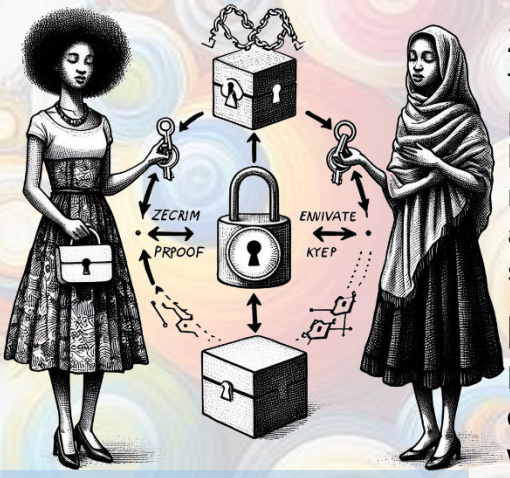
Zero-Knowledge Authentication



Zero Knowledge is a cryptographic concept designed to facilitate secure interactions between parties while preserving the privacy of sensitive information. The essence lies in proving possession of certain knowledge without actually revealing the knowledge itself. This cryptographic paradigm addresses the growing concerns around data privacy and security in various applications.

Preserving Secret Safely

Imagine opening a locked box without showing the key, but convincing someone you have it by solving puzzles associated with the lock.

Example: Peggy and Victor

Imagine a cave with two entrances: Prover (Peggy) knows a secret path that connects the two entrances. Verifier (Victor) wants to know if Peggy knows the path, but not the path itself. Here's how a zero-knowledge protocol could unfold:
Victor waits at one entrance (A), while Peggy enters the other (B). Victor calls out a specific entrance (A or B) randomly. Peggy must emerge from the designated entrance. They repeat this process multiple times. If Peggy consistently appears at the correct entrance, Victor becomes convinced that she knows the secret path, even though he never learns its details.

Key Points

Zero knowledge: Victor gains no knowledge of the path itself.
Soundness: Peggy can't consistently fool Victor
Completeness: If Peggy knows the path, she can always convince Victor.

Zero-Knowledge Logins

Applies the concept to online logins. Instead of sharing passwords, users prove they possess the correct "secret" (password) through cryptographic interactions.
The verifier challenges the user with proofs, each verifying specific aspects of the password without ever revealing it.

Zero-knowledge proof or zero-knowledge protocol is a cryptographic method by which one party can prove to another party that a given statement is true, without conveying any information beyond the mere fact of the statement's truth.

Zero-knowledge authentication is a type of scheme where one party proves to the other to **have a particular piece of knowledge** that proves ownership of the identity, without further disclosing any additional sensitive or personal information

Zero-knowledge protocols are a powerful tool for privacy and security, but they are not without their risks. ZK proofs are often considered an expensive way of enforcing honest behavior

Ji-Won (지원) is a cryptography researcher and volunteer in PakCrypt outreach program.