Solving Norm Equations

The SQISIGN  whose acronym represents Short Quaternion and Isogeny Signature is a post-quantum signature scheme based on isogenies of supersingular curves. Isogeny in mathematics refers to the special kind of map between two algebraic structures. An example is an algebraic curve that preserves the group structure and covers the entire target curve. This manuscript focuses on solving Norm equations quaternion orders and ideals. A quaternion is a mathematical object, essentially a set of four numbers, used to represent rotations in three-dimensional space. Additionally, quaternion defines the quotient of two vectors in a three-dimensional space. A quaternion algebra over a field is a central simple algebra of dimension 4 over . It is defined by two parameters and it is thus denoted as where the multiplication rules are:

. Quaternion algebras are generalizations of Hamilton’s quaternions. There are four-dimensional spaces generated by four elements and non-commutative algebras with the multiplication rules defined previously. A norm is a function from a real or complex vector space to the non-negative real numbers that behave in a certain way like the distance from the origin. Various kinds of norms include the equivalent norm, the absolute value norm, and the Euclidean norm.

The basis for this is that solving norm equations in quaternion orders has applications in cryptography. There are three KLPT-based procedures for solving norm equations which are ***KeyGenKLPT*** which is used within a key generation, ***SpecialEichlerNorm*** which solves a norm equation and ***SigningKLPT*** which solves a norm equation in the left -ideal which represents quaternion order. The left -ideal is a non-zero subset

**KeyGenKLPT Algorithm**: Given a left -ideal in a quaternion algebra , the KLPT algorithm finds an equivalent ideal of a smaller norm

Input: A left ideal where is a maximal order in the quaternion algebra .

Process: Find an equivalent ideal that has a smaller norm than The algorithm uses the reduction theory of quaternions to efficiently find by solving norm equations. Ensure that corresponds to an isogeny with a reasonable degree that makes further cryptographic computations feasible. Output: An equivalent ideal of a smaller norm.

The KLPT algorithm helps in minimizing computational overhead in constructing and verifying isogenies, making isogeny-based cryptographic schemes more practical.

**SpecialEichlerNorm Algorithm** explains the process of solving norm equations efficiently in any maximal order the idea behind the algorithm is to find , ) satisfies the constraints on the input of EichlerNorm so we can solve in 1) and then transport the output using the isomporphism between and 1.

**The SigningKLPT algorithm** is done by the generalized KLPT algorithm. The output of a SigningKLPT is of a constant degree. Some randomization is also included to ensure a good distribution.

The process of solving norm equations in quaternion orders and ideals can be seen in various algorithms which include Cornacchia’s algorithm, representing integers by special extremal order, and reduction to linear systems.

**Cornacchia’s algorithm** allows us to efficiently solve norm equations of the form

+ . The algorithm inputs which is an integer and gives a true or false value if a solution was found or not. The algorithm goes through a sequence of numbers to make sure is a prime if it is a prime, Cornacchia’s algorithm would run and return the value of x and y when found.

**Representing integers by special extremal order:** This is a follow-up from Cornacchia’s algorithm. The idea of this algorithm is to find elements in a given norm. This process allows us to solve norm equations in the sub-order where the quadratic substring of whose norm for is given by . The general form is to sample before using Cornacchia’s to see if we can find the following: . The algorithm returns a boolean if a solution was found.

**Reduction to linear systems:** This algorithm in this case can be found in EichlerModConstraint and FindLinearCombination. Both algorithms use linear algebra in / to find a quaterion of a special form. In EichlerModConstraint, we consider quaternion elements where as integer column vectors while in FindLinearCombination, we compute a basis <a1, a2, a3, a4> = and compute vectors .

The final step of solving norm equation can be seen in **Strong Approximation algorithm**. This algorithm solves norm equations inside . The algorithm finds the strong approximation mod N of some µ0 ∈ OjO. This algorithm takes in an input of a prime number two values, , the output is of the equation with μ0 μ1  which then returns a value of

The essence of solving norm equations and how these algorithms and equations are essential in cryptography is to provide for integrity and non-repudiation of cryptographic systems like in SQISIGN. Integrity provides us with the ability to make sure a message sent is a message received where nothing in the message changes. Non-repudiation provides us with the ability to verify whoever sends a digitally signed message cannot be in denial of the message coming from the person who sent it. Solving norm equations provides us with the ability to ensure that messages can be digitally secure and encoded which enhances the security of digital communications.

**Bibliography**

1. “Norm”. *Wikipedia,* <https://en.wikipedia.org/wiki/Norm_(mathematics)>
2. “Quaternion”. *Wikipedia,* <https://en.wikipedia.org/wiki/Quaternion>
3. DRP, Turkey. Salim Erdem Kocak “Isogeny Based Cryptography and KLPT Algorithm”. *YouTube,* uploaded by DRP Turkey, 5 Sept. 2024, <https://www.youtube.com/watch?v=vNc9svEBCf0&list=WL&index=1&t=751s>
4. Jorge Chavez-Saab, Maria Corte-Real Santos, Luca DeFeo, Jonathan Komada Eriksen, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Michael Meyer, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQISIGN (June 2023)
5. Leroux, Antonin. *Quaternion Algebras and Isogeny-Based Cryptography*. 6 Sept. 2022, <https://www.lix.polytechnique.fr/Labo/Antonin.LEROUX/manuscrit_these.pdf>