

Block Chain Authentication Using Elliptic Curve Digital Signature Algorithm

Saritha K.

School of Engineering & Technology, Navrachana University, Vasna-Bhayli Road, Vadodara- 391 410 Gujarat, India

Received: 17 March 2020 Revised: 13 June 2020 Accepted: 18 August 2020 Published: 9 September 2020

*Corresponding Author: sarithak@nuv.ac.in

Abstract

The block chain technology is the latest updated technique, where the data is being stored in a decentralized environment. The authentication deals with verifying who they are, what is their identity. The authentication is provided in the block chain by various techniques. One better way of providing authentication rather than using a two factor authentication where a single user name & password is available, it can be with the help of Digital Signature Algorithm(DSA), as in the case of DSA, deals with digital signature based on algebraic properties. It deals with two mutually authentication keys. The algorithm used for signing and verification of the message. The commonly used public key based algorithms are RSA and DSA. Here we use DSA which is an asymmetric algorithm, which generates a pair of keys, one public and one private. The DSA can be enhanced by using elliptic curve which serve as a better option for authentication techniques. The review paper explains the use of DSA with ECC (Elliptic Curve Cryptography) as a better option for authentication rather than using a two factor authentication for block chain technology.

Keywords

Digital Signature Standard, Elliptic Curve Cryptography

Introduction

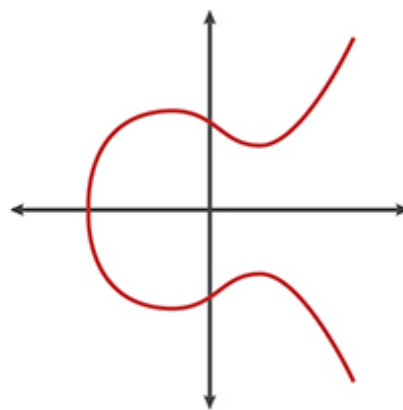
Cryptography is a technique which is used to protect data from unauthorized access. There are mechanism for secure communication that is symmetric cryptography and

asymmetric cryptography. In symmetric where same key is used for encryption and decryption. Here it deals with asymmetric key where different keys are used for encryption and decryption. One of the asymmetric techniques is Elliptic Curve Cryptography. Block chain is a type of diary or a spreadsheet containing information about transaction. Each transaction generates hash. When a transaction is approved by different nodes, then it is written in block. Each block refers to previous block and together make a block chain. Block chain is not controlled by any entity. Records are stored in any blocks. A technology to create and maintain a secure shared and distributed ledger for transaction¹. The elliptic curve Digital Signature Algorithm is applied to enhance security of the ledger, which helps in the integrity of the data or the transaction. ECCDSA that is Elliptic Curve Digital Signature Algorithm is a cryptographic algorithm used by bitcoin. Bitcoin is a cryptocurrency, which uses secure algorithm for transaction². Public key, private key and signature are used in ECCDSA.

Experimental methods

Elliptic Curve Cryptography

ECC (Elliptic Curve Cryptography, is more useful in the current scenario where more people are dealing with smartphones. It offers stronger security. It uses small key size while providing a higher security³. In the latest minimum size of ECC is 256-383 and key ratio 1:12, the security bits are 128, and it is valid till the years to come. An elliptic curve is a plane curve over finite field consisting of points with equation.



$$y^2 = x^3 + ax + b$$

Figure 1: Elliptic curve

Elliptic Curve Digital Signature Algorithm

As with ECC the bit size of public key needed for ECCDSA is twice the size of the security level. For example, security level of 80 bits, the size of as ECCDSA will be 160 bits.

Here we use signature generation algorithm and signature verification algorithm⁴. Digital Signature Algorithm is used with Elliptic Curve Cryptography to enhance the security. The algorithm works like this it takes a large prime number say p . It takes the value of a and b . Then uses a generator point. It is used to produce other points in the curve. It is working in finite field. We will use the private keys for signing⁵.

-Pick a random number k , a temporary private key
 - Produce a temporary public key ($Pk=k*G$)
 - $R = X_{Pk}$
 - $S = k^{-1} (\text{Hash}(m) + \text{prvKey} * R) \text{ mod } p$

Figure 2: Signing Algorithm

-Calculate a Point of the EC: the temporary Public key
 $P = S^{-1} * \text{Hash}(m) * G + S^{-1} * R * \text{PubKey}$

Figure 3: Verifying Algorithm

Two factor authentication

Two factor authentication techniques are better than single factor authentication; in which user provide one authentication that is password. In this mechanism they give password, as well as other credentials such as face or, fingerprint recognition.

Multifactor authentication

Here only access is provided after presenting two or more authentication factor. It enhances security as granting access is permitted with more credentials. More credentials in the sense if it is an organization then user will login. This is also controlled by the admin, who login with his or her credentials.

Results and Discussion

Analysis of ECC and ECCDSA

This figure explains the difference between ECC and ECCDSA. Elliptic Curve Cryptography, which is a secure technique for communication. In which are data are stored in x and y coordinates as it is difficult to break. Digital Signature Standard mechanism provides integrity of the message. The comparison table explains about time taken by Rivest Shamir Adleman with Elliptic Curve Cryptography.

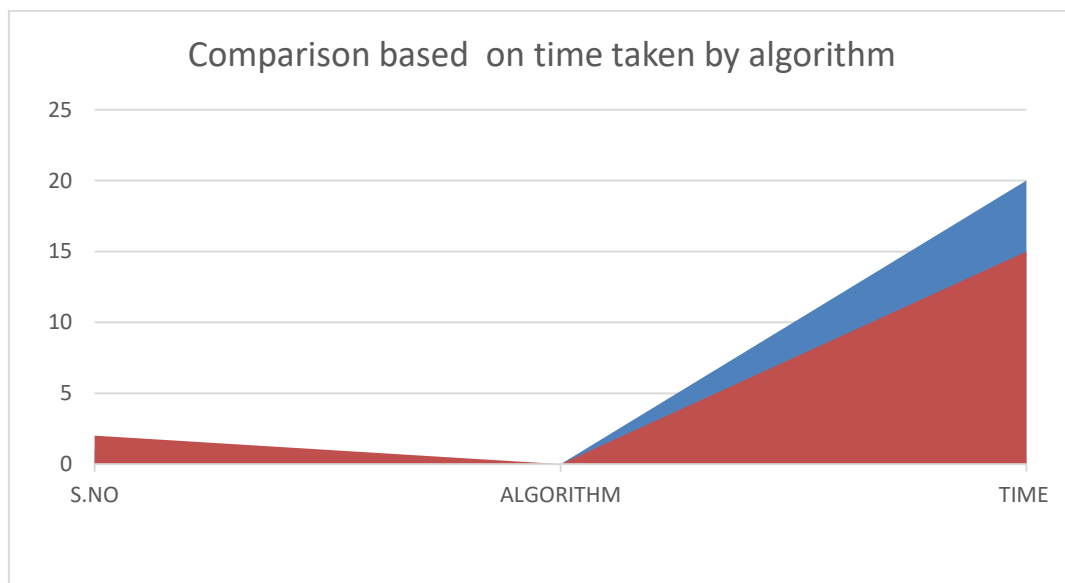


Figure 4: Comparison of ECC and ECCDSA

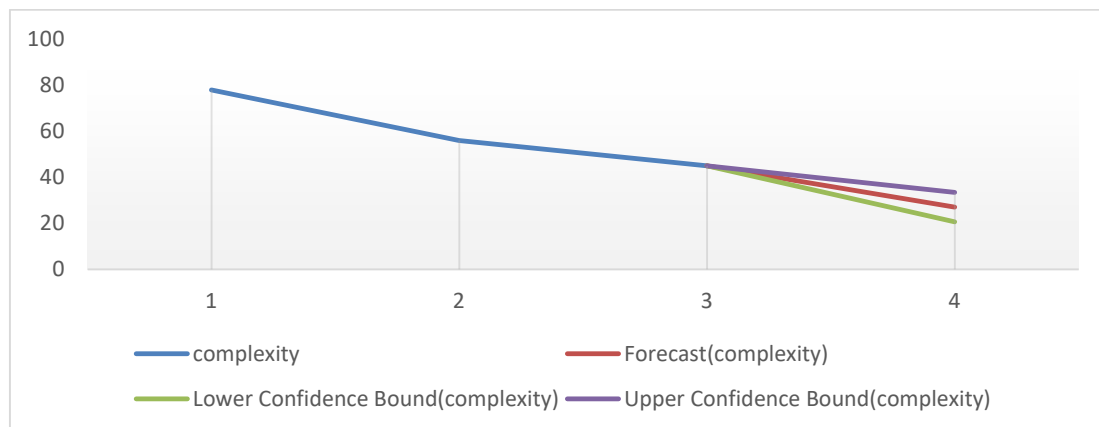


Figure 5: Time Complexity Comparison of DSA and ECCDSA

The table below explains the algorithm, key length and symmetric key length of various cryptographic techniques. It explains the performance of other authentication techniques with the proposed technique with lesser key size.

Sr. No.	Algorithm	key length	Symmetric key length
1	Rivest Shamir Adleman	1024	80
2	ECC	163	80
3	ECCDSA	160	80

Table 1: Algorithm and key sizes

Conclusion

Digital Signature Algorithm is used for providing integrity to a message by using signing and verification algorithm. The block chain technology is used for transaction in a distributed environment. The two factor authentication techniques offer less authentication approach than ECC. The ECC provide more security using less key size for block chain. In this approach integrity is also met with the help of DSA. The block chain technology can be further enhanced for IoT devices. For enhancing security in IoT ECCDSA can be applied.

References

1. Nakamoto, Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/bitcoin.pdf>
2. Vujičić, D., Jagodić, D., & Randić, S. (2018). Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview. *17th International Symposium INFOTEH-JAHORINA*, 1-6, <https://doi.org/10.1109/Infotech.2018.8345547>
3. Wei Bi, XiaoyunJia, MaolinZheng (2018). A Secure Multiple Elliptic Curves Digital Signature Algorithm for Block chain. Retrieved from <https://arxiv.org/abs/1808.02988>
4. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48 (177), 203–209.
5. Miller, V.S. (1986). Advances in Cryptology - CRYPTO' 85 Proceedings. In H. C. Williams(Ed), *Use of Elliptic Curves in Cryptography* (pp.417-426).Berlin, Heidelberg: Springer Berlin Heidelberg. D.