Zero Knowledge Bootcamp

#1. Introduction & Modular Arithmetic

RareSkills

A proposed schedule

1. Introduction and modular arithmetic
2. Groups and fields
3. Introduction to elliptic curves
4. BN128 curve arithmetic
5. Bilinear pairings
6. Arithmetic circuits
7. R1CS
8. Quadratic arithmetic program (QAP)
9. Evaluation polynomials at a EC point
10. Groth16 part 1
11. Groth16 part 2

RareSkills

What is a zero-knowledge proof?

Informally, a zero-knowledge proof is a way of proving something to someone in such a way that they gain no information about the proof other than the validity of the proof itself

RareSkills

History of zero-knowledge proofs

The Knowledge Complexity of Interactive Proof-Systems

(Extended Abstract)

Shafi Goldwasser, MIT
Silvio Micali, MIT
Charles Rackoff, University of Toronto

1. Introduction

In the first part of the paper we introduce a new theorem-proving procedure, that is a new *efficient method of communicating a proof.* Any such method implies, directly or indirectly, a definition of proof. Our "proofs" are probabilistic in nature. On input an n-bits long statement, we may erroneously be convinced of its correctness with very small probability, say, $\frac{1}{2^n}$, and rightfully be convinced of its correctness with very high probability, say, $1 - \frac{1}{2^n}$. Our proofs are *interactive.* To efficiently verify the correctness of a statement, the "recipient" of the proof must actively ask questions and receive answers from the "prover".

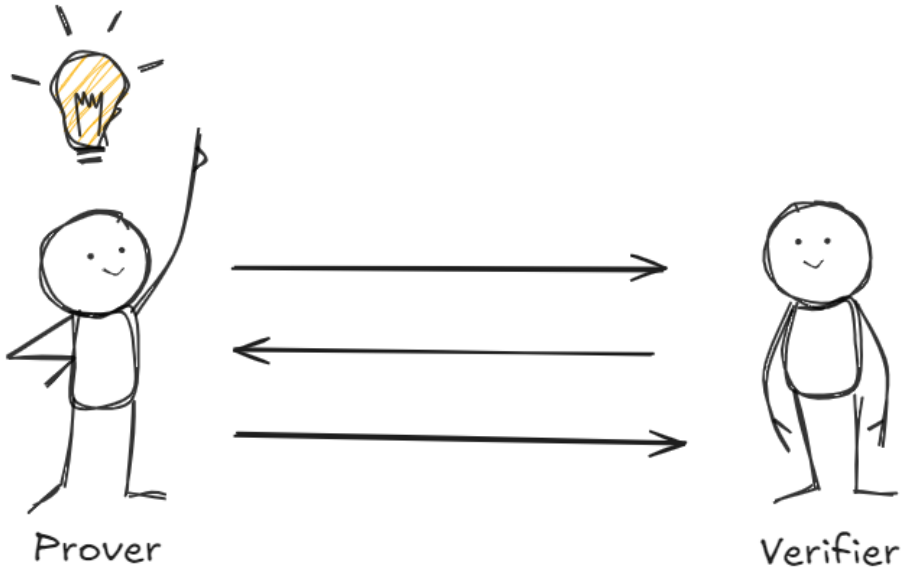
We propose to classify languages according to the amount of additional knowledge that must be released for proving membership in them.

Of particular interest is the case where this additional knowledge is essentially 0 and we show that is possible to interactively prove that a number is quadratic non residue mod m releasing 0 additional knowledge. This is surprising as no efficient algorithm for deciding quadratic residuosity mod m is known when m's factorization is not given. Moreover, all known NP proofs for this problem exhibit the prime factorization of m. This indicates that adding interaction to the proving process, may decrease the amount of knowledge that must be communicated in order to prove a theorem.

RareSkills

History of zero-knowledge proofs

The concept of interactive proofs has been introduced in this article, along with the idea of zero-knowledge proofs



At the end of the day, the verifier will be convinced of the correctness of the proof with high probability

RareSkills

zk-SNARKs

Zero-knowledge
Succinct
Non-interactive
Argument
of Knowledgment

RareSkills

A proof is an information-theoretical idea in a sense that the prover cannot cheat even if he has access to unlimited computational power

An argument is a kind of proof where the prover can't have access to unlimited computational power, otherwise he is able to prove false statements

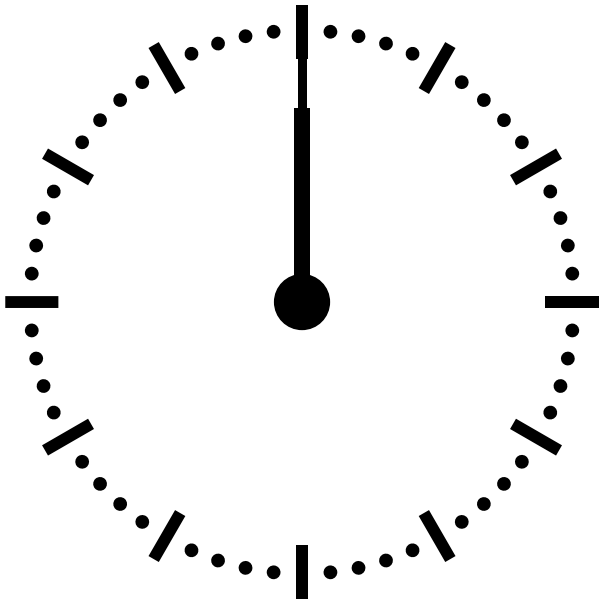
RareSkills

The SNARK zoo

- Groth16 (‘16)
- Bulletproofs (‘18)
- PLONK (‘19)
- STARK (‘19)
- …

RareSkills

Modular Arithmetic



15h = 3 PM

90h = 6h

90 = 12*7 + 6

RareSkills

Congruence

$$a \equiv b \,(mod\ n) \quad \text{if } a - b = n \cdot k$$

RareSkills

Finite field

$$\mathbb{F}_p = \{0, 1, 2, ..., p-1\} \text{ (characteristic p)}$$

$$a \oplus b = a + b \,(\text{mod p})$$

$$a \otimes b = ab \,(\text{mod p})$$

RareSkills

Addition and subtraction

$$\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$3 + 6 = 2 \pmod 7$$

$$3 - 6 = ?$$

RareSkills

Additive inverse

$$In\ \mathbb{Z}, 7 + (-7) = 0$$

$$In\ \mathbb{F}_p, q + (-q) = 0\ (\text{mod p})$$

$$\mathbb{F}_7,\ 3 + 4 = 0 \rightarrow 4 \equiv -3$$

$$\mathbb{F}_7,\ 6 + 1 = 0 \rightarrow 1 \equiv -6$$

$$\mathbb{F}_p, (-q) \equiv p - q$$

RareSkills

Multiplicative inverse

$$In\ \mathbb{Z}, 3 \cdot \frac{1}{3} = 1$$

$$In\ \mathbb{F}_p, q \cdot \frac{1}{q} = 1\ (\mathrm{mod\ p})$$

$$\mathbb{F}_7,\ 3 \cdot 5 = 1\ (\mathrm{mod}\ 7) \rightarrow 5 \equiv \frac{1}{3}$$

$$\mathbb{F}_7,\ 4 \cdot 2 = 1\ (\mathrm{mod}\ 7) \rightarrow 2 \equiv \frac{1}{4}$$

RareSkills

Multiplicative inverse

- In a field, all elements have a multiplicative inverse
- The characteristic of a field is a prime number, otherwise the structure is probably a ring
- It is not obvious to find the multiplicative inverse of a number in a finite field, but there are efficient methods for doing so

Exercise

$$\frac{1}{2} + \frac{1}{3} = \frac{5}{6} \pmod 7$$

RareSkills

Fermat's little theorem (not last theorem)

$$a^p = a \pmod{\text{p}}$$
$$a^{p-1} = 1 \pmod{\text{p}}$$
$$a^{p-2} \cdot a = 1 \pmod{\text{p}}$$

It is a way to calculate the inverse of an element in a finite field. Another way is using the Extended Euclid Algorithm

RareSkills

Quadratic residue

In $\mathbb{Z}, \{1, 4, 9, 16, 25, 36...\}$ are squares

In a finite field, any number given by $q \cdot q$ is called a quadratic residue

$$1 \cdot 1 = 1 \pmod{11}$$
$$2 \cdot 2 = 4 \pmod{11}$$
$$3 \cdot 3 = 9 \pmod{11}$$
$$4 \cdot 4 = 5 \pmod{11}$$
$$5 \cdot 5 = 3 \pmod{11}$$
$$6 \cdot 6 = 3 \pmod{11}$$
$$7 \cdot 7 = 5 \pmod{11}$$
$$8 \cdot 8 = 9 \pmod{11}$$
$$9 \cdot 9 = 4 \pmod{11}$$
$$10 \cdot 10 = 1 \pmod{11}$$

Polynomials over a finite field

$$f(x) = a_2x^2 + a_1x + a_0, \quad a_i \in \mathbb{F}_p$$

RareSkills

Polynomials in a finite field

- A polynomial of degree d has at most d roots
- If a polynomial A has degree d1 and a polynomial B has degree d2, then the degree of A + B is max(d1, d2)
- If a polynomial A has degree d1 and a polynomial B has degree d2, then the degree of A * B is d1+d2

Lagrange interpolation (and FFT/NTT)

RareSkills