INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Comparative Analysis of Different Cryptography Methods for Text and Image Data

Anu kukreja[1], Ayushi[2]

[1]Murthal University, Hindu College of Engineering,
Sonepat, Haryana. Pin no.131001
anu.kukreja1990@gmail.com
[2] Murthal University, Hindu College of Engineering,
Sonepat, Haryana. Pin no.131001
ayushibmiet@gmail.com

Abstract— *Cryptography is one of the important sciences in the current era. The importance of cryptography comes from the intensive digital transactions which we daily perform on the internet and other communication channels. In this work, we will discuss the relationship between cryptography and mathematics in the context of Elliptic Curve (EC). Elliptic Curve Cryptography has become one of the latest trends in the field of public-key cryptography. Even though, Elliptic Curve Cryptography promises a faster and more secure method of encryption compared to any other standard public-key cryptosystem, there are possibilities of making the algorithm more efficient and secure. This work illustrates a new design of Elliptic Curve Cryptography implementation which makes it more infeasible attempting any subliminal attack to break the cryptosystem. Cryptography is one of the most prominent application areas of the finite field arithmetic. Almost all public-key cryptographic algorithms including the recent algorithms such as elliptic curve and pairing-based cryptography rely heavily on finite field arithmetic, which needs to be performed efficiently to meet the execution speed and design space constraints. We present different architectures, methods and techniques for fast execution of cryptographic operations as well as high utilization of resources in the realization of cryptographic algorithms. While it is difficult to have a complete coverage of all related work, this work aims to reflect the current trends and important implementation issues of finite field arithmetic in the context of cryptography.*

Keywords— *Elliptic Curve (EC), Elliptic Curve Cryptography (ECC), Security, cryptographic algorithms, Public Key Cryptography, Biometrics Elliptic Curve Cryptography, Subliminal Channel, Public-Key Cryptosystem, Encryption, Decryption, Key Generation, Random Number Generation.*

1. INTRODUCTION

Today, the world is growing fast with electronic revolution in our day-to-day life. In this environment, any information is available at the click of a mouse button. When information is available so freely in the web, there are people who might use this information against us. So it has become mandatory to check this behavior

And control the act of attack against us. This made people to think about a solution named Encryption. The process of Encryption is to convert your information into a form which cannot be read or understood by anyone. Figure 1 shows the process of Cryptography which is the science of secret sharing. Any character or alphabet author press on the keyboard is represented as binary information.

If the entire document is converted into binary information, just imagine how difficult it would be to recognize the information. In the process of encryption, author try to mix these binary numbers after performing a few mathematical operations which converts the huge set of binary information in a newer arrangement which is difficult to understand. The entire process of encryption is to perform mathematical operations on the text that scrambles the text binaries. This is done with the help of a key. Key acts as a parameter which is passed in the encryption function along with the text which needs to be encrypted. The process of encryption then generates a Cipher text which is nothing but coded information difficult for others to understand. This can be mathematically represented as

Cipher text = Encryption (Key, Plaintext)

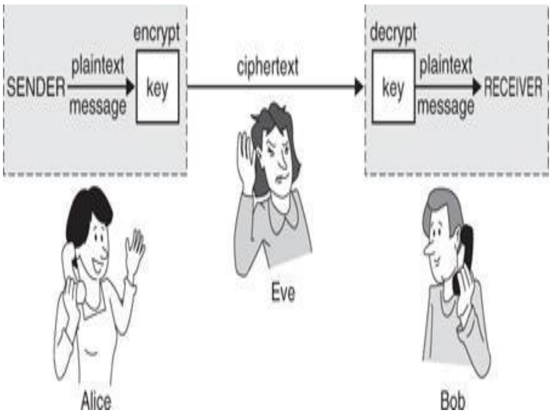

Figure 1 Process of Cryptography [1].

When it is received by the intended recipient, the Cipher text is decrypted using a Decryption function and Key. This generates back the Plaintext. This can be mathematically represented as Plaintext = Decryption (Key, Cipher text)

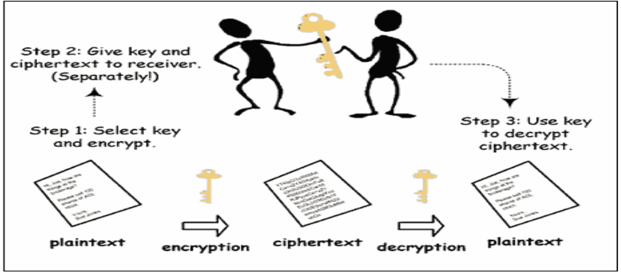
Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

Figure 2 Symmetric Key Encryption [1]

Figure. 2 shows the process of Symmetric Key Encryption involving the use of a single key. The equations (1) and (2) give us the method of generating Cipher text and Plaintext in Symmetric Key Encryption. Figure 3 shows the process of Asymmetric Key Encryption or Public Key Encryption which involves the use of two distinct keys – one to encrypt and a different one to decrypt. This work mainly focuses on Elliptic Curve Cryptography (ECC) which has a very unique property which makes it suitable for use in Cryptography. Even though, Elliptic Curve Cryptography promises a faster and more secure method of encryption compared to any other standard public-key cryptosystem, there are possibilities of making the algorithm more efficient and secure. This work illustrates a new design of Elliptic Curve Cryptography implementation which makes it more infeasible attempting any attack in Subliminal Channels to break the cryptosystem [1].

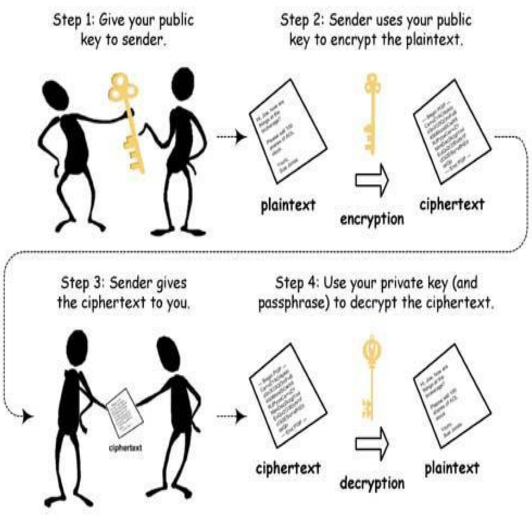
Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
ciphertext
decryption
plaintext

Figure 3 Asymmetric/Public Key Encryption

Cryptography is generally designed to provide confidentiality, authentication, integrity and accessibility services [2]. Confidentiality service is used to ensure that messages are accessible only to authorized recipients. Authentication is normally used to authenticate the identity of the connected parties. Preventing eavesdroppers from changing the content of the messages sent from source to destination is basically a service provided by the integrity service. Lastly, accessibility is designed to only allow authorized parties to use the available information resources. In modern times, cryptographic systems (cryptosystems) have been used extensively in our daily communications to provide us with high level of security. In practice, cryptography is applied in numerous applications such as: internet communication, wireless communication (mobile phones) and banking transactions. The development of the cryptographic tools and systems has played an important role in re-shaping the communication style in a significant manner [2].

Signcryption, is a cryptographic primitive which targets to support confidentiality and unforgeability simultaneously but with shorter cipher text and/or lower computational cost when compared with the traditional method of doing signature generation and data encryption separately. For evaluating the performance gain of a signcryption scheme, author compare it with the sign-then-encrypt paradigm [4], which is the conventional approach for providing both confidentiality and unforgeability. In this paradigm, a message is first signed under a sender's private key, and the message together with the signature is then encrypted under a receiver's public key [4].

In this work author proposed a new cryptography area, visual cryptography. The most notable feature of this approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography. The threshold scheme makes the application of visual cryptography more flexible. With the t out of n threshold scheme; the manager can first produces n copies of transparency drawn from the secret image, one for each of his members. If any t of them stacks their transparencies together, the content of the secret image will show up. If the number of transparencies is less than t, the content of the secret image will remain hidden [5].

Majority of cryptographic algorithms utilize arithmetic in finite mathematical structures such as finite multiplicative groups, rings, and finite fields. Having a complete set of arithmetic operations, finite fields feature a superset of operations of rings and multiplicative groups. While multiplicative groups have only one defined operation and rings do not have multiplicative inversion defined for its every element, finite fields feature addition/subtraction, multiplication/division, and both multiplicative and additive inversion operations. Since overwhelming percentage of execution time of cryptographic algorithms is spent on these arithmetic operations, efficient implementation of these operations determines the efficiency of the overall cryptographic system. The basic arithmetic operations (i.e. addition, multiplication, and inversion) in finite fields, GF(q), where $q = p^k$ and p is a prime integer, are heavily used in many cryptographic algorithms such as RSA algorithm, Diffie- Hellman key exchange algorithm, the US federal Digital Signature Standard, elliptic curve cryptography, and also recently pairing-based cryptography. Most popular finite fields that are commonly used in cryptographic applications due to elliptic curve based schemes are prime fields GF (p) and binary extension fields GF (2^n). Recently, pairing-based cryptography based on bilinear pairings over elliptic curve points stimulated a significant level of interest in the arithmetic of ternary extension fields, GF (3^n). The aforementioned three popular finite fields feature dissimilar mathematical structures. Therefore, it is important to design algorithms and architectures that will exploit the specific properties of the underlying field to give the best performance for the chosen efficiency metric. On the other hand, elements of different finite fields are represented using similar data structures inside the digital circuits and computers. Furthermore, similarity of algorithms for basic arithmetic operations in these fields allows diverse utilization of the functional units in the design [3].

2. TECHNIQUES OF CRYPTOGRAPHY

There are different methods of cryptography:

- RSA
- Elliptical curve cryptography (ECC)
- Public – key cryptography
- Diffie – Hallman cryptography
- Visual cryptography
- Pairing – based cryptography
- Author have elaborated few of them.

2.1 RSA

Rivest, Shamir and Adleman proposed a novel cryptographic algorithm in 1978 [3] that can be used for key exchange and electronic signature as well as encryption.

Its security relies on the Integer Factorization Problem which is, generally believed to be a hard problem if the related numbers are sufficiently large.

2.1.1. RSA Setup

Let us assume that Bob wants to send a secret message to Alice who should have a public-private key pair. Her public key is a pair of two large integers (n, e) and her private key is d, which is another large integer. The integer n, called the modulus, is the multiplication of two large prime numbers, p and q. It is computationally infeasible to factor n into p and q when they are sufficiently large. Euler's Totient function,$\emptyset(n) = (p-1)\ (q-1)$, is used to determine the public exponent e and private exponent d. The public exponent e can be chosen randomly provided that GCD $(e, \emptyset(n))$ =1; however it is usually chosen as a small number for fast encryption. The private exponent d is the multiplicative inverse of e with respect to modulus $\emptyset(n)$.

2.1.2. RSA Encryption/Decryption

To send a message m securely to Alice, Bob performs the modular exponentiation operation $c = m^e$ (mod n).

Upon receiving the cipher text message c, Alice performs the modular exponentiation c^d (mod n) = m.

Since Alice is the only one who knows her private key d, only she can perform this computation and obtains the plaintext message m. As one can easily observe, both RSA encryption and decryption operations are nothing but modular exponentiations over very large numbers. A modular exponentiation is comprised of many modular multiplications, which are usually difficult to perform efficiently since the operands are large integers [3].

2.2 Elliptical curve cryptography (ECC)

Over recent years, RSA was the primary cryptosystem for performing asymmetric encryption processes and generating digital signatures. The key length requirement of RSA was one of the obstacles that enabled Elliptic Curve Cryptography (ECC) to break the domination of RSA on asymmetric key cryptosystems. In other words, what makes ECC attractive compared to RSA is that it appears to offer equal security for a smaller key size, thereby minimizing the processing overhead [2]. The security of ECC is primarily based on the hardness provided by the Elliptic Curve Discrete Logarithm Problem (ECDLP). The first introduction of ECDLP started in 1985 by Koblitz and Vector Miller independently. The new proposed cryptosystem was known as Elliptic Curve Cryptosystem, whose security depends on ECDLP over the points on Elliptic curves. The ECDLP is defined as follows:

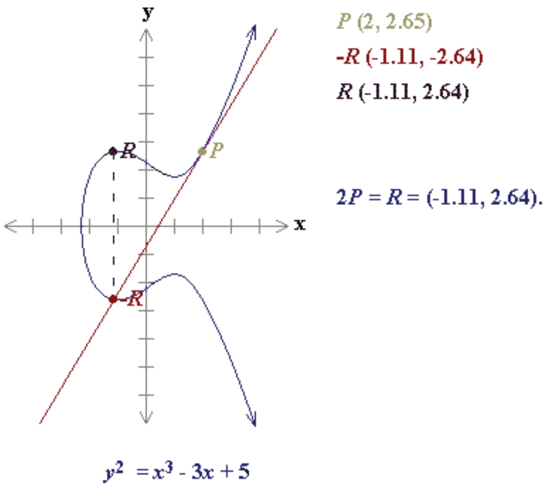

Figure 4. The geometry of point doubling on Elliptic Curve [2]

Definition (ECDLP): Given the points P and Q on elliptic curve E defined over a finite field with q (large prime number) elements Fq, find the integer k such that Q = kP. Multiplying P by an integer k means that author add the point to itself k times. An example of point multiplication is shown in Figure. 4, which describes the multiplication of integer k = 2 by the point P = (2, 2.65) in a process also known as point doubling. The result of doubling the point P is a new point R = 2P on the same curve $y^2 = x^3 - 3x + 5$. There are several cryptographic applications that have used ECDLP in their implementation. One important example is the announcement by the National Security Agency (NSA) regarding Suite B at the RSA conference in 2005 [2], which exclusively use ECC for digital signature and key exchange schemes. Other cryptographic schemes relying on ECDLP in their design are: the Elliptic Curve Diffie-Hellman key agreement (ECDH) protocol, the Elliptic Curve Digital Signature Algorithm (ECDSA), and Elliptic Curve Menezes- Qu-Vanstone (ECMQV) authentication protocol for key agreement. Intensive research and applications show that the elliptic curve cryptography has a promising future due to the provided high level of security with smaller key size, resulting in higher performance in some cryptographic primitives.

2.3 Public – key cryptography

The Public Key cryptography (PKC) concept was first pioneered by Diffie and Hellman in 1976, in their influential article, New Directions in Cryptography. This article also tackled the key exchange issue, founded on the intractability of the discrete logarithm problem. In a public key cryptography, each party has a pair of keys, one distributed in public, known as the public key, and the other is saved in a secure place, known as a private key (secret key). Public key cryptography depends on the trapdoor function, that makes decryption achievable provided the knowledge of the secret key corresponding to the public key. Bearing in mind a case like the one explained within the symmetric keys case, whereby Alice needs to send a message m to Bob. The following steps will achieve the task:

1) Alice passes Bob's public key B^4 and the message m to a suitable encryption algorithm to form the encoded message.

$C\ (\Sigma_B (m)) = E\ (\Sigma_B (m))$ (3)

2) The encrypted message was sent by Alice to Bob.

3) Bob decrypts the encoded message received by him, via his private key $\Delta_B{}^5$ and the suitable decryption algorithm.

$D_{\Delta B}\ ((\Sigma_B (m)) = D_{\Delta B}\ (E\ \Sigma_B (m)) = m$ (4)

Bob ensures that the data he received is not tampered with or leaked, as only his private key can decrypt the data. Likewise, Bob can transmit data to Alice using her public key A. The PKC scheme also fulfills the Non-Repudiation and Authenticity by utilizing inventive approaches such as Digital Signatures [2]. The PKC system is shown in Figure 5.

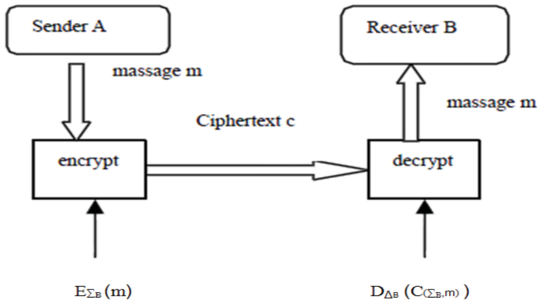

Figure 5. PKC encryption [2]

2.4 Diffie – Hallman cryptography

The Diffie-Hellman cryptography is one of the most important protocols in the field of key exchange. Say Alice and Bob want to agree on a secret key over public channel. Both of Alice and Bob will make some computation in a fixed cyclic group G with an agreed generator g. These computations are based on ECDLP. The security strengths of Diffie- Hellman lie behind the fact that Diffie-Hellman is based on NP-hard problem which cannot be broken, mathematically. The general form of Diffie-Hellman protocol is described as follows:

1) Alice chooses random a ∈ c, and sends g^a to Bob.

2) Bob chooses a random e ∈ c, and sends g^b to Alice.

3) The agreed key is g^{ab} for both Alice and Bob.

However, it is preferred that the order of G to be prime in order to prevent Pohlig- Hellman attack [2]. In the ECDLP based Diffie-Hellman, both of a and b are two points, a and b are multiplied, a new point Z will be generated on the curve E. Therefore, given z and g^{ab} , it is impossible to find a and b.)

2.5 Visual cryptography

In visual cryptography, author use sharing images as the decryption tool; that is, the final outputs are transparencies. Because the subtractive model is more suitable for printing colors on transparencies, author will use the CMY model to represent colors in what follows. Because (R, G, B) and (C, M, Y) are complementary colors, in the true color model, (R, G, B) and (C, M, Y) possess the following relationships: C = 255−R, M = 255−G, Y = 255−B: Thus, in the (C, M, Y) representation, (0; 0; 0) represents full white and (255; 255; 255) represents full black. Because most color printers use C, M, Y inks to display color, a color image must be processed by the color decomposed procedure before printing. Color decomposition mainly is to separate C, M, and Y colors from colors within every pixel of the image. These three components form three monochromatic images. (Because colored ink is expensive and the mechanical tolerances may cause the three inks to be printed slightly out of register, the black edges will suffer colored tinges. So, some printers add the black ink when printing black color, resulting in four separate color images.) These monochromatic images are like gray-level images in which every pixel has its own color level and has to be transformed into a halftone image before printing. The three monochromatic halftone images will be (cyan, white), (magenta, white) and (yellow, white) binary images, respectively. After stacking these images, all kinds of the colors in the original image can be displayed [6].

Figure 6 illustrates the procedure of printing color images. Author can see from the Figureure that every pixel Pij of the composed color image P is obtained by combining the corresponding pixels Cij, Mij, Yij in the three C, M, and Y separating halftone images, where C, M, and Y images are all binary. For any pixel, Cij, Mij or Yij , there are only two possible values: blank or not blank, where 0 denotes blank, and 1 denotes the corresponding color. Hence Pij has the following possible combinations: (0; 0; 0), (1; 0; 0), (0; 1; 0), (0; 0; 1), (1; 1; 0), (1; 0; 1), (0; 1; 1), and (1; 1; 1), where Pij (0; 0; 0) denotes a white pixel, and (1; 1; 1) denotes a black pixel. Because C, M, and Y are primitive colors in the subtractive model, they retain the usual characteristics that C (M or Y) plus C (M or Y) is C (M or Y), C (M or Y) plus white is C (M or Y), and white plus white is white, when stacking them on transparent media [5].

3. CONCLUSIONS AND FUTURE WORK

This work covers algorithms and architectures for multiplicative groups, rings, finite fields for implementing the RSA and Diffie-Hellman, elliptic curve and pairing-based cryptography.

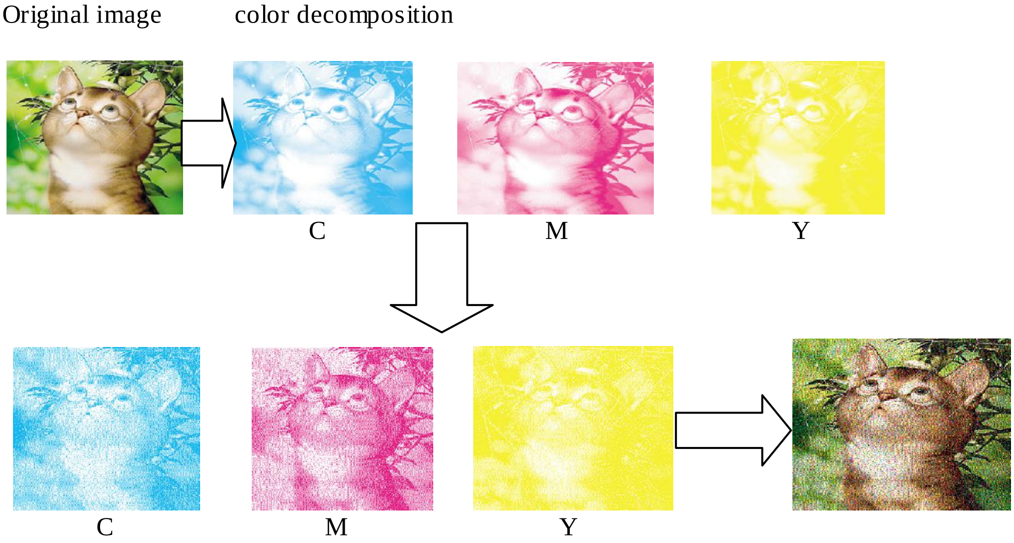

Figure 6 Color image printing [5].

The algorithms author present can be generically applied; particularly, author focused on polynomial bases for binary, ternary and general extension fields. Author gave a comprehensive summary of finite field arithmetic in cryptography, covering all basic algorithms, architectures, and building blocks in order to create time- power-, and space-efficient implementations of finite field operations. The basic arithmetic operations, i.e., addition, multiplication, and inversion in finite fields GF (q) where $q = p^k$, particularly, p is 2 or 3 or an arbitrary large prime. While these choices seem to imply a diverse set of design possibilities, it is also possible to create unified and versatile implementations where single hardware architecture supports several different fields with a little extra cost. It can be concluded that there are many challenges regarding security while transferring the data. Various kinds so security model can be designed in accordance with type of data to be encrypted. Also, one of the major issues to be considered is the computational speed of the encryption model. Existing techniques makes the computational time lesser but increase the computational speed. But, they also increase the total cost of the system because computational time of the algorithms have a and efficiency of the system. So, author need a better technique which must provide high level security, cost effective, major impact on the determining the cost effectiveness lesser computational time, higher computational speed and high efficiency. Also, the text which will be ciphered by this method must not be broken. By implementing the proposed method, this entire problem can be handled easily, by assigning various cipher letters or symbols to same plain letters.

REFERENCES

[1] Gururaja.H.S., M.Seetha, Anjan.K.Koundinya, "Design and Performance Analysis of Secure Elliptic Curve Cryptosystem" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[2] Ohood S. Althobaiti and Hatim A. Aboalsamh , "An Enhanced Elliptic Curve Cryptography for Biometric" King Saud University Riyadh, Saudi Arabia.

[3]Erkay Savas¸and Çetin Kaya Koç , "Finite Field Arithmetic for Cryptography".

[4] Chung Ki Li, Duncan S., "Wong Signcryption from randomness recoverable public key encryption" Information Sciences 180 (2010) 549–559.

[5] Young-Chang Hou, " Visual cryptography for color images" Received 6 June 2002; accepted 26 August 2002.

[6] F. Amounas and E. H. El Kinani , "ECC Encryption and Decryption with a Data Sequence" Applied Mathematical Sciences, Vol. 6, 2012, no. 101, 5039–5047.