Lesson 1

Course Plan

WEEK 1

Overview / Maths & Cryptography introduction
Introduction to zkSNARKs / Zokrates

WEEK 2

Mina and Snapps
Mathematical Background
ZKP Theory
zkSTARKs

WEEK 3

Cairo
SONIC / PLONK etc.
zk Rollups
zkSync / StarkEx

WEEK 4

ZCash / Aztec
Data privacy
Proof of computation
Cairo 2 / zkp Libraries

WEEK 5

Research areas
Review Session

Resources

Zero Knowledge Podcast
Alex Pinto's Blog
Intro to ZKPs

Course Introduction

Context

"Human dignity demands that personal information, like medical and forensic data, be hidden from the public. But veils of secrecy designed to preserve privacy may also be abused to cover up lies and deceit by institutions entrusted with Data, unjustly harming citizens and eroding trust in central institutions." - Starkware

"ZK gives out similar vibe as ML. More and more people just mention ZK as a magic solution that fixes everything with no context of its current limitation." - 0xMisaka

Introductory Maths

Numbers

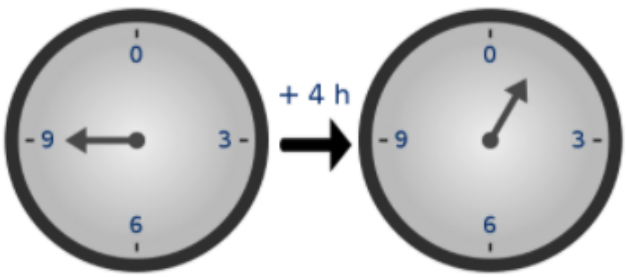
The set of Integers is denoted by $\mathbb{Z}$ e.g. $\{\cdots,-4,-3,-2,-1,0,1,2,3,4,\cdots\}$
The set of Rational Numbers is denoted by $\mathbb{Q}$ e.g. $\{\ldots 1, \frac{3}{2}, 2, \frac{22}{7}\ldots\}$
The set of Real Numbers is denoted by $\mathbb{R}$ e.g. $\{2, -4, 613, \pi, \sqrt{2}, \ldots\}$

Fields are denoted by $\mathbb{F}$, if they are a finite field or $\mathbb{K}$ for a field of real or complex numbers we also use $\mathbb{Z}_p^*$ to represent a finite field of integers mod prime p with multiplicative inverses.

We use finite fields for cryptography, because elements have “short”, exact representations and useful properties.

Modular Arithmetic

See this introduction



Because of how the numbers "wrap around", modular arithmetic is sometimes called "clock math"

When we write n mod k we mean simply the remainder when n is divided by k. Thus
25 mod 3 = 1
15 mod 4 = 3
The remainder should be positive.

FINDING AN INVERSE

From Fermat's little theorem

$a^{-1} \equiv a^{p-2}(modp)$

Let p = 7 and a = 2. We can compute the inverse of a as:
$a^{p-2} = 2^5 = 32 \equiv 4 \bmod 7$.

This is easy to verify: 2 x 4 ≡ 1 mod 7.

EQUIVALENCE CLASSES

Since
6 mod 7 = 6
13 mod 7 = 6
20 mod 7 = 6
...
we can say that 6, 13, 20 ... form an equivalence class
more formally
modular arithmetic partitions the integers into N equivalence classes, each of the form $i + kN \mid k \in \mathbb{Z}$ for some i between 0 and $N - 1$.

Thus if we are trying to solve the equation
x mod 7 = 6
x could be 6, 13, 20 ...
This gives us the basis for a one way function.

Group Theory

Simply put a group is a set of elements {a,b,c,...} plus a binary operation, here we represent this as •
To be considered a group this combination needs to have certain properties

1. Closure
   For all a, b in G, the result of the operation, a • b, is also in G
2. Associativity
   For all a, b and c in G, (a • b) • c = a • (b • c)
3. Identity element
   There exists an element e in G such that, for every element a in G, the equation e • a = a • e = a holds. Such an element is unique and thus one speaks of the identity element.
4. Inverse element
   For each a in G, there exists an element b in G, commonly denoted a^{-1} (or −a, if the operation is denoted "+"), such that a • b = b • a = e, where e is the identity element.

Fields

A field is a set of say Integers together with two operations called addition and multiplication.
One example of a field is the Real Numbers under addition and multiplication, another is a set of Integers mod a prime number with addition and multiplication.

The field operations are required to satisfy the following field axioms. In these axioms, a, b and c are arbitrary elements of the field $\mathbb{F}$.

1. Associativity of addition and multiplication: a + (b + c) = (a + b) + c and a · (b · c) = (a · b) · c.
2. Commutativity of addition and multiplication: a + b = b + a and a · b = b · a.
3. Additive and multiplicative identity: there exist two different elements 0 and 1 in $\mathbb{F}$ such that a + 0 = a and a · 1 = a.
4. Additive inverses: for every a in F, there exists an element in F, denoted −a, called the additive inverse of a, such that a + (−a) = 0.
5. Multiplicative inverses: for every a ≠ 0 in F, there exists an element in F, denoted by a^{-1}, called the multiplicative inverse of a, such that a $\cdot a^{-1}$ = 1.
6. Distributivity of multiplication over addition: a · (b + c) = (a · b) + (a · c).

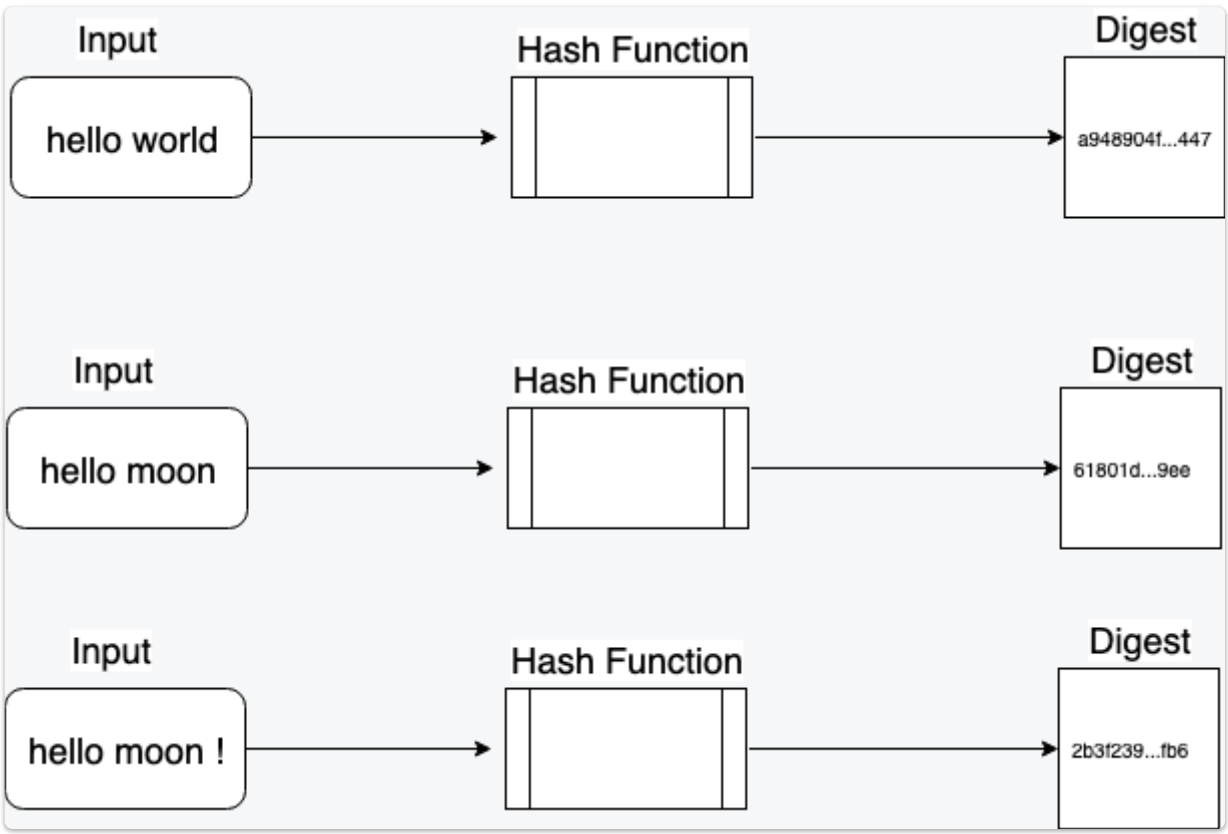
To try out operations on finite fields, see https://asecuritysite.com/encryption/finite

For a great introduction see http://coders-errand.com/zk-snarks-and-their-algebraic-structure/

The order of the field is the number of elements in the field's set.

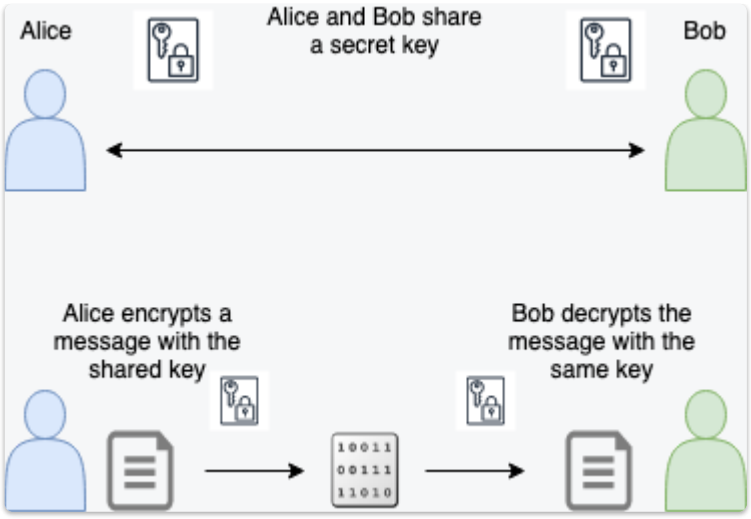
Cryptography Background

Hash Functions



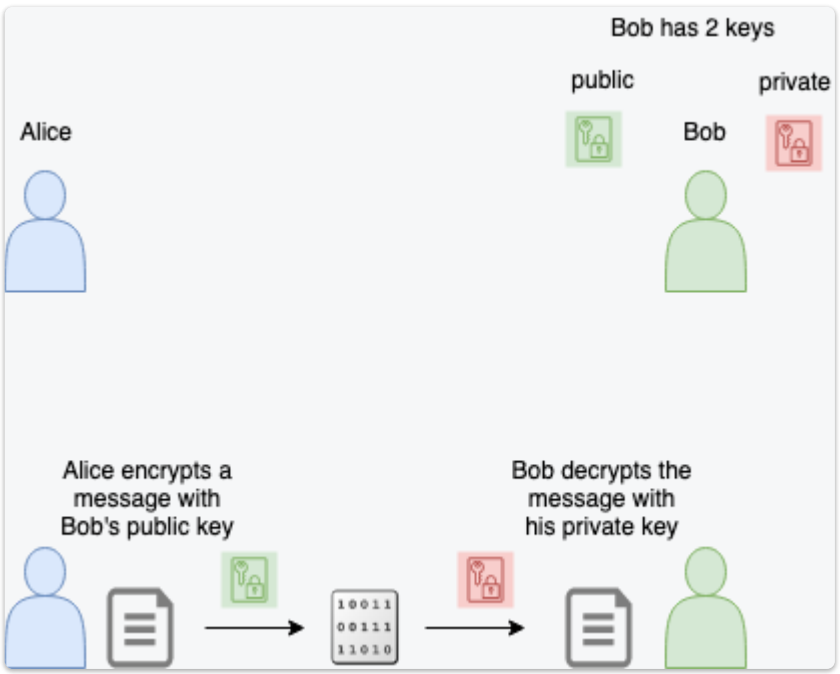
Encryption

SYMMETRIC ENCRYPTION

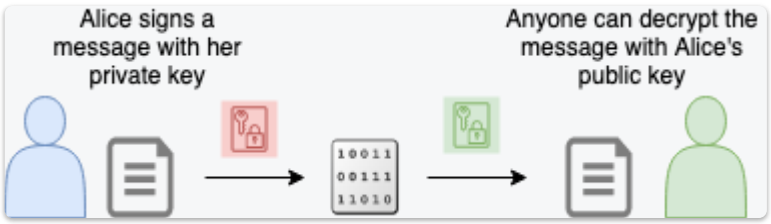


ASYMMETRIC ENCRYPTION

Sending a secret message



Proving ownership (knowledge of) of a private key



Intuitive grasp of Zero Knowledge Proofs

Introduction

It is difficult to find zero knowledge resources that avoid the extremes of either over simplyfying the subject, or presenting so much mathematical detail that the reader gets

bogged down and loses interest.
In this course I hope to find an accessible but informative middle ground.

We start with some examples to show how zero knowledge proofs can proceed, and the situations where they could be used.

What is a zero knowledge proof

A loose definition
It is a proof that there exists or that we know something, plus a zero knowledge aspect, that is the person verifying the proof only gains one piece of information - that the proof is valid or invalid.

Actors in a Zero Knowledge Proof System

- Creator - optional, maybe combined with the prover
- Prover - I will call her Peggy
- Verifier - I will call him Victor

Examples to give an Intuitive grasp of zero-knowledge proofs

1. Colour blind verifier
   This is an interactive proof showing that the prover can distinguish between a red and a green billiard ball, whereas the verifier cannot distinguish them.

```
• The prover wants to show the verifier that they have different colours
but does not want him to learn which is red and which is green.

• Step 1: The verifier takes the balls, each one in each hand, holds them
in front of the prover and then hides them behind his back. Then, with
probability 1/2 either swaps them (at most once) or keeps them as they
are. Finally, he brings them out in front.

• Step 2: The prover has to say the verifier switched them or not.

• Step 3: Since they have different colours, the prover can always say
whether they were switched or not.
But, if they were identical (the verifier is inclined to believe that),
the prover would be wrong with probability 1/2.

• Finally, to convince the verifier with very high probability, the prover
could repeat Step 1 to Step 3 k times to reduce the probability of the
prover being successful by chance to a extremely small amount.
```

2. Wheres Wally
   Based on the pictures of crowds where Wally is distinctivly dressed, the aim being to find him within a sea of similar people.
   The proof procedes as follows :
   Imagine the Peggy has found Wally in the picture and wants to prove this fact to Victor, however if she just shows him, Victor is liable to cheat and claim he also found Wally.
   In order to prove to Victor that she has indeed found Wally, without giving away his location in the picture

   ```
   1. Peggy cuts a hole in a (very) large sheet of paper, the hole should be the exact shape of Wally in the underlying picture.
   2. Peggy places the paper sheet over the original picture, so that the location of the picture beneath the paper is obscured.
   3. Victor can then see throught he hole that Wally has indeed been found, but since the alignment with the underlying picture cannot be seen, he doesn't gain any information about the location of Wally.
   ```

3. Sudoku
   An interactive proof can be created to prove the knowledge of a solution to a sudoku puzzle by placing cards in the sudoku grid. The process is descrived here Sudoku Proof

Quote from Vitalik Buterin
"You can make a proof for the statement "I know a secret number such that if you take the word 'cow', add the number to the end, and SHA256 hash it 100 million times, the output starts with `0x57d00485aa`". The verifier can verify the proof far more quickly than it would take for them to run 100 million hashes themselves, and the proof would also not reveal what the secret number is."

Zero Knowledge Proof Timeline

Changes have occurred because of

- Improvements to the cryptographic primitives (improved curves or hash functions for example)
- A fundamental change to the approach to zero knowledge
  See the excellent blog post from Starkware :
  The Cambrian Explosion

1984 : Goldwasser, Micali and Rackoff - Probabilistic Encryption.
1989 : Goldwasser, Micali and Rackoff - The Knowledge Complexity of Interactive Proof Systems
1991 O Goldreich, S. Micali and A. Wigderson. Proofs that Yield Nothing but their Validity or All Languages in NP Have Zero-Knowledge Proof Systems. Preliminary version in 1986. (Graph colouring problem)

....

2006 Groth, Ostrovsky and Sahai introduced pairing-based NIZK proofs, yielding the first linear size proofs based on standard assumptions.

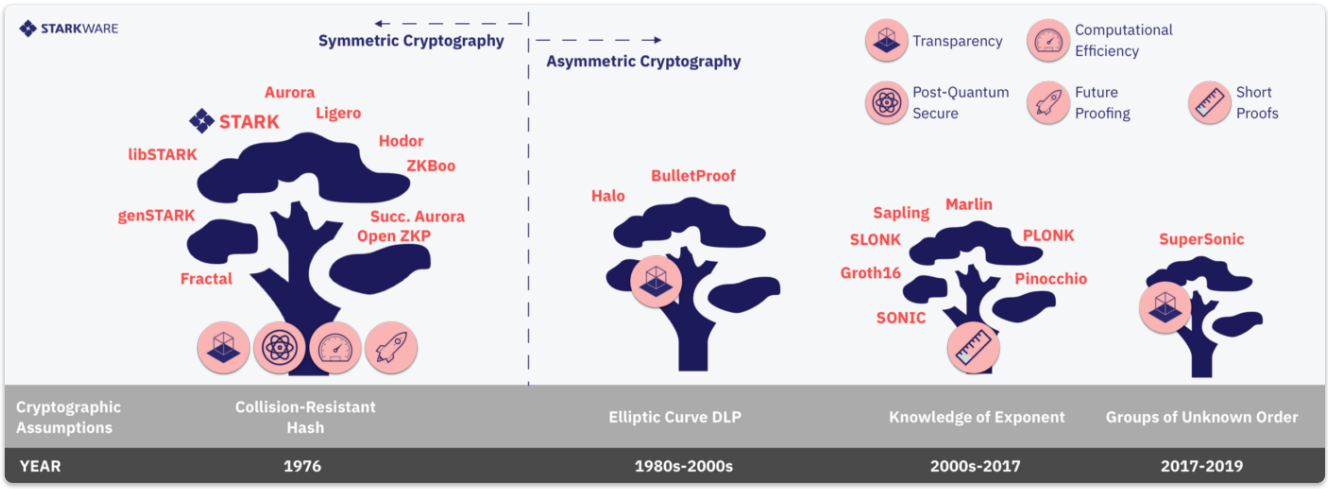
2010 Groth combined these techniques with ideas from interactive zero-knowledge arguments to give the first constant size NIZK arguments.

2016 : Jens Groth - On the Size of Pairing-based Non-interactive Arguments

From Matthew Green

Prior to Goldwasser et al., most work in this area focused the soundness of the proof system. That is, it considered the case where a malicious Prover attempts to 'trick' a Verifier into believing a false statement. What Goldwasser, Micali and Rackoff did was to turn this problem on its head. Instead of worrying only about the Prover, they asked: what happens if you don't trust the Verifier?

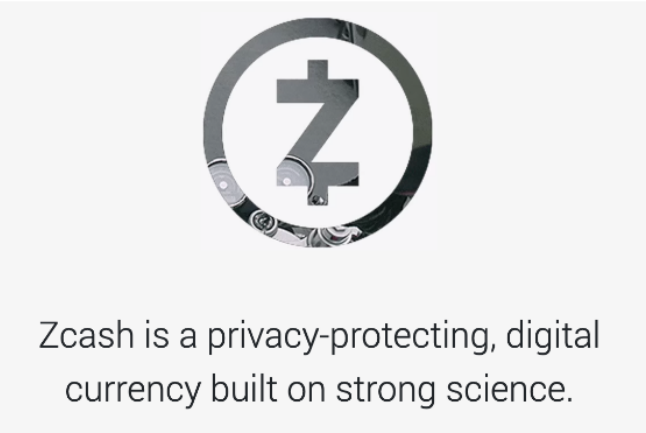
ZKP ECOSYSTEM



from
The Cambrian Explosion

ZKP Use Cases

Privacy preserving cryptocurrencies



Also Nightfall , ZKDai

Blockchain Scalability

For example
Rollups on Ethereum

"The scalability of ZK rollup will increase by up to 4x, pushing theoretical max TPS of such systems well over 1000." - Vitalik

ZkSync
ZK Sync is designed to bring a VISA-scale throughput of thousands of transactions per second to Ethereum.

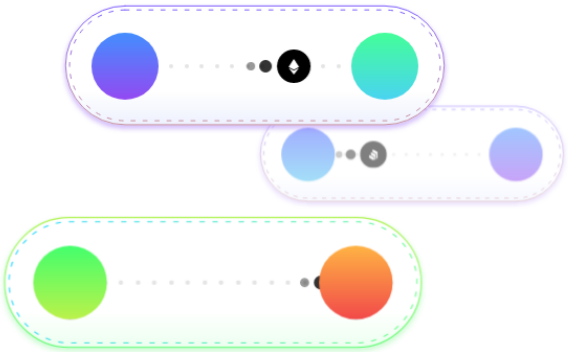
Nuclear Treaty Verification

Privacy Preserving Financial Systems

Aztec

Privacy Guarantee

The new internet of money is secured by openness, but at a high price — all your counterparties know your entire financial history. Aztec is the ultimate security shield for the internet of money, protecting user and business data on Web3.0.



Identity Privacy

With cryptographic anonymity, sender and recipient identities are hidden

Balance Privacy

Transaction amounts are encrypted, making your crypto balances private

Code Privacy

Network observers can't even see which asset or service a transaction belongs to

Identity and Privacy