Zero-Knowledge Login System using RSA Encryption

David Stupar
daviddstupar@gmail.com

Abstract:

This whitepaper introduces a novel Zero-Knowledge Login System that leverages RSA encryption and zero-knowledge proofs to enhance the security of user authentication while preserving user privacy. By integrating RSA encryption, blockchain, and zero-knowledge principles, this system presents a formidable barrier against unauthorized access and data breaches.

1. Introduction

In the realm of cybersecurity, robust user authentication systems are imperative to safeguard digital assets and sensitive data. This whitepaper presents an innovative approach to authentication, showcasing the powerful synergy between RSA encryption and zero-knowledge proofs.

2. Random Phase

At each login attempt, the server employs a cryptographically secure random number generator to create a unique random phase. This unique phase must be 256 or more for security reasons.

3. RSA Encryption

To encrypt the random phase the first step is retrieving data from the blockchain where all public keys are stored. Then the generated random phase is encrypted with the public key using RSA algorithm. When everything is done the encrypted phase is sent to the user

4. User-side Decryption

The user's browser receives the encrypted random phase. The user employs their private key, securely stored on their local machine, to decrypt the encrypted phase. The decryption process ensures that sensitive data remains confidential during transmission.

5. Zero-Knowledge Proof and Decrypted Message Upload

The decrypted random phase serves as the basis for a zero-knowledge proof. The user uploads the decrypted message to the server, allowing the server to verify the user's knowledge of the phase without actually gaining any knowledge about the private key.

6. Verification and Login Validation

The server verifies the decrypted message against the initially generated random phase. If the two match, the login attempt is validated, granting the user access.The use of a zero-knowledge proof guarantees that the server does not acquire knowledge of the user's password or decryption key.

7. Benefits and Advantages:

- Enhanced Security: The integration of zero-knowledge proofs and RSA encryption engenders an authentication mechanism that resists a broad spectrum of potential attacks.
- User Privacy: Throughout the authentication process, user privacy remains uncompromised, as the server does not directly interact with sensitive authentication data.
- Dynamic Challenges: The utilization of a unique random phase fortifies security by impeding the feasibility of attackers exploiting patterns.

8. Conclusion

The Zero-Knowledge Login System presented in this whitepaper epitomizes a monumental stride towards fortifying digital security paradigms. The seamless amalgamation of RSA encryption and zero-knowledge proofs manifests as a watershed moment in the realm of user authentication. This dynamic system transcends conventional methodologies, ushering in an era defined by impervious security, privacy preservation, and user-centricity.