SQI$_{\text{SIGN}}$

Isogeny-Based Digital Signature Scheme

Osasere Imade
Abdul Mutallif
Anjiya Shrestha
Matthew Withee
Suresh Yhap

Midterm Research Paper
CS381/780 – Post Quantum Cryptography
Dr. Delaram Kahrobaei
Queens College, Fall 2024

Osasere Imade

Abdul Mutallif

Anjiya Shrestha

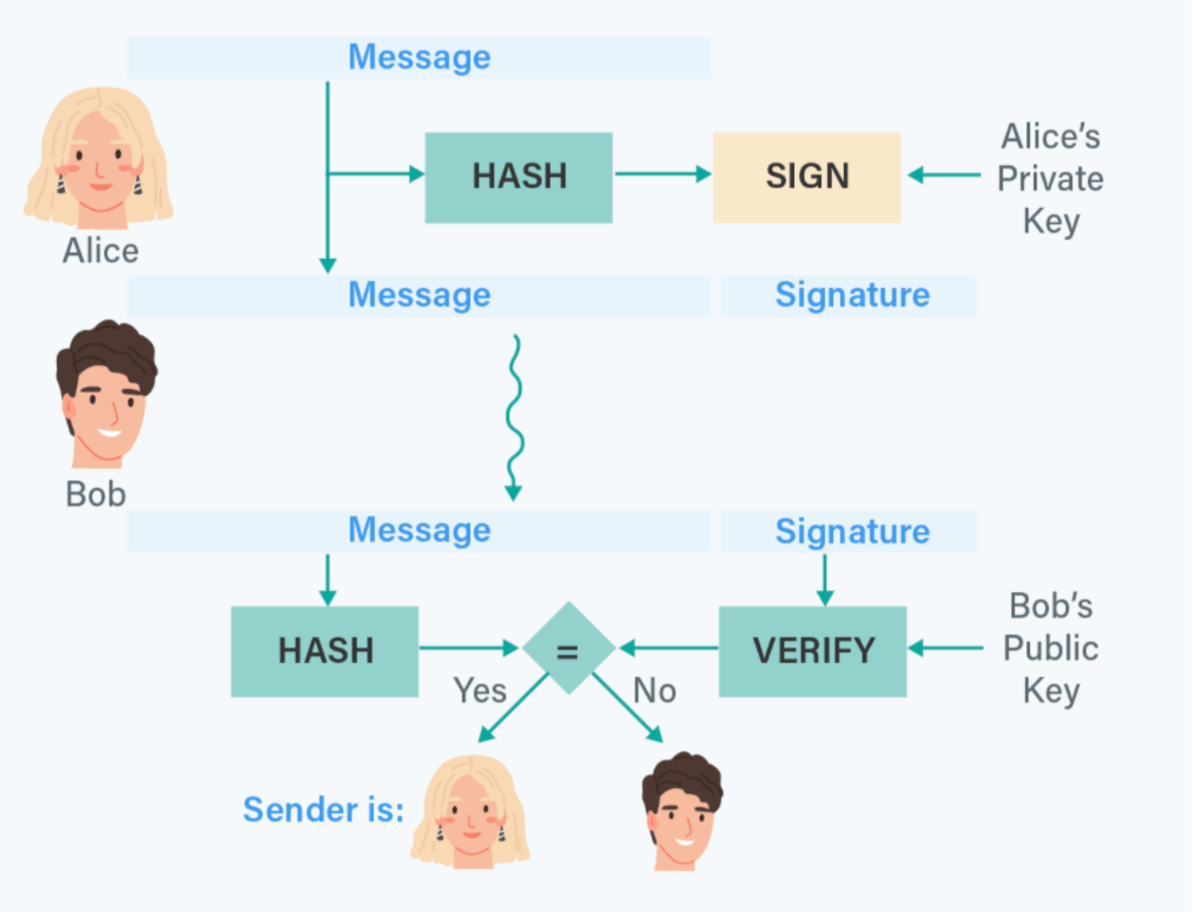
Matthew Withee

Suresh Yhap

Chapter 1

Introduction

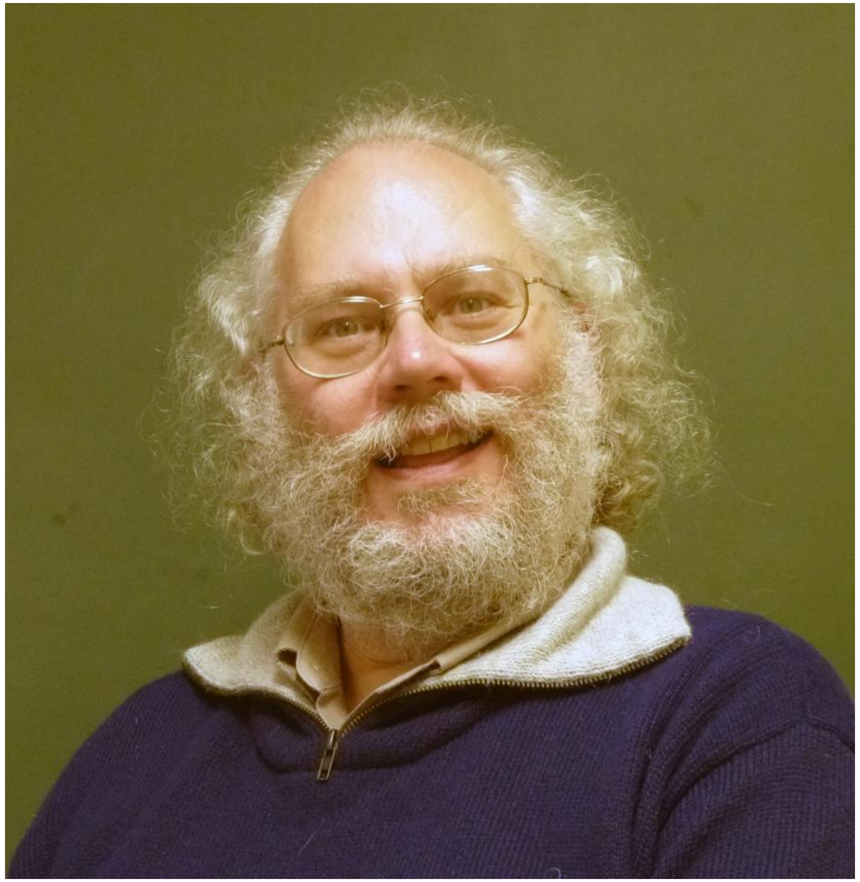
Digital Signature Review



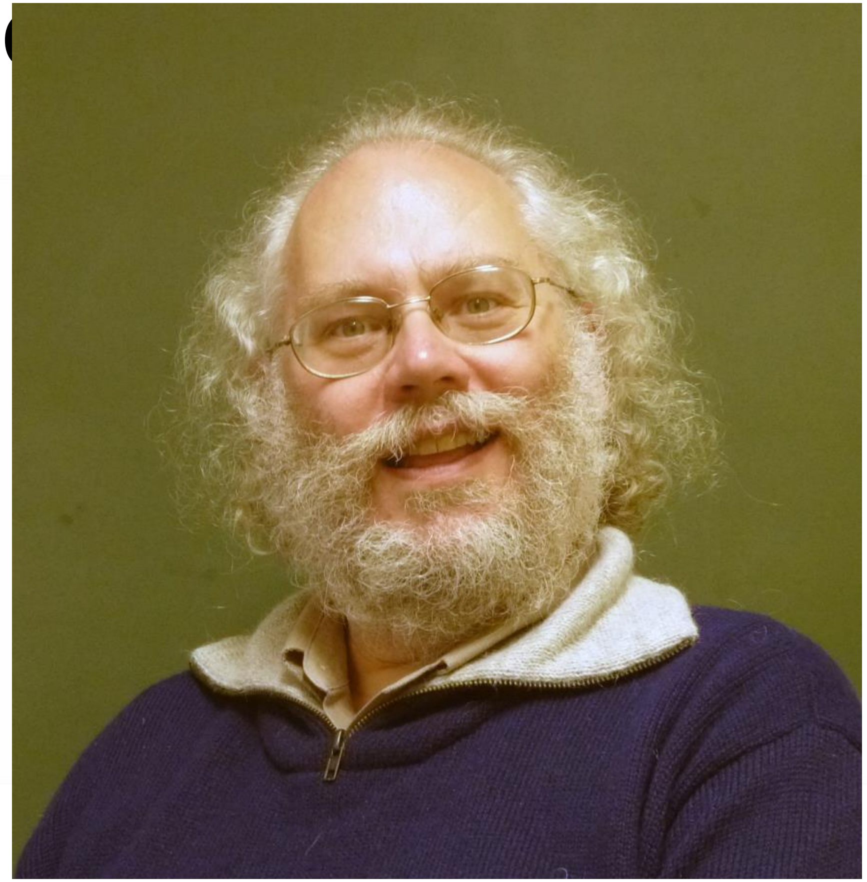
- Alice has a message to send to Bob
- Alice creates a hash of the message
- Alice signs the hash with her private key
- Alice sends Bob the message and signature
- Bob receives the message and signature
- Bob verifies the hash to ensure message integrity
- Bob verifies the signature to ensure the message came from Alice
- The message is received!

Traditional Digital Signature Schemes

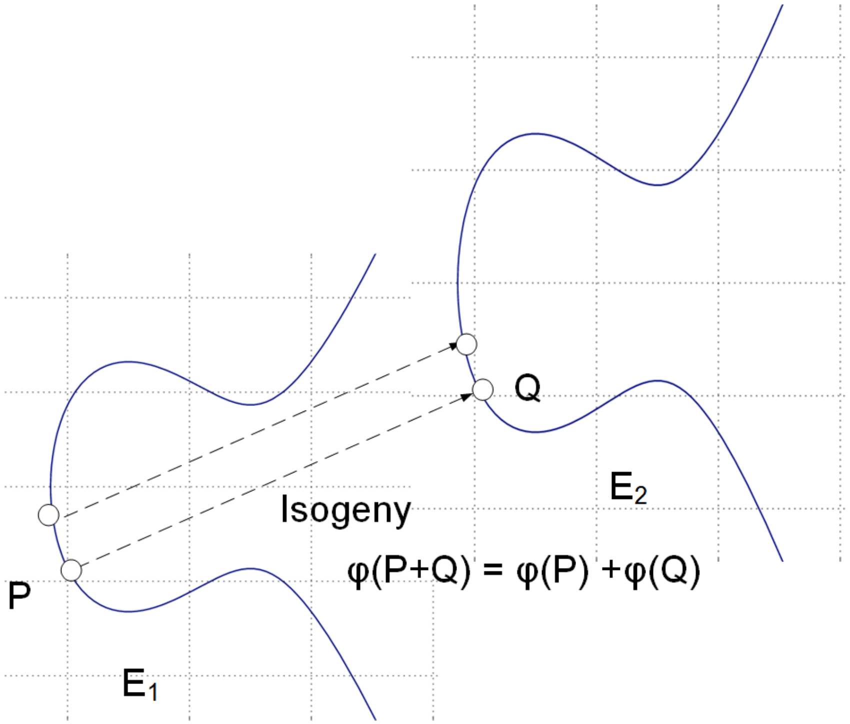
Rivest-Shamir-Adelman

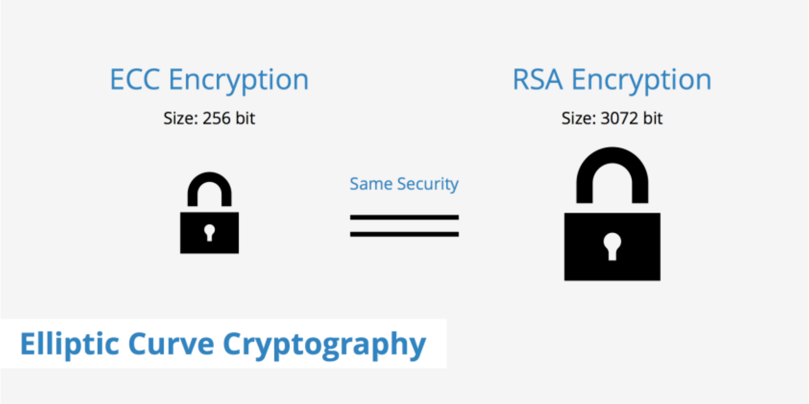


Elliptic Curve Cryptography (EC



Isogeny-Based Signature Schemes





- The “hard problem” is computing an isogeny
- The isogeny is Alice’s private key
- The destination is the public key

SQI$_{\text{SIGN}}$

- Short Quaternion Isogeny-Based Signature Scheme
- Uses supersingular elliptic curves
- The endomorphism ring of supersingular elliptic curves can be represented using quaternions.

Advantages & Disadvantages

Advantages

- Compact signature size
- No easy solution to problem
- Elegant

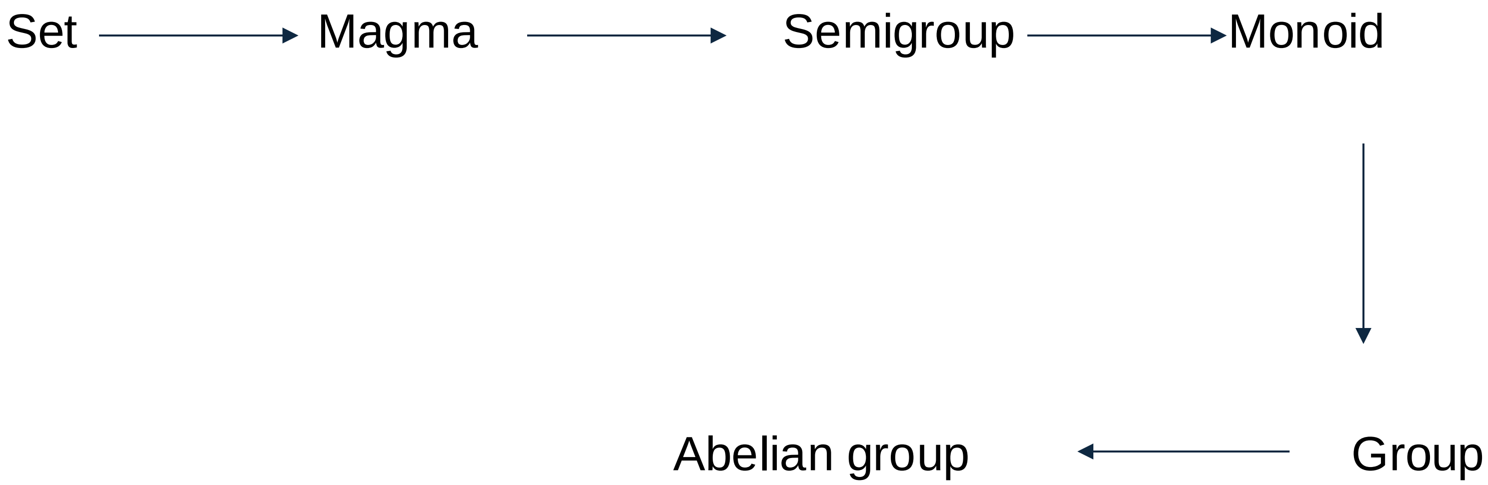
Disadvantages

- A lot of computational overhead
- Difficult to implement
- New field of study
- Potentially vulnerable

Chapter 2

Basic Operations

Abelian group



Set

Magma

Semigroup

Monoid

Group

Abelian group

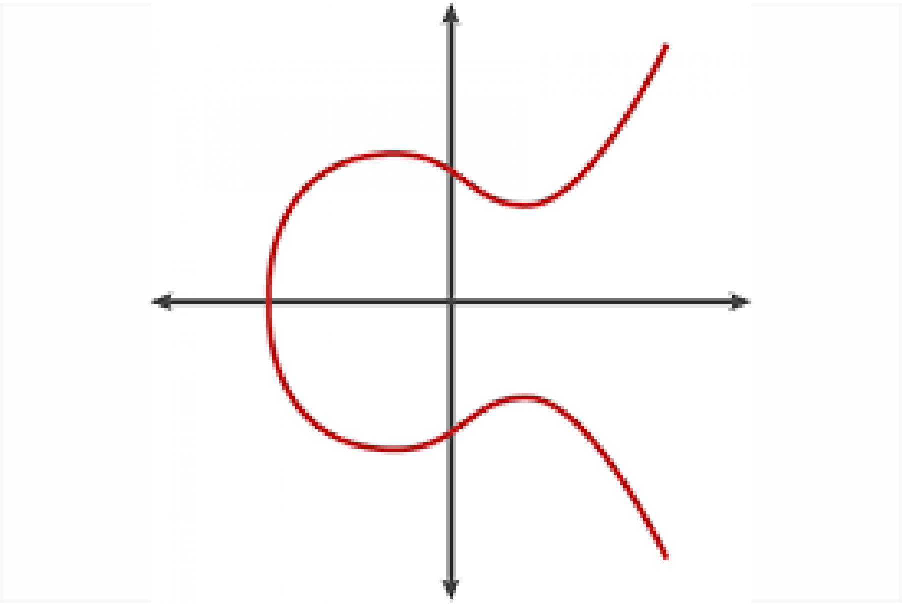
Field

$$\begin{tikzcd}
(S, +) \arrow[dr] & \\
a(b + c) = ab + ac \arrow[r] & (F, +, x) \\
(S \setminus \{0\}, x) \arrow[ur] &
\end{tikzcd}$$

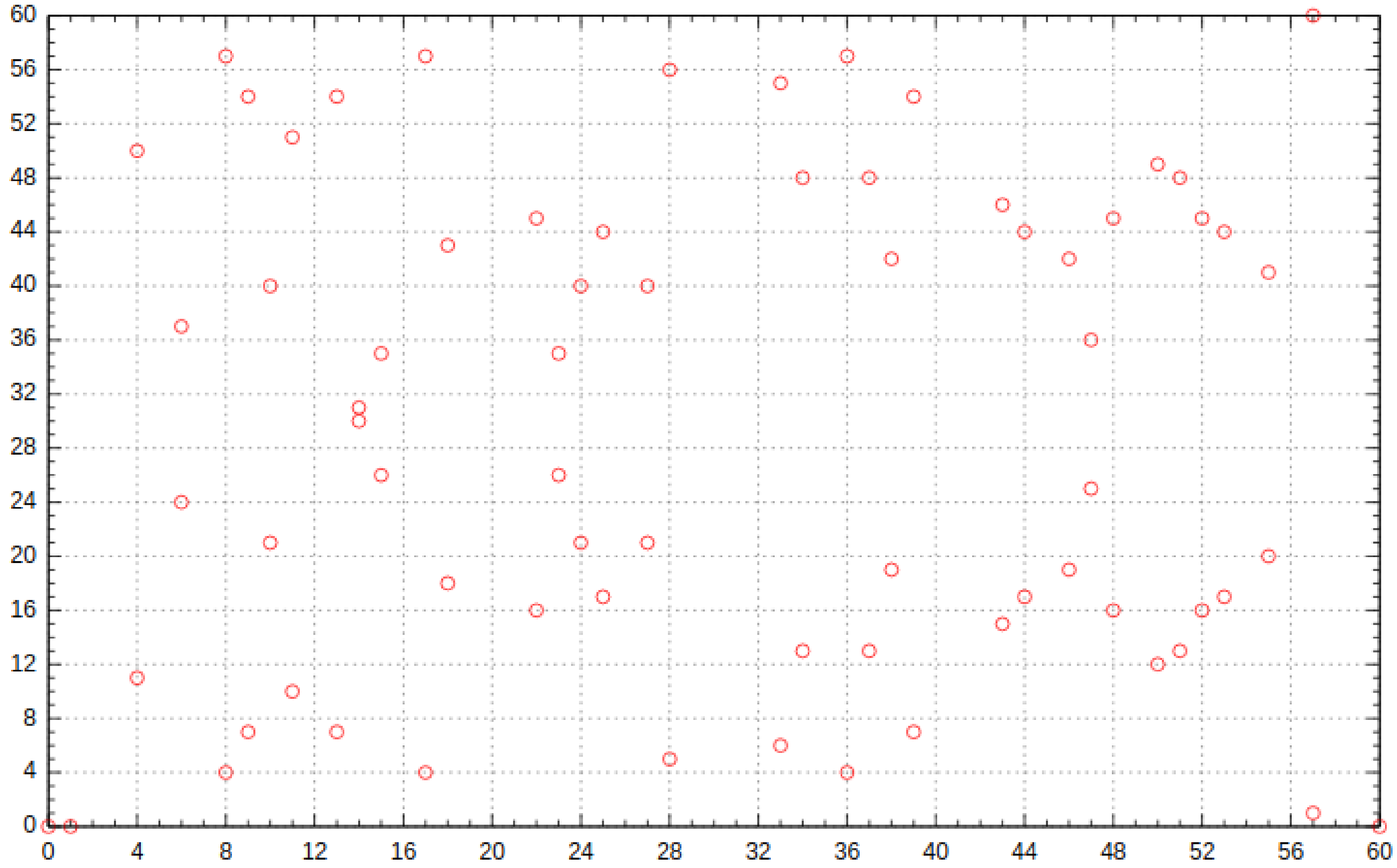
Section 2.2 - Elliptic Curves

- Montgomery elliptic curves are curves of the form: $By^2 = x^3 + Ax^2 + x$
- We also importantly consider a "point at infinity", ∞, to be part of the curve

Elliptic curve over the real numbers



An elliptic curve over the finite field, F_{61}



Group structure of elliptic curves

Collectively supplementing the points on the elliptic curve with a binary addition operation yields an abelian group!

Define the additive identity to be the point at infinity, ∞. So, for a point P on the elliptic curve, P + ∞ = ∞ + P = P.

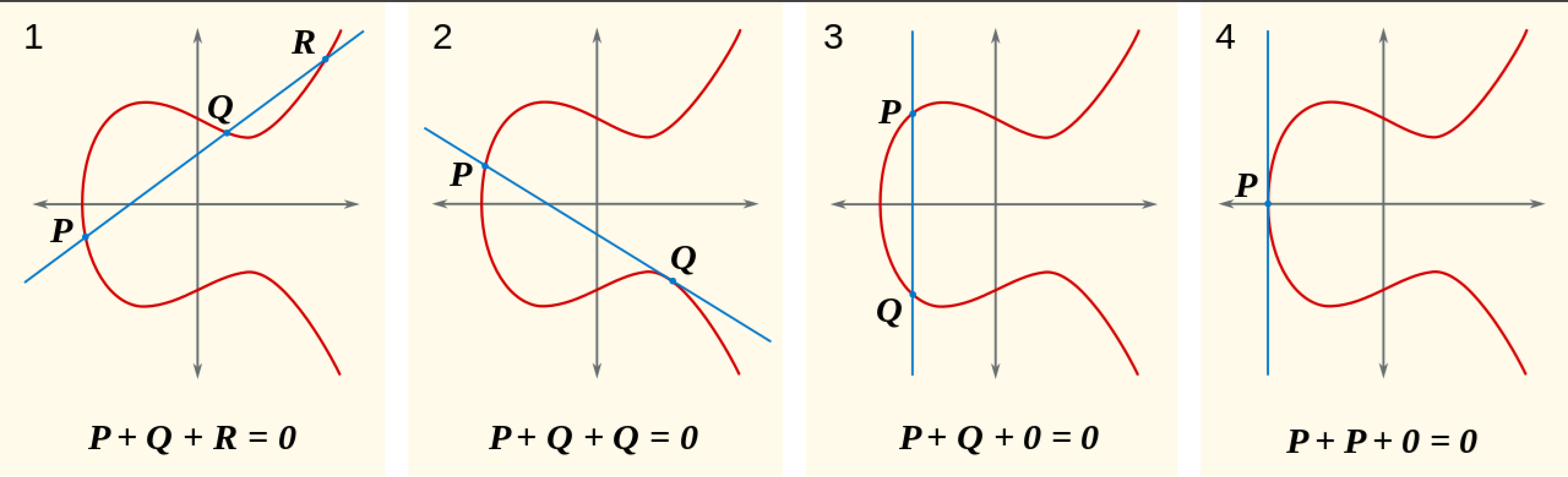
To add two points on the curve, draw a line of intersection through the points. The third point of intersection is defined as the negation of the sum of the points. This is because we define the sum of three points of intersection on a line as ∞.

To get the correct sum, reflect this point over the x-axis.

Note the third point may be ∞ if the line is vertical

Elliptic Curves

Point addition



1: $P + Q + R = 0$

2: $P + Q + Q = 0$

3: $P + Q + 0 = 0$

4: $P + P + 0 = 0$

ECClines by SuperManu. https://commons.wikimedia.org/wiki/File:ECClines.svg (partial). CC BY-SA 3.0.

Discrete logarithm problem

Scalar multiplication can be defined using repeated point doubling and addition

It is denoted: [k]P

Since we are dealing with repeated applications of an abelian group’s operation, we can naturally define a discrete log problem:

Given a point P and a scalar multiple [k]P, find k

Now knowing how “strangely” addition works and how unrelated the sum of points seem to the original points, you can imagine how difficult solving the discrete log problem will be for large k

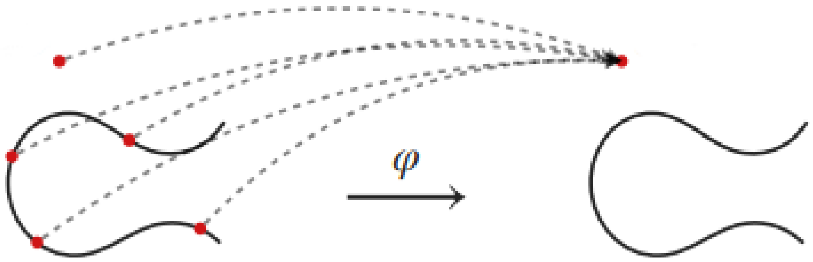
Isogenies

An isogeny φ of elliptic curves is a non-zero map E1 → E2 that is

- given by rational functions → φ(P + Q) = φ(P) + φ(Q)
- that is a group homomorphism → f(x, y) /g(x, y), where f , g are polynomials

Isogenies

- The property of being isogenous means that two curves have the same number of points when considered over the same field, F_q. This number is denoted by $\#E_1(F_q)$ and $\#E_2(F_q)$.
- An isogeny can be almost uniquely characterized by its kernel, i.e., the set ker(φ) = {P ∊ E | φ(P) = ∞} and an isogeny is uniquely defined by its kernel: {P ∊ E | φ(P) = $\mathcal{O}$. E′ }
- The degree of a (separable) isogeny is the size of its kernel.



Isogenies

Example: For each $m \neq 0$, the multiplication-by-m map

$$[m]:E \to E$$

is an isogeny from E to itself.

If $m \neq 0$ in the base field, its kernel is

$$E[m] \cong Z/m \times Z/m \; .$$

Thus, [m] is a degree-m^2 isogeny.

Isogenies

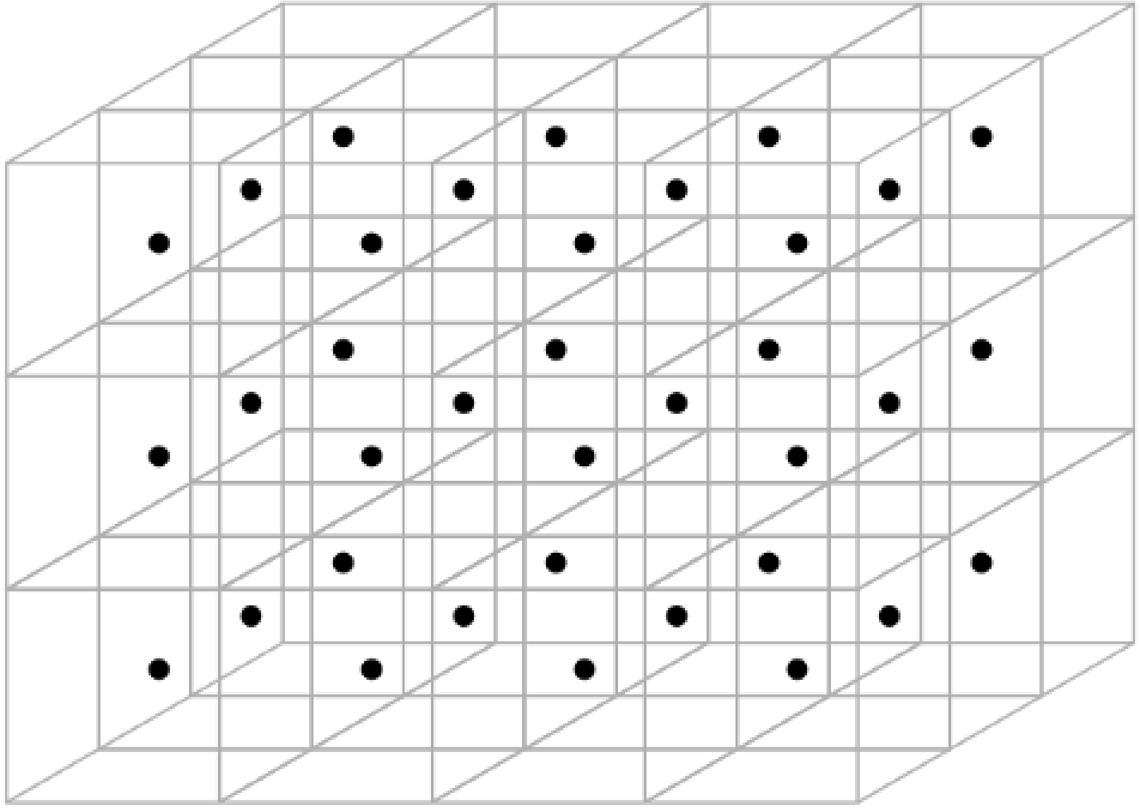
- Unique Isogeny: When given a subgroup (a smaller set that behaves like the larger group) G of points on E1, there is one specific way to create an isogeny from E1 to E2.

- If you know a subgroup G of E1 with size N, there is a unique isogeny of degree N with the subgroup G as its kernel, ker(φ) = G.

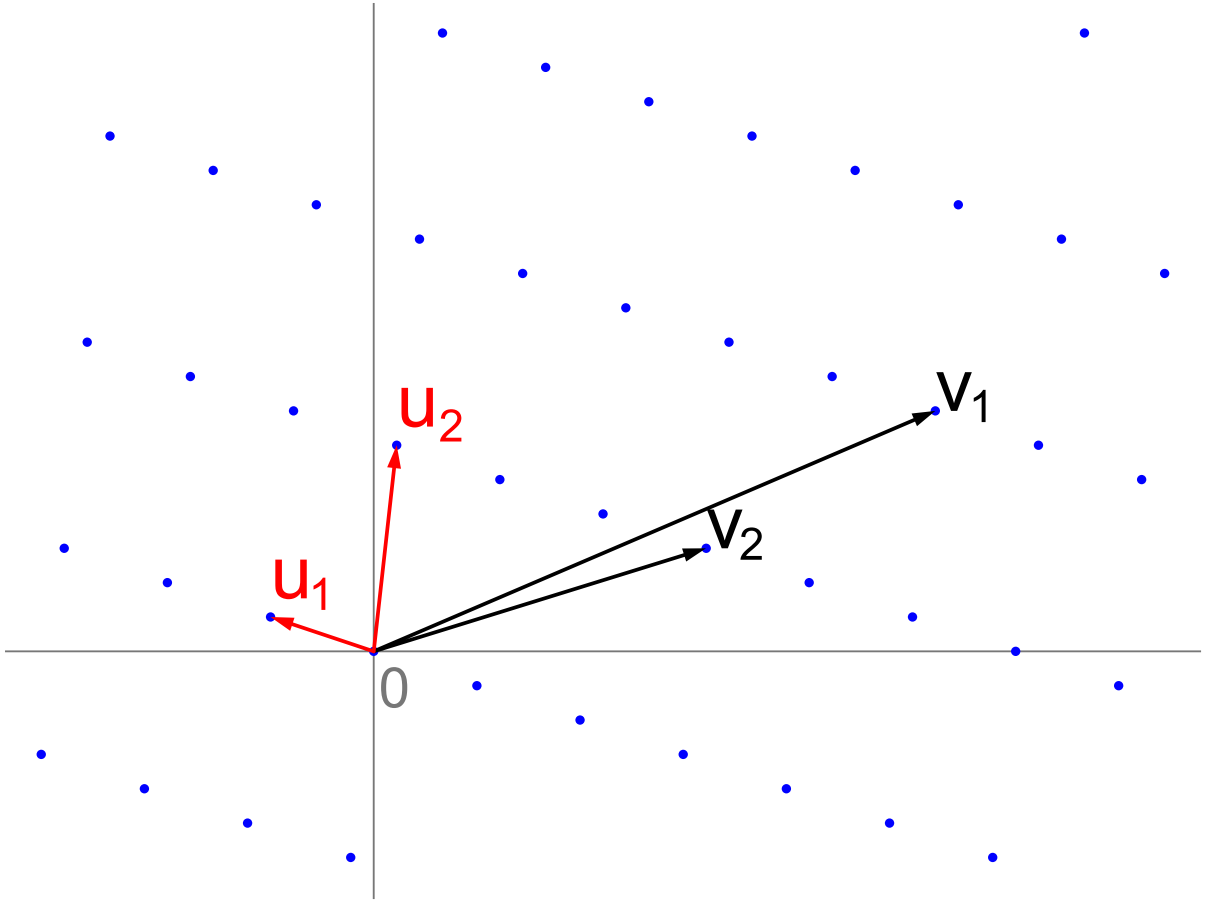
- Dual Isogeny: For every isogeny φ, there’s another isogeny that goes in the reverse direction, called the dual isogeny φ.

- Composition: When we combine the original isogeny and its dual, it’s similar to multiplying all points on E1 by a number N. This number is the same as the degree of the isogeny.

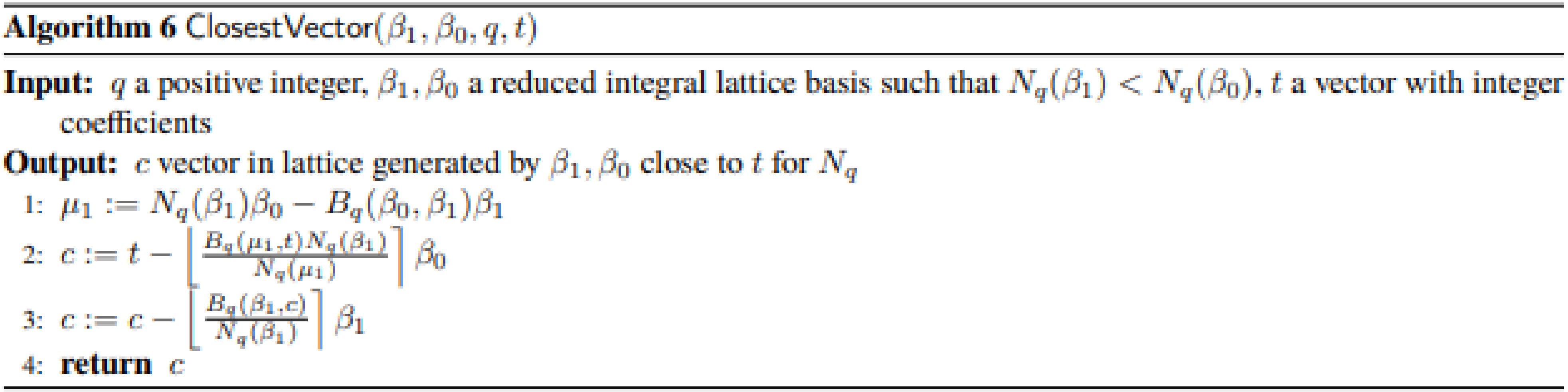
Introduction to Lattices and Cryptography



Lattice Basis Reduction: Short Basis Algorithm



Finding the Closest Vector



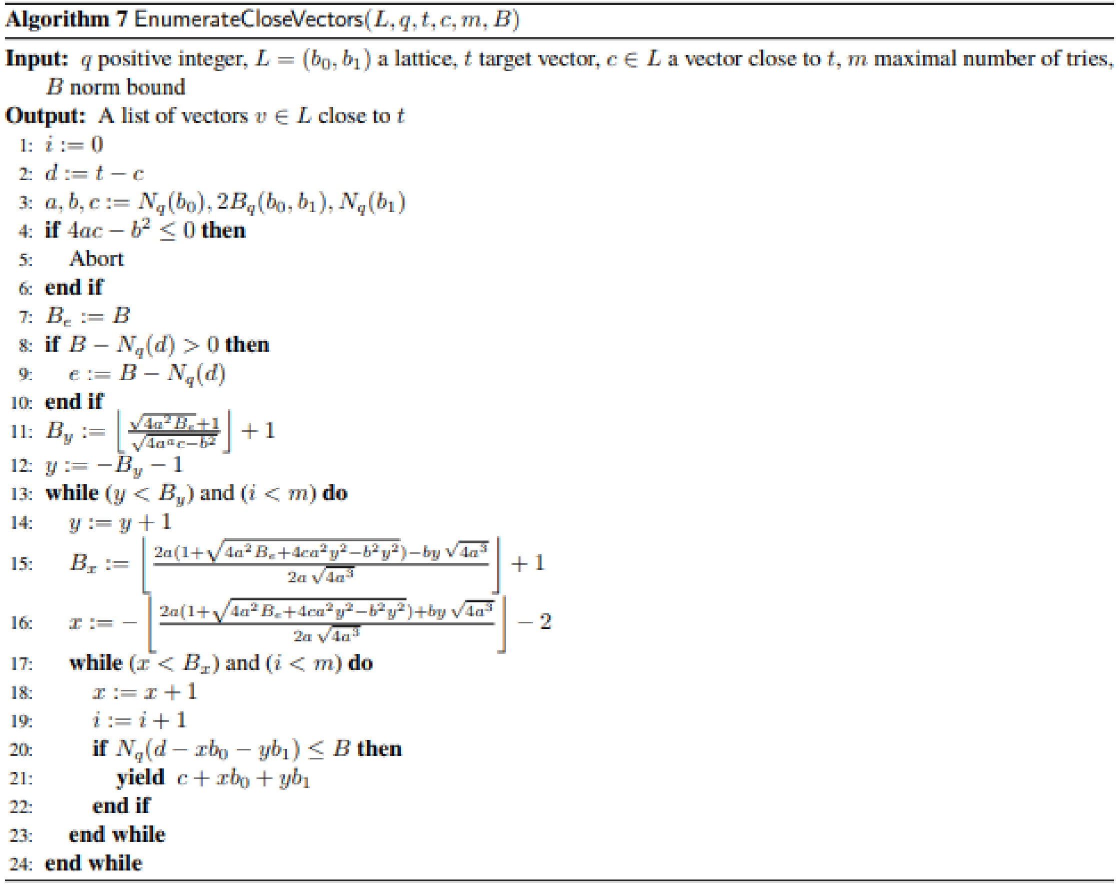
Algorithm 6 ClosestVector(β_1, β_0, q, t)

Input: q a positive integer, β_1, β_0 a reduced integral lattice basis such that $N_q(\beta_1) < N_q(\beta_0)$, t a vector with integer coefficients

Output: c vector in lattice generated by β_1, β_0 close to t for N_q

```
$\mu_1 := N_q(\beta_1)\beta_0 - B_q(\beta_0, \beta_1)\beta_1$
$c := t - \left\lfloor \frac{B_q(\mu_1,t)N_q(\beta_1)}{N_q(\mu_1)} \right\rceil \beta_0$
$c := c - \left\lfloor \frac{B_q(\beta_1,c)}{N_q(\beta_1)} \right\rceil \beta_1$
**return** $c$
```

Enumerating Close Vectors



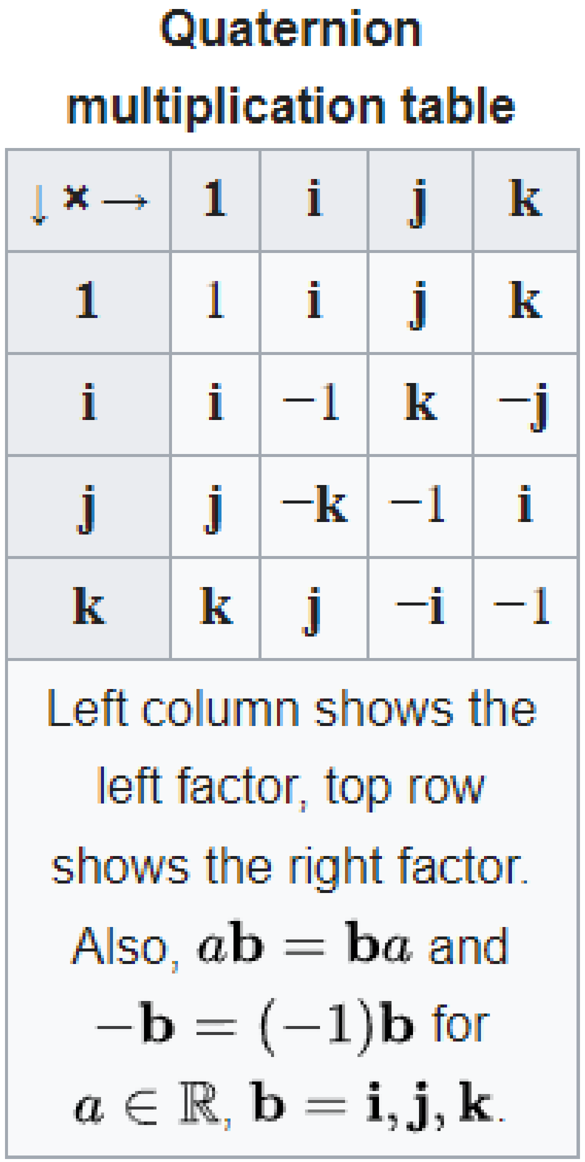
Algorithm 7 EnumerateCloseVectors(L, q, t, c, m, B)

Input: q positive integer, $L = (b_0, b_1)$ a lattice, t target vector, $c \in L$ a vector close to t, m maximal number of tries, B norm bound

Output: A list of vectors $v \in L$ close to t

```
$i := 0$
$d := t - c$
$a, b, c := N_q(b_0), 2B_q(b_0, b_1), N_q(b_1)$
if $4ac - b^2 \leq 0$ then
    Abort
end if
$B_e := B$
if $B - N_q(d) > 0$ then
    $e := B - N_q(d)$
end if
$B_y := \left\lfloor \frac{\sqrt{4a^2B_e}+1}{\sqrt{4a^a c-b^2}} \right\rfloor + 1$
$y := -B_y - 1$
while $(y < B_y)$ and $(i < m)$ do
    $y := y + 1$
    $B_x := \left\lfloor \frac{2a(1+\sqrt{4a^2B_e+4ca^2y^2-b^2y^2})-by\sqrt{4a^3}}{2a\sqrt{4a^3}} \right\rfloor + 1$
    $x := -\left\lfloor \frac{2a(1+\sqrt{4a^2B_e+4ca^2y^2-b^2y^2})+by\sqrt{4a^3}}{2a\sqrt{4a^3}} \right\rfloor - 2$
    while $(x < B_x)$ and $(i < m)$ do
        $x := x + 1$
        $i := i + 1$
        if $N_q(d - xb_0 - yb_1) \leq B$ then
            yield $c + xb_0 + yb_1$
        end if
    end while
end while
```

Quaternion Arithmetic and the Orders and Ideals



Quaternion multiplication table

↓ × →	$\mathbf{1}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{1}$	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	-1	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	-1	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	-1

Left column shows the left factor, top row shows the right factor. Also, $a\mathbf{b} = \mathbf{b}a$ and $-\mathbf{b} = (-1)\mathbf{b}$ for $a \in \mathbb{R}$, $\mathbf{b} = \mathbf{i}, \mathbf{j}, \mathbf{k}$.

Solving Norm Equations

Isogeny-Based Cryptography

Background

- The acronym $\mathrm{SQI}_{\mathrm{SIGN}}$ which stands for Short Quaternion and Isogeny Signature is a postquantum signature based on isogenies of super singular curves.
- A quaternion is a mathematical object, essentially a set of four numbers used to represent rotations in three dimensional spaces.
- A quaternion over a field k is defined by two parameters $a, b\ \in k$ and is thus denoted as:
  - $B = (\frac{a,b}{k}) = K + Ki + Kj + Kk$
- Quaternion algebras are generalization of Hamilton's quaternions. There are our-dimensional spaces generated by four elements $\{1, i, j, k\}$ and non-commutative algebras.

Key Concepts and Definitions

- Isogeny in mathematics refer to the special kind of map between two algebraic structures.
- 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. An example is:
  - Vectors can be arrows on a flat surface (for a 2D space) or in the air (for a 3D space). The norm of a vector can be compared to measuring the length of these arrows.
- There are various kinds of norms which include:
  1. The Equivalent norm
  2. The absolute value norm
  3. The Euclidean norm

Introduction to the Algorithm

- The basis for this is that solving norm equations in quaternion orders has its applications in cryptography.
- There are three KLPT-based procedures for solving norm equations which are:
  1. KenGenKLPT which is used within a key generation.
  2. SigningKLPT which solves a norm equation in the left O-ideal where O represents quaternion order.

Algorithm Process Overview

1. **<u>KeyGenKLPT Algorithm:</u>**

Input: A left ideal $I \subseteq O \, where \, O$ is a maximal order in the quaternion algebra

Output: An equivalent ideal J of a smaller norm

Key takeaway:

- The algorithm uses the reduction theory of quaternions to efficiently find J by solving norm equations.
- This algorithm enhances the security and performance of post-quantum cryptographic schemes.

Algorithm Process Overview

2. <u>The SigningKLPT algorithm:</u>

Input: K a left O-ideal

Output: A Boolean indicating a solution was found.

Key takeaway:

- This algorithm is done by the generalized KLPT algorithm.
- This algorithm generates digital signatures based on isogeny-based cryptography schemes ensuring security.

Algorithm Process Overview

The process of solving norm equations in quaternion orders and ideals can also be seen various algorithms which includes:

1. Cornacchia’s algorithm.
2. Representing Integers by smaller numbers.

Algorithm Process Overview

1. **The Cornacchia's algorithm**

Input: $m \in \mathbb{Z}$

Output: $x, y \; such \; that \; x^2 + y^2 = m$ found a Boolean indicating whether a solution was found.

Key takeaway:

- This algorithm allows us to efficiently solve norm equations of the form $x^2 + ny^2 = m$.
- This algorithm is used to solve Diophantine equations, which is essential for key generation and encryption processes in lattice-based and number theoretic cryptographic schemes.

Algorithm Process Overview

2. Representing Integers by Special Extremal Order

Input: $M \in \mathbb{Z}$ such that $M > p$

Output: found a Boolean indicating whether a solution was found.

Key takeaways:

- This algorithm is a follow up on the Cornacchia’s algorithm. The idea is to find elements in a given norm.
- This algorithm facilitates efficient computation and analysis in number theory and cryptography.
- This algorithm is utilized in cryptography for key generation, enabling the efficient construction of secure keys.

Conclusion

❖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 $\mathrm{SQI}_{\mathrm{SIGN}}$.

❖ 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.