations might still be at risk if the assumption is not valid. This new computational assumption, though emerging and not yet well-studied, has already impacted future work by enabling a more straightforward design and analysis of zero-knowledge protocols. Alternative, more established assumptions, like the strong root assumption, could be used, but they come with increased complexity.

An Improved Threshold Homomorphic Cryptosystem Based on Class Groups [5] Similar to the approach in the previous work, the authors of this paper leverage the rough order assumption (RO_C) to enhance the efficiency of their threshold homomorphic cryptosystem. By assuming RO_C, they facilitate weak reconstruction in Verifiable Secret Sharing (VSS) protocols and ensure statistical security with Pedersen commitments. This assumption is crucial for the design and analysis of efficient Σ-style zero-knowledge proofs. Under RO_C, these proofs are unconditionally set-membership sound, which means no malicious prover can prove a false statement with a probability greater than $1/C$. The paper further claims that, under this assumption, the proofs are computationally sound even for normally sampled class groups, meaning that no malicious probabilistic polynomial-time (PPT) prover can prove a false statement with a probability greater than $1/C + \mathrm{negl}(\lambda)$.

Proving this computational soundness is not straightforward. The reduction process involves deciding if a statement is false, which typically requires knowledge of discrete logs that the reduction does not possess, making the decision inefficient. However, the paper addresses this challenge by showing that these zero-knowledge proofs can be effectively used in a broader context. Specifically, they suggest that in higher-level protocols, it is generally possible to determine efficiently if the protocol has been compromised. This implies that a reduction to RO_C becomes feasible. The approach involves proving the security of the higher-level protocol in a rough-order group using the unconditional soundness of the zero-knowledge proofs. Then, it is argued that when a normal-order group

is used, the adversary's advantage in breaking the high-level protocol is at most negligibly greater. This holds true since otherwise, the adversary would imply the existence of a distinguisher for RO_C. Thus, while RO_C simplifies theoretical considerations and provides efficiency benefits, practical implementations must remain cautious due to the emerging and not yet thoroughly studied nature of this assumption. Our work further illustrates these practical risks by demonstrating how the failure of RO_C assumptions can lead to vulnerabilities, highlighting the need for continued scrutiny and potentially alternative assumptions in practical applications.

Publicly Verifiable Secret Sharing over Class Groups and Applications to DKG and YOSO [11] Similar to the other papers, this work also relies on the rough order assumption (RO_C) to construct a secure Publicly Verifiable Secret Sharing (PVSS) scheme over class groups. The paper introduces a sharing proof Π_{Sh}, which is a zero-knowledge proof designed to ensure correct secret sharing within a Distributed Key Generation (DKG) protocol. The core idea is that for any correct sharing, if a random polynomial $m^* \in \mathbb{Z}_q[X]$ is sampled, then for properly generated shares, the relation $\sum_{i=1}^{n} \sigma_i v_i m^*(\alpha_i) = 0$ must hold, where v_i are certain values derived from Theorem 1. This property allows for constructing a verification equation using group elements pk_i and B_i, enabling an efficient zero-knowledge proof of correct secret sharing. However, a potential issue arises if a malicious prover introduces elements $H_i \neq 1$ into the group, which could manipulate the proof into passing incorrectly. To address this, the paper randomizes the proof by adding a multiple of q to the values w_i, making the cancellation of malicious terms less likely unless the prover can break the rough order assumption. This additional step ensures robustness without significantly increasing communication or computational complexity. As with previous papers, if the rough order assumption fails, the security of the PVSS scheme may be compromised, particularly when small prime factors are present in the class group order. Our analysis further highlights how our attack on 3-torsion can exploit weaknesses introduced by the rough order assumption, demonstrating the importance of continued analysis and potential refinements to these assumptions in practical applications.

Countermeasures: To defend against our 3-torsion attack, it is crucial to address specific vulnerabilities associated with class groups. One effective countermeasure involves avoiding discriminants of special shapes or forms that are known to break the rough order assumption. Specifically, discriminants of the form $D = -\frac{3}{4}z^2 \pm 4$ are particularly susceptible to vulnerabilities, as demonstrated in Subsection 3.1. These special forms can lead to class groups with significant 3-torsion, thereby compromising the security of cryptographic protocols. Additionally, discriminants identified in [2], which break the low order assumption, are also dangerous as they can similarly undermine the rough order assumption and expose vulnerabilities to 3-torsion attacks. Furthermore, incorporating the Mestre-Nagao heuristic during the class group generation process,

such as when using the `CLGen` algorithm, can provide an additional layer of security. The Mestre-Nagao heuristic evaluates the potential rank of the generated class groups by assessing the number of rational points on corresponding elliptic curves. By applying this heuristic and setting a threshold to limit the heuristic score $S(k, B)$, one can filter out class groups that are likely to exhibit high ranks and substantial 3-torsion. This approach helps in reducing the likelihood of encountering vulnerabilities and enhances the robustness of cryptographic protocols against attacks related to 3-torsion.

5 Conclusion

In this paper, we have examined the rough order assumption (RO_C) and its implications for cryptographic schemes based on class groups of imaginary quadratic fields. Through our analysis, we demonstrated that the assumption is challenged when the rank of the Mordell curve E_{-16D} is at least 2. Specifically, the presence of nontrivial 3-torsion elements in the class groups of $\mathbb{Q}(\sqrt{-D})$ and $\mathbb{Q}(\sqrt{3D})$ contradicts the RO_C assumption for sufficiently large C.

Our findings indicate that the rough order assumption may not hold in scenarios where such Mordell curves have high ranks, suggesting potential vulnerabilities in cryptographic applications relying on this assumption. This result highlights the need for further investigation into alternative assumptions or strengthening of existing ones to ensure the robustness of cryptographic schemes based on class groups.

Future work could explore practical methods for detecting and mitigating the effects of such attacks, as well as evaluate other assumptions that may provide better security guarantees in the context of imaginary quadratic fields.

The following problems remain open:

- Investigating whether there are other families of rank 1 elliptic curves that might also challenge the rough order assumption, given that our attack was effective in the special case of rank 1 elliptic curves associated with specific discriminants.
- Advancing methods to determine whether an elliptic curve has rank 0. While this remains a challenging problem, progress in this area could enhance our understanding of elliptic curves and improve the practical application of the rough order assumption (RO_C).
- Extending the method to torsion structures larger than 3-torsion. While our results primarily address the 3-torsion case, exploring attacks on higher torsion elements may provide a more comprehensive understanding of the rough order assumption and its cryptographic implications.

Acknowledgments. We would like to thank Noam Elkies for his valuable contributions to Section 3, as well as Bill Allombert, Guilhem Castagnos, John Cremona, Ivan Damgård, Andrej Dujella, Péter Kutas, Guido Maria Lido and Claudio Orlandi for fruitful discussions.

References

1. Abram, D., Damgård, I., Orlandi, C., Scholl, P.: An algebraic framework for silent preprocessing with trustless setup and active security. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology – CRYPTO 2022. pp. 421–452. Springer Nature Switzerland, Cham (2022)
2. Belabas, K., Kleinjung, T., Sanso, A., Wesolowski, B.: A note on the low order assumption in class groups of imaginary quadratic number fields. Mathematical Cryptology **3**(1), 44–51 (Jul 2023), https://journals.flvc.org/mathcryptology/article/view/129193
3. Birch, B., Swinnerton-Dyer, H.P.F.: Notes on elliptic curves. i. Journal für die reine und angewandte Mathematik **212**(7), 7–25 (1963)
4. Boneh, D., Bünz, B., Fisch, B.: Batching techniques for accumulators with applications to iops and stateless blockchains. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019. pp. 561–586. Springer International Publishing, Cham (2019)
5. Braun, L., Castagnos, G., Damgård, I., Laguillaumie, F., Melissaris, K., Orlandi, C., Tucker, I.: An improved threshold homomorphic cryptosystem based on class groups. Cryptology ePrint Archive, Paper 2024/717 (2024), https://eprint.iacr.org/2024/717
6. Braun, L., Damgård, I., Orlandi, C.: Secure multiparty computation from threshold encryption based on class groups. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023. pp. 613–645. Springer Nature Switzerland, Cham (2023)
7. Buchmann, J., Hamdy, S.: A survey on IQ cryptography, pp. 1–16. De Gruyter, Berlin, New York (2001). https://doi.org/doi:10.1515/9783110881035.1, https://doi.org/10.1515/9783110881035.1
8. Buchmann, J., Williams, H.C.: A key-exchange system based on imaginary quadratic fields. J. Cryptology **1**, 107–118 (1988). https://doi.org/10.1007/BF02351719
9. Bünz, B., Fisch, B., Szepieniec, A.: Transparent snarks from dark compilers. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020. pp. 677–706. Springer International Publishing, Cham (2020)
10. Bünz, D.B.B., Fisch, B.: A survey of two verifiable delay functions. Cryptology ePrint Archive, Report 2018/712 (2018)
11. Cascudo, I., David, B.: Publicly verifiable secret sharing over class groups and applications to dkg and yoso. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 216–248. Springer Nature Switzerland, Cham (2024)
12. Castagnos, G., Catalano, D., Laguillaumie, F., Savasta, F., Tucker, I.: Two-party ecdsa from hash proof systems and efficient instantiations. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019. pp. 191–221. Springer International Publishing, Cham (2019)
13. Castagnos, G., Catalano, D., Laguillaumie, F., Savasta, F., Tucker, I.: Bandwidth-efficient threshold ec-dsa. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) Public-Key Cryptography – PKC 2020. pp. 266–296. Springer International Publishing, Cham (2020)
14. Castagnos, G., Laguillaumie, F.: On the security of cryptosystems with quadratic decryption: The nicest cryptanalysis. In: Joux, A. (ed.) Advances in Cryptology - EUROCRYPT 2009. pp. 260–277. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)

15. Castagnos, G., Laguillaumie, F.: Linearly homomorphic encryption from ddh. In: Nyberg, K. (ed.) Topics in Cryptology — CT-RSA 2015. pp. 487–505. Springer International Publishing, Cham (2015)
16. Castagnos, G., Laguillaumie, F., Tucker, I.: Practical fully secure unrestricted inner product functional encryption modulo p. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018. pp. 733–764. Springer International Publishing, Cham (2018)
17. Cohen, H., Lenstra, Jr., H.W.: Heuristics on class groups of number fields. In: Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, pp. 33–62. Springer, Berlin (1984)
18. Cox, D.A.: Primes of the form $x^2 + ny^2$. A Wiley-Interscience Publication, John Wiley & Sons Inc., New York (1989), fermat, class field theory and complex multiplication
19. Dujella, A., Švob, P.: Number Theory. Manualia universitatis studiorum zagrabiensis, Školska knjiga (2021), https://books.google.ch/books?id=sISFzgEACAAJ
20. Elkies, N.D.: Rank of an elliptic curve and 3-rank of a quadratic field via the burgess bounds. In: Algorithmic Number Theory Symposium, ANTS-XVI. MIT, July 2024 (2024)
21. Elkies, N.D., Klagsbrun, Z.: New rank records for elliptic curves having rational torsion. In: Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-14) (2020), https://msp.org/obs/2020/4-1/obs-v4-n1-p15-s.pdf, arXiv:2003.00077
22. Gebel, J., Pethö, A., Zimmer, H.G.: On mordell's equation. Compositio Mathematica **110**(3), 335–367 (February 1998). https://doi.org/10.1023/A:1000281602647, https://doi.org/10.1023/A:1000281602647
23. Hafner, J.L., McCurley, K.S.: A rigorous subexponential algorithm for computation of class groups. Journal of the American Mathematical Society **2**, 837–850 (1989), https://api.semanticscholar.org/CorpusID:51781105
24. Hartmann, M., Paulus, S., Takagi, T.: Nice - new ideal coset encryption -. In: Koç, Ç.K., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems. pp. 328–339. Springer Berlin Heidelberg, Berlin, Heidelberg (1999)
25. Lipmaa, H.: Secure accumulators from euclidean rings without trusted setup. In: Bao, F., Samarati, P., Zhou, J. (eds.) Applied Cryptography and Network Security - 10th International Conference, ACNS 2012, Singapore, June 26-29, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7341, pp. 224–240. Springer (2012). https://doi.org/10.1007/978-3-642-31284-7_14, https://doi.org/10.1007/978-3-642-31284-7_14
26. Mestre, J.F.: Construction d'une courbe elliptique de rang ≥ 12. Comptes rendus de l'Académie des sciences. Série 1, Mathématique **295**(12), 643–644 (1982)
27. Nagao, K.I.: Examples of elliptic curves over $\mathbb{Q}$ with rank ≥ 17. Proceedings of the Japan Academy, Series A, Mathematical Sciences **68**(9), 287–289 (1992)
28. Paulus, S., Takagi, T.: A generalization of the diffie-hellman problem and related cryptosystems allowing fast decryption. In: The 1st International Conference on Information Security and Cryptology, ICSCI '98, December 18-19, 1998, Seoul, Korea, Proceedings. pp. 211–220. Korea Institute of Information Security and Cryptology (KIISC) (1998)
29. Paulus, S., Takagi, T.: A new public-key cryptosystem over a quadratic order with quadratic decryption time. J. Cryptol. **13**(2), 263–272 (2000). https://doi.org/10.1007/S001459910010, https://doi.org/10.1007/s001459910010

30. Pietrzak, K.: Simple verifiable delay functions. In: Innovations in Theoretical Computer Science (ITCS 2019). Leibniz International Proceedings in Informatics (LIPIcs), vol. 124, pp. 60:1–60:15. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik (2018), https://doi.org/10.4230/LIPIcs.ITCS.2019.60
31. Scholz, A.: Über die beziehung der klassenzahlen quadratischer körper zueinander. Journal für die reine und angewandte Mathematik **166**, 201–203 (1932), http://eudml.org/doc/183472
32. Silverman, J.H.: The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106. Springer-Verlag, New York (1992)
33. Silverman, J.H., Tate, J.T.: Rational Points on Elliptic Curves. Springer Publishing Company, Incorporated, 2nd edn. (2015)
34. Wesolowski, B.: Efficient verifiable delay functions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019. pp. 379–407. Springer International Publishing, Cham (2019)