Zero-knowledge proofs in self-tallying voting protocols

Ivana Stančíková

Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic
xstanc03@stud.fit.vutbr.cz

Abstract

A zero-knowledge proof is a cryptographic encryption scheme that allows one party (a *prover*) to demonstrate to another party (a *verifier*) the knowledge of a secret without revealing the secret itself. For example, one can prove the ownership of a private key corresponding to a given public key but still keep the private key secret.

In 1985, Goldwasser et al. [2] introduced interactive zero-knowledge proofs, requiring multiple rounds of communication between the prover and verifier. Later, this concept was optimized into a non-interactive protocol [1], i.e., requiring a single message sent by the prover to the verifier.

In this work, we first demonstrate the principles and properties of interactive and non-interactive zero-knowledge proofs on easy-to-understand examples and later formally define them using theoretical computer science and cryptography constructs.

Practical use cases for zero-knowledge proofs can be found in applications where preserving privacy is essential, such as electronic voting. We show self-tallying voting protocols [3] as an example of a practical use of zero-knowledge proofs.

In self-tallying voting protocols, any interested party can compute the tally, eliminating the need for a trusted authority. To strongly protect voters' privacy, the votes are encrypted at all times using homomorphic encryption. While the homomorphic property enables tally computation over encrypted votes, it also introduces an issue – an incorrectly formed vote can cause the tally computation to fail. Therefore, we require voters to provide zero-knowledge proofs to confirm that their votes are formed correctly without revealing their choice of candidate.

References

[1] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 103–112, 1988.

[2] S GOLDWASSER. The knowledge complexity of interactive proof systems. In *Proceedings of 17th ACM Symposium on Theory of Computing*, pages 291–304, 1985.

[3] Aggelos Kiayias and Moti Yung. Self-tallying elections and perfect ballot secrecy. In *International Workshop on Public Key Cryptography*, pages 141–158. Springer, 2002.