Advances in Science, Technology and Engineering Systems Journal
Vol. 5, No. 5, 452-459 (2020)
www.astesj.com

ASTES Journal
ISSN: 2415-6698

Comparative Study of Cryptocurrency Algorithms: Coronavirus Towards Bitcoin's Expansion

Fatma Mallouli*[,1], Aya Hellal [1], Fatimah Abdulraheem Alzahrani[1], Abdulsalam Ali Almadani[2], Nahla Sharief Saeed[3]

[1] *Computer Department, Deanship of Preparatory Year and Supporting Studies, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia*

[2]*Information System Department, College of Computer and Information Sciences, Al Imam Mohammad Ibn Saud Islamic University, Riyadh 13318, Saudi Arabia*

[3]*Computer Department, Community College, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia*

ARTICLE INFO

Article history:
Received: 12 June, 2020
Accepted: 05 September, 2020
Online: 24 September, 2020

Keywords:
Corona virus (COVID−19)
Cryptocurrency
Blockchain
Asymmetric

ABSTRACT

The widespread presence of Corona virus (COVID-19) is causing organizations and individuals major economics downsizing. The way this virus is transmitted from one individual to another is the real cause of the problem. For that, researchers in different fields started seriously looking for touch-less and contact-less exchange. Particularly in the finance world, cash transactions and key pad based transactions are becoming obsolete because they are some of the major causes of the spread of this virus (and other viruses and bacteria). Cryptocurrency could be one of the solutions to the above mentioned situation. This novel money is based on Blockchain technology, which is based on cryptography algorithms for the safety and the security of the transactions. This paper exhibits a comparative study of the asymmetric cryptography algorithms. This helps the user to best choose the most secure, safe and reliable method to encrypt/decrypt the transactions created in the Blockchain.

1 Introduction

Over the last eight months, the number of corona patients has increased dramatically all over the world. The direct impact on world economy was a major decrease of financial development in numerous countries. The spread of this contagious disease is caused by the direct contact or by touching humans , objects like Credit cards, physical wallets, and cash money, or by the use of contact code ATM and other machines. The wide spread of the current epidemic caused significant losses to organizations, individuals, and governments which made the corona prevention a hot subject for all researchers. This quick corona spread forced everybody to adopt virtual and contact less applications to ensure safe and secure financial transactions. Our topic is simply one of the possible solutions that can help the finance world to adopt the Blockchain technologies for the creation of new coins called cryptocurrency. These currencies could, in the near future, take a portion of the financial transactions currently governed by banks. Our research is on how to best secure these transactions, or in other words, how to choose the best methods/algorithms to encrypt/decrypt messages while creating the Blockchains. This research is an extension of work originally presented in a conference named "International Conference on Cyber Security and Cloud Computing, CSCloud 2019". In order to introduce the new epidemic corona virus that changed the concept of dealing with physical money and lead people and investors to use innovative technology such us BlockChain and Bitcoin [1] as a preventive and safe way to cope with corona virus epidemic. The corona virus (COVID-19) flare-up in late 2019 involves a genuine danger around the globe [2]–[3]. The seriousness of the plague was enormous to such an extent that the World Health Organization(WHO) was firm to announce that corona virus (COVID-19) is a pandemic, around a month after the first apparition. The corona spread disabled all kind of vital economic [4] drivers like airports, [5] and transportation industry, education, tourism and related fields, government agencies, etc. The world started looking for alternative solutions to keep economy going while keeping a distance between the person and anything surrounding him/her. Particularly in the finance world, the correlation between Bitcoin and the equities market has obviously increased [6, 7]. The rest of this article is organized as follows. section 2 introduces corona virus dis-

*Corresponding Author: Fatma Mallouli, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia, fmmallouli@iau.edu.sa

https://dx.doi.org/10.25046/aj050556

ease and its impact on the wold economies and finances. Section 3 introduces, summarizes, and explains cryptography and its different branches in the first three subsections; then focuses on introducing BlockChain/Bitcoin and their terminologies [8]–[9]. Section 4 explains the RSA asymmetric algorithm while Section 5 does the same for El Gamal asymmetric algorithm. Section 6 presents a brief comparison between RSA and El Gamal. Section 7 explains the Elliptic Curve (ECC) asymmetric algorithm, where Section 8 presents a comparison between RSA and ECC. Finally, in Section 9, we conclude and present some promising future directions in this field .

2 Coronavirus Disease (COVID-19)

By the end of the year 2019, a new Corona virus disease appeared known as SARS-CoV-2 has resulted in the outbreak of a respiratory disease called COVID-19 [10]. It is a contagious epidemic caused by a newly discovered corona virus. People who got infected with the COVID-19 epidemy will experience fever and respiratory problems. Until today recovering do not require special treatment which is not found yet also, vaccination is not available yet. Corona virus is so dangerous specially while attacking older people, and those with underlying medical problems like cardiovascular disease, diabetes, chronic respiratory disease, and cancer. Corona virus caused many deaths in several countries. During this early period, researchers scientists exploring the main cause of this novel epidemic by investigating clinical manifestation and diagnosis. Thus, all of them agree that the causes are still not known yet, but they all agree that prevention is the only way to be safe from this danger. In fact, exchanging cash money hand to hand is one of the major causes of the rapid spread of covid-19 virus [11]. When possible it's a good idea to use contact less payments. Based on the fact that prevention is the safe procedure therefore people run away from cash money to use the digital money transactions. One of the newest applications of digital money is the Blockchain- based-cryptocurrency [12]. Are we going to see our planet without cash, without ATM-machines and without third party financial institutions?

2.1 Cryptography

In a simple way, defining Cryptography [13] is systematically hiding information. By doing so, only the authorized parties on both ends of the communication link can access the right information. The process can be considered as an art, however, it is actually a science. Broadly, Cryptosystems are classified into two main categories, the asymmetric (Figure 3) and the symmetric (Figure 2). This classification is based on the concepts of the key used.

2.2 Concepts Used in Cryptography

In the coming paragraph, we described some of the cryptography concepts [14]–[15].

Cryptography: also termed as "secret writing" is a science of concealing information so that only the intended parties can have access to the private information. It protects the privacy and modification of data which may occur due to active and passive attacks in the channel. *Encryption:* Transforming a message written in plain text into a cipher text message is the encryption process.

Decryption: The decryption process is writing back a cipher text message into its original plain text message.

Plain Text: The plain text is nothing but the raw message communicated orally or in writing using any human language. It takes the form of plain text. the plain text could be read or heard then understood by the sender, the recipient, or by any third party that has accessed the transmitted message.

Cipher Text: Cipher [16] simply the secret message or the coded message. When applying a suitable scheme to codify a plain text, the output message is named a cipher text.

Key: the most important part of the process of the encryption and decryption is the choice of the key. It is the base of security in the cryptography process. The type of the key chosen defines the class (Symmetric or asymmetric).

Symmetric key: also known as secret key cryptosystem [17]. We only use one key to encrypt and to decrypt.

Asymmetric key: also known as public key cryptosystem. contrary to the Symmetric [18] , the Asymmetric needs two keys: one to encrypt and one to decrypt.

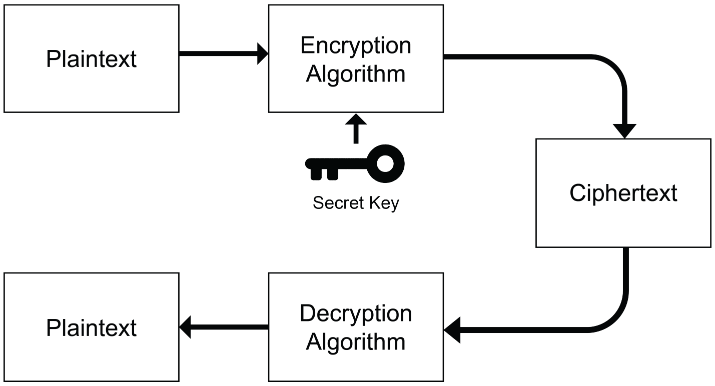

Figure 1: Symmetric Encryption

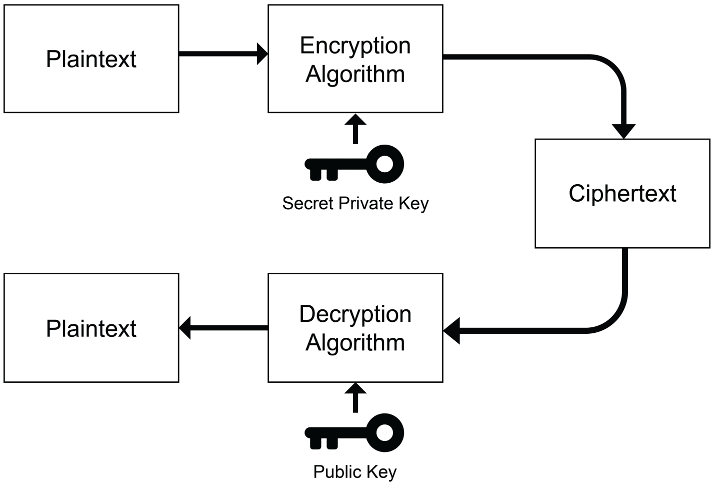

Figure 2: Asymmetric Encryption

Encryption Standard (DES)Algorithm: In 1977, IBM invented a symmetric key bloc and named it Data Encryption Standard (DES). It uses a 64-bits block size and a 56-bits key size (in which the parity bits are 8 bits) to encrypt any plain text of 64 bit in size.

Triple Data Encryption Standard (3DES): In 1978, IBM modified DES Algorithm and created a new version of it called 3DES or Triple Data Encryption Standard. The 3DES is meant to enhance the security of the data. 3DES uses a 64-bits block size and a 56-bits key size just like the DES, but it performs the same DES algorithm 3 times to every block of the data. The 3DES is definetely more secure than the DES, but it is vulnerable to brute force attack [19].

Advanced Encryption Standard (AES): Developed by the National Institute of Standard and Technology (NIST) to replace the two prior algorithms listed above after defining the weak points of the DES and the 3DES. AES-128, AES-192 and AES-256 make up the 3 block ciphers of AES. The difference between the 3 blocks is in the key size and the number of rounds. While AES-128 has a 128-bits key length and consists of 10 rounds, AES-192 has a 192-bits key length and consists of 12 rounds, and AES-256 has a 256-bits key length and consists of 14 rounds. Every round goes through a series of steps. For example: Substituting a Byte, or Shifting a row, or Mixing columns, or Adding Round Key, etc... AES Algorithm is much more secure when compared to DES or 3DES.

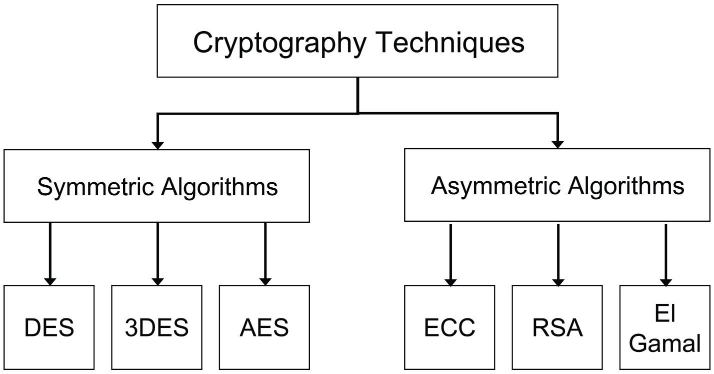

Figure 3: Cryptography Technique

There are many cryptography algorithms used to secure information divided in two groups, symmetric and asymmetric [20]. symmetric algorithms such as DES, 3DES, AES, and Asymmetric such as RSA, El Gamal and ECC [21]. Each algorithm has its own advantages and disadvantages. Therefore, the challenge is how to define the best alternative in terms of security and running time. This work is meant to focus only on comparing the asymmetric algorithms: RSA,ElGamal and ECC which will be presented and defined in the coming sections.

2.3 Need of Cryptography

Cryptography is used to achieve many goals [22], and some of the goals are listed below:

- Access Control: Only the confirmed authenticated person or group is eligible to log into the received message.
- Data Integrity: The guarantee that no change or modification has occurred to the message while in transit.
- Non-Repudiation: The sender cannot deny sending the message, and the receiver cannot deny the reception of the delivered message.
- Authentication: is identifying a special person or group to access special resources using keys.
- Confidentiality: is the fact that only the end link (receiver) is the owner of the cipher key. This is the major or the ultimate objective of cryptography.

2.4 Overview Of BlockChain Terminology and its main application: Bitcoin

Blockchain was first introduced in the early nineties of the twentieth century, but was not used in any application till 2008. The first appearance of Blockchain was to introduce the first cryptocurrency: Bitcoin. From its name, Blockchain is simply a series of blocks of information connected together like a chain [13]. The information in each block is a digital ledger (see Fig.1) linked in a database that is distributed to all users. An important feature of Blockchain is the fact that it is so hard to remove a piece of information added to the ledger. Since the base of the Blockchain is exchanging information peer-to-peer, then there is no need for a third party interference. Therefore, Blockchain is a decentralized exchange of information. The question now is why all this enthusiasm for Blockchain? and the answer is simply because of the qualities tied to this technology. Blockchain focuses on anonymity, on security, and on data integrity without having an outsider (third party such as a bank) in charge of the exchange transaction.

During this research, and while looking into different scientific papers, we noticed that over 80% of the papers concentrate on cryptocurrency like the Bitcoin framework, and less than 20% focused on other Blockchain applications like the Smart Contracts and Licensing. The researches in this field also concentrate on improving the technology of Blockchain in terms of security and privacy. Our paper in its comparison of the different algorithms used for cryptography proposes and exhibits the better performance of utilizing the elliptic curve algorithm in the creation of the digital signature associated with the Bitcoin. Digital signature is the key parameter used to identify the users (end links) and to recognize any unapproved changes occurred to the transaction [17, 23]. The digital signature within the Blockchain technology is The part that guarantees the authentication, and the non-repudiation as well as the integrity of the messages (blocks). It is an electronic verification to the beneficiary of the identity of the sender, and the integrity of the information stored in the delivered block. Technically, digital signatures use a mix of hash functions and public key cryptography. First, a hash function is applied to digest the message. Then, encoding is applied to the message digest to create the signature using the endorser's private key. Any receiver can use the public key and a similar hash function to check the transmitted signature. Up to date, most cryptocurrency frameworks have utilized an Elliptic Curve Digital Signature Algorithm (ECDSA).

2.5 Main terminology of BlockChain and Bitcoin

2.5.1 BlockChain

It is a growing list of records (blocks) linked together using cryptography. Every block is composed of:

1. Hashing
    - The hash of the prior block Hashing is the procedure that a miner on a Proof-of-Work Blockchain constantly repeats in order to find an eligible signature (aka a proof of work). In other words; it is the procedure of repeatedly inserting a random string of digits into a hashing formulae until finding a desirable output.
2. A time stamp
3. Transaction data:
    - By design, the Blockchain is an open distributed ledger that is very resistant to modification of data.
    - There is no need for a third-party approval of any transaction: decentralized.
    - The BlockChain is managed by peer-to-peer network: distributed ledger
4. Block
    - found in the Bitcoin Blockchain. Blocks connect all transactions together. Transactions are combined into single blocks and are verified every ten minutes through mining. Each subsequent block strengthens the verification of the previous blocks, making it impossible to double spend bitcoin transactions (see double spend below).

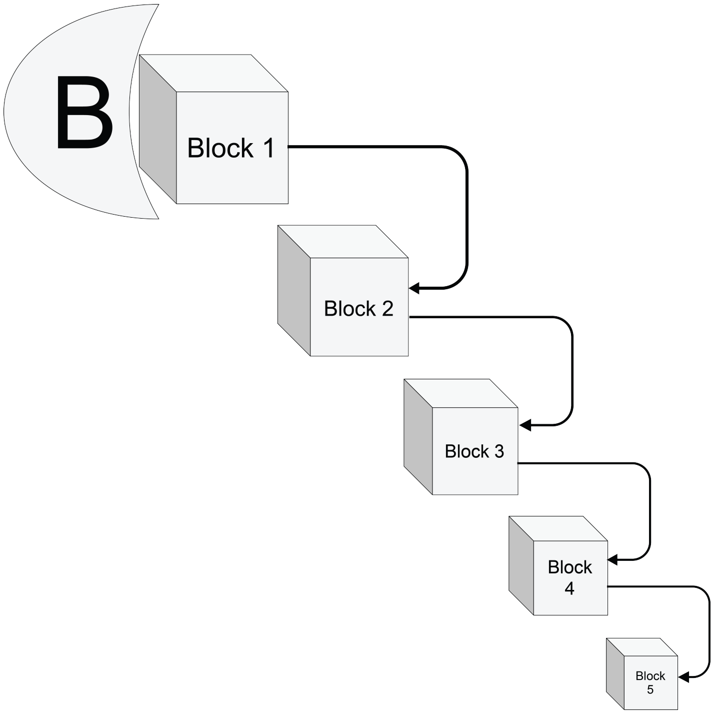

Figure 4: BlockChain System

2.5.2 Bitcoin Blockchain

Bitcoin Blockchain is a public ledger recording bit coin transactions. Blocks are created every ten minutes and distributed to all [24, 25].

1. Mining: record keeping service (using computer power)
2. Decentralized: use of public/private key is the basis of decentralization
    - No central storage (the bit coin ledger is distributed)
    - Ledger is public: any body can store it on their personal computer
    - There is no single admin: the ledger is maintained by equally privilege minors
    - Any body can become a minor
    - Issuance of bit coins is decentralized: they are issued as a reward for the creation of a new block.

3 RSA Algorithm

In 1978, and in one of MIT labs in Massachusetts, the professors Leonard Adleman ,Adi Shamir, and Ron Rivest invented the encryption algorithm RSA abbreviated from the three names of the inventors [7]. RSA is classified as an asymmetric type of encryption in which two keys are needed: the first is public and it is available to all users to encrypt their messages. The second key is private and it is used in the decoding procedure of the encrypted message. While symmetric encryption uses just one key to code and to decode the raw information, asymmetric uses two various keys. The major advantage of the asymmetric algorithm over the symmetric is the strong encryption that makes the decryption process much more complicated for hackers to interfer in the process and cause any damage to the raw message or to the signatures.

Implementing the RSA algorithm on a plain text requires several steps summarized by Adki and Hatkar as follows: first, select two prime numbers p and q.Then, a modulus n is picked for the public key and the private keys to be the product of p and q [26, 27]. The next step is to select a public key named e where e cannot be a factor of $(p-1)(q-1)$. The step after is to calculate the private key d using the following formula $(d * e) \bmod (p-1)(q-1) = 1$. The next step is to calculate the encrypted cipher text using the following formula C= Me mod n, where C is the output text, and M is the raw message text. Finally, using the same variables as the prior step M and C to calculate the decryption using the following $M = Cd \bmod n$. Note that the size of the key must be greater than 1024 bits to guarantee a high level of security, and to make it difficult for hackers to identify [13]. Example1 is a good illustration of the process.

Example 1: The following example is an excellent illustration of how the RSA public key encryption algorithm works. In this example, we picked two small prime numbers p and q to be 5 and 7 respectively. Then, using the two parameters given, we generated the public key and the private keys as follows:

- Given 5 to represent p
- Given 7 to represent q

- Computation of the modulus n: $n = p * q : n = 5 * 7 = 35$
- Compute $m = (p - 1) * (q - 1) : m = 4 * 6 = 24$
- Select e, so that e and m are co-prime numbers:
- $e = 5$
- Compute the private key d, so that d*e mod m = 1: d = 29
- The public key $\{n, e\}$ is = $\{35, 5\}$
- The private key $\{n, d\}$ is = $\{35, 29\}$
- With the public key of $\{35, 5\}$, encryption of a raw text M represented as number 23 can be illustrated as:
- Given public key $\{n, e\}$ as $\{35, 5\}$
- Given raw text M represented in number as 23
- Divide B into blocks: 1 block is enough in our example
- Compute encrypted block $C = M \wedge e \bmod n$:

$C = 23 \wedge 5 \bmod 35 = 6436343 \bmod 35 = 18$ The cipher text C represented in number is 18 With the private key of 35, 29, decryption of the cipher text C represented as number 18 can be illustrated as: Given private key n,e as 35,29 Given cipher text C represented in number as 18 Divide C into blocks: 1 block is enough Compute encrypted block:
$M = C \wedge d \bmod n$:
$M = 18 \wedge 29 mod 35 = 18 * 18 \wedge 28 \bmod 35$
$= 18 * (18 \wedge 4) \wedge 7 \bmod 35$
$= 18 * (104976) \wedge 7mod35$
$= 18 * (104976 \bmod 35) \wedge \bmod 35$
$= 18 * (11) \wedge 7 \bmod 35$
$= 18 * 19487171 \bmod 35$
$= 350769078 \bmod 35$
$= 23$
The raw text M represented in number is 23.

4 EL GAMAL Algorithm

The El Gamal method is an asymmetric cryptosystem algorithm [28]. It is so incredible as far as coding and decoding. This algorithm presents a similar structure while encrypting within the public key and private key models. Subsequently, encryption is not the same as signature check . signature creation relies upon the El Gamal signature method. The principle weaknesses of El Gamal algorithm are first the requirement for randomness, and the slow speed during coding and decoding. The primary disadvantage of this algorithm is that during encryption, the message is extended by a factor of two. This leads to having an expanded cipher text which is twice the length of the raw text. On a positive note, such message development is insignificant if the cryptosystem is utilized uniquely for secret keys exchange.

4.1 El Gamal Encryption Algorithm

```
begin: Initialisation:Domainparameters (p,q,g); recipient's public key B; encoded message m in range $0 < m < p - 1$ . OUTPUT: Ciphertext (c1,c2).
    Choose a random $k$in the range $1 < k < p - 1$
    Compute $c_{1=}g^{k}$ mod $p$
    Compute $c_{2=}m * B$ mod $p$
    Return ciphertext $(c_1, c_2)$
```

The ciphertext is the pair (c1,c2), which are both about p bits long. Neal Koblitz [KOB94] describes c2 as the message m ”wearing a mask” and c1 as a ”clue” which can be used to remove the mask, but only by someone who knows the secret key b.

4.2 El Gamal Decryption Algorithm

```
begin: Initialisation: Domain parameters $(p, q, g)$; recipient's private key b; cipher text $(c1, c2)$. OUTPUT: Message representative, m.
    Compute $m = c_1^{p-b-1} c_2$ mod $p$
    Compute $c_{2=}m * B$ mod $p$
    Return $m$
```

Note that ,$c_1^{p-b-1} = (c_1^b)^{-1}$, since for any, $c \in \mathbb{Z}_p^* Z.c^{p-b-1} = c^{-b}.c^{p-1} = c^{b^{-1}}.1$ as $c^{p-1} = 1$

5 Comparison EL GAMAL Algorithm and RSA Algorithm

El Gamal algorithm isn't automatically secure. it can not exclusively be utilized in data encryption, however in numeric signature and the security depends on the issue of divergence logarithm in finite domains [28]. The procedure steps in El Gamal algorithm to RSA starts by picking a prime number p, and two random numberg, x, where $g < p$ and $x < p$, calculate $Y = g \wedge x(\bmod p)$, of which Y, g, and p are the public Comparison of El Gamal and RSA models has been done based on security and time utilization for coding and decoding. RSA is reliable and can be utilized for application in remote system on account of its efficient running time speed, and high security level. This research examines that El Gamal algorithm is safer when contrasted with RSA method on the grounds that it generates much collocated cipher text and it was likewise moderate because when we encode and decode it, it produces more than one public key. In [29], the author demonstrates that El Gamal digital signature security is continually being tested and increasingly becoming in-genuine. An improved El Gamal comparison is proposed. Despite the fact that, El Gamal algorithm is considered secure and efficient and It has the benefit of making the equivalent plain text that gives an alternate cipher text, every time during encryption. Meanwhile, it has its own burdens. The fundamental issue that only one random number is utilized. Likewise examinations and researchers demonstrated another major disadvantage: the cipfer text is twice the length of the plain text. El Gamal Algorithm slightly different to RSA as appeared in Table 1.

Table 1: Summary Table On Asymmetric Algorithms Of RSA And El Gamal

S.NO	**Factors**	**RSA**	**El-Gamal**
1	Developed	1978	1985
2	Key Length Value	>1024 bits	1024 bits
3	Type of Algorithm	Asymmetric	Asymmetric
4	Security Attacks	Timing Attack	Meet-in-The middle Attack
5	Simulation Speed	Fast	Fast
6	Scalability	No Scalability occurs	Good scalability
7	Key Used	Different key used for Encrypt and Decrypt Process	Different key used for Encrypt and Decrypt Process
8	Power Consumptin	High	Low
9	Hardware and Software Implementation	Not very efficient	Faster and efficient

6 ELLIPTIC CURVE Algorithm

Independently and in two different years (1985 and 1987), Neal Koblitz and Victor S. Miller introduced Elliptic Curve Cryptography (ECC) [30]. Elliptic curve cryptography was a smart way of transforing a mathematical problem into an applicable computer algorithm. In general, The notion of public key cryptography is what brings complexity into any asymmetric cryptosystem. Elliptic Curve cryptography (ECC) is based upon the algebraic structure of elliptic curves over a finite field. Figure 6 is a graph illustration of the elliptic curve, and the following example 2 is a numeric illustration of the elliptic curve as well.

Example 2: $(p = 7, n = 2, a = 1, b = 6)$
$y^2 = x^3 + x + 6$
(Note:$4 + 27 * 36 = 976 = 3$ mod7)
There are 49 integer points on this “curve”
Ex: $(3, 6) \rightarrow 3 \wedge 3 + 3 + 6 = 36 \bmod 7 = 1 = 6 \wedge 2 \bmod 7$
$(4, 2) \rightarrow 4 \wedge 3 + 4 + 6 = 74 \bmod 7 = 4 = 22 \bmod 7$
$(6, 5) \rightarrow 6 \wedge 3 + 6 + 6 = 228 \bmod 7 = 4 = 52 \bmod 7$
Points on the “curve” for which there are solutions: $(1, 1), (1, 6), (2, 3), (2, 4), (3, 1), (3, 6), (4, 2), (4, 5), (6, 2), (6, 5)$
Note: $(3, 1), (2, 3), (6, 2)$ are on the same line.
$y = 2x + 7, y = x/3$ are the same line
(7 mod 7 = 0, 1/3 is the inverse of 3 which is - 2).

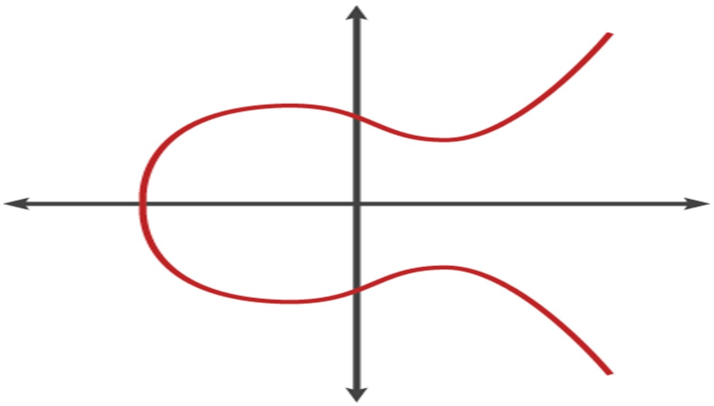

Figure 5: elliptic-curve-cryptography

7 Comparison between ECC and RSA Algorithms

While transmitting the encrypted text using RSA, the private key is not attached to the message. This feature is a primary advantage of RSA over other algorithms since it makes it impossible for a hacker to know the private key. Another very powerful feature of RSA is providing a digital signature by the public key [14]. The importance of the online digital signature comes from the fact that it solves two major security issues. The first is that the message could only be sent to the required person with no changes, and second, it guarantees the identity of the sender [31, 32]. The listed advantages eventually cause the RSA algorithm to be slow in processing, which is the major disadvantage of RSA [14].

Compared to other double key algorithms, ECC lies over a mathematical structure : elliptic curves over a finite field. The algebraic model gives this algorithm a set of advantages over RSA. The primary and most important feature is the length of the key. For the same security level, if RSA requires 1024 bit key, ECC would only require 160 bit key. This gives ECC the advantage to be very appropriate for wireless communications. Actually, in practice ECC became the number one choice for networks and for communication devices due to the size and the efficiency benefits. Today’s ‘devices that are accessing networks and services are small in size and with minimal power use: this had given ECC cryptography the edge because of the use of tiny key sizes and because of the computational efficiency tied to Elliptic Curve Cipher.

Process wise, Elliptic curve cryptography is more complicated than RSA. While in RSA, only one coding algorithm is used; in ECC, different ways of encryption are applied. When confidentiality is the objective, ECC uses arithmetic algorithms for high-level security functions, and if authentication is the objective ECC implements the digital signature processes. ECC can either be implemented in hardware or in software. ECC applies very generic procedures, therefore if a group of users agree on publicly known data, then every user can generate their own keys (private key and public key) [13, 33, 31, 30, 34, 35]. As shown in Table 2, and compared to RSA, Elliptic Curve Cryptography is clearly more efficient and can provide higher security.

Table 2: Comparison between RSA and ECC

Security bit level	RSA	ECC
80	1040	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

8 Conclusion

counting more than 200,000 detailed passings. The fear of this as of late recognized illness has closed businesses and grounded thousands of flights. When the syndrome (covid-19) virus hit the world economy in 2020, lots of people lost their jobs and business. Investors start very pessimistic about the dramatic harmful economic consequences. To rebound the market slowly within this contagious epidemic seems like a problematic situation. The new deadly corona virus is a detrimental effect on the global economy. This lead people and investors to use Bitcoin and get a way from cash money contact. the concentration on Bitcoin which is the Blockchain main application remain us to focus on the popular algorithms used in the cryptography world . Innovative technologies such as Blockchain and its major bitcoin application have interfered as promising solutions for fighting effects of corona virus epidemic on cryptocurrency. This paper presents a comparative study of different key algorithms like :RSA, El Gamal and ECC. in this study we have compared RSA, El Gamal and Elliptic Curve algorithms to demonstrate the performance of Elliptic Curve algorithm. We have shown that the elliptic curve crypto-schemes offer the highest security per bit ratio compared to any other currently known public-key cryptosystem. This is a plus point for cryptography system during corona virus epidemic where the future of Bitcoin is a hot subject. To ensure high security levels for cryptocurrency system , Elliptic Curve Cryptography is highly recommended. the pandemic of covid-19 has a negative impact on business meanwhile this disruption is a challenge to the technologies to take over the classical procedures. during the world crises of the corona virus, Blockchain help in economy Recovery and it is a pivotal engine to accelerate financial transactions. Bitcoin plays an important role in world finance transactions. it is becoming very useful today while corona epidemic drives for accelerating the use of digital money.This paper might helps the user to use the most efficient method to encrypt/decrypt the transactions created in the Blockchain. However, Elliptic curve crypto-schemes offer a lot of promise in terms of security and memory requirement than any other present crypto-schemes. more research is needed in this field for better understanding and effective correlation of bitcoin and ECC.

References

[1] F. Mallouli, A. Hellal, N. S. Saeed, F. A. Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 173–176, 2019, doi:10.1109/CSCloud/EdgeCom.2019.00022.

[2] E. Livingston, K. Bucher, "Coronavirus disease 2019 (COVID-19) in Italy," Jama, **323**(14), 1335–1335, 2020, doi:10.1001/jama.2020.4344.

[3] R. E. Ferner, J. K. Aronson, "Chloroquine and hydroxychloroquine in covid-19," 2020, doi:10.1136/bmj.m1375.

[4] M. Kumar, S. Srivastava, "Image authentication by assessing manipulations using illumination," Multimedia Tools and Applications, **78**, 12451–12463, 2018.

[5] Z. Allam, D. S. Jones, "On the coronavirus (COVID-19) outbreak and the smart city network: universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management," in Healthcare, volume **8**, 46, Multidisciplinary Digital Publishing Institute, 2020, doi:10.3390/healthcare8010046.

[6] P. S. S. H. Vikrant M. Adki, "A Survey on Cryptography Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, **6**, 2016.

[7] V. K. Mitali, A. Sharma, "A Survey on Various Cryptography Techniques," International Journal of Emerging Trends & Technology in Computer Science, **3**, 2014.

[8] G. Brown, R. Whittle, Algorithms, Blockchain & Cryptocurrency: Implications for the Future of the Workplace, Emerald Group Publishing, 2020.

[9] A. Hachicha, F. Hachicha, "Analysis of the bitcoin stock market indexes using comparative study of two models SV with MCMC algorithm," Review of Quantitative Finance and Accounting, 1–27, 2020.

[10] R. a. Vishvkarma, "The Dedicated Databases for COVID-19 Research," GMJ Medicine, **4**(1), 2020, doi:10.29088/GMJM.2020.256.

[11] H. Aldawsari, A. Alnagada, "Coronavirus Economic Effects on the Seven Largest Advanced Economies in the World (G7)," 2020, doi:10.2139/ssrn.3613725.

[12] J. Bouoiyour, R. Selmi, "Coronavirus Spreads and Bitcoin's 2020 Rally: Is There a Link?" 2020, doi:10.13140/RG.2.2.16003.86561.

[13] S. K. G. Omar G. Abood, "A Survey on Cryptography Algorithms," International Journal of Scientific and Research Publications, **8**, 2018, doi: 10.29322/IJSRP.8.7.2018.p7978.

[14] A. Kahate, Cryptography and Network Security, McGraw Hill Education, 2013.

[15] A. Shah, M. Engineer, "A survey of lightweight cryptographic algorithms for iot-based applications," in Smart Innovations in Communication and Computational Sciences, 283–293, Springer, 2019.

[16] M. M. Hammood, K. Yoshigoe, A. M. Sagheer, "RC4-2S: RC4 stream cipher with two state tables," in Information Technology Convergence, 13–20, Springer, 2013.

[17] R. L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Commun. ACM, **21**(2), 120–126, 1978, doi:https://doi.org/10.1145/359340.359342.

[18] S. A. Ritu Tripathi, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," International Journal of Advance Foundation and Research in Computer, **1**, 2014.

[19] R. K. Hussein, A. Alenezi, H. F. Atlam, M. Q. Mohammed, R. J. Walters, G. B. Wills, "Toward confirming a framework for securing the virtual machine image in cloud computing," Advances in Science, Technology and Engineering Systems, **2(4)**, 44–50, 2017, doi:doi:10.25046/aj020406.

[20] D. Jost, U. Maurer, J. L. Ribeiro, "Information-Theoretic Secret-Key Agreement: The Asymptotically Tight Relation Between the Secret-Key Rate and the Channel Quality Ratio," in A. Beimel, S. Dziembowski, editors, Theory of Cryptography — TCC 2018, volume **11239** of *LNCS*, 345–369, Springer International Publishing, 2018.

[21] A. Poojari, H. Nagesh, "A Comparative Analysis of Symmetric Lightweight Block Ciphers," in Emerging Technologies in Data Mining and Information Security, 705–711, Springer, 2019.

[22] K. N. Jassim, A. K. Nsaif, A. K. Nseaf, A. H. Hazidar, B. Priambodo, E. Naf'an, M. Masril, I. Handriani, Z. P. Putra, "Hybrid cryptography and steganography method to embed encrypted text message within image," Journal of Physics: Conference Series, **1339**, 012061, 2019, doi: :10.1088/1742-6596/1339/1/012061.

[23] U. M. Christian Badertscher, B. Tackmann, "On Composable Security for Digital Signatures," in Public-Key Cryptography, volume **10769** of *LNCS*, 494–523, Springer, 2018.

[24] S. Underwood, "Blockchain beyond Bitcoin," Communications of the ACM, **59**, 15–17, 2016, doi:10.1145/2994581.

[25] U. M. D. T. Christian Badertscher, Juan Garay, V. Zikas, "But Why does it Work? A Rational Protocol Design Treatment of Bitcoin," 2018.

[26] X. Meng, X. Peng, L. Cai, A. Li, Z. Gao, Y. Wang, "Cryptosystem based on two-step phase-shifting interferometry and the RSA public-key encryption algorithm," Journal of Optics A: Pure and Applied Optics, **11**(8), 085402, 2009, doi:10.1088/1464-4258/11/8/085402.

[27] M. Kumar, "Advanced RSA cryptographic algorithm for improving data security," in Cyber Security, 11–15, Springer, 2018.

[28] R. Ansah, E.-P. Samuel, D. Attuabea, B. Adjei, B.-R. K Bawuah, P. Antwi, "Relevace of Elliptic Curve Cryptography In Modern-Day Technologie," **3** (**2**), 1–10, 2018.

[29] R. Ansah, R. Boadi, W. Obeng-Denteh, A. Y Omari-Sasu, "Review of the Birch and Swinnerton-Dyer Conjecture," 182–189, 2016, doi:10.5923/j.ajms.20160604.07.

[30] A. U. Hardik Gohel, "Study of Cyber Security with Advance Concept of Digital Signature," International Journal of Advanced Research in Computer Science, **6**, 2015.

[31] H. Adki, V. M., "A Survey on Cryptography Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, **6**, 2016.

[32] Z. Xi, L. Li, G. Shi, S. Wang, "A comparative study of encryption algorithms in wireless sensor network," in Wireless Communications, Networking and Applications, 1087–1097, Springer, 2016.

[33] X. Sun, M. Xia, "An Improved Proxy Signature Scheme Based on Elliptic Curve Cryptography," in 2009 International Conference on Computer and Communications Security, 88–91, 2009.

[34] D. M. Behrouz A Forouzan, Cryptography and Network Security, McGraw-Hill Education, 2011.

[35] G. Shen, B. Liu, "Research on Efficiency of Computing kP in Elliptic Curve System," in 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 1–4, 2010.