# Insert Title

Juntian Zheng, Zihao Zhen, and Wuwei Yuan

Tsinghua University

**Abstract.**

## 1 Introduction

Write Something Here.

## 2 Preliminary

Write Something Here.

## 3 SIDH

Write Something Here.

## 4 Implementation

### 4.1 Parameter Choices

Although $p$ can be arbitrary for our protocol, the implementation of the protocol benefits from some special forms of $p$. Choosing $p \equiv -1 \pmod 4$ means that $-1$ is not a square in $\mathbb{F}_{p^2}$ and hence $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ for $i^2 = -1$, which makes the arithmetic simpler.

In our implementation, we follow [CLN16] and choose

$$p = 2^{372} \cdot 3^{239} - 1.$$

*TODO* Write something about the balance of $2^{372} \approx 3^{239}$.

*TODO* Write something about the choice of the curve and etc.

### 4.2 Implementation Details

We use the GMP library [Gt12] as our high precision arithmetic library. Based on GMP library, we build up several C++ classes based on our purpose.

- Integer class: we wrap the GMP library into the integer class, which is more convenient to use.
- Fp class: we implement the basic $\mathbb{F}_p$ field using Integer class as well as computing the square root of an element.
- Fp2 class: similar to $\mathbb{F}_p$, we implement the basic $\mathbb{F}_p$ field containing the square root algorithm.
- Curve class:
- RPoint class:
- Isogeny class:
- IsogenyChain class:

### 4.3 Experiments

## 5 Conclusion

Write Something Here.

cite example [DF17]

## References

CLN16. C. Costello, P. Longa, and M. Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. In *CRYPTO 2016, Part I*, *LNCS* 9814, pages 572–601. Springer, Heidelberg, August 2016.

DF17. L. De Feo. Mathematics of isogeny based cryptography, 2017.

Gt12. T. Granlund and the GMP development team. *GNU MP: The GNU Multiple Precision Arithmetic Library*, 5.0.5 edition, 2012. `http://gmplib.org/`.