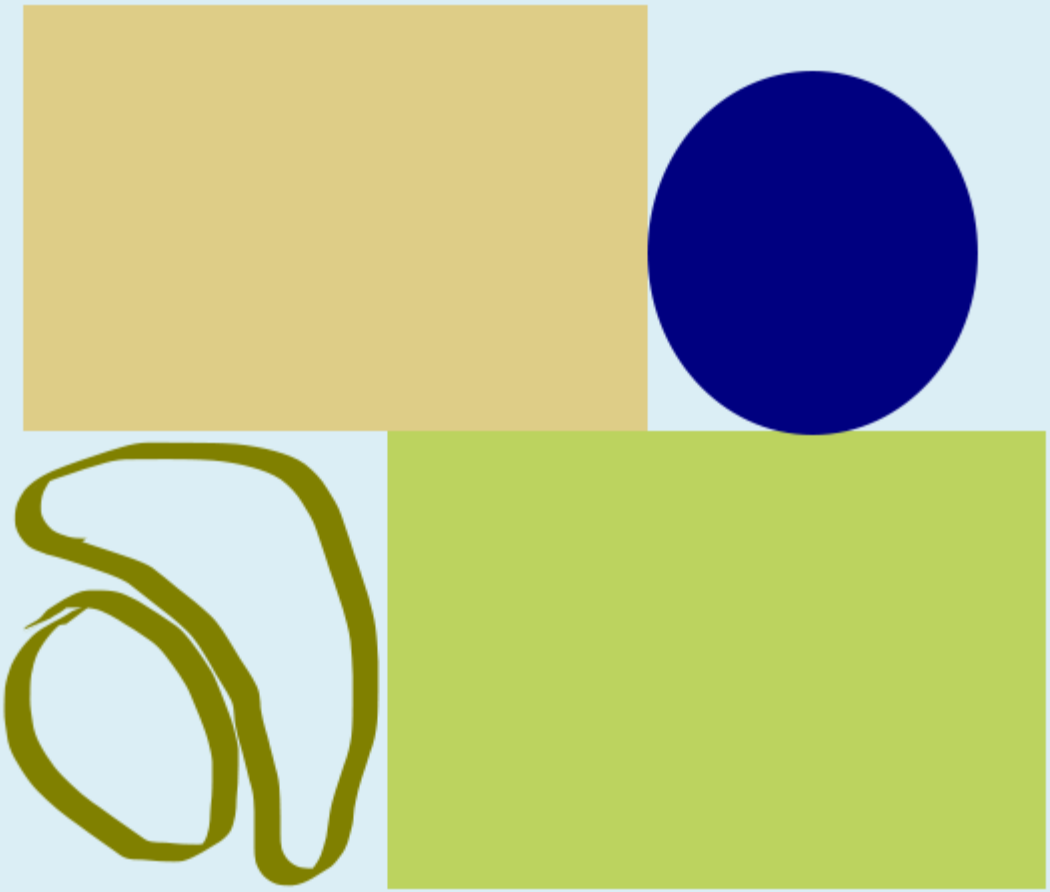
Global Open Versity – Information Security Research Journal

Elliptic Curve Cryptography Theory



Kefa Rabah

Elliptic Curve Cryptography

Kefa Rabah
Center for Advance Research in Cryptography & Cyberscurity (CAREC)
Global Open Versity, Vancouver, BC Canada
URL: www.globalopenversity.org Email: krabah@globalopenversity.org

Abstract
Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem for hand-held portable devices. Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, which results in faster computations; lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile/wireless environments which are typically limited in terms of their CPU, power and network connectivity. This work describes the mathematics needed to implement Elliptic Curve Cryptography (ECC) with special attention to its implementation in Galois Field. Here we will also explain the functionality of ECC, its advantages and challenges over other cryptosystems. Comparison with other cryptographic systems will also be undertaken based on aspects such as efficiency, size of the key needed to attain a certain level of security (this has implications on computational costs and time), known and probable attacks, current and predicted future (based on the current growth of technology) and their prevention techniques. ECC reliability will also be looked into.

Keywords
Elliptic Curve Cryptography (ECC), Internet Security and attacks, Wireless, Secure Socket Layer (SSL)

1.0 Introduction to cryptographic Systems

With the rapid growth of the use of computers to exchange information electronically, the physical way of providing security by locks, sealing and signing documents, and so on, is eliminated. However the need to exchange information securely is still very important, and is therefore provided in electronic documents; usually by encryption and digital signatures. The science of keeping messages secure is called cryptography. Cryptography involves encryption and decryption of messages. Encryption is the process of converting a plaintext into ciphertext by using an algorithm and decryption is the process of getting back the encrypted message, see **Fig. 1**. A cryptographic algorithm is the mathematical function used for encryption and decryption. In addition to providing confidentiality, cryptography is often required to provide Authentication, Integrity and Non-repudiation.

The essence of cryptography is traditionally captured in the following problem: Two parties (the tradition is to call them *Bob* and *Alice*) wish to communicate over an insecure public communication channel in the presence of malevolent eavesdropper (the tradition *Eve*). Bob and Alice could be military jets, e-business or just friend trying to have a private conversation, see **Fig. 1**. They can't stop Eve listening to their radio signals (or tapping their phone line, or whatever), so what can they do to keep their communication secret? One solution is for Alice and Bob to exchange a digital key, so they both know it, but it's otherwise secret.

Moreover, it is worthy to note right from the start that the hardest part of computer security is the piece between the computer and the user. While the hardest part of encryption is maintaining the security of the data when it's being entered into the keyboard and when it's being displayed on the screen. In case of the digital signatures, the hardest part is proving that the text signed is the same text that the user viewed. And finally the hardest part of computer forensics is to know who is sitting in front of a particular computer at any time.

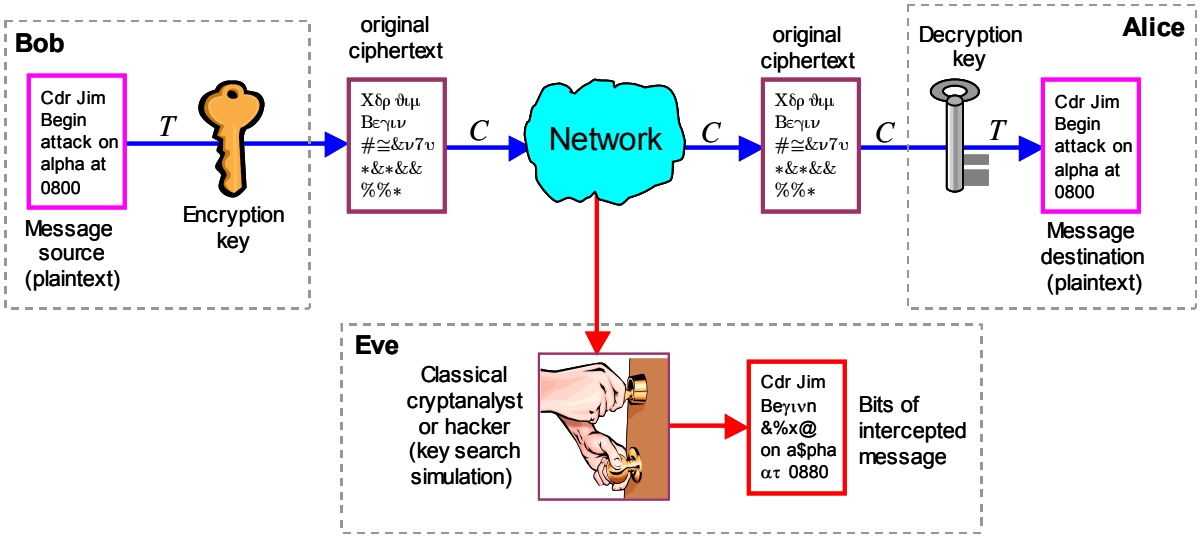


Figure 1 shows a schematic classical cryptographic data communication.

There are two popular kinds of cryptographic protocols: *symmetric-key* and *asymmetric-key* protocols. In the symmetric-key protocols, a common key (the secret-key) is used by both communicating partners to encrypt and decrypt messages **[1]**. Among these are DES, IDEA and AES. These symmetric-key cryptosystems provide high speed key and communication but have the drawback that a common (or session) key must be established for each pair of participants **[2]**. However, in 1976, W. Diffie and M. Hellman introduced *Public-Key Cryptography* **[3]**. The encoding function here is a *trapdoor* function – one whose inverse is impractical to implement, unless some extra information is available. This extra information (called the *decrypting-key*) *is not required for encrypting the message*, yet is *essential for decrypting* it in reasonable time. This makes it much easier to encrypt messages than to decrypt them. The beauty of such a system is that the encrypting process need not be kept secret. Each user has his own or a personal encrypting-function, which is *public information* (hence the name *Public-Key*), and a decoding key, which he keeps *secret*.

The public-key protocol employs a pair of different but associated keys. One of these keys (the public-key) is used either for encryption (*signature*) of the messages and; a different key (the private-key) is used for either decryption (*confidentiality*) of the message **[4]**. Different public-key cryptographic systems are used to provide public-key security. Among these we can mention the RSA **[5]**, Diffie-Hellman (DH) key exchange algorithm **[3]**, Digital Signature Algorithm (DSA) **[6,7]**, and ElGamal cryptosystem **[8]**. These systems provide these services by relying on the difficulty of different classical mathematical problems, hence provide the services in different ways.

The public-key cryptosystems are, however, slower than the symmetric ones but provide arbitrary high levels of security and do not require an initial private key exchange between two communicating parties. In the asymmetric protocol the public-key is released to the public while the other, the private-key, is known only to its owner. Because of this feature, these cryptosystems are considered to be indispensable for secure communication and authentication over open (insecure) networks **[9]**. It is designed to be computationally intractable to calculate a private-key from its associated public-key; that is, it is believed that any attempt to compute it will fail even when up-to-date technology and equipment are used **[10]**. With a public-key cryptosystem, the sender can encrypt a message using the receiver's public key-without

needing to know the private-key of the receiver. Therefore, they are suitable for communication among the general public. Public-key cryptosystems can also be used to make a digital signature **[11]**.

However, in real applications, both symmetric and asymmetric protocols are used. The public-key algorithm is first used for establishing a common symmetric-key over insecure channel. Then the symmetric system is used for secure communication with high throughput. Due to comparative slowness of the public-key algorithms, dedicated hardware is desirable for efficient implementation and operation of the cryptographic systems.

In the mid 1980s researchers noticed that another source of hard problems might be discovered by looking at the elliptic curves **[12,13]**. The invention of Elliptic Curve Cryptography (ECC) offered a new level of security for public key cryptosystems **[14-16]**, which provide both encryption and digital signatures services. One potential use of elliptic curves is in the definition of public-key cryptosystems that are close analogs of existing schemes like RSA, ElGamal, DSA and DH etc. Furthermore, elliptic curve can provide versions of public-key methods that, in some cases, are faster and use smaller keys, while providing an equivalent level of security. Their advantage comes from using different kind of mathematical *group* for public-key arithmetic.

To date many research papers in Elliptic Curve Cryptography (ECC) have been published by researchers all over the world, as can be viewed in the refs. However, the idea of using elliptic curves in cryptography is still considered a difficult concept and is neither widely accepted nor understood by typical technical people. The problem may stem from the fact that there is a large gap between the theoretical mathematics of elliptic curves and the applications of elliptic curves in cryptography.

2.0 Introduction and History of Elliptic Curve

The name "elliptic curve" is based on the ellipse. Elliptic curves were first discovered after the 17th century in the form of Diophantine equation **[17]**, $y^2 - x^3 = c$, for $c \in \mathbb{Z}$. Further, it is important to note that, however, it is easy to calculate the surface of the ellipse, it is hard to calculate the circumference of the ellipse. The calculation can be reduced to an integral:

$$\int \frac{1}{\sqrt{x^3 + Ax + B}} \mathbf{d}x \qquad (3)$$

This integral, which cannot be solved easily, was the reason to consider the curve $Y^2 = X^3 + AX + B$. This was done already during the 18th century. Probably, it was Abel in ca. 1820 who introduced the addition of points on the curve. At the moment there are several definitions for an elliptic curve. However, the following definition is used usually:

Definition – An elliptic curves *E*, defined over an arbitrary field K, is a non-supersingular plain projective third degree curve over K with a K-rational point *O* (i.e., with coordinates in K) over curve *E*.

Such a curve can be described by its so-called Weierstraβ form, in homogeneous coordinates x, y, z:

$$E : y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3 \qquad (2)$$

where $a_1,\ldots,a_6 \in K$, such that the discriminant $\Delta \neq 0$. This discriminant is a polynomial expression in the coefficient $a_1,\ldots,a_6$. The restriction $\Delta \neq 0$ is necessary and sufficient for E in order to be a non-singular. The curve E has exactly one K-rational point at 'infinity', i.e., $z=0$, the point $(0:1:0)$. This point plays the role of O (origin). Sometimes we want to express that a curve E is based over field K. We do this by notation E/K.

In general, we will restrict ourself to the affine part $(z \neq 0)$ of elliptic curves E:

$$E:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (3)$$

For fields K of characteristic >2 such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{F}_p$ with $p>3$ we can transform the Weierstraβ form for the affine curve by the coordinate transform:

$$X = x + \frac{a_1^2 + 4a_2}{12} \qquad \text{and} \qquad Y = y + \frac{a_1}{2}x + \frac{a_3}{2} \qquad (4)$$

to a curve of the form: $E/K:\ Y^2 = X^2 + aX + b$

where $a,b \in K$ such that the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. This form also known as Weierstraβ short form will be used later.

Remark – For practical applications finite field of the form $K = GF(2^m) = \mathbb{F}_{2^m}$ are very important. For such elliptic curves the theory as mentioned above has to be modified.

In 1955, Yutaka Taniyama asked some questions about elliptic curves, i.e., curves of the form $y^2 = x^3 + ax + b$ for constants a and b **[18]**. Hellegouarch studied the application of elliptic curves for solving Fermat's Last Theorem in 1971 **[19]**. Elliptic curves can also be looked at as mathematical constructions from number theory and algebraic geometry, which in recent years have found numerous applications in cryptography **[12]**.

Kefa Rabah is the Founder of Global Technology Solutions Institute. Kefa is knowledgeable in several fields of Science & Technology, Information Security Compliance and Project Management, and Renewable Energy Systems. He is also the founder of Global Open Versity, a place to enhance your educating and career goals using the latest innovations and technologies.