Chapter 9

Zero Knowledge Proofs: A Survey

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

Mala K.
Mepco Schlenk Engineering College, India

ABSTRACT

Zero knowledge protocols provide a way of proving that a statement is true without revealing anything other than the correctness of the claim. Zero knowledge protocols have practical applications in cryptography and are used in many applications. While some applications only exist on a specification level, a direction of research has produced real-world applications. Zero knowledge protocols, also referred to as zero knowledge proofs, are a type of protocol in which one party, called the prover, tries to convince the other party, called the verifier, that a given statement is true. Sometimes the statement is that the prover possesses a particular piece of information. This is a special case of zero knowledge protocol called a zero-knowledge proof of knowledge. Formally, a zero-knowledge proof is a type of interactive proof.

INTRODUCTION

A Zero-Knowledge Proof system is an example of a two-party computation where a prover tries to prove something to a verifier without revealing anything more than what is being proved. For example, the prover can prove to the verifier that he knows a password without actually revealing the password. The Zero Knowledge Proofs are a special case of type of Proof systems called Interactive Proof. In this chapter, we provide a number of examples to show how zero knowledge proofs can be constructed. We also discuss the variations of the zero knowledge proofs and their applications.

This chapter is about proof schemes, protocols with which Peggy “the Prover” can try and prove something to Veronica “the Verifier” who can either accept or reject Peggy’s claim. Suppose that Peggy wishes to prove to Veronica that she knows the code to a safe. Peggy could simply tell Veronica the code. This is a perfectly good proof scheme but Veronica ends up knowing not just that Peggy knows the code, but the code itself too. Peggy could also just state that she knows the code. This protects Peggy’s secret

DOI: 10.4018/978-1-5225-2915-6.ch009
knowledge, but might not convince Veronica. However, Peggy could also let Veronica observe the closed safe, ask her to look away then enter the code and open the safe, allowing Veronica to deduce that Peggy knows the code without Veronica gaining the ability to open the safe herself. This is what cryptographic proof schemes aim to achieve, security guarantees for both Peggy’s secret and Veronica’s trust.

**ZERO-KNOWLEDGE PROTOCOLS**

Peggy’s knowledge is protected by properties such as zero-knowledge, which informally says that Veronica gains no extra knowledge from Peggy by following a proof scheme with her, beyond whatever Peggy wanted to prove in the first place. The security properties for Veronica can include a protocol being sound, i.e. Peggy cannot convince Veronica of a false claim. The scheme can also be a “proof of knowledge” which informally means that Peggy cannot convince Veronica unless she actually knows what she claims to know.

Zero knowledge protocols provide a way of proving that a statement is true without revealing anything other than the correctness of the claim. Zero knowledge protocols have practical applications in cryptography and are used in many applications. While some applications only exist on a specification level, a direction of research has produced real-world applications.

Zero knowledge protocols, also referred to as zero knowledge proofs, are a type of protocol in which one party, called the prover, tries to convince the other party, called the verifier, that a given statement is true. Sometimes the statement is that the prover possesses a particular piece of information.

This is a special case of zero knowledge protocol called a zero-knowledge proof of knowledge. Formally, a zero-knowledge proof is a type of interactive proof.

An interactive proof system is an interaction between a verifier and a prover satisfying the following properties:

- **Completeness**: If the statement being proven is true, an honest verifier, a verifier correctly following the protocol, will be convinced after interacting with an honest prover.
- **Soundness**: If the statement is false, no prover, either honest or dishonest, will be able to convince an honest verifier, except with some small probability.

For an interactive proof to be a zero-knowledge proof it must also satisfy the condition of zero knowledge. A proof is zero knowledge if any knowledge known by the prover or the verifier before performing the proof is the same as the knowledge known by either party after performing the proof. In other words, no additional knowledge is gained by either party because of the proof. Another way of thinking about this is that the proof reveals zero knowledge (Mohr, 2007).

**THE MAGICAL CAVE**

The classic example for zero knowledge protocols is the cave example.

Peggy has stumbled across a magical cave. Upon entering the cave there are two paths, one leading to the right and one leading to the left. Both paths eventually lead to a dead end. However, Peggy has discovered a secret word that opens up a hidden door in the dead end, connecting both paths.
Related Content

The Quadratic Sieve Algorithm for Integer Factoring
[www.igi-global.com/chapter/the-quadratic-sieve-algorithm-for-integer-factoring/188526?camid=4v1a](www.igi-global.com/chapter/the-quadratic-sieve-algorithm-for-integer-factoring/188526?camid=4v1a)

Review of Link Structure Based Ranking Algorithms and Hanging Pages
[www.igi-global.com/chapter/review-of-link-structure-based-ranking-algorithms-and-hanging-pages/153086?camid=4v1a](www.igi-global.com/chapter/review-of-link-structure-based-ranking-algorithms-and-hanging-pages/153086?camid=4v1a)

Discovering Periodicity in Network Flows for Security Monitoring
[www.igi-global.com/chapter/discovering-periodicity-in-network-flows-for-security-monitoring/153076?camid=4v1a](www.igi-global.com/chapter/discovering-periodicity-in-network-flows-for-security-monitoring/153076?camid=4v1a)

Current Application Areas
[www.igi-global.com/chapter/current-application-areas/176870?camid=4v1a](www.igi-global.com/chapter/current-application-areas/176870?camid=4v1a)