USE OF ELLIPTIC CURVES IN CRYPTOGRAPHY:
AN OVERVIEW

M. T. Wankhede-Barsagade & Suchitra A. Meshram

Abstract: Elliptic curve cryptography is based on deep mathematics involving elliptic curves in a finite field. It relies on the difficulty of solving the elliptic curve discrete logarithmic problems.

Elliptic curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA.

Many manufacturers including 3COM, Cylink, Motorola, Pitny, Bowes, Siemens, TRW and Verifone have included support for ECC in their products.

Keywords: Elliptic curves, Public key, Discrete logarithmic problems.

1. INTRODUCTION

Properties and functions of elliptic curves have been studied in Mathematics for 150 years. Use of Elliptic curves in cryptography was virtually unheard before 1985. Elliptic curve cryptography (ECC) was introduced by Victor Miller and Neal Koblitz in 1985. ECC is a public key cryptography. ECC is based on properties of a particular type of equation created from the mathematical group. Equations based on elliptic curve have a characteristic that is very valuable for cryptographic purpose. The main reason for attractiveness of ECC is the fact that there is no sub-exponential algorithm known to solve the discrete logarithmic problem on a properly chosen elliptic curve. This means that significantly smaller parameters can be used in ECC than in other competitive systems such as RSA and DSA, but with equivalent levels of security.

Elliptic curves are the basis for a relative new class of public-key schemes. It is predicted that elliptic curves will replace many existing schemes in near future. It is thus of great interest to develop algorithms which allow efficient implementations of elliptic curve cryptosystem.
2. DEFINITION OF ELLIPTIC CURVE

Let $K$ be a field of characteristic $\neq 2, 3,$ and let $x^3 + ax + b$ (where $a, b \in K$) be a cubic polynomial with no multiple roots. An elliptic curve over $K$ is the set of points $(x, y)$ which satisfy the equation

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

together with single element denoted by $O$ and called the “point at infinity”.

If $K$ is a field of characteristic 2, then an elliptic curve over $K$ is the set of points satisfying an equation of the type either

$$y^2 + cy = x^3 + ax + b$$
or else

$$y^2 + xy = x^3 + ax^2 + b$$
together with a “point at infinity” $O$.

If $K$ is a field of characteristic 3, then an elliptic curve over $K$ is the set of points satisfying an equation

$$y^2 = x^3 + ax^2 + bx + c$$
together with a “point at infinity” $O$.

3. GROUP LAW FOR ELLIPTIC CURVE

Let $K$ be a field of real numbers and let $y^2 = x^3 + ax + b$ be an elliptic curve defined over $K$.

Let $E$ be the set of all points $(x, y)$ lying on the elliptic curve.

Let $P$ and $Q$ be any two points on the elliptic curve, the addition $P + Q$ is defined to be a point $R$ lying on the curve such that $-R$ lies on the curve and the line joining $P$ and $Q$. $R$ is the reflection of the point $-R$ on the curve with respect to $x$ axis.

Case I: Let $P = (x_1, y_1), Q = (x_2, y_2)$ and $P \neq Q$, we will calculate the value of $R$ using above condition.

Let $R = (x_3, y_3) = P + Q$.

Let the equation of line $PQ$ be $y = mx + c$, then the slope of line $PQ = m = (y_2 - y_1)/(x_2 - x_1)$ if $x_1$ and $x_2$ are not same i.e., the point $P$ and $Q$ are different.

Since the point $(x, mx + c)$ lies on the curve $y^2 = x^3 + ax + b$, it will satisfy the equation

$$(mx + c)^2 = x^3 + ax + b$$

$$x^3 - (mx + c)^2 + ax + b = 0.$$
Since \( x_1, x_2, x_3 \), are the roots of the above equation, \( x_1 + x_2 + x_3 = m^2 \) and hence

\[
x_3 = m^2 - x_1 - x_2 = [(y_2 - y_1)/(x_2 - x_1)]^2 - x_1 - x_2.
\]

Also \( y_3 = - (mx_3 + c) = -mx_3 - c = -mx_3 - (y_1 - mx_1) = -y_1 + m(x_1 - x_3). \)

Thus if \( P = (x_1, y_1) \) and \( Q = (x_2, y_2) \) then for two different values of \( x_1 \) and \( x_2 \), \( P + Q \) is given by, \( R = (x_3, y_3) \) where \( x_3 \) and \( y_3 \) are to be calculated as above.

**Case II:** Let \( P = (x_1, y_1) \), \( Q = (x_2, y_2) \) and \( x_1 = -x_2 \) then \( P + Q = P + (-P) \) is defined to be an identity element, which is the point at infinity.
**Case III:** Let $P = (x_1, y_1), Q = (x_2, y_2)$ and $P = Q$ then the tangent of the curve through the point $P$ will meet the curve at point $-R$, where $-R$ is the reflection of the point $R$ with respect to $x$-axis. Addition $P + Q = P + P = 2P = R$ is defined as follows:

![Graph of the curve $y^2 = x^3 + 3x + 5$.](image)

Let $R = (x_3, y_3)$ then since the line $PQ$ is tangent to the curve $y^2 = x^3 + ax + b$, the slope of the tangent line can be evaluated by implicitly differentiating the equation of curve with respect to $x$.

Calculating values of $x_3, y_3$ as in Case I and replacing $m$ by $(3x_1^2 + a)/2y_1$ we get the value of $R$.

---

4. **BASIC NOTIONS OF CRYPTOGRAPHY**

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the plaintext and the disguised message is called the ciphertext. The plaintext and the ciphertext are written in some alphabet consisting of a certain number $N$ of letters. The process of converting a plaintext to a ciphertext is called encryption, and the reverse process is called decryption.

The plaintext and ciphertext are broken into message units. An *enciphering transformation* is a function that takes any plaintext message unit and gives us a ciphertext message unit. The *deciphering transformation* is the inverse function which goes back and recovers plaintext from the ciphertext.

4.1 **Classical Cryptosystem**

The cryptosystem in which, once the enciphered information is known, the deciphering of transformation can be implemented in approximately the same order of magnitude of time...
as the enciphered transformation. Classical cryptosystem provide secure communication for a pair of user. In classical key cryptosystem, the encryption key can be calculated from the decryption key and vice versa. In most cryptosystem, the encryption key and decryption key are the same. The security of the classical key cryptosystem rests in the key. As long as the key remains secret, the communication remains secret.

4.2 Public Key Cryptosystem

The public key cryptographic system is a family of encryption transformation and a family of decryption transformation in such a way that, given a member of one family, it is infeasible to find the corresponding member of the other.

In this cryptosystem, there is no need to send the secret key via secure channel. Every user A in the system has one pair of keys, a public key for encryption and a private key for decryption. With the help of private key, the user calculates the public key. It is computationally infeasible to recover the private key using his public key.

5. ELLIPTIC CURVE CRYPTOGRAPHIC SYSTEM

Elliptic curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA.

The principal attraction of ECC is that it offers equal security for a far smaller key size, thereby reducing processing overhead. To form a cryptographic system using elliptic curve, we need to find systems, that rely on the difficulty of a mathematical problem for their security. To explain the concept of difficult mathematical problem, notion of an algorithm is required. When looking for a mathematical problem on which to base a public key cryptographic system, cryptographers search for a problem for the fastest algorithm takes exponential time. The longer it takes to compute the best algorithm for a problem, the more secure a public key cryptosystem based on that problem will be.

There are three types of systems that are considered secure and efficient.

1. The Integer Factorization systems (RSA)
2. The Discrete logarithmic system (DSA) and
3. The elliptic curve system (EC Discrete logarithmic system)

In RSA, given an integer $n$, which is the product of two large primes $p$ and $q$ such that

$$n = pq.$$
It is easy to calculate $n$ given $p$ and $q$ but it is difficult to determine $p$ and $q$ given $n$ for large value of $n$.

Given an integer $k$ between 0 and $p – 1$ and $y$ which is the result of exponentiation of $k$, we have, $y = k^x \pmod{p}$ for some $x$.

The discrete logarithm problem modules $p$ is to determine $x$ given $k$ and $y$.

The elliptic curve cryptosystem, whose security rests on the discrete logarithmic problem over the points on the elliptic curve.

ECC takes full exponential time. RSA, DSA takes sub exponential time. These means that significantly smaller parameters can be used in ECC than more systems such as RSA and DSA but with equivalent levels of security.

6. ELLIPTIC CURVE DISCRETE LOGARITHMIC PROBLEM (ECDLP)

ECDLP is the inversion to scalar multiplication and it is defined as:

Let $k$ be a positive integer and $P$ be a point on Elliptic curve. The process of finding $k$, given points $Q$ and $P$, such that $Q = kP$ is called ECDLP.

**Example:** Consider an Elliptic Curve given by an equation $y^2 = x^3 + 9x + 17 \pmod{23}$.

Let $P = (4, 5)$ and $Q = (16, 5)$, ECDLP problem is to find an integer $k$ such that $kP = Q$.

The integer $k$ can be found by repeated point doubling till we get $Q$.

Since $P = (16, 5)$, $2P = (20, 20)$, $3P = (14, 14)$, $4P = (19, 20)$, $6P = (7, 3)$, $7P = (8, 7)$, $9P = (4, 5) = Q$.

Thus $9P = Q$ and hence $k = 9$.

The given example is the simple illustration but actually finding the value of $k$ for a very large prime modulo $p$ would be difficult.

6.1 The El Gamal Elliptic Curve key exchange Algorithm

Let $E$ be an elliptic curve and $p$ be a point on elliptic curve. Let $A$ (Allice) and $B$ (Bob) be two users of the system.

**Step 1:** Bob chooses integer $d$ and calculate $Q = dP$.

**Step 2:** Allice maps the plaintext $m$ to point $M$ on the curve.

**Step 3:** Allice chooses a random integer $k$. 
Step 4: Alice encrypts M as $c_1 = kP$ and $c_2 = M + kQ$.

Step 5: Bob decrypts by calculating $M = c_2 - dkP = M + kQ - dkP = M + kdP - dkP = M$.

A spy would know $c_1, c_2$ but not $k$. The spy may know $(E, P, Q)$, but finding $k$ from this is infeasible.

Example: Consider an elliptic curve $y^2 = x^3 + 2x + 3$ (mod 67),

Let $d = 4$ and $P = (2, 22)$ then $Q = dP = 4P = (13, 45)$.

Let $k = 2, M = (24, 26)$ then $c_1 = kP = 2(2, 22) = (35, 1)$ and $c_2 = M + kQ = (21, 24)$. $M = c_2 - c_1d = (21, 24) - 4(35, 1) = (24, 26)$.

7. CONCLUSION


Elliptic curves have been extensively studied for over a hundred years, and there is vast literature on the topic. Elliptic curves have recently become a tool in several important applied areas including coding theory and number theory algorithms for primality proving and for integer factorization.

In 1985, Koblitz and Miller independently proposed using the group of points on an elliptic curve defined over a finite field in discrete log cryptosystems. Elliptic curves also appear in RSA cryptosystem as proposed by Koyama et al.

Elliptic curve cryptography is based on deep mathematics involving elliptic curves in a finite field. It relies on the difficulty of solving the elliptic curve discrete logarithmic problems.

Successful attacks have been found only for a few special families of curves i.e., MOV attacks using the Weil – pairing on super singular elliptic curves and Index calculus attack on traditional mod P discrete log based cryptosystem.

Weil Descent has been proposed for embedding elliptic curves in higher dimensional abelian varieties where attacks are known, but has not yielded a good attack on elliptic curve in general.

Currently the best known attacks on elliptic curves discrete log system run in time proportional to the square root of the group size of the elliptic curves using Pollard rho, Pollard kangaroo or Baby step Giant step algorithms.
REFERENCES


M. T. Wankhede-Barsagade
Assistant Professor and Head,
Department of Mathematics,
B.N. Bandodkar college of Science,
Thane, Maharashtra, India.
E-mail: minaltbw@gmail.com

Suchitra A. Meshram
Associate Professor,
Department of Mathematics,
R.T.M. Nagpur University,
Nagpur, Maharashtra, India.