Applied Mathematics, 2016, 7, 304-312
Published Online February 2016 in SciRes. http://www.scirp.org/journal/am
http://dx.doi.org/10.4236/am.2016.73027

Cryptographic Schemes Based on Elliptic Curves over the Ring $Z_p[i]$

Manoj Kumar, Pratik Gupta

Department of Mathematics and Statistics, Gurukula Kangri Vishwavidyalaya, Haridwar (Uttrakhand), India
Email: sdmkg1@gmail.com, pratikgupta1810@gmail.com

Received 9 January 2016; accepted 26 February 2016; published 29 February 2016

Abstract

Elliptic Curve Cryptography recently gained a lot of attention in industry. The principal attraction of ECC compared to RSA is that it offers equal security for a smaller key size. The present paper includes the study of two elliptic curve $E_{a,b}$ and $E_{a,-b}$ defined over the ring $Z_p[i]$ where $i^2=-1$. After showing isomorphism between $E_{a,b}$ and $E_{a,-b}$, we define a composition operation (in the form of a mapping) on their union set. Then we have discussed our proposed cryptographic schemes based on the elliptic curve $E=E_{a,b}\cup E_{a,-b}$. We also illustrate the coding of points over *E*, secret key exchange and encryption/decryption methods based on above said elliptic curve. Since our proposed schemes are based on elliptic curve of the particular type, therefore the proposed schemes provides a highest strength-per-bit of any cryptosystem known today with smaller key size resulting in faster computations, lower power assumption and memory. Another advantage is that authentication protocols based on ECC are secure enough even if a small key size is used.

Keywords

Elliptic Curve, Ring, Finite Field, Isomorphism, Cardinality, Encryption/Decryption

1. Introduction

Elliptic curve cryptography has been an active area of research since 1985 when Koblitz (Ref. [1]) and Miller (Ref. [2]) independently suggested using elliptic curves for public-key cryptography. A lot of work has been done on elliptic curve cryptography (Ref. [3]-[7]). Because elliptic curve cryptography offers the same level of security as compared to RSA with considerably shorter keys, it has replaced traditional public key cryptosystems, especially, in environments where short keys are important. Public-key cryptosystems are computationally demanding and, hence, the fact that elliptic curve cryptography has been shown to be faster than traditional pub-

How to cite this paper: Kumar, M. and Gupta, P. (2016) Cryptographic Schemes Based on Elliptic Curves over the Ring $Z_P[i]$. *Applied Mathematics*, **7**, 304-312. http://dx.doi.org/10.4236/am.2016.73027

lic-key cryptosystems is of great importance. Elliptic Curve Cryptographic (ECC) schemes are public-key mechanisms that provide the same functionality as RSA schemes. However, their security is based on the hardness of a different problem, namely the Elliptic Curve Discrete Logarithmic Problem (ECDLP). Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA schemes. The competing system to RSA is an elliptic curve cryptography. The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size.

2. Auxiliary Result

In this section first we discuss some essential arithmetic of elliptic curves, and then we mention some auxiliary results which are necessary to prove the main result. Although a lot of literature exist on arithmetic of elliptic curves (Ref. [8]-[11]), a simple and easier arithmetic of elliptic curves are given by the following (Ref. [10]):

An elliptic curve $E(F_p)$ over a finite field F_p is defined by the parameters $a,b \in F_p$ (*a* and *b* satisfy the relation $4a^3 + 27b^2 \neq 0$), consists of the set of points $(x,y) \in F_p$, satisfying the equation $y^2 = x^3 + ax + b$. The set of points on $E(F_p)$ also include point *O*, which is the point at infinity and which is the identity element under addition. Actually elliptic curve are not ellipse. They are so called because they are described by cubic equation similar to those are used for calculating the circumference of an ellipse.

The Addition operation is defined over $E(F_p)$ and it can be seen that $E(F_p)$ forms an abelian group under addition.

- $P + O = O + P,\ \forall P \in E(F_p)$.
- If $P = (x,y) \in E(F_p)$, then $(x,y) + (x,-y) = O$. (The point $(x,-y) \in E(F_p)$ and is called the negative of *P* and is denoted $-P$).
- If $P = (x_1,y_1) \in E(F_p)$ and $Q = (x_2,y_2) \in E(F_p)$ and $P \neq Q$, then $R = P + Q = (x_3,y_3) \in E(F_p)$, where $x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1$, and $\lambda = (y_2 - y_1)/(x_2 - x_1)$.
- Let $P = (x,y) \in E(F_p)$. Then the point $Q = P + P = 2P = (x_1,y_1) \in E(F_p)$,

where $x_1 = \lambda^2 - 2x, y_1 = \lambda(x - x_1) - y$, and $\lambda = (3x^2 + a)/2y$.

Now we discuss the auxiliary result of this section. For a prime number *p*, let $Z_p[i] = \{a + bi : a,b \in Z_p\}$ where $i^2 = -1$, be a ring having p^2 elements. Then we have the following assertion:

Lemma 2.1. (Ref. [12]) An element $a + ib$ is invertible in $Z_p[i]$ if only if $a^2 + b^2 \neq 0(\text{mod } p)$.

Proof. Let $a + ib$ be invertible then there exists an element $c + id$ in $Z_p[i]$ such that

$$(a+ib)(c+id) = 1 \tag{1}$$

which implies $(ac - bd) + i(bc + ad) = 1$ *i.e.* $ac - bd = 1$ and $bc + ad = 0$.

In (1) take the conjugate

$$(a-ib)(c-id) = 1 \tag{2}$$

Multiply (1) and (2), we get

$$(a+ib)(a-ib)(c+id)(c-id) = 1$$

We deduce

$$(a^2 + b^2)(c^2 + d^2) = 1, \text{ so } a^2 + b^2 \neq 0(\text{mod } p).$$

Lemma 2.2. (Ref. [13] [14]) Let *p* be a prime number. Then $Z_p[i]$ is field iff $p \equiv 3(\text{mod } 4)$.

Proof. Assume that $Z_p[i]$ is not field if $p \equiv 3(\text{mod } 4)$ then $\exists$ an element $a + bi \in Z_p[i]$, which is not invertible. By Lemma 2.1, we have $a^2 + b^2 = 0(\text{mod } p)$. So $a^2 + b^2 = k$, where $k \in Z$. We can write $a = ta_1$, $b = tb_1$ with $g.c.d(a_1,b_1) = 1$. Suppose *a* is not divisible by *p* then *p* does not divide *t* but *p* divides $a_1^2 + b_1^2$. Using proposition 1.2 [3], we obtain $a_1^2 + b_1^2 = kp$. We have $p \neq 3(\text{mod } 4)$. Supposing $p = 2$, we can write $1^2 + 1^2 = 0(\text{mod } 2)$ then $1 + i$ is not invertible. Assume $p = 1$, then $\exists$ an element $c \in Z_p[i]$ such that $c^{\frac{p-1}{2}} \neq 1$ because $c^{p-1} = 1$ this implies that $c^{\frac{p-1}{2}} = -1$ and hence $(c^k)^2 = c^{2k} = -1$. So $1^2 + (c^k)^2 = 1 - 1 = 0$. We deduce that $c^k + i$ is not invertible. This completes the proof of the result.

Theorem 2.3. For two isomorphic abelian groups $(G_1,*)$ and $(G_2,\circ)$ with the same unit element *e*, let $E=G_1\cup G_2$ and also let $\oplus: E\times E\to E$ be a mapping defined by

$$(x,y)\to x\oplus y$$

such that

$$x\oplus y=\begin{cases} x*y & \text{if } x,y\in G_1 \\ x\circ y & \text{if } x,y\in G_2 \\ f(x)\circ y & \text{if } x\in G_1, y\notin G_1 \\ x\circ f(y) & \text{if } x\notin G_1, y\in G_1 \end{cases}$$

where *f* is the isomorphism between G_1 and G_2. Then $\oplus$ is an internal composition law, commutative with identity element *e* and all elements in E are invertible.

Proof. It is clear that $\oplus$ is an internal composition law over *E*.

To show that *e* is the identity element with respect to binary operation $\oplus$.

Let *x* in *E*. If $x\in G_1$ then

$$x\oplus e=x*e=e*x=e\oplus x=x,$$

because $x\in G_1$ and *e* is the unit element of $(G_1,*)$.

Else $x\in G_2$, then

$$x\oplus e=x\circ e=e\circ x=e\oplus x=x,$$

because $x\in G_2, f(e)=e$ and *e* is unit element of $(G_2,\circ)$.

$\oplus$ **is commutative**

We have $(G_1,*)$ and $(G_2,\circ)$ two abelian groups with the same unit element *e*.

Let $x,y\in E$. If $x,y\in G_1$ then

$$x\oplus y=x*y=y*x=y\oplus x$$

If $x,y\in G_2$ then

$$x\oplus y=x\circ y=y\circ x=y\oplus x$$

If $x\in G_1, y\notin G_2$ then

$$x\oplus y=f(x)\circ y=y\circ f(x)=y\oplus x$$

If $x\notin G_1, y\in G_2$ then

$$x\oplus y=x\circ f(y)=f(y)\circ x=y\oplus x.$$

3. Elliptic Curve over the Field $Z_p[i]$

Let $E_{a,b}, E_{a,-b}$ be two elliptic curve over the field $Z_p[i]$, where *p* is a prime number such that $p\equiv 3(\bmod 4)$, defined by

$$E_{a,b}=\{(x,y): y^2=x^3+ax+b\}\cup\{O\} \text{ and } E_{a,-b}=\{(x,y): y^2=x^3+ax-b\}\cup\{O\}$$

where *O* is the point at infinity.

Corollary 3.1. If $b\neq 0$ then $E_{a,b}\cap E_{a,-b}=\{O\}$.

Proof. Let $(x,y)\in E_{a,b}\cap E_{a,-b}$, then

$$y^2=x^3+ax+b \text{ and } y^2=x^3+ax-b$$

This implies that

$$b=-b \quad i.e. \quad b=0$$

which is a contradiction.

Hence

$$E_{a,b}\cap E_{a,-b}=\{O\}.$$

4. Main Result

Theorem 4.1. Let *f* be a mapping from $E_{a,b}$ to $E_{a,-b}$ defined by

$$f(x,y)=(-x,iy) \text{ and } f(O)=O$$

Then *f* is a bijection.

Proof. First we show that *f* is well defined.

Let $(x,y)\in E_{a,b}$ then $y^2=x^3+ax+b$, then $-y^2=-x^3-ax-b$ *i.e.* $(iy)^2=(-x)^3+a(-x)-b$ therefore $(-x,iy)\in E_{a,-b}$

Hence *f* is well defined.

f **is one-one.** Let $(x_1,y_1),(x_2,y_2)\in E_{a,b}$ such that

$$f(x_1,y_1)=f(x_2,y_2)$$

$$(-x_1,iy_1)=(-x_2,iy_2)$$

This implies that $x_1=x_2$ and $iy_1=iy_2$ *i.e.* $x_1=x_2$ and $y_1=y_2$

So, $(x_1,y_1)=(x_2,y_2)$

Hence, *f* is one-one.

f **is onto.** Let $(x,y)\in E_{a,-b}$. Then $y^2=x^3+ax-b$ or $-y^2=-x^3-ax+b$

This implies that $(-x,iy)\in E_{a,b}$ because $(iy)^2=(-x)^3+a(-x)+b$ and $f(-x,iy)=(x,y)$

Thus, *f* is onto.

f **is homomorphism.** Let $(x_1,y_1),(x_2,y_2)\in E_{a,b}$ there is three cases arise:

Case I. When $x_1\neq x_2$

As we know that addition of two different points (x_1,y_1) and (x_2,y_2) on elliptic curve is given by

$$(x_1,y_1)+(x_2,y_2)=\left(\lambda_{a,b}^2-x_1-x_2,\lambda_{a,b}(x_2-x_3)-y_2\right)$$

where $\lambda_{a,b}=\dfrac{y_2-y_1}{x_2-x_1}$ and $x_3=\lambda_{a,b}^2-x_1-x_2$

So we have

$$f\left((x_1,y_1)+(x_2,y_2)\right)=f\left(\lambda_{a,b}^2-x_1-x_2,\lambda_{a,b}(x_2-x_3)-y_2\right)$$
$$=\left(-\lambda_{a,b}^2+x_1+x_2,i\lambda_{a,b}(x_2-x_3)-iy_2\right)$$

where $\lambda_{a,b}=\dfrac{y_2-y_1}{x_2-x_1}$ and $x_3=\lambda_{a,b}^2-x_1-x_2$

Again

$$f\left((x_1,y_1)\right)+f\left((x_2,y_2)\right)=(-x_1,iy_1)+(-x_2,iy_2)$$
$$=\left(\lambda_{a,-b}^2+x_1+x_2,\lambda_{a,-b}(-x_2-x_4)-iy_2\right)$$

where $\lambda_{a,-b}=\dfrac{iy_2-iy_1}{-x_2+x_1}$ and $x_4=\lambda_{a,-b}^2+x_1+x_2$.

It is obvious that $\lambda_{a,-b}=\dfrac{i(y_2-y_1)}{-(x_2-x_1)}=-i\lambda_{a,b}$ this implies that $\lambda_{a,b}^2=-\lambda_{a,-b}^2$ and $x_3=-x_4$.

Therefore

$$f\left((x_1,y_1)+(x_2,y_2)\right)=f\left((x_1,y_1)\right)+f\left((x_2,y_2)\right).$$

Case II. When $x_1=x_2$ and $y_1=y_2$

$$f\left((x_1,y_1)+(x_2,y_2)\right)=f\left(\lambda_{a,b}^2-2x_1,\lambda_{a,b}(x_1-x_3)-y_1\right)$$
$$=\left(-\lambda_{a,b}^2+2x_1,i\lambda_{a,b}(x_1-x_3)-iy_1\right)$$

where $\lambda_{a,-b}=\frac{3x_1^2}{2y_1}$ and $x_3=\lambda_{a,b}^2-2x_1$.

Again

$$f\left(\left(x_1,y_1\right)+\left(x_2,y_2\right)\right)=\left(-x_1,iy_1\right)+\left(-x_2,iy_2\right)$$
$$=\left(\lambda_{a,-b}^2+2x_1,\lambda_{a,-b}\left(-x_1-x_4\right)-iy_1\right)$$

where $\lambda_{a,-b}=\frac{3\left(-x_1\right)^2}{2y_1}$ and $x_4=\lambda_{a,-b}^2+x_1+x_2$.

It is evident that $\lambda_{a,-b}=-i\frac{3x_1^2}{2y_1}=-i\lambda_{a,b}$ then, $\lambda_{a,b}^2=-\lambda_{a,-b}^2$ and $x_3=-x_4$.

Therefore,

$$f\left(\left(x_1,y_1\right)+\left(x_2,y_2\right)\right)=f\left(\left(x_1,y_1\right)\right)+f\left(\left(x_2,y_2\right)\right)$$

Case III. When $x_1=x_2$ and $y_1=-y_2$

We have

$$f\left(\left(x_1,y_1\right)+\left(x_2,y_2\right)\right)=f\left(\left(x_1,y_1\right)+\left(x_1,-y_1\right)\right)=f\left(O\right)=O$$

and

$$f\left(\left(x_1,y_1\right)\right)+f\left(\left(x_2,y_2\right)\right)=\left(-x_1,iy_1\right)+\left(-x_2,iy_2\right)=\left(-x_1,iy_1\right)+\left(-x_1,-iy_1\right)=O$$

Thus

$$f\left(\left(x_1,y_1\right)\right)+f\left(\left(x_2,y_2\right)\right)=f\left(\left(x_1,y_1\right)+\left(x_2,y_2\right)\right)$$

Therefore, in either case *f* is an homomorphism. Hence *f* is a bijection.

Corollary 4.2. For two isomorphic abelian groups $E_{a,b}$ and $E_{a,-b}$ with the same unit element *O*, let $E=E_{a,b}\cup E_{a,-b}$ and also let $\oplus:E\times E\to E$ be a mapping defined by

$$\left(P,Q\right)\to P\oplus Q$$

such that

$$P\oplus Q=\begin{cases}P+Q & \text{if } P,Q\in E_{a,b}\\ P+Q & \text{if } P,Q\in E_{a,-b}\\ f\left(P\right)+Q & \text{if } P\in E_{a,b},Q\notin E_{a,b}\\ P+f\left(Q\right) & \text{if } P\notin E_{a,b},Q\in E_{a,b}\end{cases}$$

where *f* is the isomorphism between $E_{a,b}$ and $E_{a,-b}$. Then $\oplus$ is an internal composition law, commutative with identity element *O* and all elements in E are invertible.

Proof. Keeping in view the result of theorem-2.3, corollary-2.4, and theorem-3.1, it is evident that $\oplus$ is an internal composition law, commutative with identity element *O* and all elements in *E* are invertible.

Corollary 4.3. If $E_{a,b}$ and $E_{a,-b}$ are isomorphic groups *i.e.* they are both abstractly identical of groups then $Card\left(E\right)=2Card\left(E_{a,b}\right)-1$.

Proof. Since $E_{a,b}$ is isomorphic to $E_{a,-b}$ this implies $Card\left(E_{a,b}\right)=Card\left(E_{a,-b}\right)$

Now,

$$E=E_{a,b}\cup E_{a,-b}$$

This implies that

$$Card\left(E\right)=Card\left(E_{a,b}\right)+Card\left(E_{a,-b}\right)-Card\left(E_{a,b}\cap E_{a,-b}\right)$$

Therefore,

$$Card(E) = 2Card(E_{a,b}) - 1.$$

5. Cryptographic Applications

In this section we shall illustrate our proposed methods for coding of points on Elliptic Curve, then exchange of secret key and finally use them for encryption/decryption.

5.1. Coding of Element on Elliptic Curve

It is described with the help of illustration 5.1 and illustration 5.2.

Illustration 5.1. For $p = 3, a = 1$ and $b = 1$, Then codes of elements of $E = E_{a,b} \cup E_{a,-b}$ are given by

$$E = \{00100, 00101, 00201, 10001, 10101, 10201, 20001, 01101, 01201, 11001,$$
$$11101, 11201, 21001, 02101, 02201, 12001, 12101, 12201, 22001\}$$

Since, $E_{1,1} = \{(x,y) : y^2 = x^3 + x + 1\} \cup \{O\}$ and $E_{1,-1} = \{(x,y) : y^2 = x^3 + x - 1\} \cup \{O\}$

Therefore

$$E_{1,1} = \{(0,1),(0,2),(1,0),(i,1),(i,2),(1+i,0),(2i,1),(2i,2),(1+2i,0)\} \cup \{O\}.$$

and

$$E_{1,-1} = \{(1,1),(1,2),(2,0),(1+i,1),(1+i,2),(2+i,0),(1+2i,1),(1+2i,2),(2+i,0)\} \cup \{O\}.$$

Coding of element $E = E_{1,1} \cup E_{1,-1}$ are described as follow

Let $P = [x_0 + x_1 i; y_0 + y_1 i; z]$, where $x_j, y_j \in Z_3$ for j = 0 or 1 and z = 0 or 1. Then coding method is given by $x_0 x_1 y_0 y_1 z$ which produces the following codes

$$E = \{00100, 00101, 00201, 10001, 10101, 10201, 20001, 01101, 01201, 11001,$$
$$11101, 11201, 21001, 02101, 02201, 12001, 12101, 12201, 22001\}$$

Illustration 5.2. For $p = 7, a = 2 + 3i$ and $b = 1 + i$. The coding of points of $E_{a,b} \cup E_{a,-b}$ can be described as

$$E_{2+3i,1+i} = \{(x,y) : y^2 = x^3 + (2+3i)x + 1 + i\} \cup \{O\}$$
$$E_{2+3i,-(1+i)} = \{(x,y) : y^2 = x^3 + (2+3i)x - (1+i)\} \cup \{O\}$$

Let $P = [x_0 + x_1 i; y_0 + y_1 i; z]$, where $x_j, y_j \in Z_7$ for j = 0 or 1 and z = 0 or 1. Then coding method is given by $x_0 x_1 y_0 y_1 z$ which produces the following codes

$$E = \{00100, 00131, 00361, 00411, 00641, 01021, 01051, 01351, 01421, 02111, 02661, 03141, 03631,$$
$$04311, 04461, 05161, 05161, 05611, 06201, 06231, 06501, 06541, 10121, 10241, 10531, 10651,$$
$$12251, 12521, 14031, 14041, 14111, 14661, 15021, 15051, 15351, 15421, 16201, 16231, 16501,$$
$$16541, 20011, 20061, 23141, 23631, 25251, 25521, 26311, 26461, 31141, 311631, 33001, 33321,$$
$$33451, 35301, 35401, 36341, 36431, 41331, 41441, 42031, 42041, 44001, 44241, 44531, 46311,$$
$$46461, 50101, 50601, 51141, 51631, 52221, 52551, 54311, 54461, 60261, 60321, 60451, 60511,$$
$$61021, 61051, 61351, 61421, 62201, 62231, 62501, 62541, 63161, 63301, 63401, 63611, 65221, 65551\}$$

The above scheme helps us to encrypt and decrypt any message of any length.

5.2. Exchange of Secret Key

1) For a publically integer *p*, and an elliptic curve $E(Z_p[i])$ let $P \in E(Z_p[i])$ of order *n*.

2) *P* generates a subgroup say $G = \langle P \rangle$ which is used to encrypt the message *m*.

Now, key exchange between Alice and Bob can be described as follows

3) Alice chooses a random number $0 \le N_A \le n-1$, computes $K = N_A P$ and sends it to Bob.

4) Bob chooses a random number $0 \le N_B \le n-1$, computes $K' = N_B P$ and sends it to Alice.

5) Alice computes $N_A K' = N_A \cdot N_B P$.

6) Bob computes $N_B \cdot K = N_B \cdot N_A P$.

7) Alice and Bob are agree with a point $S = N_A \cdot N_B P$,choose the binary code of point *S* as a private key, which transformed on the decimal code $\langle\langle S' \rangle\rangle$.

Remark. With the secret key S' such as the decimal code of point *S* Alice and Bob can encrypt and decrypt the message (*m*).

Illustration 5.3. Let $E_{3,45} = \{(x,y): y^2 = x^3 + 3x + 45\} \cup \{O\}$ and $E_{3,-45} = \{(x,y): y^2 = x^3 + 3x - 45\} \cup \{O\}$ are two elliptic curve defined over the same field $Z_{8831}[i]$ having 8831^2 element, where 8831 be a prime number such that $8831 \equiv 3(\mathrm{mod}\, 4)$ and a point $P = (4,11) \in Z_{8831}[i]$ of order 4427.

1) Alice chooses a random number $N_A = 12$, compute $K = 12(4,11) = (814,5822)$ and sends it to Bob.

2) Bob chooses a random number $N_B = 23$ and compute $K' = 23(4,11) = (3069,3265)$ and sends to it Alice.

3) Alice computes $N_A K' = 12 \cdot (3069,3265) = (3076,265)$.

4) Bob computes $N_B \cdot K = 23 \cdot (814,5822) = (3076,265)$.

5) Alice and Bob are agree with a point $S = (3076,265)$, choose the binary code of point *S* as a private key, which transformed on the decimal code $\langle\langle 30760000265000001 \rangle\rangle$.

5.3. ECC Key Generation Phase

Now, exchange of secret key involves the following steps:

1) Encode the message *m* on the point P_m.

2) Choose a random number *k*, compute $Q = k \cdot P_m$ and calculate $P_b = S' \cdot Q$.

3) Public key is (a,b,p,P,P_b,Q).

4) Private key is (N_A, N_B, k, S').

5.4. ECC Encryption Phase

To encrypt P_m, a user choose an integer $\langle\langle r \rangle\rangle$ at random and sends the point $(r \cdot Q, P_m + r \cdot P_b)$. This operation is shown in **Figure 1**.

5.5. ECC Decryption Phase

Decryption of the message (m) is done by multiplying the first component $(r \cdot Q)$ of the received point $(r \cdot Q, P_m + r \cdot P_b)$ and the secret key $\langle\langle S' \rangle\rangle$, and the result is subtracted from the second component $(P_m + r \cdot P_b)$ *i.e.*:

$$(P_m + r \cdot P_b) - S' \cdot (r \cdot Q) = P_m + r \cdot S' \cdot Q - S' \cdot r \cdot Q = P_m$$

This operation is shown in **Figure 2**.

Illustration 5.4. The

$$E_{3,45} = \{(x,y): y^2 = x^3 + 3x + 45\} \cup \{O\}$$

and

$$E_{3,-45} = \{(x,y): y^2 = x^3 + 3x - 45\} \cup \{O\}$$

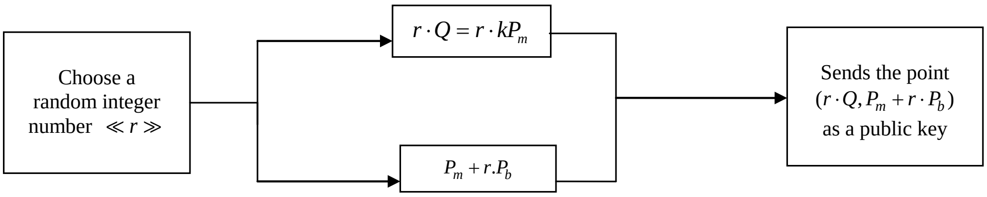
Choose a random integer number $\ll r \gg$
$r \cdot Q = r \cdot kP_m$
$P_m + r.P_b$
Sends the point $(r \cdot Q, P_m + r \cdot P_b)$ as a public key

Figure 1. The encryption operation.

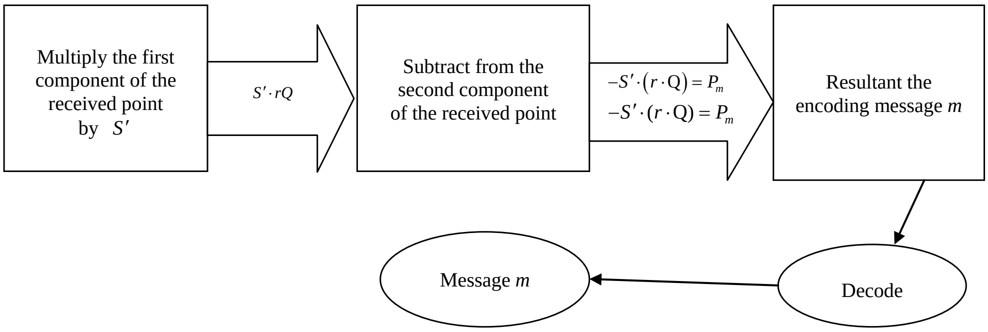
Multiply the first component of the received point by S'
$S'\cdot rQ$
Subtract from the second component of the received point
$-S'\cdot(r\cdot Q)=P_m$
$-S'\cdot(r\cdot Q)=P_m$
Resultant the encoding message m
Decode
Message m

Figure 2. The decryption operation.

are two elliptic curves defined over the same field $Z_{8831}[i]$ having 8831^2 element where 8831 be a prime number such that $8831\equiv 3(\mathrm{mod}\,4)$ and a point $P=(4,11)\in Z_{8831}[i]$ of order 4427.

Alice's message is the point $P_m=(5,1743)$.

Bob has chosen his secret random number $k=3$ and computed

$$Q=k\cdot P_m=3\cdot(5,1743)=(445,3115)$$

and calculated

$$P_b=S'\cdot Q=30760000265000001(445,3115)=(7093,2868)$$

Bob publishes the point. Alice chooses the random number $r=8$ and computes

$$r\cdot Q=8\cdot(445,3115)=(7966,6354)$$

and

$$P_m+r\cdot P_b=(5,1743)+8\cdot(7093,2868)=(5011,2629)$$

Alice sends (7966,6354) and (5011,2629) to Bob, who multiplies the first of these point by

$$S'\cdot(r\cdot Q)=30650000265000001\cdot(7966,6354)=(6317,6201).$$

Bob then subtracts the result from the last point that Alice sends him. Note that he subtracts by adding the point with the second coordinate negated:

$$P_m+r\cdot P_b-S'\cdot(r\cdot Q)=(5011,2629)-(6317,6201)=(5,1743)=P_m$$

Bob has therefore received Alice's message.

Acknowledgements

This research work is supported by University Grant commission (UGC) New Delhi, India under the Junior Research Fellowship student scheme..

References

[1] Koblitz, A.H., Koblitz, N. and Menezes, A. (2011) Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift. *Journal of Number Theory*, **131**, 781-814. http://dx.doi.org/10.1016/j.jnt.2009.01.006

[2] Miller, V. (1985) Use of Elliptic Curves in Cryptography. *Advances in Cryptology-CRYPTO*, **85**, 417-426.

[3] Chillali, A. (2011) Elliptic Curve over Ring. *International Mathematical Forum*, **6**, 1501-1505.

[4] Koblitz, N. (1987) Elliptic Curve Cryptosystem. *Journal of Mathematics Computation*, **48**, 203-209. http://dx.doi.org/10.1090/S0025-5718-1987-0866109-5

[5] Kumar, S., Suneetha, C. and Chandrasekh, A. (2012) Encryption of Data Using Elliptic Curve over Finite Fields. *International Journal of Distributed and Parallel Systems* (*IJDPS*), **3**, No. 1.

[6] Schoof, R. (1985) Elliptic Curves over Finite Fields and the Computation of Square Roots Mod p. *Mathematics of Computation*, **44**, 483-494.

[7] Srivastava, K. and Nand, G. (2015) Elliptic Curves for Data Provenance. *Procedia Computer Science*, **45**, 470-476. http://dx.doi.org/10.1016/j.procs.2015.03.082

[8] Hankerson, D., Menezes, J.A. and Vanstone, S. (2004) Guide to Elliptic Curve Cryptography. Springer-Verlag, Germany.

[9] Silverman, J. (1986) The Arithmetic of Elliptic Curves. Springer, New York. http://dx.doi.org/10.1007/978-1-4757-1920-8

[10] Stinson, D.R. (2006) Cryptography Theory and Practice. Chapman and Hall/CRC, United Kingdom.

[11] Washington, L.C. (2008) Elliptic Curves Number Theory and Cryptography. Chapman and Hall/CRC, United Kingdom. http://dx.doi.org/10.1201/9781420071474

[12] Gilbert, W.J. (2004) Modern Algebra with Application. Willey-Interscience, New York.

[13] Hardy, G.H. and Wright, E.M. (1938) An Introduction to the Theory of Numbers. Oxford University Press, United Kingdom.

[14] Gallian, J.A. (1998) Contemporary Abstract Algebra. Narosa Publishing House, New Delhi.