On the discrete logarithm problem in the ideal class group of multiquadratic fields

Semyon Novoselov

Immanuel Kant Baltic Federal University

LatinCrypt'23

Content

Definitions

Multiquadratic field:

$$K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$$

Class group Cl_K:

- quotient of fractional ideals modulo principal ideals
- $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ is a set of prime ideals that generates Cl_K
- $\mathrm{Cl}_K \simeq \langle \mathfrak{g}_1 \rangle \times \ldots \times \langle \mathfrak{g}_k \rangle$

Discrete logarithm problem (DLP) in Cl_K:

Given an ideal I, find integers $\ell_1, \ldots, \ell_k$ s.t. $[I] = [\mathfrak{g}_1^{\ell_1} \cdot \ldots \cdot \mathfrak{g}_k^{\ell_k}]$.

Note: DLP for $I = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$ is simple.

Motivation

Lattice-based crypto: ideals of number fields is a source of structured lattices.

Basic problem: find short vectors in such lattices.

- efficient algorithm $\Longrightarrow$ broken scheme

[BBVLvV'17]: short vectors in principal ideals (SPIP) of multiquadratic fields in quasi-polynomial time

Our ultimate goal: finding short vectors in ***non-principal*** ideals of multiquadratic field.

Finding short vectors in non-principal ideals

Approach of [CDW'21] and [BLNR'22] for cyclotomics (*Sketch*):

1. Compute DLOG for a target ideal
2. Find short basis for the $\log$-S-unit lattice (Stickelberger ideal + tricks)
3. Reduce result of DLOG computation:
   - using $\log$-S-unit lattice and its short basis (Babai's alg.)
   - using $\log$-unit lattice (SPIP)

In this work we consider first step for multiquadratic fields.

Prior work

[BD'91]: algorithm for any number field, complexity: $L_{\Delta_K}(1/2)$[1]

[BEFHY'22]: CDW-algorithm for number fields with norm relations

- ineffective (in general case) since it uses random walks
- short bases description is missing for non-cyclotomics
- complexity analysis is given only for cyclotomics

Our work: DLOG computation based on Pohlig-Hellman approach with complexity estimates.

[1] $L_x(\alpha) = e^{(\log x)^{\alpha}(\log \log x)^{1-\alpha}}$

Reducing the problem to subfields

Multiquadratic fields admit norm relation:

$$I^2 = \frac{I_\sigma \cdot I_\tau}{\sigma(I_{\sigma\tau})} = \frac{N_{K/K_\sigma}(I) \cdot N_{K/K_\tau}(I)}{\sigma(N_{K/K_{\sigma\tau}}(I))}$$

where σ, τ are order 2 automorphisms, and K_σ, K_τ, $K_{\sigma\tau}$ are fixed fields.

$$\Downarrow$$

1. Find DLOGs for I_σ, I_τ, $I_{\sigma\tau}$ in subfields $K_\sigma, K_\tau, K_{\sigma\tau}$
2. Combine this data to obtain DLOG for I^2:

$$I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$$

3. Compute square root of $\alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$ that is equal to I.

Square root of decomposed ideal

Problem:

Given an ideal I and $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$ find α' and $f_1, \ldots, f_d$ s.t. $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$.

Idea: reduce the problem to cyclic subgroups of

$$\mathrm{Cl}_K \simeq \langle \mathfrak{g}_1 \rangle \times \ldots \times \langle \mathfrak{g}_k \rangle \simeq C_{b_1} \times \ldots \times C_{b_k}.$$

- This gives us multiple square roots (up to 2^k).
- Use saturation technique to efficiently select correct square root.

Note: We assume that $\alpha\mathcal{O}_K \neq \prod_{i=1}^{d} \mathfrak{p}_i^{a_i}$, otherwise the problem is trivial.

Saturation technique

FindSquare: Allows us, for a given set $T = \{a_1, \ldots, a_m\} \subset K$ and an element $h \in K$, to find efficiently the set of exponent vectors $\vec{e}$ such that $h \cdot a_1^{e_1} \cdot \ldots \cdot a_m^{e_m}$ is a square.

- described and used for multiquadratics in prior work
- based on quadratic characters computation

Example: Let $I = h\mathcal{O}_K$ and T is a set of generators of $\mathcal{O}_K^{\times}$. Then

$$\sqrt{I} = \sqrt{h \cdot a_1^{e_1} \cdot \ldots \cdot a_m^{e_m}}\mathcal{O}_K$$

Square roots in cyclic groups

TLDR. Taking square roots is simple since we know the generators.

Consider finding square root of $\mathfrak{g}^e$ in cyclic group $\langle \mathfrak{g} \rangle$ of order b.

CycSqrt:

1. If b is odd then square root is $\mathfrak{g}^{e(\frac{\mathrm{b}+1}{2})}$.
2. Let $\mathrm{b} = 2^{\mathrm{r}} \cdot \mathrm{t}$ where t is odd. Then

$$\sqrt{\mathfrak{g}^e} \in \{\mathfrak{h}, \mathfrak{h} \cdot \mathfrak{g}^{\frac{\mathrm{b}}{2}}\},$$

where $\mathfrak{h} = \mathfrak{g}^{e(\frac{\mathrm{t}+1}{2})} \cdot (\mathfrak{g}^{\mathrm{t}})^{-\frac{\ell}{2}}$ for $\ell = \mathrm{DLOG}_{\mathfrak{g}^{\mathrm{t}}}(\mathfrak{g}^{\mathrm{t} \cdot e})$.
Since $\# \langle \mathfrak{g}^{\mathrm{t}} \rangle = 2^{\mathrm{r}}$ computing the DLOG is simple.

* Carl Pomerance. Elementary thoughts on discrete logarithms. `https://math.dartmouth.edu/~carlp/PDF/dltalk4.pdf`

Applying CycSqrt to our ideal

$$I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} \Rightarrow [I^2] = [\prod_{i=1}^{d} \mathfrak{p}_i^{e_i}] = [\prod_{j=1}^{k} \mathfrak{g}_j^{g_j}]$$

$\Downarrow$ **CycSqrt** $\Downarrow$

$$[I^2] = [\prod_{j=1}^{k} (\mathfrak{a}_j^{x_j} \mathfrak{b}_j)^2], x_j \in \mathbb{F}_2.$$

Then we have

$$I^2 = \frac{\alpha\beta}{\prod_{j=1}^{k} \alpha_j^{x_j}} \prod_{j=1}^{k} (\mathfrak{a}_j^{x_j} \mathfrak{b}_j)^2,$$

where $\mathfrak{a}_j^2 = \langle \alpha_j \rangle$ and $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} / \prod_{j=1}^{k} \mathfrak{b}_j^2 = \langle \beta \rangle$.

Now, we can write the ideal I as

$$I = \sqrt{\frac{\alpha\beta u}{\prod_{j=1}^{k} \alpha_j^{x_j}} \prod_{j=1}^{k} \mathfrak{a}_j^{x_j} \mathfrak{b}_j}$$

for some $u \in \mathcal{O}_K^\times$ and any suitable set of x_j.

Problem: there are 2^k variants of x to enumerate.

Solution: apply the saturation technique (**FindSquare**).

Complete IdealSqrt algorithm

Input: An ideal $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

Output: The ideal $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

Complete IdealSqrt algorithm

Input: An ideal $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

Output: The ideal $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

1. Compute $\mathfrak{g}$ s.t. $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{k} \mathfrak{g}_j^{g_j}$

Complete IdealSqrt algorithm

Input: An ideal $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

Output: The ideal $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

1. Compute $\mathfrak{g}$ s.t. $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{k} \mathfrak{g}_j^{g_j}$
2. Compute $(\mathfrak{a}_j \mathfrak{b}_j, \mathfrak{b}_j) = \mathrm{CycSqrt}(\mathfrak{g}_j^{g_j})$ for all $j = 1, \ldots, k$

Complete IdealSqrt algorithm

Input: An ideal $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

Output: The ideal $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

1. Compute $\mathfrak{g}$ s.t. $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{k} \mathfrak{g}_j^{g_j}$
2. Compute $(\mathfrak{a}_j \mathfrak{b}_j, \mathfrak{b}_j) = \mathrm{CycSqrt}(\mathfrak{g}_j^{g_j})$ for all $j = 1, \ldots, k$
3. Compute $\beta \in K$, s.t. $\beta \mathcal{O}_K = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} / \prod_{j=1}^{k} \mathfrak{b}_j^2$
4. Compute $\alpha_j \in K$, s.t. $\alpha_j \mathcal{O}_K = \mathfrak{a}_j^2$

Complete IdealSqrt algorithm

Input: An ideal $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

Output: The ideal $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

1. Compute $\mathfrak{g}$ s.t. $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{k} \mathfrak{g}_j^{g_j}$
2. Compute $(\mathfrak{a}_j \mathfrak{b}_j, \mathfrak{b}_j) = \mathrm{CycSqrt}(\mathfrak{g}_j^{g_j})$ for all $j = 1, \ldots, k$
3. Compute $\beta \in K$, s.t. $\beta \mathcal{O}_K = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} / \prod_{j=1}^{k} \mathfrak{b}_j^2$
4. Compute $\alpha_j \in K$, s.t. $\alpha_j \mathcal{O}_K = \mathfrak{a}_j^2$
5. Compute generators $u_1, \ldots, u_r$ of $\mathcal{O}_K^\times$

Complete IdealSqrt algorithm

Input: An ideal $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

Output: The ideal $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

1. Compute $\mathfrak{g}$ s.t. $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{k} \mathfrak{g}_j^{g_j}$
2. Compute $(\mathfrak{a}_j \mathfrak{b}_j, \mathfrak{b}_j) = \mathrm{CycSqrt}(\mathfrak{g}_j^{g_j})$ for all $j = 1, \ldots, k$
3. Compute $\beta \in K$, s.t. $\beta \mathcal{O}_K = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} / \prod_{j=1}^{k} \mathfrak{b}_j^2$
4. Compute $\alpha_j \in K$, s.t. $\alpha_j \mathcal{O}_K = \mathfrak{a}_j^2$
5. Compute generators $u_1, \ldots, u_r$ of $\mathcal{O}_K^\times$
6. $x = \mathrm{FindSquare}(\alpha \cdot \beta, \alpha_1^{-1}, \ldots, \alpha_k^{-1}, u_1^{-1}, \ldots, u_r^{-1})$

Complete IdealSqrt algorithm

Input: An ideal $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

Output: The ideal $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

1. Compute $\mathfrak{g}$ s.t. $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{k} \mathfrak{g}_j^{g_j}$
2. Compute $(\mathfrak{a}_j \mathfrak{b}_j, \mathfrak{b}_j) = \mathrm{CycSqrt}(\mathfrak{g}_j^{g_j})$ for all $j = 1, \ldots, k$
3. Compute $\beta \in K$, s.t. $\beta \mathcal{O}_K = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} / \prod_{j=1}^{k} \mathfrak{b}_j^2$
4. Compute $\alpha_j \in K$, s.t. $\alpha_j \mathcal{O}_K = \mathfrak{a}_j^2$
5. Compute generators $u_1, \ldots, u_r$ of $\mathcal{O}_K^\times$
6. $x = \mathrm{FindSquare}(\alpha \cdot \beta, \alpha_1^{-1}, \ldots, \alpha_k^{-1}, u_1^{-1}, \ldots, u_r^{-1})$
7. Return $\sqrt{\frac{\alpha\beta}{\prod_{i=1}^{k} \alpha_i^{x_i} \prod_{i=1}^{r} u_i^{x_{i+k}}}} \prod_{j=1}^{k} \mathfrak{a}_j^{x_j} \mathfrak{b}_j$

Algorithm for DLOG

Input: an ideal I of multiquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$.

Output: the ideal I represented by a pair $(\alpha', f) \in K \times \mathbb{Z}^d$ such that $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$.

Algorithm for DLOG

Input: an ideal I of multiquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$.

Output: the ideal I represented by a pair $(\alpha', f) \in K \times \mathbb{Z}^d$ such that $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$.

1. **if** $[K : \mathbb{Q}] = 2$ **then** compute DLOG with Buchmann-Düllmann

Algorithm for DLOG

Input: an ideal I of multiquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$.

Output: the ideal I represented by a pair $(\alpha', f) \in K \times \mathbb{Z}^d$ such that $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$.

1. **if** $[K : \mathbb{Q}] = 2$ **then** compute DLOG with Buchmann-Düllmann
2. Select distinct $\sigma, \tau, \sigma\tau \in G_K$ of order 2
3. $I_\sigma = N_{K/K_\sigma}(I)$, $I_\tau = N_{K/K_\tau}(I)$, $I_{\sigma\tau} = N_{K/K_{\sigma\tau}}(I)$

Algorithm for DLOG

Input: an ideal I of multiquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$.

Output: the ideal I represented by a pair $(\alpha', f) \in K \times \mathbb{Z}^d$ such that $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$.

1. **if** $[K : \mathbb{Q}] = 2$ **then** compute DLOG with Buchmann-Düllmann
2. Select distinct $\sigma, \tau, \sigma\tau \in G_K$ of order 2
3. $I_\sigma = N_{K/K_\sigma}(I)$, $I_\tau = N_{K/K_\tau}(I)$, $I_{\sigma\tau} = N_{K/K_{\sigma\tau}}(I)$
4. $J_\sigma = \mathrm{mqCLDL}(I_\sigma, S_\sigma)$ for $S_\sigma = \{\mathfrak{p} \cap K_\sigma \mid \mathfrak{p} \in S\}$
5. $J_\tau = \mathrm{mqCLDL}(I_\tau, S_\tau)$ for $S_\tau = \{\mathfrak{p} \cap K_\tau \mid \mathfrak{p} \in S\}$
6. $J_{\sigma\tau} = \mathrm{mqCLDL}(I_{\sigma\tau}, S_{\sigma\tau})$ for $S_{\sigma\tau} = \{\mathfrak{p} \cap K_{\sigma\tau} \mid \mathfrak{p} \in S\}$

Algorithm for DLOG

Input: an ideal I of multiquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$.

Output: the ideal I represented by a pair $(\alpha', f) \in K \times \mathbb{Z}^d$ such that $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$.

1. **if** $[K : \mathbb{Q}] = 2$ **then** compute DLOG with Buchmann-Düllmann
2. Select distinct $\sigma, \tau, \sigma\tau \in G_K$ of order 2
3. $I_\sigma = N_{K/K_\sigma}(I)$, $I_\tau = N_{K/K_\tau}(I)$, $I_{\sigma\tau} = N_{K/K_{\sigma\tau}}(I)$
4. $J_\sigma = \mathrm{mqCLDL}(I_\sigma, S_\sigma)$ for $S_\sigma = \{\mathfrak{p} \cap K_\sigma \mid \mathfrak{p} \in S\}$
5. $J_\tau = \mathrm{mqCLDL}(I_\tau, S_\tau)$ for $S_\tau = \{\mathfrak{p} \cap K_\tau \mid \mathfrak{p} \in S\}$
6. $J_{\sigma\tau} = \mathrm{mqCLDL}(I_{\sigma\tau}, S_{\sigma\tau})$ for $S_{\sigma\tau} = \{\mathfrak{p} \cap K_{\sigma\tau} \mid \mathfrak{p} \in S\}$
7. $J = \mathrm{Lift}(J_\sigma) \cdot \mathrm{Lift}(J_\tau) / \mathrm{Lift}(\sigma(J_{\tau\sigma})) = \alpha \cdot \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = I^2$
8. Return $\mathrm{IdealSqrt}(J)$

Complexity

$$K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$$

- $D = d_1 \cdot \ldots \cdot d_n$ is the largest discriminant of quadratic subfield of K
- $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ is a set of all prime ideals generating the ideal class group Cl_K

Main theorem

Let I be an ideal of K and $m = \deg K$. Then computing exponents $f_1, \ldots, f_d$ such that $I = \alpha' \prod_i \mathfrak{p}_i^{f_i}$ for some $\alpha' \in K$ takes time

$$e^{\widetilde{\mathcal{O}}(\max(\log m, \sqrt{\log D}))}$$

field operations.

to be compared with: $L_{\Delta_K}(1/2) = e^{\widetilde{\mathcal{O}}(\sqrt{m \log D})}$

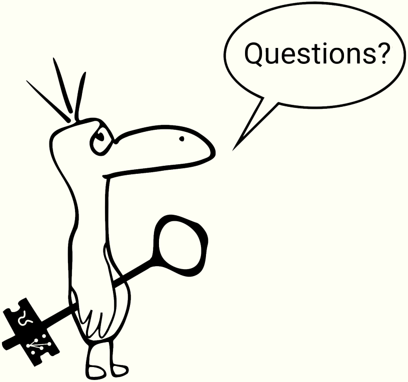
Experiments

Table 1: DLOG computation for multiquadratic fields.

$\deg K$	Field	Alg. 5	Sage	Cl_K
16	real	325	0.19	C_4^2
32	real	1607	64	$C_2 \times C_4 \times C_8^4$
64	real	4743	-	$C_2^9 \times C_4^3 \times C_8 \times C_{16}^4 \times C_{48} \times C_{240}$
16	imag.	159	0.41	$C_8 \times C_{48}$
32	imag.	1487	26	$C_2 \times C_4^3 \times C_{24} \times C_{48}^2 \times C_{3360}$
64	imag.	3941	-	$C_2^2 \times C_4^9 \times C_8^3 \times C_{16} \times C_{48} \times C_{96}^2 \times$
				$C_2^2 \times \times C_{192}^2 \times C_{6720}^2 \times C_{927360}$

* Timings are given in seconds.

- Implementation is made in SageMath v.10.0
- Computations were done on Intel Core i7-8700 clocked at 3.20GHz and 64 GB of RAM.



Contact

snovoselov@kantiana.ru

crypto-kantiana.com/semyon.novoselov

References

BD'91 Buchmann, J., Düllmann, S. «On the computation of discrete logarithms in class group»

BBVLvV'17 Bauch, J., Bernstein, D.J., Valence, H.d., Lange, T., van Vredendaal, C. «Short generators without quantum computers: the case of multiquadratics»

CDW'21 Cramer R., Ducas L., Wesolowski B. «Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time»

BLNR'22 Bernard, O., Lesavourey, A., Nguyen, T.H., Roux-Langlois, A. «Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP»

BEFHY'22 Biasse, J.F., Erukulangara, M.R., Fieker, C., Hofmann, T., Youmans, W. «Mildly Short Vectors in Ideals of Cyclotomic Fields Without Quantum Computers»