1 Introduction

Succinct Non-Interactive Argument of Knowledge (SNARK) is a non-interactive protocol where a prover convinces a verifier that they know the proof of a (mathematical) statement in a succinct manner (short proof and efficient verification time).
• (Construction) Compile an informatic theoretical object interactive oracle protocol (IOP) with a commitment scheme.
• We construct a type of IOP Hyperplonk [1] over a lattice-friendly cyclotomic ring instead of a finite field in the original paper.
• A lattice-based commitment scheme that works over a cyclotomic ring can compile IOP natively.

2 Preliminary

• Field is a set F with two operators (+, ·), where addition, multiplication, subtraction, division are well defined.
  - a + b = a + (−b)
  - a + b = (a · b)
  - Any element in F has its own inverse in F.
  - (e.g. rational field \( \mathbb{Q} \), \( \mathbb{R} \) and \( \mathbb{C} \)
• Ring is more general than a field and is a set \( \mathbb{Z} \) with two operators (+, ·), where addition, multiplication, and subtraction are well defined but not division.
• An element in \( \mathbb{R} \) does not have to have its own inverse in \( \mathbb{R} \).
  - (e.g. integer ring \( \mathbb{Z} \), \( \mathbb{Z}/2\mathbb{Z} \) and \( \mathbb{Q} \))
• Isomorphism \( f : \mathbb{R} \rightarrow \mathbb{R} \) is a map between two rings that satisfies:
  - for all \( a, b \in \mathbb{R} \), \( f(a + b) = f(a) + f(b) \) and \( f(ab) = f(a) \cdot f(b) \)
  - \( f \) is bijection
• Primitive \( n^{th} \) root of unity is \( \zeta_n \) such that \( \zeta_n^r = 1 \) and \( \zeta_n^k \neq 1 \) for any positive integer \( k < n \).
  - e.g. 4\(^{th}\) root of unity is \( ±i \) but \( ±i \) are only primitive.
• Cyclotomic polynomial \( \Phi_n(x) \) is a polynomial defined as
  - \( \Phi_n(x) = \prod_{\zeta_n^k \neq 1} (x - \zeta_n^k) \)

3 Cyclotomic Ring splits into Finite Fields [2]

The cyclotomic ring of \( m^{th} \) cyclotomic fields is defined as \( R = \mathbb{Z}(/\zeta_m) \), where \( \zeta_m \) is the primitive \( m^{th} \) root of unity. We denote the modulus version (modulo \( q \)) of the \( m^{th} \) cyclotomic ring by \( R_q = \mathbb{Z}_q(/\zeta_m) = \mathbb{Z}_q[\zeta_m] \), where \( q \in \mathbb{N} \).

It is known that \( R_q \) is isomorphic to \( \mathbb{Z}[\zeta_q]/\Phi_q(X) \):

\[
R_q \cong \frac{\mathbb{Z}[X]}{\Phi_q(X)}
\]

(1)

where \( \mathbb{Z}[X] \) is the set of all polynomials whose coefficients are in \( \mathbb{Z} \) and \( \Phi_q(X) \) is the \( m^{th} \) cyclotomic polynomial.

There is an isomorphism between \( \frac{\mathbb{Z}_q[X]}{\Phi_q(X)} \) and \( \Phi_q(X) \) of any finite fields \( F_p \) with its size \( q^r \) for some parameters \( q, r \).

\[
\frac{\mathbb{Z}_q[X]}{\Phi_q(X)} \cong \mathbb{F}_q^m \times \cdots \times \mathbb{F}_q^m
\]

(2)

Thus

\[
R_q \cong \mathbb{Z}_q[\zeta_q]/\mathbb{F}_q^m
\]

(3)

The equation 3 implies that given \( q \) many elements from a finite field, one can transform them into a single element in a cyclotomic ring \( R_q \) via isomorphisms, run a computation over \( R_q \), and transform the result back to \( q \) many elements in the finite fields via the inverses of those isomorphisms.

4 Interactive Oracle Proof (IOP)

IOP is a multi-round interactive protocol where a prover convinces the verifier that the prover knows the proof of a statement where a prover sends a verifier a proof string and a verifier sends a randomly picked message in one round. In addition, the verifier can query to a fragment of any proof string that has been sent at any point of the interaction.

5 Hyperplonk [1] over \( R_q \)

Hyperplonk is an IOP proposed recently. Suppose that the statement a prover want to prove against a verifier in a IOP over a finite field is \( k \) field elements. Then, by the equation 3, we can convert \( q \) slots of different statements into a single slot of \( k \) ring elements via isomorphisms. The prover can prove \( q \) many statements over a field parallelly.

6 Conclusion

• We constructed an IOP - Hyperplonk over a cyclotomic ring where many lattice-based cryptographic scheme operate on. This allows us to construct a post-quantum SNARK by combining the IOP with a lattice-based commitment scheme.
• Furthermore, our protocol enables to run a IOP over a finite field parallelly for multiple slots of input by converting slots of input over a finite field into a single slot of input over a cyclotomic ring and running IOP over \( R_q \).

References