BREAKING THE DECISIONAL DIFFIE-HELLMAN PROBLEM IN TOTALLY NON-MAXIMAL IMAGINARY QUADRATIC ORDERS

ANTONIO SANSO

Abstract. This paper introduces an algorithm to efficiently break the Decisional Diffie-Hellman (DDH) assumption in totally non-maximal imaginary quadratic orders, specifically when $\Delta_1 = 3$, and f is non-prime with knowledge of a single factor. Inspired by Shanks and Dedekind's work on 3-Sylow groups, we generalize their observations to undermine DDH security.

1. Introduction

The Decision Diffie–Hellman assumption (DDH) is essential for demonstrating the security of numerous widely employed protocols, including Diffie–Hellman key agreement, El Gamal encryption and more advanced functionalities. The DDH problem posits that given a finite cyclic group $G = \langle g \rangle$ with a generator g, it is hard to distinguish between (g, g^x, g^y, g^{xy}) and (g, g^x, g^y, g^z), where x, y, and z are chosen randomly in G.

It is well known that one can defeat the DDH assumption in $\mathbb{F}_p^*$ employing the Legendre symbols and in class groups (and for class group actions [1, 2]) via *genus theory*. Therefore, G is selected as a cyclic prime-order subgroup within the multiplicative group $\mathbb{F}_p^*$ of a finite prime field. For class groups (and class group actions), one must operate within the set of square elements (*principal genus*). The Legendre symbol acts as a group homomorphism mapping from $\mathbb{F}_p^* \to \{1, -1\}$. For any prime $\ell \mid (p-1)$, a homomorphism from $\mathbb{F}_p^*$ to H can be constructed where H is a subgroup with an order of ℓ. Consequently, when $(p-1)$ encompasses various small factors, an algorithm can be developed to distinguish Diffie-Hellman quadruples from random quadruples, leading to the resolution of the DDH problem. This can be extended to any group with a known order and is not restricted to $\mathbb{F}_p^*$. The amazing aspect of *genus theory* is that it provides an efficiently computable character even when the order of the group is unknown. This is typically the case in the class group of *maximal order* of an imaginary quadratic field $Cl(\Delta)$, and these characters can be used to break DDH (the fix as mentioned above is to work in the group of squares). In this paper we focus on the special case of *totally non-maximal imaginary quadratic orders* $\mathcal{O}_{\Delta_f}$ such that $\Delta_f = \Delta_1 f^2$ and the class number of the maximal order $h(\Delta_1) = 1$. The key feature of these totally non-maximal orders is the immediate knowledge of the class number of the maximal order $h(\Delta_1) = 1$. Consequently, the class number of the non-maximal order Δ_f, where the conductor f is prime, is also known immediately and is equal to $h(\Delta_f) =$

Ethereum Foundation

$f-\left(\frac{\Delta_1}{f}\right)$, where $\left(\frac{\Delta_1}{f}\right)$ represents the Kronecker symbol. In [3] it was shown that the discrete logarithm problem in totally non-maximal imaginary quadratic orders $\mathcal{O}_{\Delta_f}$ for prime f, can be reduced to the discrete logarithm problem in F_f^* (if $\left(\frac{\Delta_1}{f}\right) = 1$) or $F_{f^2}^*$ (if $\left(\frac{\Delta_1}{f}\right) = -1$) respectively. In a broader context, the study conducted in [4] demonstrated that the calculation of discrete logarithms within $Cl(\Delta_f)$ can be simplified to the computation of discrete logarithms within the class group $Cl(\Delta_1)$ of the maximal order, along with the computation of discrete logarithms within various smaller groups derived from the factorization of f. It becomes evident that the DDH problem can be readily undermined in the case of totally non-maximal imaginary quadratic orders by computing $h(Cl(\Delta_f)$ when the factorization of f is known.

Our contribution. The main contribution of this paper is an algorithm that breaks efficiently DDH for totally non-maximal imaginary quadratic orders with $\Delta_1 = 3$ in cases where f is non-prime, and the knowledge of a single factor of f is available. The inspiration for writing this paper comes from [5, §8], where Shanks provides an interesting characterization of 3-Sylow groups for binary quadratic forms. He quotes some results contained in a work by Dedekind [6], where the 3-Sylow subgroup for certain discriminants relates to the set of quadratic forms representing all primes that have a prescribed composite integer a as a cubic residue:

> For example cf. Dedekind [6], one has discriminant $h(-4 \cdot 243) = 9$ with a group $C(3) \times C(3)$. There are four subgroups of order 3, not merely one as would be the case if the group were cyclic. One of these four, comprising $I = (1, 0, 243)$ and the forms $(9, \pm 6, 28)$, represents all primes having 2 as a cubic residue. Another: I and $(4, \pm 2, 61)$ has 3 as a cubic residue; the third: I and $(7, \pm 6, 36)$ has 6; and the last: I and $(13, \pm 4, 19)$ has both $12 = 4 \cdot 3$ and $18 = 2 \cdot 9$ as cubic residues. The discriminant $-4 \cdot 675$, with a group $C(3) \times C(6)$, may be used similarly for a = 2, 5, 10, 20, and 50.

In this paper, we generalize this observation to efficiently break the DDH in the aforementioned case.

Outline. This paper is organized as follows. In Subection 1.1, we give a mathematical foundation for understanding the concepts employed in the manuscript. In subsection 1.2 we present a brief survey that contextualizes the existing literature and provides insights into the current state of the field. Section 2, the main contribution of the paper, offers a detailed description of the algorithm used for the break. Finally, we draw conclusions in Section 3.

1.1. **Preliminaries.** In this subsection, we will discuss properties and notations related to imaginary quadratic orders. For formal definitions and detailed information on quadratic orders, refer to [21].

A *quadratic* field K is a subfield of the complex numbers $\mathbb{C}$ with a degree of 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 $n = 1 \pmod 4$ and $4n$ otherwise. An *order* $\mathcal{O}$ in K is a subset of K that forms a subring of K, containing 1, and functioning as a free $\mathbb{Z}$-module of rank 2. The ring $\mathcal{O}_{\Delta_K}$ of integers in K is the *maximal order*, containing all other orders

of K. It can be represented as $\mathbb{Z} + \frac{1}{2}(\Delta_K + \sqrt{\Delta}_K)\mathbb{Z}$. If we denote the finite index of any order $\mathcal{O}$ in $\mathcal{O}_{\Delta_K}$ as $f = [\mathcal{O}_{\Delta_K} : \mathcal{O}]$, then $\mathcal{O}$ 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 $\mathcal{O}$. The discriminant of the order $\mathcal{O}$ can be written as $\Delta_f = f^2\Delta_K$. When referring to this specific order, denoted as O_{Δ_f}, we classify it as a *non-maximal order*. The standard representation of an $\mathcal{O}_\Delta$-ideal, for a discriminant Δ, is

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

with $q \in \mathbb{Z}$, $a \in \mathbb{N}$ 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 singularly defined, and we will denote a primitive ideal by (a, b). This also indicates 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. An integer m is *represented* by a form $f(x, y)$ if the equation

$$m = f(x, y)$$

has an integer solution in x and y. If x and y are relatively prime, we say that m is *properly represented* by $f(x, y)$.

1.2. **A brief survey of cryptosystems based on imaginary quadratic orders.** Buchmann and Williams initiated the exploration of cryptography centered on class groups of imaginary quadratic orders, as outlined in their work [7]. After a prolonged period without apparent real-world applications, Lipmaa proposed the utilization of these techniques to construct secure accumulators without a trusted setup [8]. This approach leverages the *unknown order* property of class groups of imaginary quadratic fields. In recent years, we have witnessed the application of this unknown order property as a foundation for developing Verifiable Delay Functions (VDF) [9, 10], cryptographic accumulators, and vector commitments tailored for blockchain applications [11]. Additionally, polynomial commitments based on this property have been employed in zero-knowledge proofs [12].

It's important to note that, alongside the primary exploration of *maximal order* in cryptography, there is concurrent progress in cryptographic analysis focusing on *non-maximal orders*.

For example, at EUROCRYPT 2009, Castagnos and Laguillaumie [13] presented a breakthrough in cryptographic analysis, unveiling a polynomial time chosen-plaintext total break of the NICE family of cryptosystems [14, 15, 16]. This pivotal work not only marked a significant advancement but also introduced a constructive technique that influenced subsequent research. Building on this foundation, Castagnos and Laguillaumie continued their innovative contributions in CT-RSA 2015, where they introduced a novel linearly homomorphic encryption scheme [17], operating within the class group of a *non-maximal order of an imaginary quadratic field*. Continuing this line of research, at ASIACRYPT 2018, Castagnos, Laguillaumie, and Tucker addressed practical challenges in achieving secure inner product functional encryption modulo p, exploring schemes based on standard assumptions like DDH and Learning-with-Errors (LWE) [18]. In CRYPTO 2019, Castagnos, Catalano, Laguillaumie, Savasta, and Tucker shifted their focus to distributed variants of the ECDSA digital signature standard, introducing a method

for achieving simulation-based security without non-standard interactive assumptions [19]. Lastly, in Advances in Cryptology - CRYPTO 2022, Abram, Damgård, Orlandi, and Scholl presented collaborative work on a group-theoretic framework for secure computation tools, unifying approaches based on number-theoretic assumptions like DDH, Decision Composite Residuosity (DCR), and Quadratic Residuosity (QR) [20].

2. The algorithm

Our algorithm is based on the two following theorems of Dedekind, as presented in [6].

Theorem 2.1. *If at least one of the two natural numbers $a, b > 1$, and ab is not divisible by the square of any natural prime number, further, let $k = 3ab$ or ab, depending on whether $(a^2–b^2)$ is indivisible or divisible by 9, then the number of all non-equivalent, positive, primitive binary quadratic forms $(A, \frac{1}{2}B, C)$ of the discriminant $B^2–4AC = D = -3k^2$ is always a multiple of 3 $(3k'')$, and one-third of the form classes represented by these forms constitute a composition group $\mathfrak{K}$, characterized by the following property: Let p be any natural prime number congruent to 1 $\pmod 3$ and not dividing D, then, through the k'' forms of the group $\mathfrak{K}$, all and only those prime numbers p can be represented for which ab^2, and hence a^2b, is a cubic residue, while through the forms of the remaining $2k''$ classes, all and only those prime numbers p can be represented for which ab^2 is a cubic non-residue.*

Theorem 2.2. *If D denotes the fundamental number of a cubic body K, then the number of classes into which the original binary quadratic forms decompose from the discriminant D is a multiple of 3, and one-third of these classes forms a composition group characterized by the following property: If p is any natural prime not dividing D, of which D is a quadratic residue, then p in the body K is divisible by three different prime ideals or is itself a prime number, depending on whether p is representable by a form of the group or not.*

In the paper [6], Dedekind makes reference to an unpublished note by Gauss. This note contains the same example that we previously cited from Shanks [5, §8]:

A very elegant observation made by induction.
2 is a cubic residue or non-residue of the prime number p in the form $3n + 1$, depending on whether p is representable by the form

$$xx + 27yy$$

or $4xx + 2xy + 7yy$
3 is a residue or non-residue, depending on whether p is representable by
$xx + 243yy$ *or* $4xx + 2xy + 61yy$
$7xx + 6xy + 36yy$ *or* $9xx + 6xy + 28yy$

...

.

In the upcoming part, we will demonstrate how to efficiently leverage Theorem 2.1 to break the Decisional Diffie-Hellman (DDH) problem for totally non-maximal imaginary quadratic orders with $\Delta_1 = 3$. This holds true even in cases

where the factorization of f—and hence $h(Cl(\Delta_f))$ (namely, the order of this group)—is unknown. Our approach relies solely on the availability of knowledge regarding a single factor of f. In the remainder of the paper, we will refer to the composition group $\mathfrak{K}$ of Theorem 2.1 as the *principal 3 genus*, and $\chi : Cl(\Delta_f) \to \pm 1$ will act as a distinguisher. The character χ corresponds to the single known factor of f (denoted as a in Theorem 2.1), and it can be efficiently computed.

Computing the character χ. Let $\Delta_f = -3f^2$ with $f = 3ab$ or ab, depending on whether $(a^2 - b^2)$ is indivisible or divisible by 9. With the factorization of b being unknown, the character χ is defined as:

$$\chi : (\mathbb{Z}/\Delta_{\mathcal{O}_f})^* \to \{\pm 1\} : [\mathfrak{r}] \mapsto \left(\frac{a}{p}\right)_3$$

where $\left(\frac{\cdot}{\cdot}\right)_3$ denotes the cubic residue symbol. Here, p is a prime number such that $p \equiv 1 \pmod 3$ and not dividing Δ_f, represented by the class $[\mathfrak{r}]$. The ideals $\mathfrak{r}$ for which $\chi(\mathfrak{r}) = 1$ for the genus character χ, constitute the *principal 3 genus*.

Impact on decisional Diffie–Hellman in totally non-maximal imaginary quadratic orders. It is evident that the character χ, which is non-trivial, can be employed to ascertain whether a quadruple (g, g^x, g^y, g^z) constitutes a genuine Diffie-Hellman sample for discriminants with the described shape. Indeed, if g is not in the *principal 3 genus* but g^{xy} is , then either g^x or g^y must also be. If the sample g^z is not a true Diffie-Hellman sample, this will be detected with a probability of 1/3.

Implementation. We implemented the attack in SageMath to demonstrate the correctness of the algorithm and prove its feasibility. The source code is freely available on GitHub at the following URL: `https://gist.github.com/asanso/6d0b5127512a94a64e83ad783144fb6c`.

Countermeasures. The simplest approach is to restrict to elements which are cubes, i.e., the *principal 3 genus*, as the character χ becomes trivial on $Cl(\mathcal{O})^3$. However, if we consider the standard countermeasure of working on the group of squares, i.e., the *principal genus*, we would need to work on $Cl(\mathcal{O})^6$.

3. Conclusions

In this paper, we introduced an algorithm designed to investigate the Decisional Diffie-Hellman assumption in non-prime, totally non-maximal imaginary quadratic orders. Our specific emphasis lies in cases where $\Delta_1 = 3$ and there is partial knowledge of f. We demonstrate that the classical countermeasure of working in the group of squares, i.e., the *principal genus*, is not effective in addressing the identified issues. While this advancement poses a challenge to the security of DDH-dependent cryptographic protocols in these specific contexts, it's crucial to recognize that additional enhancements in this particular direction might be unlikely. Future work could, therefore, pivot towards exploring alternative approaches or extending the algorithm's applicability to related cryptographic challenges.

Acknowledgments. We would like to thank Karim Belabas, Guilhem Castagnos, Luca De Feo, Péter Kutas, Simon-Philipp Merz and Benjamin Wesolowski for fruitful discussions.

References

[1] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional diffie-hellman problem for class group actions using genus theory. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 92–120, Cham, 2020. Springer International Publishing.

[2] Wouter Castryck, Marc Houben, Frederik Vercauteren, and Benjamin Wesolowski. On the decisional Diffie-Hellman problem for class group actions on oriented elliptic curves. In *Fifteenth Algorithmic Number Theory Symposium, ANTS-XV*, Fifteenth Algorithmic Number Theory Symposium, ANTS-XV, Bristol, United Kingdom, August 2022. 18 pp.

[3] Detlef Hühnlein and Tsuyoshi Takagi. Reducing logarithms in totally non-maximal imaginary quadratic orders to logarithms in finite fields. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *Advances in Cryptology - ASIACRYPT'99*, pages 219–231, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[4] Detlef Hühnlein, Michael Jacobson, Jr, and Damian Weber. Towards practical non-interactive public-key cryptosystems using non-maximal imaginary quadratic orders. *Designs Codes and Cryptography*, 30:281–299, 11 2003.

[5] D. Shanks. Class number, a theory of factorization, and genera. In *Proceedings of Symposia in Pure Mathematics*, 1971.

[6] R. Dedekind. Ueber die anzahl der idealklassen in reinen kubischen zahlkörpern. *Journal für die reine und angewandte Mathematik*, 121:40–123, 1900.

[7] Johannes Buchmann and Hugh C. Williams. A key-exchange system based on imaginary quadratic fields. *J. Cryptology*, 1:107–118, 1988.

[8] Helger Lipmaa. Secure accumulators from euclidean rings without trusted setup. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *Applied Cryptography and Network Security - 10th International Conference, ACNS 2012, Singapore, June 26-29, 2012. Proceedings*, volume 7341 of *Lecture Notes in Computer Science*, pages 224–240. Springer, 2012.

[9] Benjamin Wesolowski. Efficient verifiable delay functions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 379–407, Cham, 2019. Springer International Publishing.

[10] K. Pietrzak. Simple verifiable delay functions. *Cryptology ePrint Archive, Report 2018/627*, 2018.

[11] Dan Boneh, Benedikt Bünz, and Ben Fisch. Batching techniques for accumulators with applications to iops and stateless blockchains. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 561–586, Cham, 2019. Springer International Publishing.

[12] Benedikt Bünz, Ben Fisch, and Alan Szepieniec. Transparent snarks from dark compilers. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 677–706, Cham, 2020. Springer International Publishing.

[13] Guilhem Castagnos and Fabien Laguillaumie. On the security of cryptosystems with quadratic decryption: The nicest cryptanalysis. In Antoine Joux, editor, *Advances in Cryptology - EUROCRYPT 2009*, pages 260–277, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[14] Michael Hartmann, Sachar Paulus, and Tsuyoshi Takagi. Nice - new ideal coset encryption -. In Çetin K. Koç and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems*, pages 328–339, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[15] Sachar Paulus and Tsuyoshi Takagi. 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*, pages 211–220. Korea Institute of Information Security and Cryptology (KIISC), 1998.

[16] Sachar Paulus and Tsuyoshi Takagi. A new public-key cryptosystem over a quadratic order with quadratic decryption time. *J. Cryptol.*, 13(2):263–272, 2000.

[17] Guilhem Castagnos and Fabien Laguillaumie. Linearly homomorphic encryption from ddh. In Kaisa Nyberg, editor, *Topics in Cryptology — CT-RSA 2015*, pages 487–505, Cham, 2015. Springer International Publishing.

[18] Guilhem Castagnos, Fabien Laguillaumie, and Ida Tucker. Practical fully secure unrestricted inner product functional encryption modulo p. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 733–764, Cham, 2018. Springer International Publishing.

[19] Guilhem Castagnos, Dario Catalano, Fabien Laguillaumie, Federico Savasta, and Ida Tucker. Two-party ecdsa from hash proof systems and efficient instantiations. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 191–221, Cham, 2019. Springer International Publishing.

[20] Damiano Abram, Ivan Damgård, Claudio Orlandi, and Peter Scholl. An algebraic framework for silent preprocessing with trustless setup and active security. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 421–452, Cham, 2022. Springer Nature Switzerland.

[21] David A. Cox. *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.