Asian Journal of Information Technology 16 (9): 722-726, 2017
ISSN: 1682-3915

Identification of Ideal Digital Signature Algorithm for Optimising Bitcoin Transactions

Sussan Elias and Shoney Sebastian
Department of Computer Science, Christ University, Bengaluru

Abstract: An electronic peer to peer cash system called Bitcoin does not need a third party to transfer digital currency from one to another. This system provides an efficient way of transaction between different users without any question of trust. Digital signature plays an important role in this. It provides security, integrity and non-repudiation for safe and secure transaction. Electronic signature is used to identify authenticate users. Not many authors have proposed the best digital signature algorithm to authenticate Bitcoin transactions. In this study, the well-known digital signature scheme known as ECDSA is compared with RSA and DSA signature schemes to identify the optimal signature scheme for digital currency, Bitcoin.

Key words: Security, Bitcoin, digital signatures, RSA, DSA, ECDSA

INTRODUCTION

Technology has developed over few years to make human kind available with everything possible on a single click. Computers that are smart enough to act and behave like humans are developed which makes the work effort of people less. Thus, systems are made available for any kind of work. Networks on the other hand rapidly grew that connect people every where in the world and bridges the gap between communications. Networking is a means of communication between multiple users in exchange of data and information. With the help of internet each and every thing is made possible on our fingertip. From large organizations to small enterprises, different transactions are done online in various fields. A lot more new ideas and web solutions are developed to make these online transactions simpler and better.

Many online shopping websites like Flipkart, EBay, Amazon, etc. and money transfer mediators such as Paypal came into existence as a part of the development. As a result, e-Currency became popular and is widely used. e-Currency or electronic currency is the money that is exchanged over the internet without buying or selling goods by exchanging physical cash. Buying and selling of goods are made possible worldwide using e-Currency transactions. These services actually fulfil the meaning of World Wide Web.

Bitcoin is a digital currency that is made and maintained electronically. Bitcoin is not controlled and printed by anybody. Bitcoins are produced for business purposes by people using software that is capable of solving mathematical problems. Bitcoin is the first known cryptocurrency. It is used to trade digitally in exchange of goods. The idea behind Bitcoin is to have a digital currency which does not have a trusted third party support for transactions which can be instantly transferred electronically with less transaction fee. Mathematical calculations are used to create Bitcoins. They can be held by multiple users and it is anonymous. Certain financial institutions serve as trusted third parties to process electronic payments. It works well with most of the transactions but does not mediate disputes. The cost of transaction increases as the mediation increases. These cost and uncertainties can be avoided in use of physical currency. But this cannot be done in the case of payments made where there are no mediators (Nakamoto, 2012).

In such scenarios, it is the duty of the receiving party to make sure that the transaction is sent from the actual sender. And also, the Bitcoins should reach the receiver without any changes. To ensure this certainty of transactions, digital signatures can be used. Digital signature is a framework that can be used to ensure non-repudiation, confidentiality, integrity, security and authenticity. The Bitcoins that are sent should be signed digitally by the sender to achieve these features. The main characteristic of digital signature is non-repudiation which is very significant in identifying the actual sender of bitcoin. Once the digital signature is sent by the sender to the receiver, the receiver neither can reject it nor can the sender deny it. Haraty *et al.* (2006) say that digital signature is used for the following necessities:

- The receiver can only check for the signature of the transmitter and cannot change it

Corresponding Author: Sussan Elias, Department of Computer Science, Christ University, Bengaluru

- Once a message is received at the receiver's end, he cannot reject it
- If there is any doubt on the content of the information that was send, digital signatures can always made use as a proof

In a peer to peer transaction system such as Bitcoin, digital signatures play a vital role. Method such as time stamping servers already exists in implementing trusted transactions. But it is very essential to understand and choose the best scheme to digitally sign Bitcoin transactions

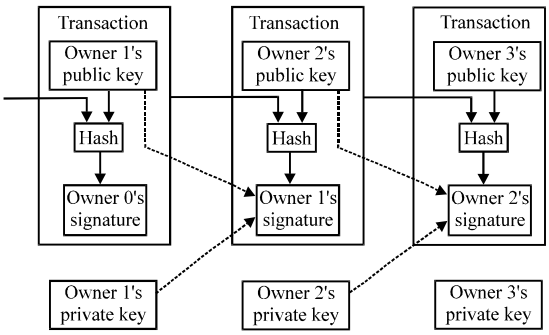

Fig. 1: Transaction system

Literature review: Barber *et al.* (2012) proposed that Bitcoin is the best e-Currency. A comparative study based on different factors shows the reason why Bitcoin is popular among e-Currencies. Flaws of Bitcoin are identified and put forth solutions to the same. It is identified that instantiation of Bitcoin is poor due to improper parameters. But it could be supported by its core design.

Nakamoto (2012) states that digital coin is considered as a chain of digital signatures. Once the Bitcoin is installed in the system, a Bitcoin address is created which can be used for transactions. All the transaction details rely on a public ledger called block chain. A hash is created when a transaction takes place. For next transaction the owner signs the previous hash and public key of the current user. This is added to the end of coin. The ownership can be verified by verifying the signature. This is not very feasible for verifying double spending. After each transaction the coin has to be returned to mint in order to issue new coin. The coin is trusted not to be double spent only if the coin is issued directly by the mint. The issue with this system is that after each transaction the system has to go through mint just like bank do (Fig. 1).

The solution to this issue is a time stamping server. The hash block of items to be time stamped is selected and published in public. The time stamp gives a proof that the content existed. As mentioned, each time stamp contains the previous hash within it. Digital signature plays a vital role in signing the hash. It is very crucial to identify the correct and best digital signature scheme out of many that is available.

Islam (2015) proposed a new approach called three layer securities for electronic money transaction. An algorithm is developed by combining conventional password system, biometric system and GPS methods which would provide security and reliable transaction to users. The proposed framework is useful in transferring money from one account to another for bill payments and for e-Coin generation. The authenticate user must go through all the layers of verification in order to transfer money electronically.

Milanov (2009) explains the working and implementation details of RSA algorithm. RSA algorithm was introduced in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman. It is a cryptographic algorithm which was proposed in order to replace the less secure NBS algorithm. It is used for public key crypto system and for digital signatures. The researcher claims that till date, it was impossible to break the code because it is really difficult to factorize large prime number which makes the cornerstone of the scheme. Compared to certain symmetric cryptosystems, RSA is slower.

Johannes *et al.* (2001) describes the Digital Signature Algorithm (DSA). A brief description about techniques that can be used to generate and validate digital signatures are explained. DSA provides security as well as non-repudiation. Different security measures are mentioned and this can be used to implement the DSA algorithm.

Khalique *et al.* (2010) say that Elliptic Curve Digital Signature Algorithm (ECDSA) is an alteration of Elliptic Curve Cryptography (ECC). It is an alternative scheme that was proposed for DSA and RSA. Also ECDSA gained a lot of attention. Certain factors such as key size, fact that there is no sub-exponential algorithm to solve elliptic curve discrete logarithm gives additional advantage to ECDSA.

MATERIALS AND METHODS

ECDSA algorithm is compared with two other prominent algorithms such as RSA and DSA. The study proves that ECDSA is the most ideal algorithm that can be used in Bitcoin transaction. Bitcoin is decentralised and there is no third party for transactions. In such a scenario, properties of ECDSA satisfy the requirements of Bitcoin.

The following parameters for ECDSA algorithm is analysed on the basis of different requirements of Bitcoin. They are:

- Key length
- Signature length
- Time efficiency
- Key strength
- Performance

By Alrehily *et al.* (2015) and Asmaa *et al.*, says that, the key length plays a vital role in the signature generation and its efficiency. The length of the key should not exceed a limit. In Bitcoin transactions, it is very necessary to keep this point in mind because signature is produced to sign digital currency which contains very specific details and hence it's smaller in size.

According to Wang (2014), unlike the digital signature schemes such as RSA and DSA which depends upon the public key and private key, the key generation for ECDSA depends upon the curve parameters which act as the cornerstone of ECDSA. Both sender and receiver must agree upon the parameters. In addition to it, ECDSA has an elliptic curve base point which helps with large prime order n. Hence, n is the multiplicative order on the curve. For efficient transfer and storage of digital signature, the length of the signatures should always be average in size. The standard size of a digital signature is up to 80 bit. The key length of ECDSA is lesser compared to other digital signature algorithms. The key produced by RSA and DSA is a combination of different parameters such as p and q which are very huge in size. Hence, the key produced by these algorithms are huge in size whereas the key length of ECDSA algorithms is shorter and efficient.

Time efficiency is calculated to see how fast the signature can be produced. Bitcoins are transferred by millions of people at the same time. Hence, time delay should not occur in transaction since, it would affect other transactions too. ECDSA generates signature much faster than any other digital signature algorithms.

By Alrehily *et al.* (2015), digital signatures can have different key strengths. The optimal scheme is chosen according to the need based on the key strength. The key strength can vary for each scheme. To digitally sign Bitcoin, the key strength must have an average strength. Neither too strong nor too weak keys could be used for signing Bitcoins.

RSA algorithm is slower compared to DSA and ECDSA in verifying the signatures that are produced. RSA key generation is slower because of key pair generation. Rather than digitally signing Bitcoin, RSA would perform both encryption and decryption too. This causes RSA to generate signature with a time delay. It is able to detect error which occurs in computational operations or the process of data transfer. Also it is capable of correcting such errors. Applied in cloud computing. DSA improves the computational speed. Without using the pre-computation condition, verification is speedup. It does not require modular inversion operation in verification.

By identifying the various ways in which the three schemes works, it is quite evident that implementation of elliptic curve digital signature algorithm is efficient compared to any other prominent digital signature schemes for making Bitcoin transactions safe and secure. ECDSA is compatible and satisfies all the requirements of Bitcoin money transfer. Its salient features such as keys of feasible length, signature generated of optimal strength, faster generation of efficient signature and improved performance makes ECDSA the optimal digital signature algorithm for signing Bitcoin transactions.

RESULTS AND DISCUSSION

To identify the features of the signature schemes RSA, DSA and ECDSA, the three different algorithms were implemented in a platform. The language used here is the object oriented programming language, Java. Eclipse served as the suitable framework to execute the three algorithms. Below mentioned are the steps followed to implement the algorithms to identify the significant differences between the same (Fig. 2):

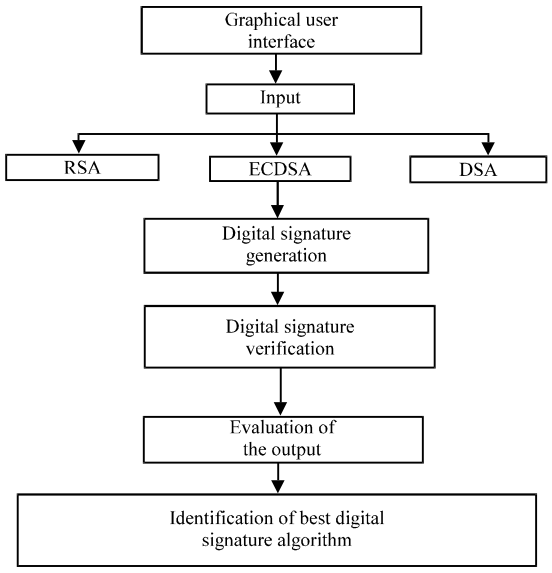

Fig. 2: Work flow

- Step 1: set the parameters; key length, signature length, time efficiency, key strength
- Step 2: identify the algorithm
- Step 3: obtain the result of the algorithm based on different parameters
- Step 4: repeat steps 2 and 3 for different algorithms
- Step 5: compare the results
- Step 6: identify the best algorithm that serves for Bitcoin

Below mentioned are the steps followed to implement ECDSA scheme which would generate efficient signatures for Bitcoin. Parameter generation is done using the following steps:

- A and b are the two field elements. Also, G consists of xG and yG as two field elements. $E(F_q)$ is elliptic curve defined over f_q
- $\frac{[h = E(F]q)}{n}$ is the cofactor

The following steps are used to create the key:

- A random integer number d is chosen within the interval [1, n-1]
- Calculate Q = dP
- Public key of the sender is Q and d is the private key

The following steps are followed in generating the signature:

- m stands for message
- Domain parameters are D = (q, ?, ?, a, b, G, n, h). A random integer k is selected within the interval [1, n-1]
- Compute kP(x_1(1)$y_1$1; 1 and r = x_1 mod n such that integer number lies between 0 and q-1.po
- If r = 0 return to first step
- Compute k^{-1} mod n
- Also, compute s = k^{-1}h(m)+dr mod n such that h is a secure hash algorithm (SHA)
- (r, s) is the signature of message m

The following steps are used to verify the signature:

- The integers r and s are within the interval [1, n-1]
- Calculate w = s^{-1} mod n and h(m)
- Calculate u_1 = h(m)w mod n and u_2 = rw mod n
- Calculate $u_1P+u_2Q = (x_0, y_0)$ and v = x_0 mod n
- If the value of v and r is equal, signature is valid

The observation shows that ECDSA uses key of smaller length compared to RSA and DSA. This is because RSA and DSA are combination of huge prime numbers which constitutes n value which is difficult to be factorized. Whereas ECDSA is just one number of a defined size. This helps to reduce the complexity of the signature generation (Table 1 and 2) (Fig. 3).

Table 1: Key length

Algorithm	p-values	q-values
RSA	1976	-
DSA	2048	256
ECDSA	-	250

Table 2: Signature length

Algorithm	Length (bytes)
RSA	128
DSA	46
ECDSA	70

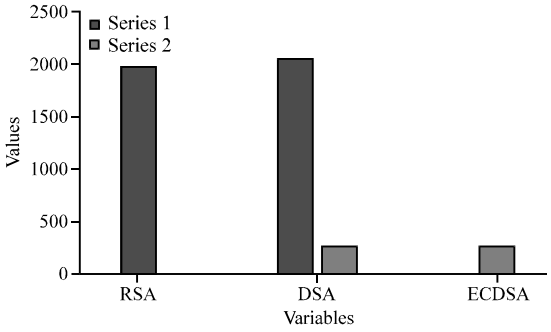

Fig. 3: Key length

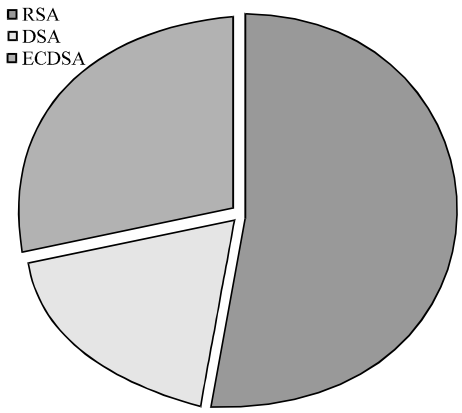

Fig. 4: Signature length

Table 3 and Fig. 4 show the length of the signature produced by three different schemes. The signature produced using RSA algorithm is huge in size whereas DSA produces signatures of smaller size. Compared to RSA and DSA, ECDSA is optimal in producing neither too strong nor too weak signatures (Brier and Joye, 2002). This helps in stability of the scheme. Due to smaller key strength and signature length, the time taken to

Table 3: Time efficiency

Algorithm	Time (NS)
RSA	117752219222
DSA	25645753793
ECDSA	222416433

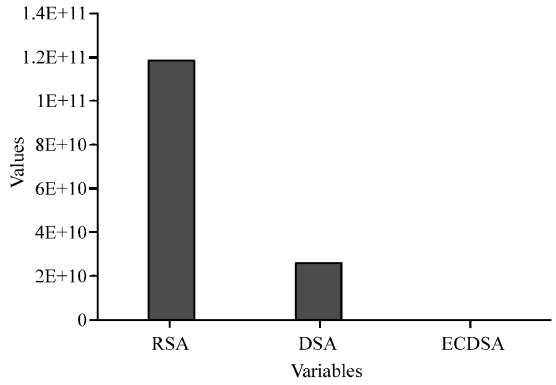

Fig. 5: Time efficiency

produce the signature by ECDSA is Much lesser compared to other schemes. ECDSA is more time efficient (Fig. 5).

CONCLUSION

Technology has invaded the entire universe in terms of development. Commerce is greatly influenced by technology. Hence, a good amount of transaction happens online. Payment system such as Bitcoin has improved the quality of online transactions. Integrity, non-repudiation, authenticity and security are factors that are necessary for such transaction. Digital signature can be applied to sustain these features in a transaction. RSA, DSA, ECDSA are three well known and most popular digital signature schemes that prevailing in the current world. By understanding the merits, demerits and efficiency of the algorithms, ECDSA is proposed as the best option for digitally signing the transaction details in Bitcoin. This helps to make sure that the Bitcoins were sent from the actual sender.

REFERENCES

Alrehily, A.D., A.F. Alotaibi, S.B. Almutairy, M.S. Alqhtani and J. Kar, 2015. Conventional and improved digital signature scheme: A comparative study. J. Inform. Security, 6: 59-67.

Barber, S., X. Boyen, E. Shi and E. Uzun, 2012. Bitter to better-how to make bitcoin a better currency. Proceedinga of the International Conference on Financial Cryptography and Data Security, February 27-March 2, 2012, Springer, Berlin, Germany, pp: 399-414.

Brier, E. and M. Joye, 2002. Weierstraß elliptic curves and side-channel attacks. Proceedings of the International Conference on Public Key Cryptography, February 12-14, 2002, Springer, Berlin, Germany, pp: 335-345.

Haraty, R.A., A.N. El-Kassar and B. Shibaro, 2006. A comparative study of RSA based digital signature algorithms. J. Math. Statist., 2: 354-359.

Islam, M.S., 2015. An algorithm for electronic money transaction security (three layer security): A new approach. Intl. J. Secur. Appl., 9: 203-214.

Johnson, D., A. Menezes and S. Vanstone, 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). Int. J. Inform. Secur., 1: 36-63.

Khalique, A., K. Singh and S. Sood, 2010. Implementation of elliptic curve digital signature algorithm. Int. J. Comput. Appl., 2: 21-27.

Milanov, E., 2009. The RSA algorithm. RSA Laboratories, Bedford, Massachusetts.

Nakamoto, S., 2012. Bitcoin: A peer-to-peer electronic cash system 2009. Master Thesis, Pennsylvania State University, Pennsylvania.

Wang, D., 2014. Secure Implementation of ECDSA Signature in Bitcoin. University College London, London, England.