Diophantine Argument of Knowledge

rkm0959 (Gyumin Roh)

January 30th, 2021

Outline

Integer Commitment Scheme of [DF02]

Diophantine Argument of Knowledge of [Lip03]

Transparent SNARKS from DARK of [BFS20]

Implementation of [Lip03]

Table of Contents

Integer Commitment

Integer Commitment

- Consider a deterministic commitment function C
- To commit $x \in \mathbb{Z}$, we take random r and calculate $C(x, r)$

We want the following properties to hold -

- **Binding** : "Once you commit, you cannot go back".
- **Hiding** : "Commitment does not leak information on x".

List of Tools : Homomorphism

We want our commitment scheme to have more properties.

- **Proving we know how to open** : Prove the knowledge of x, r such that $C = C(x, r)$ in ZK

If we have three commitments $C(x_i, r_i)$ of integers x_i, $(1 \leq i \leq 3)$

- **Summation Protocol** : If $x_3 = x_1 + x_2$, we can prove it ZK
- **Multiplication Protocol** : If $x_3 = x_1 x_2$, we can prove it ZK

while only using the commitment values.

Compare with homomorphic encryption.

The scheme of [DF02]

[DF02] constructs a scheme with all of these properties by using **groups of unknown order**. Our limitations/specifications are -

- Integers must be in a pre-defined interval $[-T, T]$
- **Trusted Setup** (if we use RSA group)

Table of Contents

Interim Check

The three ZK protocols of [DF02] serves as a building block to

- **Integer Coefficient Multivariable Polynomial Evaluation** : We can prove $y = f(x_1, x_2, \cdots, x_n)$ in ZK only using commitments of values, for all integer coefficient multivariable polynomial f, if all interim values are in $[-T, T]$.

However, not all proofs we want to do are like that...

Diophantine Sets

Diophantine Sets

A set $S \subset \mathbb{Z}^k$ is called Diophantine iff $\exists P \in \mathbb{Z}[X, Y]$ such that

$$\mu \in S \iff (\exists \omega \in \mathbb{Z}^{k'})\ P(\mu, \omega) = 0$$

P is called *representing polynomial* of S, ω is *witness* for μ.
A lot of sets are Diophantine. (c.f. Matiyasevich's Theorem)

Diophantine Sets

Assume S is Diophantine with P is the representing polynomial.

We can prove $\mu \in S$ in ZK by

- Finding a witness ω
- Proving $P(\mu, \omega) = 0$ in ZK

Question : For what sets S is this practical, i.e. ω has small length (subquadratic to the length of input) and can be found efficiently?

Concrete Examples : Set Intersection & Union

S_1, S_2 are Diophantine sets with representing polynomials P_1, P_2.
How do we find the representing polynomial for $S_1 \cap S_2$, $S_1 \cup S_2$?

- **Intersection** : $P_\cap(\mu, \omega_1, \omega_2) = P_1(\mu, \omega_1)^2 + P_2(\mu, \omega_2)^2$
- **Union** : $P_\cup(\mu, \omega_1, \omega_2) = P_1(\mu, \omega_1) \cdot P_2(\mu, \omega_2)$

We can now use and/or operations for our prepositions.

Concrete Examples : Range Proofs

How do we prove $x \geq 0$ in ZK?

- **Lagrange's Four Square Theorem** :
  $x \geq 0 \iff x = a^2 + b^2 + c^2 + d^2$ for some $a, b, c, d \in \mathbb{Z}$.
- Use $P(x, a, b, c, d) = x - a^2 - b^2 - c^2 - d^2$
- Witness a, b, c, d can be found efficiently.

Concrete Examples : Exponential Relation

Figure 1: Proof of Exponential Relatiion

Theorem 3. *Assume* $\mu_1 > 1$, $\mu_3 > 0$ *and* $\mu_2 > 2$. *The exponential relation* $[\mu_3 = \mu_1^{\mu_2}]$ *belongs to* **PD**. *More precisely, let* $E(\mu_1, \mu_2, \mu_3)$ *be the next equation:*

$$
\begin{aligned}
&[(\exists \omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6)(\exists_b \omega_7, \omega_8)] \\
&\quad [(\omega_2 = \omega_1\mu_1 - \mu_1^2 - 1) \wedge (\omega_2 - \mu_3 - 1 \geq 0) \wedge && (E1 - E2) \\
&\quad (\mu_3 - (\mu_1 - \omega_1)\omega_7 - \omega_8 = \omega_2\omega_3)) \wedge (\omega_1 - 2 \geq 0) \wedge && (E3 - E4) \\
&\quad ((\omega_1 - 2)^2 - (\mu_1 + 2)(\omega_1 - 2)\omega_5 - \omega_5^2 = 1) \wedge && (E5) \\
&\quad (\omega_1 - 2 = \mu_2 + \omega_6(\mu_1 + 2)) \wedge (\omega_7 \geq 0) \wedge (\omega_7 < \omega_8) \wedge && (E6 - E8) \\
&\quad (\omega_7^2 - \omega_1\omega_7\omega_8 - \omega_8^2 = 1) \wedge (\omega_7 = \mu_2 + \omega_4(\omega_1 - 2)] \ , && (E9 - E10)
\end{aligned}
$$

where "$\exists_b$*" signifies a bounded quantifier in the following sense: if* $\mu_3 = \mu_1^{\mu_2}$ *then* $E(\mu_1, \mu_2, \mu_3)$ *is true with* $W = \Theta(\mu_2^2 \log \mu_1) = o(M^2)$. *On the other hand, if* $\mu_3 \neq \mu_1^{\mu_2}$ *then either* $E(\mu_1, \mu_2, \mu_3)$ *is false, or it is true but the intermediate witnesses* ω_7 *and* ω_8 *have length* $\Omega(\mu_3 \log \mu_3)$, *which is equal to* $\Omega(2^M \cdot M)$ *in the worst case.*

Concrete Examples : Bounded Arithmetic

Bounded Arithmetic

We work over the nonnegative integers, using the operations

- $0, +, \cdot, \leq, \lfloor x/2 \rfloor, \lfloor x/2^k \rfloor$
- $x \ominus y = \max(x - y, 0)$
- $\sigma : \sigma(x) = x + 1$
- $|x|$: bitwise length of x
- $x \sharp y = 2^{|x| \cdot |y|}$

Our previous examples as "building blocks" show everything in Bounded Arithmetic can be proved ZK. It seems that bounded arithmetic is quite researched, and a lot of useful prepositions can be written using the bounded arithmetic language.

Table of Contents

Common Ideas

- groups of unknown order for integer commitments
- similar assumptions used for security proof

Key Differences

- polynomials over $\mathbb{F}_p$ encoded as integers by evaluation
- therefore, DARK is now a polynomial commitment scheme
- class groups, not RSA groups are used (for transparency)

Table of Contents

Implementation

Implementation is on my GitHub (rkm0959)

- setup processes
- proving how to open
- summation, multiplication protocol
- proving nonnegativity
- proving $a \ominus b = c$
- proving $\lfloor x/2^k \rfloor = y$

Concluding

Blog Post : https://rkm0959.tistory.com/193
Future : read more ZK papers/theory
Future : possibly implement some parts of [BFS20]