IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 5, October 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Overview and Applications of Zero Knowledge Proof (ZKP)

Jahid Hasan

Master of Engineering in Information and Communication Engineering
Nanjing University of Posts and Telecommunications, Nanjing, China

Abstract - This paper disclosed Zero Knowledge Proof (ZKP) to prove any statement that is true but without revealing the secret of that information to the verifier. After that, it includes a formal example to show how a ZKP works. We showed two computational protocols to prove ZKP and these are: Schnorr's protocol and Fiege-Fiat-Shamir Identification to verify the situation is true or false. The paper concludes the application of ZKP in usage of Blockchain, zk-SNARKs, Zcash cryptocurrency in real life examples. In summarize, it describes the field of ZKP systems and provides a brief its algorithm and applications. Also it concludes with the present and future research interest on ZKP.

Keywords - *ZKP, Schnorr's protocol, Fiege-Fiat-Shamir Identification, Blockchain, zk-SNARKs, Zcash.*

1. Introduction

The most abstract and intriguing ideas in today's applied cryptography is Zero Knowledge Proof (ZKP). As their name suggests, ZKP are cryptographic protocols that do not disclose the data or secrecy to any eavesdropper during the protocol. MIT scientists Shafi Goldwasser, Silvio Micali and Charles Rackoff first suggested the concept of ' zero knowledge ' in the 1980s. They have shown that, it is feasible to demonstrate that some theorems are true without providing the slightest indication of why they are true. For example, where a first party or a prover try to persuade the second party or verifier that the statement is true without sharing any hints or information to the verifier.

ZKP proved to be very constructive in both theory of complexity and in cryptography. There was no succulent observation, and it appeared in several parenthetical observations in Goldwasser, in Micali and Rackoff [1985], in the Choir, in Goldwasser, in Micah and Awkuch [1985], in the Galil, Haber, and in the Yung [1985], that knowledge could be used instead of presence of testimonials. The following were written in Choum [1986] and several others [1].

An interactive verificator input must necessarily be needed for a protocol that implements zero knowledge proofs. Usual interactive information takes the form of one or more tasks in order to persuade the verifier to answer the prover when the declaration is true, that is to say, when the prover possesses the information asserted. If not, the verifier could record and replay the execution of the protocol to persuade someone else to possess confidential data. The adoption by the new party is either justified because the prover does have the data (including that it was not proven in the zero knowledge that the protocol was leaked), or because the request was misleading, which means that it was accepted by someone who does not have the data.

A evidence of zero knowledge must fulfill three characteristics [2]:

i. **Completeness:** If the statement is true, an honest prover will be convinced of this truth by that honest verifier (i.e. one correctly following the Protocol).
ii. **Soundness:** If the statement is false, the honest verifier can not be persuaded by any cheating prover that it is true except with a tiny probability.
iii. **Zero-Knowledge:** If the statement is true, no verifier knows anything other than that the declaration is true.

The first two are features of more general interactive proof schemes, and the third is what makes the zero-knowledge proof.

This paper, mainly focus on the overall applications and some protocols that we can implement to prove the ZKP. I will introduce two common protocols mostly used one is Schnorr's protocol and another one is Fiege-Fiat-Shamir Identification tools. During this study, I will also talk about its applications that are currently used in different applications like Blockchain and other cryptographic systems.

2. Overview of ZKP

Zero Knowledge Proof (ZKP) are cryptographical techniques that enable someone (the prover), without requiring that the prover disclosure any underlying data on the claim, to validate a statement made by a second party (the prover). In this section, we will briefly discuss about the overview of ZKP in using one concrete example to show know its working principles. In this example of "Two balls and the colour-blind friend [2]" will illustrates that how a ZKP is work in real life applications.

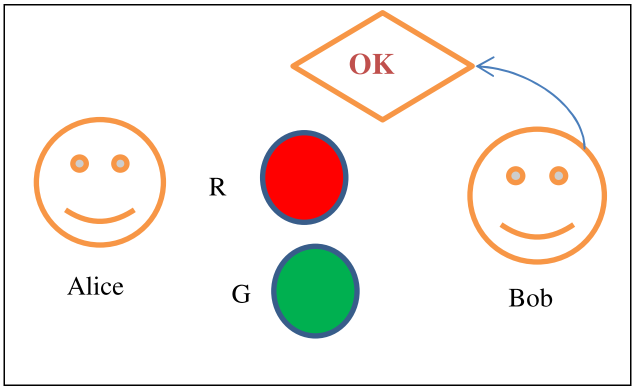

Fig. 1: Example of Two balls and the colour-blind friend.

From above figure, imagine Bob is Red(R) and Green(G) color-blind (while Alice is not) and Alice has two balls R and G, but otherwise identical. They are identical and it's skeptical for Alice's friend Bob that they can be distinguished. Alice want to prove to Bob that they are, in fact, different-colored, but nothing else; in particular, Alice don't want to disclose which one is the R and which one is the G ball.

Now, the proof of this examples are like: Alice gives two balls to Bob, and Bob is putting them behind his back. Next, Bob takes and shows one of the balls from behind his back. Then he puts it back behind his back again and then chooses to disclose just one of the two balls, to pick one of the two at random with the same probability. He is going to tell you, "Have I changed the ball?" All this is then repeated as often as required. By looking at their colors, of course, you can tell with certainty if he changed them or not. On the other hand, if they were the same color and therefore indistinguishable, with a probability higher than 50%, there is no way you could guess correctly. Since you have chances of randomly recognizing a different switch / non-switch is 50%, the chances of random success are zero ("soundness") at each switch / non-switch. If Alice repeat this "proof" several times (e.g. 10 times) with Bob, he should be persuaded ("completeness") that the balls are actually colored differently. The aforementioned proof is zero-knowledge because Bob will never learns which ball is R or G ; indeed, he does not gain knowledge of how to differentiate the balls.

3. Computational Algorithms

3.1 Schnorr Non-Interactive Zero Knowledge (NIZK)

In this section, suppose that a prover wants to prove it knows the Discrete Logarithm (DLOG) x of some group element $h = g^w \in G$, where G is a group of prime order q. Here $R = (h,w) \in Z_q \times G : g^w = h$, where the group G and the generator g are public parameters [3]. Assume P has two queries e_1 and e_2 for the same first message a.

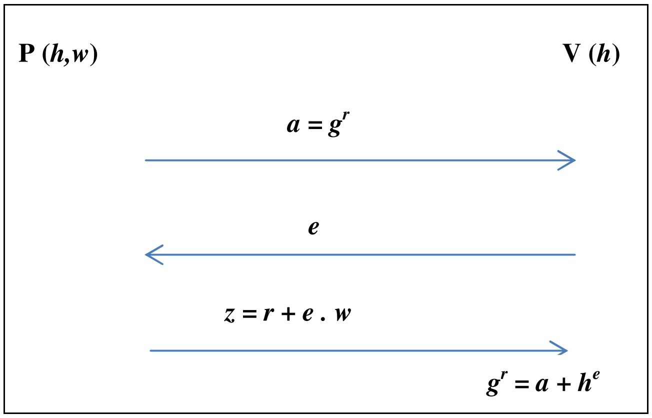

Fig. 2: The Schnorr' s Protocol [4].

So, at first the Prover (P) sends a message a to the Verifier (V), after that the verifier choose a random challenge e of the length t. After substitution we have,

$$g^z{}_1 = a \,.\, h^e{}_1 \;\; and \;\; g^z{}_2 = a \,.\, h^e{}_2$$

Thus, $$a = g^z{}_1 \,.\, h^{e\text{-}1} = g^z{}_2 \,.\, h^{e\text{-}2}$$

So, $$g^{z}{}_1{}^{-z}{}_2 = h^{e}{}_1{}^{-e}{}_2$$

Therefore, $$DLOG_g\,(h) = (t_1 - t_2)\,(e_1 - e_2)^{-1} \; mod \; q$$

Completeness: if $z = r + e.w$, then $g^z = g^{r\,+e.w} = g^r .(g^w)^e = a.h^e$

Commitment Schemes:

Binding: After the commitment phase, the commitment can't be altered it's value.
Hiding: The receiver doesn't know anything about the commitment.

Protocol:

I. P: picks random r in $[1..q]$, sends $z = g^r \; mod \; q$,
II. V: sends random challenge e in $[1..2t\,]$
III. P: sends $z = r + e.w \; mod \; q$
IV. V: accepts if $z = (g^r.h^e \; mod \; q)$

The Schnorr protocol is therefore full and an honest verifier can always be convinced. The addition is that the Schnorr NIZK proof is usually helpful and versatile for a wide range of application.

3.2 Fiege-Fiat-Shamir Identification

The protocol created by Uriel Fiege, Amos Fiat, and Adi Shamir in 1988 is one of the most common implementations of a zero-knowledge proof.The Fiat Shamir protocol is based on the square-root difficulty.The claimant demonstrates a large modulus n understanding of a square root module [5].

The Feige-Fiat-Shamir Identification Scheme includes two entities, Prover and Verifier, according to the principle of all ZKP. The Prover has a secret token and seeks authentication and must demonstrate to another entity, the Verifier, who must authenticate the Prover on the basis of the Prover's secret token through a sequence of problems without knowing the secret token of the Prover.[6].

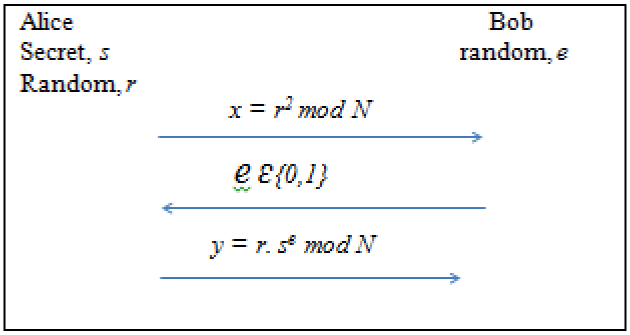

Fig. 3: Fiege-Fiat-Shamir Identification.

One Time Set-up:
A trusted center publishes a modulus $n = p \cdot q$ that is the product of two primes. Each potential claimant (prover) selects a secret s co-prime to N and publishes $v = s^2 \; mod \; N$ as its public key.

Public:
i. Here modulus N and $v = s^2 \; mod \; N$
ii. Alice selects r, Bob chooses $e \; \varepsilon\{0,1\}$
iii. Bob must verify: $y^2 = x.V^c \; mod \; N$
Because, $y^2 = r^2.s^{2e} = r^2.(s^2)^e = x.V^e \; mod \; N$

For example if we choose $e = 1$ then,
Public:
i. Here modulus N and $v = s^2 \; mod \; N$
ii. Alice selects r, Bob chooses $e = 1$
iii. If $y^2 = x.v \; mod \; N$ then Bob accepts it that means Alice passes this iteration to the protocol.
Hence, Alice must know S in this case.

4. Applications

In this section, we will mainly discuss on some major applications of ZKP in real life. As it' s promising-

4.1 Blockchain Technology

A ZKP is a strong cryptographic technique, and its use in blockchain seems promising when current blockchain systems can adapt a ZKP to address particular information protection company demands or their data privacy. ZKPs can be used to ensure the validity of transactions, even though sender, recipient and other transaction data is unknown. The blockchain relates to a decentralized collection of miners running the Global State's secured consensus protocol. Therefore, we will consider the blockchain as a trusted conceptual group that is trusted for accuracy and accessibility, but not trusted for privacy. In addition to maintaining a worldwide ledger that stores the equilibrium for each pseudonym, the blockchain also runs user-defined programs [7]. The most prominent blockchain-based system that uses ZKP is ZCash, which was also the first cryptocurrency to implement zk-SNARKs.

4.2 Zk-SNARKs

A zk-SNARK (zero-knowledge Succinct Non-Interactive Arguments of Knowledge) is a Zero Knowledge proof that is a way to prove some computational facts about the data without the disclosure of the data [8]. Zk-SNARKs are the cryptographic instrument that underlies Zcash and Hawk, both building ZKP blockchains. These SNARKs are used in the case of Zcash to verify transactions, and they are also used in the case of Hawk to verify smart contracts. This is achieved as the privacy of users is still protected. Because zk-SNARKs can be rapidly checked, the evidence is low, the integrity of the computer can be protected without burdening non-participants. It is worth noting that this technology is just beginning to mature but has constraints.

4.3 Zcash

Zcash can be described as an open, unauthorized, replicated ledger encrypted. A cryptographic protocol on a government blockchain for placing personal information [9]. It's functioning work is almost same as Bitcoin. Transaction validators are miners and complete nodes. Zcash utilizes POW, a power supplier which provides miners with a verification of ZKP's connected to each transaction. Zcash utilizes ZKPs to encrypt all the information and only allows approved parties to view such information by giving decryption keys. This could not be performed on a government blockchain until now, since it will stop miners from checking whether transactions are valid if everything has been encrypted in the past. In order to achieve a zk-SNARK, the most "weavy" component, in practice, Zerocash involves carefully installing the cryptographic ingredients of the structure.

4.4 Other Approaches

Authentication Systems: It is an important propositions that adopted in ZKP. Authentication schemes were used for research in ZKP proofs, where a party wishes to demonstrate its identity to a second party through some secret data such as password but does not want the second party to know anything about this secret. However, a password is typically any random numbers to use in this ZKP schemes. A password proof with zero knowledge is a particular kind of certificate of knowledge that addresses the restricted size of passwords. The authentication protocols with zero know-how provide an alternative to public key cryptography authentication protocols [10]. Low processing and memory consumption make it particularly appropriate for use in microprocessors for smart cards that are severely restricted in processing power and storage room.

Ethical Behavior: One of the uses of honest evidence or proof is to promote genuine conduct while preserving privacy within cryptographic protocols. The concept is roughly to force a user to demonstrate that his conduct is right in accordance with the Protocol using a null-knowledge evidence. Because of soundness, we know that the user must really act honestly in order to be able to provide a valid proof. Because of zero knowledge, we know that the user does not compromise the privacy of its secrets in the process of providing the proof.

5. Conclusion and Future Work

In conclusion, for both the mathematicians and cryptographers, the evidence of ZKP is of significant theoretical and practical concern. From this, we can find how a ZKP works on those protocols and see their behavior. In contrast, we have introduced its applications in real life examples. Mostly, nowadays, Blockchain technology adopting this ZKP techniques for the secured and authentic transaction between two parties. Moreover, ZKP is more promising and advance research area in the field of Blockchain technology and on its distributed ledger systems.

This part of work is a brief display of my another research work on this ZKP in Blockchain cryptography. On that paper, I will show those protocols in advanced computation and also using some programming language to prove it. The more work on this ZKP schemes will done in next papers.

Acknowledgments

Many thanks to my supervisor Dr. Xu Ming Hai, Dr. Zhang Yingzhou and Professor Rongfang Song for their encouraging support, technical and spiritual.

References

[1] Uriel Feige, Amos Fiat and Adi Shamir, " Zero Knowledge Proofs of Identity," 1987 ACM 0-89791-221"7/87/0006-0210.

[2] ZKP online wiki link: https://en.wikipedia.org/wiki/Zero-knowledge_proof.

[3] Dima Kogan, " Proofs of Knowledge, Schnorr' s protocol, NIZK," CS 355: Topics in Cryptography, Spring 2019.

[4] Kiayias, "Crypto: Primitives and Protocols," Lecture 7.

[5] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. 5th Ed. CRC Press, 2001.

[6] Joseph M. Kizza, "Feige-Fiat-Shamir ZKP Scheme Revisited," Journal of Computing and ICT Research, Vol. 4, No. 1,pp. 9-19.

[7] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy.

[8] ZK-SNARKs Available: https://z.cash/technology/zksnarks/.

[9] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza,

"Zerocash: Decentralized Anonymous Payments from Bitcoin," 2014 IEEE Symposium on Security and Privacy.

[10] Niranjanamurthy M, Shashank K S, Sumanth P Gowda, Suhas Bhatta, "RESEARCH STUDY ON TWO FACTOR ZERO KNOWLEDGE PROOF AUTHENTICATION SYSTEM," International Journal of Advance Research in Science and Engineering, Vol. No.5, Special issue no. (01), February 2016.

Author :

Jahid Hasan Currently pursuing his Master's degree in Nanjing University of Posts and Telecommunications, China. His research interests include Information cryptography, Blockchain technology, 5G network, wireless communications etc.