Indraprastha Institute of Information Technology

A

Project Report

On

Zero Knowledge Proofs for Authenticated and Secure Communication

Submitted by – Ritesh Gupta (MT24132)

and Bhargav Jani (MT24115)

Under the guidance of

Dr Ravi Anand

(Assistant Professor CSE)

Abstract

Zero-knowledge proofs (ZKPs) have emerged as a powerful cryptographic tool for establishing trust in secure communication without revealing sensitive information. This paper explores the application of ZKPs in enabling authenticated and secure communication channels. By leveraging ZKPs, parties can verify each other's identities and validate critical data exchanges without disclosing private details, thus preserving confidentiality. We detail the integration of ZKPs with cryptographic protocols like key exchange mechanisms and authentication frameworks, ensuring robust protection against eavesdropping, impersonation, and other security threats. Our findings demonstrate that ZKPs enhance communication security in privacy-critical environments, such as financial transactions, secure messaging, and blockchain systems, by achieving both authenticity and data integrity while minimizing exposure of private information. This paper also discusses the computational efficiency and challenges associated with implementing ZKPs in real-world scenarios, underscoring their potential in advancing privacy-preserving secure communication technologies.

Table of Contents

1. Introduction

In today’s digital landscape, ensuring secure and authenticated communication is paramount as cyberattacks and privacy breaches become increasingly sophisticated. Traditional security protocols often rely on revealing sensitive information or pre-shared secrets, which can expose vulnerabilities if intercepted or misused. Zero-knowledge proofs (ZKPs) offer a revolutionary approach to address this challenge by allowing one party (the prover) to prove knowledge of specific information to another party (the verifier) without revealing the information itself.

The concept of zero-knowledge proofs, introduced by Goldwasser, Micali, and Rackoff, has gained widespread recognition for its ability to balance security and privacy. In secure communication, ZKPs can verify identities, authenticate messages, and validate transactions while ensuring that no extraneous data is disclosed during the process. This property makes ZKPs an ideal candidate for applications requiring high security and privacy, such as encrypted messaging, financial systems, and distributed ledger technologies.

This paper examines the application of zero-knowledge proofs in establishing authenticated and secure communication channels. We explore how ZKPs can integrate with existing cryptographic protocols, enhancing their ability to protect against common attacks such as man-in-the-middle, replay, and impersonation. Additionally, we address the computational efficiency of ZKP-based systems and the challenges of deploying them at scale. Through this investigation, we aim to highlight the transformative potential of ZKPs in safeguarding digital communication in an era of increasing data sensitivity and cybersecurity threat

2. Motivation

As the world becomes increasingly interconnected, the demand for secure and private communication channels has grown exponentially. From financial transactions to personal messaging and critical government communications, ensuring confidentiality, integrity, and authenticity of data is essential. However, conventional cryptographic protocols often require the sharing of sensitive information, such as passwords, keys, or other secrets, which can become points of vulnerability if intercepted or exposed.

Zero-knowledge proofs (ZKPs) offer a compelling solution to this dilemma by enabling verification without disclosure. The ability to prove possession of knowledge or authorization without revealing the underlying data eliminates a critical attack vector in traditional authentication and communication methods. This innovation aligns perfectly with the needs of privacy-conscious users and organizations, particularly in domains like financial technology, blockchain systems, and secure government communications, where privacy and security are paramount.

Moreover, the rapid advancements in quantum computing and sophisticated cyberattacks underscore the need for stronger, more future-proof security measures. ZKP-based solutions not only meet current security standards but also exhibit resilience against evolving threats, providing a robust foundation for next-generation cryptographic systems.

The motivation behind this research is to harness the unique capabilities of ZKPs to design communication protocols that achieve the dual goals of authentication and security while preserving privacy. By addressing the challenges of implementing ZKPs in practical systems, this work aspires to pave the way for a more secure and trust-enhanced digital ecosystem.

3. Zero-knowledge proofs

Zero-knowledge proof is a method by which one party, the prover, can convince another party, the verifier, that they possess knowledge of some information without revealing the knowledge itself. A prover can for example convince a verifier that a confidential transaction is valid without revealing why that is the case, i.e. without leaking the transacted values. While the prover can prove his possession of some knowledge by simply revealing that knowledge to the verifier, the challenge of ZKP is to prove such knowledge without revealing the information itself or any additional information at all.

3.1 Intuition

There is a cave with a single entrance but with two interconnected tunnels that form a ring. In the ring, there is a locked door on the opposite side of the entrance which opens when some secret code is input on its puzzle-lock.

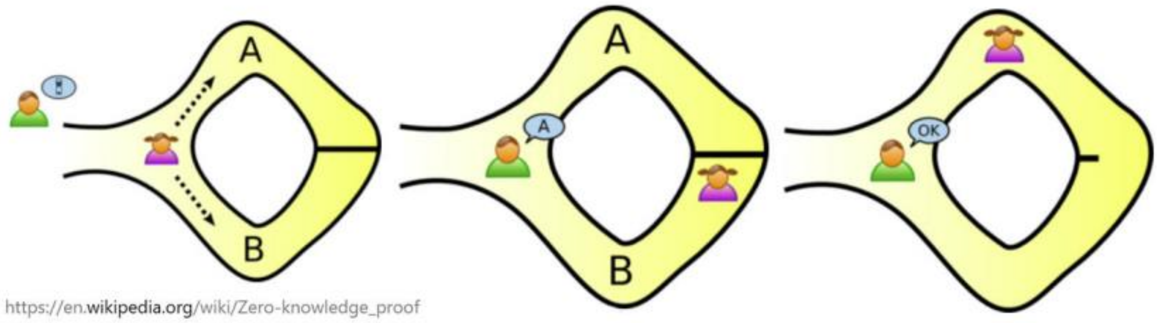

Figure 1: Ali Baba Cave Story(Wikipedia)

Example 1: The figure 1 shows the layout of this cave. Peggy, wearing a pink shirt in the figure 1, knows the puzzle-lock secret and she, as prover, wants to demonstrate to the verifier Victor, who is wearing the green shirt, that she knows the code that unlocks the door but without revealing the secret code itself. To proceed with this proof, they engage in the following protocol:

- *Peggy enters the cave from one of the two tunnels to the ring, A or B, while Victor waits outside.*
- *Then, Victor goes to the cave entrance and shouts to Peggy, asking her to leave the cave from either side A or B. Victor must choose his exit request randomly.*
- *If Peggy is on side B and Victor requested exit through side A, she can open the door and leave the cave from the right side. Otherwise, she can just leave the cave from the same side B. The point is that if Peggy knows the door secret, she should always be able to satisfy Victor's exit request regardless of what Victor chooses.*

Because there is a 50% probability that Victor will request Peggy to exit from the same side that she entered from, Peggy may get lucky and satisfy Victor's requests without actually knowing the secret code. However, if request for exit side is truly random, and the protocol is repeated enough times, the probability of Peggy satisfying all of Victor's requests without knowing the secret becomes vanishingly small.

3.2 Definition

Zero-knowledge proof is defined by a protocol involving two parties, prover and verifier, in which prover convinces the verifier that a statement of the form u ∈ L holds true where L is a language in NP. A witness w is a piece of information that allows one to efficiently verify that that the statement u ∈ L is true. The protocol must satisfy three properties:

- Completeness: A prover holding a witness w to u ∈ L can convince the verifier.
- Soundness: A cheating prover P ∗ cannot convince the verifier when u 6∈ L except with some small probability.
- Zero-knowledge: The interaction only shows that statement u ∈ L is true. It reveals nothing else, in particular it does not disclose anything of the witness w.

3.3 Interactive Proofs

Figure 2 shows the typical structure of interactive zero-knowledge proofs. This structure, also known as Sigma protocol, comprises of three communication steps between prover and verifier:

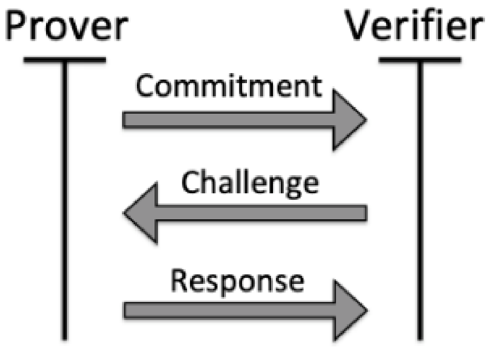

Figure 2: ZKPs - Sigma Protocol

1. Commitment: Prover commits to a particular value and transfers the commitment to the verifier. In the cave story, this step is equivalent to Peggy choosing one of the two sides to enter the cave, and letting verifier know once she has entered the cave.

2. Challenge Verifier sends a random challenge to the prover. This step is equivalent to Victor challenging Peggy to exit from one of two sides chosen at random.

3. Response Prover computes a response based on the challenge and witness, and sends it to verifier for the task of verification. This step corresponds to Peggy leaving the cave from the side requested by Victor given her secret knowledge. Victor, waiting at the mouth of the cave, can check whether Peggy returns from the requested side.

The interactive ZKP protocols are rarely used in practice due to the restrictions they impose on the proof system. First, the interactive protocol often assumes that prover is very powerful with unbounded computational capacity since prover may have to conduct exponentially large number of rounds to convince an honest verifier that the proof is valid. Second, it is a synchronous protocol meaning that prover and verifier need to interact with each other in real time to execute the protocol. It goes without saying that such restrictions limit the suitability of these proofs for most applications which require concurrency and non-interactivity.

3.4 Non-Interactive Proof

In several settings, it is necessary to have an offline verification process. For example, in cryptocurrency, zero-knowledge proofs can be useful in validating integrity of a transaction stored in the blockchain while protecting the participant's information. This validation needs to be performed by several validators in the blockchain. It is not practical to make transaction participants interact with all the validators. Moreover, they will most likely not be available to interact with each other at the same time. Therefore, a mechanism to allow a verification process that does not depend on interaction between prover and verifier is very useful in this example as well as many other applications of ZKPs.

Fortunately, there is a very simple and powerful construction to transform a interactive proof into a non-interactive proof under some assumptions. Fiat-Shamir heuristic [11] takes an interactive proof and creates a non-interactive version provided that the original proof is public coin. This assumption basically states that the challenges made by the verifier on the interactive protocol are public. The central idea of this protocol is to use a hash function on the commitment aiming to generate a random and unpredictable challenge from the perspective of the prover. This way, even though the prover generates an entire transcript of the protocol without interacting with verifier, the prover cannot cheat as the output of the hash function is beyond his control. Figure 3 presents the structure of non-interactive protocol where challenge is replaced by hash of the previous commitments in the protocol. Point cheval and Stern proved that Fiat-Shamir protocol is secure against chosen message attack as long as the hash function used behaves like a random oracle. The resulting Fiat-Shamir transcript is a digital signature of the proof and it can be verified multiple times and at any time the verifier wants to check the proof.

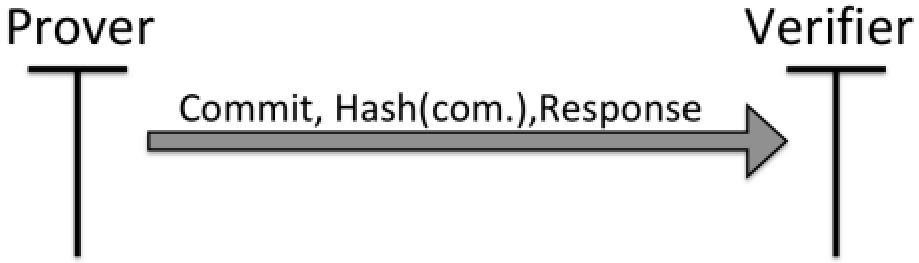

Figure 3: Zero-knowledge proof - Fiat Shamir heuristic

4. Preliminaries

To understand the role of zero-knowledge proofs (ZKPs) in authenticated and secure communication, it is essential to first establish the foundational concepts and cryptographic principles that underpin this technology.

1. **Zero-Knowledge Proofs (ZKPs)**

   A zero-knowledge proof is a cryptographic protocol in which a prover convinces a verifier that they possess certain knowledge (e.g., a secret or solution) without revealing the knowledge itself. ZKPs satisfy three key properties:

   - **Completeness:** If the prover possesses the claimed knowledge and follows the protocol, the verifier will be convinced.
   - **Soundness:** If the prover does not possess the claimed knowledge, they cannot convince the verifier, except with negligible probability.

- **Zero-Knowledge:** No information about the secret is revealed to the verifier beyond the fact that the prover possesses it.

2. **Cryptographic Protocols for Secure Communication**

   Secure communication protocols involve mechanisms to ensure the confidentiality, integrity, and authenticity of exchanged messages. These typically rely on techniques such as:

   - **Symmetric Encryption:** Shared-key algorithms for encrypting data.
   - **Asymmetric Encryption:** Public-key cryptography for secure key exchanges.
   - **Digital Signatures:** For verifying the authenticity of messages and their sources.

3. **Authentication and Key Exchange**

   Authentication is the process of verifying the identity of communicating parties, often achieved using passwords, digital certificates, or shared keys. Key exchange protocols, such as Diffie-Hellman or elliptic curve cryptography (ECC), are used to establish shared secrets securely between parties.

4. **Applications of ZKPs**

   ZKPs are increasingly used in various security-critical applications:

   - **Blockchain Systems:** To verify transactions without revealing details (e.g., zk-SNARKs in cryptocurrencies).
   - **Secure Voting:** Ensuring voter privacy while maintaining election integrity.
   - **Authentication Systems:** Password less authentication to eliminate exposure of credentials.

5. **Types of ZKPs**

   - **Interactive ZKPs:** Require multiple rounds of communication between the prover and verifier.
   - **Non-Interactive ZKPs (NIZKs):** Allow proofs to be precomputed and verified independently, making them suitable for distributed systems and real-time applications.

The above section lays the groundwork for understanding how ZKPs can be integrated into secure communication protocols, enabling privacy-preserving authentication and ensuring robust protection against common cyber threats.

5. Proof Requirements

In order to start visualizing the concept of ZKP, we can start with a couple of toy examples that are helpful. Here and in the rest of the text we will refer to the prover as Peggy and to the verifier as Victor.

Example 2. Assume that Victor is completely colourblind16. Peggy wants to prove to Victor that she is not colourblind, so she devises an experiment. Peggy takes two balls completely identical, save for their colour, and gives them to Victor, one in his left and one in his right hand. Peggy asks Victor to put the balls behind his back, and to decide whether to swap them or not, without telling her. She then asks Victor to show the two balls. Peggy concludes by telling Victor whether he swapped the balls or not. This is a zero-knowledge proof in the sense that:

1. *If Peggy were colourblind, she would not be able to tell whether Victor switched the balls or not, and so the best she could do is guess, getting it right half (1/2) of the time.*
2. *If Peggy is not colourblind, she will be able to answer correctly every time, and thus convince Victor*
3. *Victor does not learn anything else about his environment, apart from the fact that Peggy is not colourblind.*

This illustrates the general idea of Zero Knowledge Proofs. The proof part is devised as an experiment or challenge from the verifier to the prover, that the prover can only answer by having the necessary piece of information or "power". The prover cannot fool the verifier consistently and an honest prover and honest verifier will agree on the fact. Furthermore, no new information is learned by the verifier. Also, if external observers were to have witnessed the exchange they would not be convinced of the fact (as Peggy and Victor could have coordinated their answers). Note however that in this case a simpler protocol can actually fulfil the requirement. For example, Peggy could go into the cave, showing Victor which entrance, she took, and come out from the other entrance. This in effect amounts to removing the need of an interaction between Peggy and Victor, which is something that is quite desirable in real world applications. In particular we will see this in Section 8, with regards to Schnorr signatures. Note that this transformation also removes the probability aspect, which instead is something that in general we cannot do for non-trivial languages, but I digress.

5.1 Parties in play

In the sequel, we will have two parties interacting, the prover and the verifier that, as before, will be colloquially referred to as Peggy and Victor. In mathematical notation we will have P, V always referring, respectively, to prover and verifier. As in maths, we aim to have the verification procedure be as efficient as possible, while most of the computational burden will be placed on the prover. This mirrors the definition of NP we used above, as the class of all problems whose solution can be efficiently verified. Furthermore, it is crucial to understand that the verifier inherently does not trust the prover (otherwise there would not be need for the proof to be provided), and as such Victor will be sceptical of everything that Peggy says. The general situation will be Peggy and Victor having access to some common input, plus each one possibly having access to some additional private input, which will often be related from the shared input.

5.2 Soundness

The condition of soundness asserts that an honest verifier cannot be tricked into accepting a false statement by a possibly cheating prover. In the first example, this is equivalent to stating that, if Peggy is indeed colourblind, then she cannot convince Victor that she is not. In the second one, if Peggy were not to know the password to the gate, then she would not be able to convince Victor who will then not be fooled. It is important to note that in the above example we actually allow for a dishonest prover to be able to successfully fool Victor with a bounded above probability.

5.3 Completeness

Conversely, the condition of completeness states that an honest prover will be able to convince an honest verifier of the veracity of the claim, if the claim is indeed true. So, moving back to the first example, Peggy will be able to prove she is not colourblind if that is indeed true and Victor acts honestly satisfying the protocol. While in the examples Victor is always positively convinced at the end of the interaction, this is not a strict requirement, instead (similarly as in Soundness) we just require the interaction to succeed with a strictly bounded below probability. As an example of when this might be the case, consider the following:

Example 3: Peggy claims that coffee tastes differently when brewed by an espresso machine compared to one made in a cup. Victor wants to verify that claim, so he brews a coffee choosing randomly between the two options (in way that Peggy does not see which is which). Peggy then tastes the coffee, and gives her opinion on how it was brewed. The experiment is repeated n times, and Victor is convinced if Peggy is right more than c times, where c depends on how certain we want to be of Peggy's ability.

5.4 Zero Knowledge

Formalizing the notion of zero knowledge requires a bit more work. We would like to be able to say that in any interaction with the prover the verifier does not gain any knowledge that it did not possess already. That shifts the conversation to what it means to gain knowledge. Let us consider for example the interaction of a prover and a verifier with a common input of a suitably large graph. If the prover reveals to the verifier whether the graph is connected or Eulerian or the average degree of its vertexes then in a sense the verifier does not gain any knowledge, as these are all easily (polynomial time) computable without any additional information. Instead, if the prover reveals whether the graph is Hamiltonian, or the chromatic number of the graph, or a k-colouring of it then the verifier gains knowledge, as it would have not been able to answer that question itself using an efficient procedure. This gives us a hint of what gaining knowledge can entail. In particular, we say that the verifier gains knowledge from an interaction with the prover if, after the interaction, it can efficiently compute something which it would have not been able to do before. How to rigorously express this is non-trivial, and we defer the discussion to the following sections.

6. Future work

One important step of the reverse auction workflow is the bid commitment phase. Our proposed setup assumes that every bidder knows all bid commitments from all other bidders. This previous knowledge is necessary to make the proof consistent. The losing bidders receive proofs that the difference of their bid values and the winning bid value is positive. Hence, they need to confirm that this winning value is part of the original commitments, otherwise they would not be confident that the auctioneer did not create a fake commitment to benefit somebody else. As a result, all bidders must know all other commitments. However, this leads to another problem, which is related to the malleability of Pedersen commitments, which are used in the Bulletproofs. One bidder could generate a lower value commitment based on previous commitments already sent. Therefore, a dishonest bidder could exploit opportunity to take advantage in the process. However, this bidder will not be able to open this commitment since he does not know the original value neither the hiding factor of the commitment, assuming that the openings are not public. Hence, it seems reasonable to leave all commitments public. It is still necessary though to have a setup that allows all participant bidders to track which commitments are part of the auction. One possible solution could be the usage of smart contract and blockchain to guarantee transparency and immutability of this information. For example, a smart contract could collect all bid commitments and store them all in the blockchain. This way, everybody could check how this smart contract was implemented and trace all bid commitments into the blockchain. This should provide trust to all bidders that nobody could create a fake commitment to take advantage in the auction. Although this approach seems to be reasonable to solve this problem, it should be implemented and tested to check its robustness and consistency. For sure, this topic should be an area of future work.

7. Conclusion

This project allowed us to gain an insight into an exciting albeit complex field of zero-knowledge cryptography. We delved into the implementations of zero-knowledge proofs and designed a proof system to generate transparency alongside privacy in online auctions. This cryptographic construction is very fascinating as it enables us to put together the two contrasting objectives of privacy and transparency. As mentioned in the earlier sections, transparency in public reverse auctions is a big concern and addressing it properly can bring several benefits to the society. We have seen that there are several zero-knowledge proofs cryptographic constructions that can be used in this problem. We decided to use Bulletproof construction, which represents a good trade-off between the security assumption and performance of the proof system. The experiments that we ran gave us several insights about how this system should work in practice but as we discussed in the previous section, there are other aspects that need to be considered from the design standpoint.

The prototype construction was very important as a thought experiment. Our solution design changed significantly as we worked on the proof of concept because we had substantial practical feedback from the available implementations and testing environment. Some concepts such as usage of public commitments for the bids were envisioned after we put together the prototype. Therefore, the development of such proof concepts is crucial to achieve a solid solution design.

Finally, zero-knowledge proof cryptography has become a hot research area in the wake of advances in cryptocurrency and blockchain technology. However other application domains, including auctions, could also benefit from this very useful technology. The need for transparency is more relevant than ever before due to massive digitization of organizational workflows, especially in the public sector and zero-knowledge proofs could be a cryptographic tool to generate confidence among the players and stake holders involved. However, the current implementations for zero-knowledge proofs are still experimental and not very user or developer friendly. The lack of production ready tools is an obstacle for broad adoption in the near future but it can be overcome as people continue to work on it.

8. References:

i. https://en.wikipedia.org/wiki/Zero-knowledge_proof

ii. https://chain.link/education/zero-knowledge-proof-zkp

iii. https://www.solulab.com/zero-knowledge-proof-uses/

iv. https://www.stlouisfed.org/-/media/project/frbstl/stlouisfed/publications/review/pdfs/2023/10/02/an-introduction-to-zero-knowledge-proofs-in-blockchains-and-economics.pdf?sc_lang=en&hash=DD10B114D2CBAA2DBBE859E7A0489131