Mathematics for Cryptographers. Preliminaries.

ZKDL Camp

July 18, 2024

Plan

Some words about the course

About ZKDL

- ZKDL Camp is a series of lectures and workshops on zero-knowledge proofs and cryptography.
- Here, we will learn state-of-the-art zero-knowledge systems: what are SNARKs, how they work under the hood from total scratch.
- Note, that this is not a regular course: we require a lot of commitment and the material is fairly complex.
- If possible, we will conduct workshops, where we will show practical implementations of the theoretical material.

Approximate Camp Structure

1. Basic Mathematics: group and number theory, finite fields, polynomials, elliptic curves etc.
2. Deep Delve into SNARKs: General definition, arithmetic circuits, commitment schemes, encryption etc.
3. Analysis of modern zero-knowledge proving systems: Groth16, Plonk, BulletProofs, STARK etc.
4. Specialization topics: low-level optimizations, advanced protocols such as folding schemes, Nova etc.

Number Theory

Basic Group Theory

Why groups

Group Definition

Definition

Group, denoted by $(\mathbb{G}, \oplus)$, is a set with a binary operation $\oplus$, obeying the following rules:

1. **Closure:** Binary operations always outputs an element from $\mathbb{G}$, that is $\forall a, b \in \mathbb{G} : a \oplus b \in \mathbb{G}$.
2. **Associativity:** $\forall a, b, c \in \mathbb{G} : (a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity element:** There exists a so-called identity element $e \in \mathbb{G}$ such that $\forall a \in \mathbb{G} : e \oplus a = a \oplus e = a$.
4. **Inverse element:** $\forall a \in \mathbb{G}\ \exists b \in \mathbb{G} : a \oplus b = b \oplus a = e$. We commonly denote the inverse element as $(\ominus a)$.

Group Examples

Example

A group of integers with the regular addition $(\mathbb{Z}, +)$ (also called the *additive* group of integers) is a group. Indeed, an identity element is $e = 0$, associativity obviously holds, and an inverse for each element $a \in \mathbb{Z}$ is $(\ominus a) := -a \in \mathbb{Z}$.

Example

The multiplicative group of positive real numbers $(\mathbb{R}_{>0}, \cdot)$ is a group for similar reasons. An identity element is $e = 1$, while the inverse for $a \in \mathbb{R}_{>0}$ is defined as $\frac{1}{a}$.

Example

The additive group of natural numbers $(\mathbb{N}, +)$ is not a group. Although operation of addition is closed, there is no identity element nor inverse element for, say, 2 or 10.

Explanation for Developers

```rust
/// Trait that represents a group.
pub trait Group: Sized {
    /// Checks whether the two elements are equal.
    fn eq(&self, other: &Self) -> bool;
    /// Returns the identity element of the group.
    fn identity() -> Self;
    /// Adds two elements of the group.
    fn add(&self, a: &Self) -> Self;
    /// Returns the negative of the element.
    fn negate(&self) -> Self;
    /// Subtracts two elements of the group.
    fn sub(&self, a: &Self) -> Self {
        self.add(&a.negate())
    }
}
```

Polynomials

Field

Definition

Field K is a set equipped with appropriate **addition** and **multiplication** operations with the corresponding well-defined inverses, where you can perform the basic arithmetic.

Field

Definition

Field K is a set equipped with appropriate **addition** and **multiplication** operations with the corresponding well-defined inverses, where you can perform the basic arithmetic.

- $\mathbb{R}$ (real numbers) is a field.
- $\mathbb{Q}$ (rational numbers) is a field.
- $\mathbb{C}$ (complex numbers) is a field.
- $\mathbb{N}$ (natural numbers) is not a field: there is no additive inverse for 2 (-2 is not in $\mathbb{N}$).
- $\mathbb{Z}$ (integers) is not a field: additive inverse is defined, but the multiplicative is not (2^{-1} is not defined).

Thanks for your attention!