Chapter 1: Introduction

As the promise of quantum computing draws closer and closer to reality, the safeguards in place today allowing society to protect itself in the digital realm are clearly becoming less sufficient. The rapidly emerging field of post-quantum cryptography has been building on the classical concepts and algorithms already in use while finding innovative new ways to defend against the threat of cyberattacks. Classical algorithms such as digital signature schemes are highly effective when used for defending against classical computers, but the computational power from a quantum attack would leave a huge amount of vulnerability, so innovations are required to prepare for the future. One such notable innovation in post-quantum cryptography consists of the development of an isogeny-based digital signature scheme. There are a few types of isogeny-based algorithms, but the one that will be discussed here is something called SQIsign, which stands for Supersingular Quaternion Isogeny-based Signature, a scheme where the digital signature is generated using isogenies between supersingular elliptical curves. This technique is gaining a lot of attention due to its efficiency in securing data while maintaining a compact signature size.

First, a brief review of digital signatures. A digital signature is a cryptography mechanism with three major security functions: authentication, integrity of information, and non-repudiation.

1. Authentication refers to the verification of the identity of the sender of information, achieved through the use of public key cryptography where the sender ‘signs’ a message with their private key and the message is then verified by the receiver using the sender’s public key.
2. The second function of a digital signature, integrity, refers to the process of ensuring that the message has not been altered in any way by an ‘in-between’ party.
3. Non-repudiation, the third security function of a digital signature, is a way to prove that someone actually sent the message, essentially ensuring that someone that sends a message can’t deny it later because they are the one that had the private key. These functions are the cornerstone of secure digital communication.

A digital signature is composed of two important mechanisms, a private key and a public key, both generated by the sender of the message, with the public key available for anyone that wants to view it.

Traditionally, the private and public keys are generated with algorithms such as Rivest-Shamir-Adleman (RSA) or Elliptic Curve Cryptography (ECC). In RSA, the private key consists of two large prime numbers and the sender encrypts either the message of a hash (summary) of the message. The public key has a mathematical relationship to both these prime numbers. Because factoring very large prime numbers is unrealistic for a modern computer, this algorithm ensures that the encryption remains secure. In ECC, the private key is a randomly chosen number and the public key is created by solving the Elliptic Curve Discrete Logarithm Problem to generate a number. The public key in ECC is linked to the private key. While ECC offers smaller key sizes than RSA (thereby making it a more efficient algorithm), it’s still vulnerable to a quantum attack with something like Shor’s algorithm able to solve the discrete logarithm problem at the center of its security. So, as technical advances in quantum computing become closer to reality, there is a need for algorithms that are quantum resistant.

One promising approach to a quantum resistant cryptography scheme comes in the form of what is called isogeny-based cryptography. An isogeny is a special function (essentially a map) that connects elliptical curves while preserving their group structure. Multiple points from the first curve can map to a single point on the target curve depending on the degree of the isogeny, but an isogeny must be surjective. Isogenies are useful in cryptography because computing one at random can be very complicated, and, importantly, virtually impossible to reverse the process even for a quantum computer, which is why it is deemed to be quantum-resistant.

There are many types of isogeny-based cryptography schemes, including Supersingular Isogeny Diffie-Hellman (a key exchange protocol that builds upon classical Diffie-Hellman, but incorporating points on the elliptical curves to compute a shared secret) and Supersingular Isogeny Key Encapsulation (a key encapsulation scheme that actually builds on SIDH by using a key encapsulation mechanism). These algorithms, like most isogeny-based algorithms, have small key sizes when compared to other quantum-resistant algorithms, and, at least in theory, they should be secure and efficient. However, both have been broken already by modern attacks that have shown weaknesses in their general structures.

While these algorithms have their own merits and shortcomings, this paper will discuss in detail a robust and promising new algorithm called SQIsign,a digital signature schemewhich relies on what’s known as supersingular elliptical curves, which are elliptical curves with a special property where their associated endomorphic rings are a quaternion algebra. Quaternion algebra will be broken down further later on, but for now it can be described as a four-dimensional, non-commutative algebra that has more complex quadratic fields, making it more complex to be able to compute and resistant to attack, an important feature for a quantum-resistant algorithm. The private key is generated by randomly choosing one of these isogenies. A common analogy is to imagine standing at the beginning of a maze where you can see the, but you don’t know the exact path to take through the maze until you start walking it. The path that you walk to finish the maze is essentially your private key. The public key would be a map that you made that shows you found the exit, but doesn’t show which path you walked in order to get there. In reality, what’s happened is the isogeny has been applied to a target curve to generate the public key. Another important feature (indeed, what could be considered the defining feature) of SQIsign is that the keys and signature are quite small when compared to other similar algorithms, making it highly efficient not only in terms of storage but also time it takes to send the message.

When looked at with future demands in mind, it becomes increasingly obvious that SQIsign, with its smaller key and signature sizes, is one of the most promising and exciting fields in post-quantum cryptography. In this paper, the mathematical properties of SQIsign will be examined in greater detail, including the generation of the keys, the process of signing and verification, as well as an analysis of the performance and security of the algorithm, while also discussing the potential challenges and shortcomings.