Aalto University
School of Science

Lattice-Friendly Interactive Proof Oracle over cyclotomic ring

Shuto K.
Department of Computer Science, Aalto University

1 Introduction

Succinct Non-Interactive Argument of Knowledge (SNARK) is a non-interactive protocol where a prover convinces a verifier that they knows the proof of a (mathematical) statement in a succinct manner (short proof and effcient 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 $\mathbb{F}$ with two operators $(+,\cdot)$, where addition, multiplication, subtraction, division are well defined.
  - ⋄ $a-b \overset{\text{def}}{=} a+(-b)$
  - ⋄ $a/b \overset{\text{def}}{=} a\cdot(b^{-1})$
  - ⋄ Any element in $\mathbb{F}$ has its own inverse in $\mathbb{F}$.
    (e.g. rational field $\mathbb{R}$, $3.14 \in \mathbb{R}$ and $1/3.14 \in \mathbb{R}$)
- Ring is more general than a field and is a set $\mathscr{R}$ with two operators $(+,\cdot)$, where addition, multiplication, and subtraction are well defined but not division.
  - ⋄ An element in $\mathscr{R}$ does not have to have its own inverse in $\mathscr{R}$.
    (e.g. integer ring $\mathbb{Z}$, $3 \in \mathbb{Z}$ but $1/3 \notin \mathbb{Z}$)
- Isomorphism $f:\mathscr{R}_1 \to \mathscr{R}_2$ is a map between two rings that satisfies:
  - ⋄ for all $a,b \in \mathscr{R}_1$, $f(a)+f(b)=f(a+b)$ $f(a)\cdot f(b)=f(a\cdot b)$
  - ⋄ f is bijection
- Primitive n^{th} root of unity is ζ_n such that $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$ for any positive integer $k<n$.
  - ⋄ e.g. 4^{th} root of unity is $\pm 1, \pm i$ but $\pm i$ are only primitive.
    $(\pm i)^4 = 1,\ 1^1 = 1,\ (-1)^2 = 1$
- Cyclotomic polynomial $\Phi_n(X)$ is a polynomial defined as
  - ⋄ $\Phi_n(x) = \prod_{\text{primitive } n^{th} \text{ root of unity } \zeta} (x-\zeta)$ e.g. $\Phi_4(x) = x^2+1$

3 Cyclotomic Ring splits into Finite Fields [2]

The cyclotomic ring of m^{th} cyclotmoic fields is defined as $R = \mathbb{Z}[\zeta_m]$, where ζ_m is the primitive m^{th} root of unity. We dentote the modulus version (modulo q) of the m^{th} cyclotmoic ring by $R_q := R/qR = \mathbb{Z}_q[\zeta_m]$, where $q \in \mathbb{N}$.
It is known that R_q is isomorphic to $\mathbb{Z}[X]/\Phi_m(X)$:

$$R_q \cong \frac{\mathbb{Z}_q[X]}{\Phi_m(X)}, \tag{1}$$

where $\mathbb{Z}_q[X]$ is a set of all polynomials whose coefficients are in $\mathbb{Z}_q$ and $\Phi_m(X)$ is the m^{th} cyclotmoic polynomial.
There is an isomorphism between $\frac{\mathbb{Z}_q[X]}{\Phi_m(X)}$ and φ slots of any finite fields $\mathbb{F}_{q^e}$ with its size q^e for some parameters φ, e.

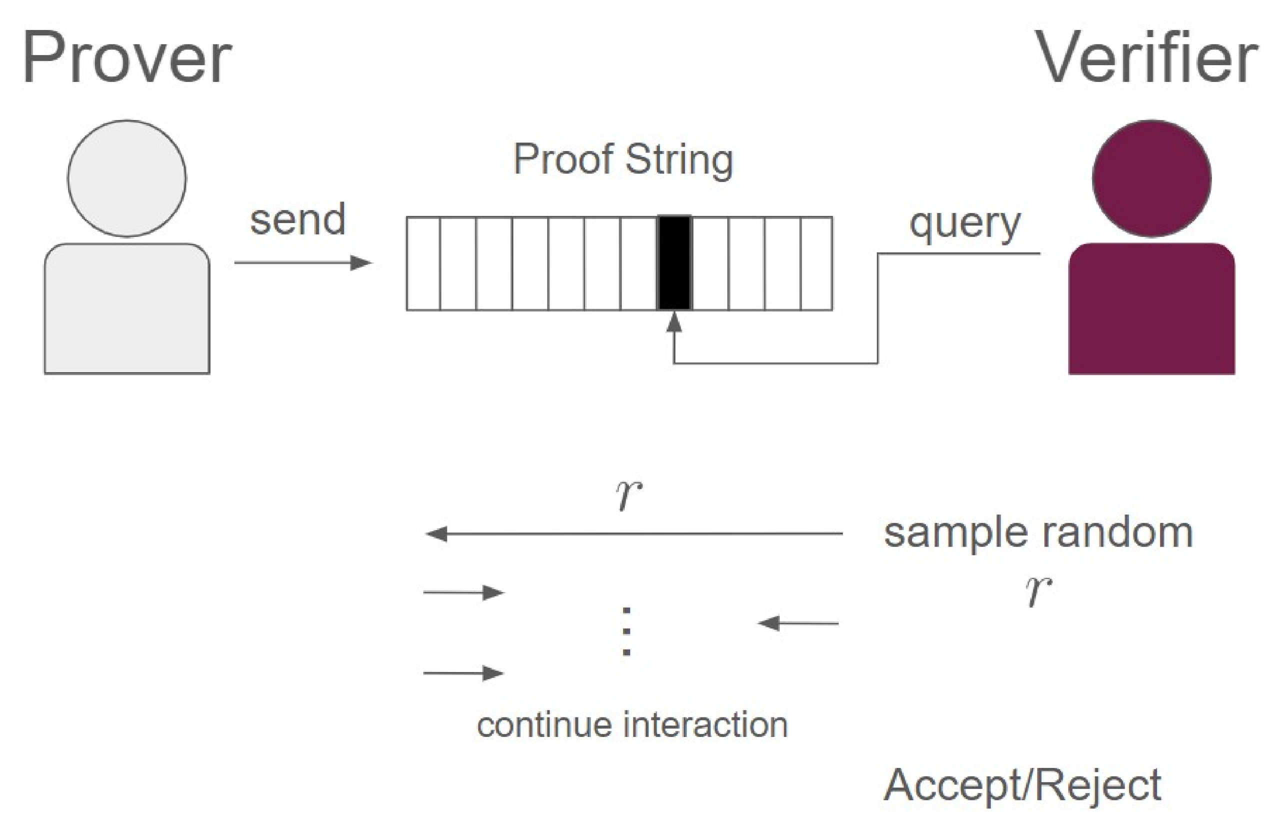
$$\frac{\mathbb{Z}_q[X]}{\Phi_m(X)} \cong \mathbb{F}_{q^e}^{\varphi} = \underbrace{\mathbb{F}_{q^e} \times \cdots \times \mathbb{F}_{q^e}}_{\varphi}. \tag{2}$$

Thus

$$R_q := \mathbb{Z}_q[\zeta_m] \overset{(1)}{\cong} \frac{\mathbb{Z}_q[X]}{\Phi_m(X)} \overset{(2)}{\cong} \mathbb{F}_{q^e}^{\varphi}. \tag{3}$$

The equation 3 implies that given φ 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 φ many elements in the finite fields via the inverses of those isomorphisms.

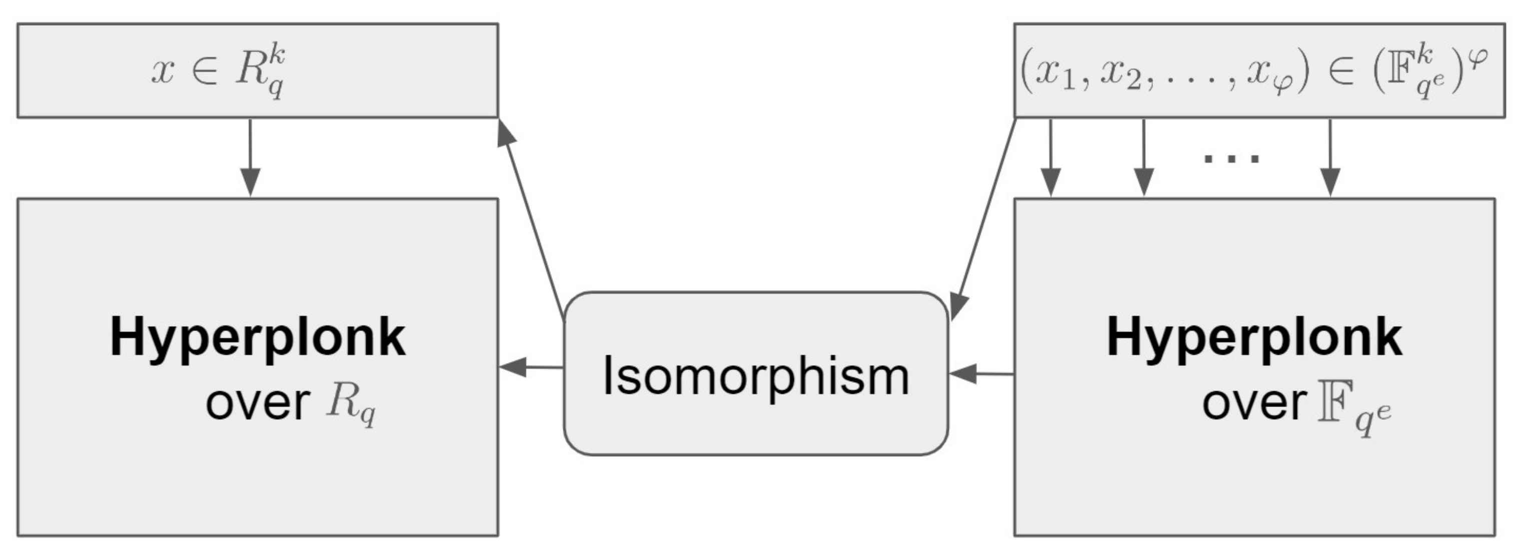
4 Interactive Oracle Proof (IOP)



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 φ slots of different statements into a single slot of k ring elements via isomorphisms. The prover can prove φ many statements over a field parallelly.



Combining it with a lattice-based commitment scheme, we can construct a post-quantum secure SNARK with parallelising feature.

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

[1] Binyi Chen, Benedikt Bünz, Dan Boneh, and Zhenfei Zhang. HyperPlonk: Plonk with linear-time prover and high-degree custom gates. Cryptology ePrint Archive, Paper 2022/1355, 2022. https://eprint.iacr.org/2022/1355.

[2] Vadim Lyubashevsky and Gregor Seiler. Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs. Cryptology ePrint Archive, Paper 2017/523, 2017. https://eprint.iacr.org/2017/523.

Department of Computer Science
School of Science
Aalto University, Finland

Contact information for comments & improvement ideas: Shuto Kuriyama
Email: shuto.kuriyama@aalto.fi