Abstract: Zero-Knowledge Proofs (ZKPs), a cryptographic tool known for decades, have gained significant attention in recent years due to advancements that have made them practically applicable in real-world scenarios. ZKPs can provide unique attributes, such as succinctness, non-interactivity, and the ability to prove knowledge without revealing the information itself, making them an attractive solution for a range of applications.

This paper aims to critically analyze the applicability of ZKPs in various scenarios. We categorize ZKPs into distinct types: SNARKs (Succinct Non-Interactive Arguments of Knowledge), Commit-then-Prove ZKPs, MPC-in-the-Head, and Sigma Protocols, each offering different trade-offs and benefits. We introduce a flowchart methodology to assist in determining the most suitable ZKP system, given a set of technical application requirements. Next, we conduct an in-depth investigation of three major use cases: Outsourcing Computation, Digital Self-Sovereign Identity, and ZKPs in networking. Additionally, we provide a high-level overview of other applications of ZKPs, exploring their broader implications and opportunities. This paper aims to demystify the decision-making process involved in choosing the right ZKP system, providing clarity on when and how these cryptographic tools can be effectively utilized in various domains — and when they are better to be avoided.

@misc{cryptoeprint:2024/050, author = {Jens Ernstberger and Stefanos Chaliasos and Liyi Zhou and Philipp Jovanovic and Arthur Gervais}, title = {Do You Need a Zero Knowledge Proof?}, howpublished = {Cryptology ePrint Archive, Paper 2024/050}, year = {2024}, note = {\url{https://eprint.iacr.org/2024/050}}, url = {https://eprint.iacr.org/2024/050} }

https://eprint.iacr.org/2024/050