Difference between ECDSA with ED25519 and Their Future

Yiming Luo *

Department of Mathematics and Computer Sciences, Nanchang University, Nanchang, China

* Corresponding author email: 6109119053@email.ncu.edu.cn

Abstract. It is always a trendy topic about virtual currency nowadays in the world. These virtual currencies like Bitcoin and Monero are precious and cryptic, which play a more critical role in the economy since no departments or governments control their transactions and deals. How could the transaction system provide users with security and protect their property? What's more, one of the most important characteristics is that all the transactions are untraceable, which means that the governments and the users cannot figure out the identity of another user. This paper discusses some principles of Bitcoin and Monero. For instance, some encryption algorithms like ECDSA and ED25519 are applied to help users to verify the whole transaction, and Ring signature is used in Monero to conceal the user's identity. Meanwhile, this article will also compare some encryption algorithms' security and efficiency. Moreover, there would be a discussion about some advanced communication technologies. For example, there would be a brief introduction to quantum communication and entanglement. Then, it would also have an intense debate about the future of ECDSA and ED25519 if quantum communication and quantum entanglement were invented.

Keywords: Bitcoin; Monero; Encryption Algorithm; ECDSA; ED25519.

1. Introduction

In 2009, an innovative form of digital currency premiered in the marketplace — Bitcoin. Bitcoin is a peer-to-peer payment network developed by Satoki Nakamoto (Nakamoto). Nakamoto created Bitcoin as the ultimate digital currency, meaning no governmental oversight, central database, or tracking system. Bitcoin, a so-called "cryptocurrency," is a digital currency with encrypted messages that are not accessible to third parties. Bitcoin is leading the cryptocurrency market with pioneering technology concepts such as limited distribution and secure information systems [1]. Besides attracting a billion-dollar economy, Bitcoin revolutionized the field of digital currencies and influenced many adjacent areas [2]. At first, it combines with many encryptions' algorithm, which makes it so unique at that time because it gives people chances to have transactions with others in secret. Moreover, the invention of Bitcoin also brings the blockchain. Emerging smart contract systems over decentralized cryptocurrencies allow mutually distrustful parties to transact safely without trusted third parties. In the event of contractual breaches or aborts, the decentralized blockchain ensures that honest parties obtain commensurate compensation [3]. No governments or banks could check people's accounts or trace their transaction records. With such characteristics, it would be called decentralized. Although, it might relate to online criminals and a currency for hackers at the first time. For instance, a review of Australian case law over the last decade confirms that early adopters of cryptocurrencies included those using this new technology for illegal purposes [4]. However, today's situation has changed entirely. Major tech companies and banks are investing in cryptocurrencies, and the users are also in a broader range.

Moreover, the blockchain also promotes the invention of Ethereum, which has grown to secure approximately 30 billion USD of currency value and above 300,000 daily transactions [5]. They are decentralized and give people chances to transfer money online. These technics are prevalent nowadays. In the short future, users would continue to be explored in large numbers, and these could also bring much more data to the whole system. The system could face some problems in securely storing the numerous data and protecting the users' property. So, how could such systems remain stable and protect the user's security?

DSA, ECCDSA, and the ED25519 are some of the famous Digital Signature technics that could be both stable and hard for an adversary to attack. Such algorithms are based on some intricated

mathematics, which are related to the Discrete Log problem (DLP), and some are also combined with the elliptical curve. For instance, to authorize payments, Bitcoin and Ethereum use the Elliptic Curve Digital Signature Algorithm (ECDSA) [6]. In this circumstance, the Digital Signature could help the receiver to confirm whether the sender is valid and whether the message has been changed.

Moreover, Monero uses the EdDSA to help users verify the whole transaction and examine the message. The elliptic curve signature scheme EdDSA and one instance are called ED25519, combining hash functions and classic encryption algorithms [7]. Besides, the Monero also needs to conceal the sender's identity before the receiver can confirm whether the sender is valid. To illustrate it, if there is a transaction, a sender wants to send an important message to a receiver. The sender wants to conceal his identity as a few a valid group, which means the receiver cannot figure out who he is in the group. However, the receiver has to confirm that the sender belongs to a valid group instead of a group of hackers or invalid users. Only the sender belongs to a valid group, the receiver would examine the message. In such circumstances, a ring signature could solve such problems. Rivest proposed it in 2001, and it developed for 20 years. It is also used in the Monero, almost making the Monero the most cryptic virtual currency. It could hide the user's identity in a large group. The group is a big ring, and the ring consists of many valid users. Once the receivers get the ring signature, they can verify it and determine whether the sender is valid. However, the receiver could not get any information from the signature about who the sender is. The receiver could only guess the sender in a large group. How could the Monero be more cryptic than the Bitcoin. How could improve their security. Whether spending much more time and money to develop these encryption algorithms like ECDSA and ED25519 would be worthwhile. This paper introduces the ECDSA and elliptic curve in the “Elliptic Curve Digital Signature Algorithm” section. Moreover, the introduction of ED25519 and its difference with ECDSA would be discussed in “ED25519 and the difference with ECDSA”. At last, there would be a debate about the development of these encryption algorithms and some advanced future communication technologies in section “The future of ECDSA and ED25519”.

2. Elliptic Curve Digital Signature Algorithm

ECDSA (Elliptic Curve Digital Signature Algorithm) is based on Discrete Log Problem, and the process seems like the DSA. Some critical algorithms exist in elliptic curves, point addition, and point multiplication. Also, the base point is significant. Firstly, the elliptic curve like $y^2 = x^3 - 4 \times x + 7$, the picture of the function would be as shown in figure 1. Then, there is a line like which is $y = 3 \times x + 2$, through the function, there would be three intersections, point P, point Q, and point R as shown in figure 2. So, the point addition means point P plus point Q that will be equal to point S when the point S and point R are symmetric about the X-axis.

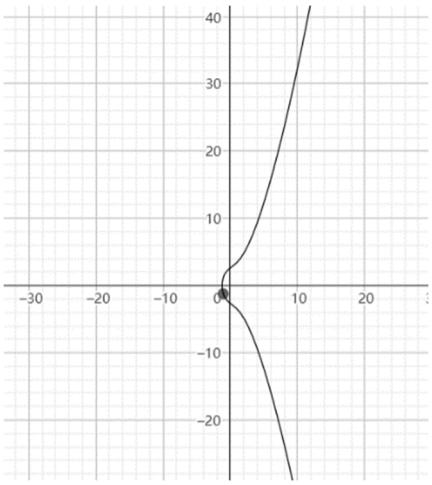

Fig 1. Elliptic curve

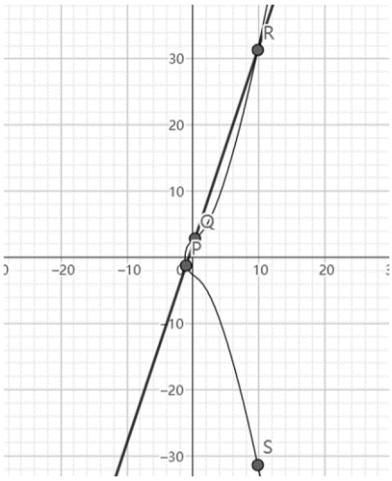

Fig 2. Three intersections

Moreover, the most important concept about point addition is when the line is just a tangent of the function. This would lead to point P plus point P, which will be equal to S, then S is equal to 2 times P. In this circumstance, after choosing the base point like point P, it could turn out numerous points based on the base point. Meanwhile, this process gives crypticity to many encryption algorithms, like point M, which is equal to 6 times the base point, like point P. It could be two times three times P, or four times P plus two times P. So, it is extremely hard for an adversary to figure out the track which leads from the origin to the end since there are many different steps to achieve it.

The users in Bitcoin use ECDSA to verify the whole deal. In the process of generating the signature in the ECDSA, the first step is to generate the private key, like the number d, which is randomly selected. This method to generate the private key will fit the randomized encryption. Generating the same private key in several times could make the system less security. In a digital signature process, only the private key is concealed, which means that all of other information are shared and visible for everyone. Secondly, the public would be generated by the private key times base point after generating the private key. The adversary could not gain the private key if he knows the base point and public key since the elliptic curve provides the crypticity. Thirdly, use function $r = x \bmod n$ to generate number r. Fourthly, a hash function like the SHA-256 would combine messages to generate e.

At last, there would be a function like $s = k^{-1} \times (e + d \times r) \bmod n$ to generate s. Then, the signature is formed like (r, 2). Then, the sender could send his message and signature to the receiver. After the receiver gets the message and signature, he could use them to verify whether there is an adversary in the transaction and whether the message has been changed.

3. ED25519 and the Difference with ECDSA

Compared to Bitcoin, the users in Monero use the ED25519 to verify the transactions, which makes the Monero more cryptic than Bitcoin. Moreover, it could also save the storage space. The ED25519 uses the elliptical function $y^2 = x^3 + 486662 \times x^2 + x$. In the process of generating the signature at the ED25519, the first step is to generate the private key, like the k, which is randomly selected. The first step to generate the private key is the same as the ECDSA. Then, it also needs to generate the public key. This step is the most different process between ECDSA with ED25519. In ED25519, it should use a hash function to generate the information of h at first, such as $H(k) = (h_0, h_1, \ldots, h_{2b-1})$. Secondly, it should generate an integer number like a, which would be generated by a complicated function like $a = 2^{b-2} + \sum_{3 \ll i \leq b-3} 2^i \in \{2^{b-2}, 2^{b-2} + 8, \ldots, 2^{b-1} - 8\}$. At last, the public key like A will equal to a times B. In the process, the b is equal to 256, and the B is the base point in the elliptical curve after generating the private key like k and the public key like A. The signature could be generated by following steps. Firstly, compute the information of r by using a hash

function like $r = H(h_b, \ldots, h_{2b-1}, M)$. M means the message that the sender wants to send to the receiver. Secondly, R would be equal to r times B. Thirdly, the S would be generated by a function like $S = (r + H(R, A, M) \times a) mod\ l$.

l would be equal to $2^{252} + 27742317777372353535851937790883648493$. At last, the signature is generated, such as (R, S). In this circumstance, the users could verify the whole transaction. Once there is a hacker who has changed the message, the user could find that the message has been changed when he uses the signature to verify the deal.

What are some of the differences between them? Which one could be more efficient, which one could save more resources, or which could be more secure? Moreover, it is always a hard task for a successful system to be both secure and efficient, whether some of the Digital Signatures could solve both problems or what is the more important problem for them to solve.

It should be admitted that ED25519 has significant better performance compared to ECDSA [8]. Between the ECDSA and the ED25519, generating the public key in ED25519 is more complex than in ECDSA. It will combine a hash function with a sophisticated mathematical function. In this case, generating the public would be much more intricate. The private key only generates one component of the public key, which makes the process like secondary encryption. In this circumstance, except for generating the private key, the ED25519 eliminates reliance on randomness. So, it avoids the possibility which could happen in the ECDSA, that the adversary could break the system if the private key is keeping the same for several times. For an adversary, getting the private key in ED25519 becomes harder than ECDSA. Considering these benefits of ED25519, it would be better than ECDSA.

4. The Future of ECDSA and ED25519

However, with the development of quantum computers, many algorithms based on the Discrete Log problem (DLP) might not be safe enough in the future, because the quantum computer could solve all these hard discrete problems efficiently. So, whether DSA, ECDSA, and ED25519 would be safe and how to change and reuse them in the future. To start with, it obviously that the DSA is becoming less competitive than the ECDSA and the ED25519. It would need more storage space to reach the same security compared to ED25519 and ECDSA. What's more, the calculation speed in ECDSA and ED25519 would be much faster. So, it would be more effective to use ECDSA and ED25519 nowadays.

Although the ED25519 and the ECDSA seem safe enough for people nowadays, they might not be worthwhile or unsafe to use in the short future. As previously mentioned, the development of quantum computers could solve the Discrete Log problem efficiently, which could significantly change the whole of cryptography because many algorithms are based on the Discrete Log problem. So, the ED25519 and the ECDSA might be unsafe in the future. In this circumstance, it would tremendously attack the virtual currency system. Adversity could steal virtual currencies effectively if they could break the system by using quantum computers. Most virtual currencies might need to improve their encryption algorithms to be more secure.

What methods could be used to make these algorithms safer? For example, these algorithms could use One-Time Pad, which could reach perfect secrecy in some cases. The One-Time Pad (OTP) is the only known unbreakable cipher, proved mathematically by Shannon in 1949. Despite several practical drawbacks of using the OTP [9]. Since the One-Time Pad is one of the Symmetric-key algorithms, the drawbacks are about how to generate the numerous random keys and safely transport the key to the receiver. However, the One-Time Pad has such shortcomings. Suppose some algorithms like ED25519 effectively combine the One-Time Pad algorithm, which could make them against the quantum computer.

Moreover, there might be a more secure and effective method to offer people a chance to communicate in the future, like quantum communication and quantum entanglement. Recent advances in quantum information theory reveal the deep connections between entanglement and

thermodynamics, many-body theory, quantum computing, and its link to macroscopicity [10]. Undoubtedly, quantum communication and entanglement will play an important role in the future. They are much different from nowadays' encryption algorithms, which must go through the internet to transport the message. This theory is based on the quantum, which is the One-Time Pad. Because there would not be the same quantum, and adversaries could not reproduce the quantum, using some quantum to form a secret key could make the deal safer. The sender and receiver could find whether there is adversity in the transaction quickly. It would be a perfect theory for the digital signature.

However, there are many discussions and debates about this theory. Objectors insist on that this theory could only find the adversaries but cannot eliminate them. However, the digital signature's role is only to verify whether there would be an adversary in the deal, and it does not consider how to eliminate the adversary. Moreover, with quantum communication and quantum entanglement, people can communicate via the quantum. There is might no need for people to encrypt the message. In this circumstance, all encryption algorithms could be meaningless in the future, so whether it is worthwhile for people to continue to develop such algorithms, and whether all of their functions would be replaced by quantum communication and quantum entanglement.

5. Conclusion

The paper has discussed the blockchain, Ethereum, Bitcoin and Monero, all of them have play an important role in economy nowadays. Meanwhile, the article introduces the ECDSA which is applied in Bitcoin and the ED25519 which is applied in Monero. All of them are used like Digital Signature Algorithm to help users verify the transaction. In the discussion about the ECDSA and ED25519, it is obviously that ED25519 are more secure and beneficial than ECDSA. It is also the reason why the Monero are more cryptic than Bitcoin. What's more, the quantum computer would be invented in a short future like about 10 years. There is no doubt that these encryption algorithms like ECDSA and ED25519 would not be enough secure, because the quantum computer could solve Discrete Log problem efficiently. The article proposes a solution that these encryption algorithms could combine with the One-Time Pad to be against to the quantum computer, which is a perfect method in encryption in some cases. Moreover, there is a topic about the quantum communication and quantum entanglement. It should be admitted that if the quantum communication and quantum entanglement are invented, there is no need to waste time to develop these encryption algorithms like ECDSA and ED25519. The quantum communication could be better whether in efficiency or the security.

References

[1] Sanders, T. (2014). Bitcoin: The Revolutionary Currency. The Record Reporter, February.

[2] Tschorsch F, Scheuermann B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies[J]. IEEE Communications Surveys & Tutorials, 2016:2084-2123.

[3] Kosba A , Miller A, Shi E , et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]// 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016.

[4] Adam L. Aaron M. Lane and Lisanne Adam 'Lurking in the Dark Web: Bitcoin and Criminal Entrepreneurs'. 2019.

[5] Hildenbrandt, E., Saxena, M., Zhu, X., Rodrigues, N., Daian, P., Guth, D., & Roşu, G. (2017). Kevm: A complete semantics of the ethereum virtual machine.

[6] Mayer H . ECDSA Security in Bitcoin and Ethereum: a Research Survey. 2016.

[7] Moller N, Josefsson S . EdDSA and Ed25519[J]. 2015.

[8] [CP García, Sovio S . Size, Speed, and Security: An Ed25519 Case Study.[J]. Nordic Conference on Secure IT Systems, 2021.

[9] Nagaraj N . One-Time Pad as a nonlinear dynamical system[J]. Communications in Nonlinear Science & Numerical Simulation, 2012, 17(11):4029-4036.

[10] Vedral, Vlatko. Quantum entanglement[J]. Nature Physics, 2014, 10(4):256-258.