***V. Kurylo**, BA student*
***O. Pasichnyk**, PhD in Ped., As. Prof., language advisor*
Khmelnytskyi National University

ZERO-KNOWLEDGE PROOFS: THE MATHEMATICS OF PRIVACY

In the modern digital landscape, we are constantly faced with a fundamental privacy dilemma: how can we prove that a statement is true without revealing the sensitive information behind it? Historically, proving one's identity or qualifications required the disclosure of vast amounts of personal data. To prove you are of legal age, you show an ID card that also reveals your exact birth date, address, and full name. To prove financial stability, you share bank statements that expose your entire transaction history.

Zero-Knowledge Proofs (ZKP) represents a revolutionary shift in this paradigm. Originating from the field of cryptography, ZKPs allow one party to convince another that they possess a specific piece of information without ever disclosing the information itself. It is a mathematical solution to the problem of "trust but verify," where verification no longer requires the sacrifice of privacy.

The concept of Zero-Knowledge Proofs was first introduced in 1985 by researchers Shafi Goldwasser, Silvio Micali, and Charles Rackoff [1]. At its core, a ZKP is a protocol involving two parties: the Prover and the Verifier. The Prover claims to know a secret or a solution to a mathematical problem, and the Verifier's job is to confirm this claim without learning what the secret actually is.

For a protocol to be considered a true Zero-Knowledge Proof, it must satisfy three essential properties:

1. Completeness: If the statement is true and both parties follow the rules, the Verifier will be convinced by the Prover. This ensures that the system works under honest conditions.
2. Soundness: If the statement is false, it is mathematically impossible (or statistically highly improbable) for a cheating Prover to convince the Verifier otherwise. This prevents fraud and ensures the integrity of the proof.
3. Zero-Knowledge: If the statement is true, the Verifier learns nothing other than the fact that the statement is true. They do not gain any additional insights into the Prover's secret.

Early versions of these proofs were interactive. They functioned like a high-stakes game of "Twenty Questions," where the Verifier would challenge the Prover through multiple rounds of communication. In each round, the Prover would provide a response that increased the Verifier's confidence. While effective, this required both parties to be online and communicating simultaneously.

The evolution of the field led to Non-Interactive Zero-Knowledge Proofs (NIZK). These allow a Prover to generate a single, static proof that can be verified by anyone at any time without further interaction. The most prominent modern implementation is known as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). These proofs are "succinct," meaning they are very small in size and can be verified in milliseconds, even if the underlying statement being proven is incredibly complex.

The mathematical elegance of ZKPs has profound implications for several industries [1; 2]:

Blockchain and Finance: This is perhaps the most well-known application. In public blockchains like Bitcoin, every transaction is visible to everyone. However, using ZKPs,

networks like Zcash or Ethereum (via Layer-2 scaling solutions) can prove a transaction is valid—meaning the sender has enough funds and the signature is correct – without revealing the sender, receiver, or the amount sent.

Identity Management: ZKPs enable "Self-Sovereign Identity." Users can prove they are over 18, hold a specific citizenship, or have a clean criminal record without sharing their actual documents. The verifier receives a mathematical "Yes" or "No" instead of a photocopy of a passport.

Secure Voting: In a digital voting system, ZKPs can prove that a vote was counted correctly and that the voter was eligible, all while maintaining the absolute secrecy of the ballot. This solves the long-standing challenge of making electronic voting both transparent and private.

Cybersecurity: ZKPs can replace traditional password systems. Instead of sending a password to a server (where it could be stolen in a data breach), a user can simply prove they know the password through a zero-knowledge exchange. The server never sees the password, so it has nothing for hackers to steal.

To understand the theory of how a Prover can convince a Verifier without revealing a secret, cryptographers often use the "Ali Baba Cave" analogy [4]. Imagine a circular cave with a single entrance that splits into two paths, Path A and Path B. At the back of the cave, there is a magic door that connects the two paths, but it can only be opened by someone who knows a secret password.

The Prover (Alice) wants to prove to the Verifier (Bob) that she knows the password without telling it to him. To do this, Alice enters the cave while Bob waits outside, choosing either Path A or Path B. Once Alice is out of sight, Bob walks to the entrance and shouts which path he wants Alice to return from (e.g., "Come out through Path B!").

If Alice truly knows the password, she can open the magic door and return via whichever path Bob chooses. If she doesn't know the password, she can only return via the path she originally took. If they repeat this process forty times, and Alice successfully returns via the requested path every single time, the mathematical probability that she is "guessing" becomes so small that Bob can be certain she knows the secret. Yet, at no point did Bob hear the password or see the door. This is the essence of a zero-knowledge exchange.

Despite the mathematical elegance of Zero-Knowledge Proofs, their implementation is not without hurdles. One of the most significant theoretical and practical challenges is the "Trusted Setup." Many ZKP systems, particularly early versions of zk-SNARKs, require an initial phase where specific mathematical parameters are generated.

If the individuals performing this setup are dishonest, they could potentially create "fake" proofs that look valid, undermining the entire system's integrity. To combat this, developers often use "Multi-Party Computation" (MPC) ceremonies, where dozens of people from around the world contribute to the setup. As long as at least one participant is honest and destroys their part of the data, the system remains secure. Newer iterations, such as zk-STARKs, aim to eliminate this requirement entirely, moving toward a "transparent" model that requires no initial trust.

The shift toward ZKPs is more than just a technical upgrade; it is a movement toward data sovereignty. In the current "Surveillance Capitalism" model, users are the product, and their data is the raw material. ZKPs flip this script. By allowing for "Privacy by Design," companies can offer services—such as credit scoring, medical analysis, or social networking—without ever actually "possessing" the user's raw data.

From a legal perspective, this could redefine compliance with regulations like the GDPR. If a company never stores a user's date of birth but only a proof that the user is over 18, the risk of a data breach is neutralized. This "mathematical shield" protects not only the individual from identity theft but also protects the corporation from the immense liability associated with holding sensitive information.

REFERENCES

1. Understanding Zero Knowledge Proofs and Their Importance [Electronic resource]. – Available at: https://subquery.medium.com/understanding-zero-knowledge-proofs-and-their-importance-8d01813fa3ad (accessed: 22.03.2026).
2. Isabel M., Rodriguez-Nunez C., Rubio A. Scalable Verification of Zero-Knowledge Protocols // *2024 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2024. – P. 1794-1812. – DOI: 10.1109/SP54263.2024.00133.
3. Abbas S. S., Sierra-Sosa D., Kumar A., Elmaghraby A. IoT in Smart Cities: A Survey of Technologies, Practices and Challenges // *Smart Cities*. – 2021. – Vol. 4, No. 1. – P. 429-475.
4. Tabacaru R., Anghel F., Asandoaiei D., Simion E. The challenges of proving solvency while preserving privacy [Electronic resource] // *Cryptology ePrint Archive*. – Available at: https://eprint.iacr.org (accessed: 22.03.2026).