WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

- **Foundational Mathematics for Web3 Builders**

Lecture 25

June 17, 2024

1 Zero-knowledge proofs

- Zero-knowledge (ZK) proofs are a concept in cryptography that allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any additional information beyond the validity of the statement itself.
- In other words, the prover convinces the verifier that they know a piece of information without revealing what that information actually is.
- The term "zero-knowledge" stems from the fact that, ideally, after the proof is completed, the verifier learns nothing except the fact that the statement being proven is true.
- Here's a simplified example to illustrate the concept:
  Imagine that you want to prove to me that you know the solution to a particular puzzle without revealing the solution itself.

We use a zero-knowledge proof as follows:

a) Setup: You and I agree on a puzzle, let's say a Sudoku puzzle, and you know the solution.

b) Challenge: I select a random row, column, or block from the Sudoku grid and ask you to prove that you know the numbers in that row, column, or block without revealing them.

c) Proof: You perform a series of steps that convinces me that you know the solution to that specific part of the puzzle. For example, you could provide a series of swaps of numbers within the selected region that preserves the overall correctness of the puzzle.

d) Verification: I check the steps you performed to ensure they are valid swaps that preserve the correctness of the puzzle.

If they are, I conclude that you must indeed know the solution to the puzzle without learning any new information about the solution itself.

- Zero-knowledge proofs have numerous applications in cryptography, including authentication protocols, digital currencies (like Zcash), secure multi-party computation, and more.
- They are particularly valuable in scenarios where privacy and confidentiality are paramount, as they allow parties to prove statements without revealing sensitive information.
- To better understand the zero-knowledge technique, consider an example of a proof using the Square Root Problem (SQRTP). Remember that getting square roots modulo n is difficult and similar to factorization.

Algorithm 1 (Zero-knowledge proof)

Cyprian selects two huge primes, p and q, and publishes $n = pq$. He also selects a secret value x with $\gcd(x, n) = 1$ and computes $x^2 \bmod n$ then publishes this value. These two values define his identity. Suppose Alex wants to confirm if Cyprian knows the secret value x. They follow the protocol outlined below:

1. Cyprian selects a random unit u_1 modulo n with $\gcd(u_1, n) = 1$ and calculates
   $u_2 = x(u_1)^{-1} \bmod n$. Note that $u_1 u_2 = x$
2. Cyprian then computes $x_1 = (u_1)^2 \bmod n$ and $x_2 = (u_2)^2 \bmod n$ and sends Alex x_1 and x_2.
3. Alex then check $x_1 x_2 = x^2 \bmod n$.
4. Alex then randomly asks for $\sqrt{x_1}$ or $\sqrt{x_2}$.
5. Cyprian sends Alex the quantity he requested.

Algorithm (conti...)

6. When Alex requests $\sqrt{x_1}$, he squares it and compares it to the value $x_1 \mod n$ that Cyprian sent earlier. If Alex requests $\sqrt{x_2}$, he squares the value and compares it to $x_2 \mod n$ that Cyprian sent earlier. If the value agrees upon, Cyprian passes.

   The challenges are repeated until Alex is satisfied that Cyprian does indeed know the secret x.

Example 1

Let $n = 14863$, and $x^2 = 12903 \mod 14863$. Now suppose Cyprian claims to know x, the square root of 12903, but is unwilling to disclose it. Alex challenges Cyprian to prove that he knows x.

- Cyprian chooses $u_1 = 317$. Computes $(u_1)^{-1} = 317^{-1} \mod 14863 = 12800$. Since he knows $x = 583$, he computes $u_2 = x \cdot (u_1)^{-1} \mod 7081 = 583 \cdot 12800 \mod 7081 = 1174$.

Example (conti...)

- Cyprian sends Alex the message $x_1 = (u_1)^2 \bmod 14863 = 11311$ and $x_2 = (u_2)^2 \bmod 14863 = 10880$.
- Alex checks that $x_1 \cdot x_2 \bmod 14863 = 11311 \cdot 10880 \bmod 7081 = 12903 = x^2$.
- Alex sends Cyprian the message "send me $\sqrt{x_1}$ or $\sqrt{x_2}$."
- Cyprian responds with the message $\sqrt{x_1} = 317$ or $\sqrt{x_2} = 1174$.
- Alex checks $(x_1)^2 = 317^2 = 11311 \bmod 14863$ and $(x_2)^2 = 1174^2 = 10880 \bmod 14863$. Alex is now convinced that Cyprian knows x, or otherwise he could not tell the square root of x_1 or x_2.

$u_1 = 317 \bmod 14863$

$317^{-1} \bmod 14863$

$x = 583$

Solution (Explanations)

Euclid's

$14863 = 46 \cdot 317 + 281$

$317 = 1 \cdot 281 + 36$

$281 = 7 \cdot 36 + 29$

$36 = 1 \cdot 29 + 7$

$29 = 4 \cdot 7 + 1$

Extended Euclidean

Algorithm

Solution (Explanations)

$317^{-1} \bmod 14863 = 12800$

$u_1^{-1} = 12800$

$u_2 = 583 \times 12800 \bmod 14863$

$u_2 = 1174$

$\frac{1}{2}$ pro f

$372158 \bmod 14863$

Solution (Explanations)

$x_1 = (u_1)^2 = 317^2 \bmod 14863$

$= 11311$ ✓

$x_2 = (u_2)^2 = 1174^2 \bmod 14863$

$= 10880$ ✓

Alex $x_1 x_2 \bmod 14863$

$= 12903$ ✓

$\sqrt{11371}$ ✓

Example 2

Let $n = 7081$ and $5629 \equiv x^2 \bmod n$. Now suppose Cyprian claims to know x, the square root of 5629, but is unwilling to disclose it. Alex challenges Cyprian to prove he knows x.

- Cyprian chooses $u_1 = 211$. Computes $(u_1)^{-1} = 211^{-1} \bmod 7081 = 1980$.
- Since Cyprian knows $x = 301$, he computes $u_2 = x \cdot (u_1)^{-1} = 301 \cdot 1980 \bmod 7081 = 1176$.
- Cyprian sends Alex the message $x_1 = (u_1)^2 \bmod 7081 = 2035$ and $x_2 = (u_2)^2 \bmod 7081 = 2181$.
- Alex checks that $x_1 \cdot x_2 \bmod 7081 = 2035 \cdot 2181 \bmod 7081 = 5629 = x^2$.
- Alex sends Cyprian the message "send me $\sqrt{x_1}$ or $\sqrt{x_2}$."
- Cyprian responds with the message $\sqrt{x_1} = 211$ or $\sqrt{x_2} = 1176$.

Example (conti...)

- Alex checks $(x_1)^2 = 211^2 = 2035 \bmod 7081$ and $(x_2)^2 = 1176^2 = 2181 \bmod 7081$. Alex is now convinced that Cyprian knows x, or otherwise he could not tell the square root of x_1 or x_2.

$u_1 = 211$ $\quad x = 301$

$n = 7081$

$(u_1)^{-1} \bmod 7081 = 211^{-1} \bmod 7081$

Solution (Explanations)

Euclid's

$$7081 = 33 \cdot 211 + 118$$

$$211 = 1 \cdot 118 + 93$$

$$118 = 1 \cdot 93 + 25$$

$$93 = 3 \cdot 25 + 18$$

$$25 = 1 \cdot 18 + 7$$

$$18 = 2 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

Solution (Explanations)

Using extended Euclid's algorithm

we find $u_1^{-1} = 1980$

$u_2 = x(u_1)^{-1} = 301 \times 1980 \bmod 7081$

$= 1176$

Now square u_1 and u_2

$\Rightarrow x_1 = (211)^2 \bmod 7081 = 2035$

$\Rightarrow x_2 = (1176)^2 \bmod 7081 = \underline{2181}$

Solution (Explanations)

Alex verify $x_1 \cdot x_2$

$2035 \times 2181 \bmod 7081$

$= 5629 \checkmark = x^2$

$\sqrt{x_1} = 211$

$\sqrt{x_2} = 1176$

Take $211^2 \bmod 7081 = 2035$

$1176^2 = 2181$

Example 3

Eve attempts to impersonate Cyprian in the example 2. Alex challenges Eve to prove she knows x.

- Eve knows $n = 7081$ and $5629 \equiv x^2 \bmod n$, since these were published by Cyprian, but she does not know x.
- Eve chooses $u_1 = 170$ and then computes $(u_1)^2 = 170^2 \bmod 7081 = 576$.
- She then computes $(u_1^2)^{-1} = 576^{-1} \bmod 7081 = 2053$. Then computes

$x^2 = u_1^2 \times u_2^2$

$$u_2^2 = x^2 \cdot (u_1^2)^{-1} = 5629 \cdot 2053 \bmod 7081 = 145$$

- Eve sends to Alex $x_1 = (u_1)^2 = 576$ and $x_2 = (u_2)^2 = 145$.
- Alex checks that $x_1 \cdot x_2 \bmod 7081 = 576 \cdot 145 \bmod 7081 = 5629 = x^2$.
- Alex sends Eve the message "send me $\sqrt{x_1}$."

Example (conti...)

- Eve responds with the message $\sqrt{x_1} = 170$. Eve passes this round.

  145 mod 7081)

- Alex sends Eve another message "send me $\sqrt{x_2}$."
- Eve is unable to find $\sqrt{x_2}$.
- Thus, Eve fails the challenge, and now Alex knows she is an impostor. ✓

1.1 To confirm that this protocol is a zero knowledge proof, we examine three things:

a) The test must be complete: Cyprian can always pass it.

b) The test must be sound. That is, to pass the test, intruder Eve must know the value of x. To pass the test, Eve must be able to compute $\sqrt{x_1}$ and $\sqrt{x_2}$ modulo n. If she can do this, then she can compute x, since it's the same as knowing it. If Eve does not know x, she can only provide one of the two values $\sqrt{x_1}$ or $\sqrt{x_2}$ when challenged by Alex, giving her a 50% chance of passing the test.

c) The test needs to be zero-knowledge, meaning intruder Eve can't learn the secrets by eavesdropping in on actual conversations between Cyprian and Alex.