Group 9

ZERO KNOWLEDGE PROOF

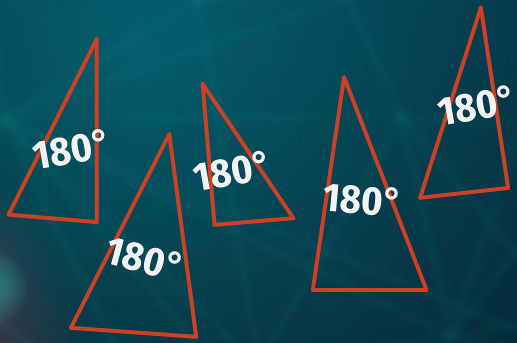
Ilan Halioua, Ismael Barroso, Alejandro Fernandez-Paniagua

01 Anonymous Verifiable Voting

02 Customer ability to pay a debt

Proof

- Convincing steps through logic that can be verified
- Basis of mathematics
- The way to know if something is absolutely true



Zero-Knowledge Proof

- Authentication and validation protocol
- Between **prover** and **verifier**
- Prover **demonstrates** the verifier the truth of a statement **without** *revealing* the content
- **Probabilistic** demonstration

ZKP ROOTS

1985

The method was first introduced by researchers from MIT in a 1985 paper.

- **Inventors**: Goldwasser, Micali, Rackoff

- They received the Gödel Prize
- Paradigm shift
- Huge advance in how something can be validated without sharing any information.

ZKP TYPES

Interactive

Prover proves the statement to a **specific** verifier if after a certain number of 'questions' done by the verifier, the prover answered correctly, making **this** verifier convinced.

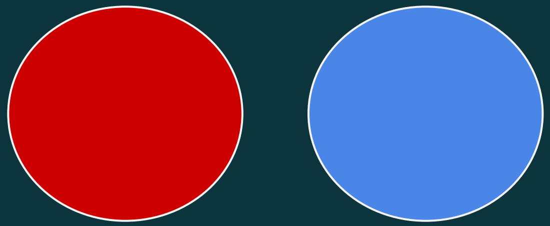
Non-Interactive

There does **not** exist interaction between prover and verifier. The prover creates a proof in such a way that **anyone** who wants to verify the statement, can do it.

Interactive ZKP Example

<u>Likelihood</u>: the more iterations the less likely it is to succeed by luck

<u>Color blind example:</u>



Where n stands for number iterations

$$\frac{1}{2^n}$$

If you increment number of choices to 100 then the probability turns out to be:

$$\frac{1}{100^n}$$

With just a few repetitions (20 for example) for two possible elections then, the intruder has a chance of 0.00009%

Non-Interactive ZKP Example

1. Alice wants to prove to Bob that she knows a value such that $y = g^a$ to base g.
2. Alice picks random value v from the set of values Z, and computes $t = g^v$.
3. Alice computes $c = H(g, y, t)$ where H() is a hash function.
4. Alice computes $d = v - c \cdot a$.
5. Bob or anyone can then check if $t = g^d \cdot y^c$.

Fiat–Shamir heuristic allows us to replace interactive step 3 with non-interactive random oracle access, but in practice, Hash function is used.

In Interactive ZKP, Bob would have picked random value c from set Z and sends it to Alice.

INHERENT PROPERTIES

Completeness

Verification + Privacy preservation

Soundness

Lying resistance

Zero-Knowledge

The icing on the cake

Pros

- Computational secure
- Quantum secure
- Mantain’s users’ privacy
- Scalability
- Simplicity
- Safety

Cons

- Security flaws
- Not efficient
- Very **weak** to **information recovery** once it has been lost

Most Popular Interactive/Non-Interactive ZKPs

S N A R K

Succinct Non-Interactive ARguments of Knowledge (SNARK)

S T A R K

Scalable Transparent ARgument of Knowledge (STARK)

V P D

Verifiable Polynomial Delegation (VPD)

S N A R G

Succinct Non-interactive ARGuments (SNARG)

ZKP EVOLUTION

PINOCCHIO
zk-SNARK
NOT Transparent
NOT Universal
NOT Post-Quantum Secure
Procedural

2013

2021

ZILCH
zk-STARK
Transparent
Universal
Post-Quantum Secure
Object-Oriented

APPLICATIONS

Better performance in terms of privacy

BLOCKCHAIN

Clients privacy for certain bank operations

FINANCE

Allows voters to check if their vote was included, maintaining their privacy

ONLINE VOTING

User authentication without need of confidential info exchange

AUTHENTICATION

Lets owners of ML algorithms to convince people of the model’s outcomes, without showing details of the model

MACHINE LEARNING

CONCLUSIONS