Integer Points on Elliptic Curve

Weiping Zhou
School of Mathematics and Computational Science, Anqing Normal University, Anqing 246133, Anhui, China

Abstract
Elliptic curve is an important problem in integer factorization and cryptography. Using the elementary number theory, it proves that the non-negative integer points of the elliptic curve $x^2 - 12qy^2 = 1$ have the structure of $\left(6qa^2 + 1, a\sqrt{3qa^2 + 1}\right)$ where $a$ is a non-negative integer such that $3qa^2 + 1$ is square, when $q = 12s^2 + 5$ is prime where $s$ is a non-negative integer. This result gives the method of solving the above elliptic curve. And it proves that the elliptic curve $y^2 = x^3 + (p - 4)x - 2p$ has up to two groups of positive integer points besides $(x, y) = (2, 0)$, where $12s^2 + 5, 6s^2 + 1$ and $p = 36s^2 + 7$ are primes, and $s$ is a non-negative odd integer. The two groups of positive integer points can be taken as the key of password if they are exist, and this result can avoid the invalid algorithm of integer factorization using elliptic curves.

Key words: Elliptic Curve, Diophantine Equation, Integer Points, Key of Password, Integer Factorization

1. INTRODUCTION
The prime test and the integer factorization algorithm based on the elliptic curve are the hot issue at present. The researching of elliptic curve’s integer points have become an interesting subject in integer factorization and cryptography.

In 1987, Zagier provided whether there is one non-negative integer point on the elliptic curve (Zagier, 1987)

$$y^2 = x^3 + 27x - 62$$ (1)

For elliptic curve (1), Zhu and Chen proved there are only two non-negative integer points $(x, y) = (2, 0)$ and $(x, y) = (28844402, \pm 154914585540)$ using algebraic number theory and $p$-adic analysis (Zhu and Chen, 2009). Guan proved the elliptic curve (Guang, 2014)

$$y^2 = x^3 + (p - 4)x - 2p$$ (2)

has integer points $(x, y) = (2, 0)$ and $(x, y) = (28844402, \pm 154914585540)$ when $p = 31$, and there is only one integer point $(x, y) = (2, 0)$ when $p \neq 31$, where $p = 36s^2 - 5$ is prime and $s$ is a non-negative integer such that $12s^2 + 1, 6s^2 - 1$ are primes. And the related conclusions are as follows.

Lemma 1 If $D$ is not square integer, then the equation (Pan and Pan, 1992)

$$x^2 - Dy^2 = 1$$ (3)

has infinite many positive integer solution. Let $(x_0, y_0)$ denote the basic solution of (5), then the all integer solutions $(x_n, y_n)$ can be written as follows

$$x_n + y_n\sqrt{D} = (x_0 + y_0\sqrt{D})^n, n \in \mathbb{Z}^+$$

Lemma 2 If $D$ is not square integer, then the equation (Walsh, 1999)

$$x^2 - Dy^2 = 1$$ (4)

has two sets of non-negative integer solutions at most, and which has just two sets of non-negative integer points if and only if $D = -1785$ or $D = 28650$ or $2x_0$, $y_0$ are square where $(x_0, y_0)$ is (5)’s basic solution.

Lemma 3 If the non-negative integer solution $(x_n, y_n)$ of (5) satisfy $x_n > \frac{1}{2} y_n^2 - 1$, then $(x_n, y_n)$ is the basic solution of (5) (Luo and Yuan, 2001).

Lemma 4 If the equation (6) just has one non-negative integer solution $(x, y)$ (Wu, 2010), then
where \((x_0, y_0)\) is the basic solution of equation (5), and \(k \in \mathbb{Z}^+\), \(k = 2 \text{ or } 2 \mid k\).

First, this paper proves the non-negative integer solutions of the elliptic curve

\[ x^2 - 12qy^2 = 1 \]  

are \((6qa^2 + 1, a\sqrt{3qa^2 + 1})\), where \(q = 12s^2 + 5\) is prime, \(s\) and \(a\) are non-negative integers, \(3qa^2 + 1\) is square. This conclusion gives the method of solving the elliptic curve (3).

Second, it proves when \(p = 36s^2 + 7, q = 12s^2 + 5, r = 6s^2 + 1\) are prime and \(s\) is odd, the elliptic curve

\[ y^2 = x^2 + (p - 4)x - 2p \]  

has up to two groups of positive integer solutions if it has other solutions besides \((x, y) = (2, 0)\), and its structure is presented. Using this result, the integer point of the elliptic curve (4) can be taken as the key of password. And this result can avoid the invalid algorithm of integer factorization using elliptic curves.

2. INTEGER POINTS ON TWO CLASSES OF ELLIPTIC CURVE

2.1. Integer points on Binary Quadratic Elliptic Curve

**Theorem 1** Let \(s\) be an integer such that \(q = 12s^2 + 5\) is prime, then the non-negative integer solutions of the elliptic curve

\[ x^2 - 12qy^2 = 1 \]  

have the structure of \((6qa^2 + 1, a\sqrt{3qa^2 + 1})\), where \(a\) is a non-negative integer such that \(3qa^2 + 1\) is square.

**Proof:** (7) is equivalent to

\[ x^2 - 1 = (x - 1)(x + 1) = 12qy^2, \quad q = 12s^2 + 5 \text{ prime} \]  

It is obviously that \((\pm 1, 0)\) are (8)'s solutions. Let \((x, y)\) be a (8)'s solution, because \(\gcd(x + 1, x - 1) = 2\), we consider (8) in four cases.

**Case 1**

\[
\begin{cases}
  x + 1 = 2qa^2, \\
  x - 1 = 6b^2, \\
  y = \pm ab, \\
  \gcd(qa, b) = 1
\end{cases}
\]  

Then \(2 = 2qa^2 - 6b^2\).

If \(y\) is odd, then \(y^2 \equiv 1 \text{ or } 9 \text{ mod } 12\), \(a, b\) are odd, and \(2 = 2qa^2 - 6b^2 \equiv 4 \text{ or } 0 \text{ mod } 12\), which is contradictory.

If \(y\) is even, then \(y^2 \equiv 0 \text{ or } 4 \text{ mod } 12\), one of \(a, b\) is odd and the other is even. Because \(q = 12s^2 + 5\), so \(2 = 2qa^2 - 6b^2 \equiv 6, 0 \text{ or } 10 \text{ mod } 12\), which is contradictory.

So (9) has no solution.

**Case 2**

\[
\begin{cases}
  x + 1 = 6qa^2, \\
  x - 1 = 2b^2, \\
  y = \pm ab, \\
  \gcd(qa, b) = 1
\end{cases}
\]  

Then \(2 = 6q - 2y^2\).

If \(y\) is odd, then \(a, b\) are odd, and \(2 = 6qa^2 - 2b^2 \equiv 4 \text{ or } 0 \text{ mod } 12\), it is contradictory.

If \(y\) is even, then one of \(a, b\) is odd and the other is even, and \(2 = 6qa^2 - 2b^2 \equiv 6 \text{ or } 2 \text{ mod } 12\), which is contradictory.

So (10) has no solution.

**Case 3**

\[
\begin{cases}
  x + 1 = 6b^2, \\
  x - 1 = 2qa^2, \\
  y = \pm ab, \\
  \gcd(2qa^2, 6b^2) = 2
\end{cases}
\]  

Then \(2 = 6b^2 - 2qa^2\).
If $y$ is odd, then $2 = 6b^2 - 2qa^2 = -4or0 \mod 12$, which is a contradictory.
If $y$ is even, then one of $a, b$ is odd and the other is even. If $a$ is odd and $b$ is even, then
$$2 = 6b^2 - 2qa^2 = 2a^2 \mod 12$$
we have $1 = a^2 \mod 12$, so $3b^2 = 1 + qa^2 = 6 \mod 12$, but $3b^2 = 0 \mod 12$, which is a contradiction. If $b$ is odd and $a$ is even, then $3 = 3b^2 = 1 + qa^2 = 1or0 \mod 12$, which is contradictory.

So (11) has no solution

Case 4

$$\begin{align*}
x + 1 &= 2b^2 \\
x - 1 &= 6qa^2,
\end{align*}$$

(12)

Then $2 = 2b^2 - 6qa^2$.

If $y$ is odd, then $a, b$ are odd, and $2 = 2b^2 - 6qa^2 = -4or0 \mod 12$, which is contradictory.
If $y$ is even, then one of $a, b$ is odd and the other is even, and $b^2 = 1 + 3qa^2 = 1or4 \mod 12$, so $b^2 = 3qa^2 + 1$. $x = b^2 + 3qa^2 = 6qa^2 + 1$.

So equation (7) has non-negative integer solutions with structure $(6qa^2 + 1, \sqrt{3qa^2 + 1})$, where $a$ is any non-negative integer such that $3qa^2 + 1$ is square.

2.2. Integer Points on Binary Cubic Elliptic Curve

**Theorem 2** Let $s$ be an odd number such that $p = 36s^2 + 7, q = 12s^2 + 5$ and $r = 6s^2 + 1$ are prime. If the elliptic curve

$$y^2 = x^3 + (p - 4)x - 2p$$

(13)

has other non-negative integer solution in addition to $(x, y) = (2, 0)$, then it has two set of non-negative integer solution at most with has structure of $(x, y) = (3qa^2 + 2, 3qab), a = 2f, b = f^4 + 24rg^2$. $f$ is odd and $g$ is even such that $f^2 = 1 \mod 12$, and $(f^2 - 6g^2, g)$ is the solution of the elliptic curve

$$X^2 - 12qY^4 = 1$$

(14)

i.e. There is a square number $d$ which can be divided by 4 such that

$$\left(\left[f^2 - 6g^2\right], g^2\right) = \left(6qd^2 + 1, d\sqrt{3qd^2 + 1}\right)$$

and $3qd^2 + 1$ is fourth power number.

**Proof**: The elliptic curve (13) can be written as follows

$$y^2 = (x - 2)(x^2 + 2x + p)$$

(15)

It is easy to verify that $(x, y) = (2, 0)$ is a set of solution. We consider the case $x > 2$ and $y \neq 0$.

Let $d = \gcd(x - 2, x^2 + 2x + p), x - 2 = dt, t \in Z^+, then$

$$x^2 + 2x + p = (dt)^2 + 6dt + p + 8 \gcd(x - 2, x^2 + 2x + p) = \gcd(x - 2, p + 8) = \gcd(x - 2, 36x^2 + 15)$$

Because $q = 12s^2 + 5$, so $\gcd(x - 2, x^2 + 2x + p) = \gcd(x - 2, 3q), a = 1, 3, q, or 3q$. We consider $d$ in four cases.

Case 1 If $d = 1$, let

$$x = 2 = a^2, x^2 + 2x + p = b^2, y = \pm ab, \gcd(a, b) = 1$$

$$\Rightarrow b^2 - (x + 1)^2 = p - 1, x = a^2 + 2$$

$$\Rightarrow b^2 - (a^2 + 3)^2 = 36x^2 + 6 \equiv 0 \mod 8$$

so $b, a^2 + 3$ are both odd or even, i.e. One of $b, a$ is odd and the other is even. If $b$ is odd and $a$ is even, then

$$b^2 - (a^2 + 3)^2 = 1 - 1 = 0 \mod 8$$

and if $a$ is odd and $b$ is even, then
\[ b^2 \equiv 0 \text{or} 4 \mod 8, (a^2 + 3)^2 \equiv 0 \mod 8 \]
\[ \Rightarrow b^2 - (a^2 + 3)^2 \equiv 0 \text{or} 4 \mod 8 \]

But \( b^2 - (a^2 + 3)^2 = 36s^2 + 6 \equiv 6 \mod 8 \), which is contradictory.

**Case 2.** If \( d = 3 \), let
\[ x - 2 = 3a^2, x^2 + 2x + p = 3b^2 \]
so \( x = 3a^2 + 2 \) and \( p = 36s^2 + 7 \), thus \( x^2 + 2x + p = 3b^2 \) is equivalent to
\[ (3a^2 + 1)^2 + 12s^2 + 2 = b^2 \]
\[ \Rightarrow b^2 - 3(a^2 + 1)^2 = 12s^2 + 2 \equiv 2 \mod 4 \]

Thus \( b, a^2 + 1 \) are both odd or even, i.e. One of \( b, a \) is odd and the other is even. If \( b \) is odd and \( a \) is even, then
\[ b^2 - (a^2 + 3)^2 \equiv 1 \equiv 0 \mod 4 \]

If \( a \) is odd and \( b \) is even, then
\[ b^2 \equiv 0 \mod 4, (a^2 + 3)^2 \equiv 0 \mod 4 \]
\[ \Rightarrow b^2 - (a^2 + 3)^2 \equiv 0 \mod 4 \]
but \( b^2 - 3(a^2 + 1)^2 = 12s^2 + 2 \equiv 2 \mod 4 \), which is contradictory.

**Case 3.** If \( d = q \), let
\[ x - 2 = qa^2, x^2 + 2x + p = qb^2 \]
so \( x = qa^2 + 2 \) and \( p = 3q-8 \), thus \( x^2 + 2x + p = qb^2 \) is equivalent to
\[ (qa^2 + 3)^2 + 3q - 9 = qb^2 \]
\[ \Rightarrow 3(a^2 + 1)^2 + (q-3)a^2 = b^2 \]

By \( q = 12s^2 + 5 \) and know that \( b, a^2 + 1 \) are both even or both odd, i.e. One of \( b, a \) is odd and the other is even. If \( b \) is odd and \( a \) is even, then
\[ 0 \equiv (q-3)a^4 = b^2 - 3(a^2 + 1)^2 + (q-3)a^4 \equiv 1-3 = 6 \mod 8 \]
which is contradictory. If \( a \) is odd and \( b \) is even, then
\[ 2 \equiv (q-3)a^4 = b^2 - 3(a^2 + 1)^2 + (q-3)a^4 \equiv 0 \mod 4 \]
which is contradictory.

**Case 4.** If \( d = 3q \), let
\[ x - 2 = 3qa^2, x^2 + 2x + p = 3qb^2 \]
so \( x = 3qa^2 + 2 \) and \( p = 3q-8 \), thus \( x^2 + 2x + p = 3qb^2 \) is equivalent to
\[ (3qa^2 + 3)^2 + 3q - 9 = 3qb^2 \]
we have
\[ (3a^2 + 1)^2 + 3(q-3)a^4 = b^2 \]

By \( q = 12s^2 + 5 \) we know that \( b, 3a^2 + 1 \) are both odd and both even, i.e. One of \( b, a \) is odd and the other is even. If \( b \) is even and \( a \) is odd, then
\[ b^2 \equiv 0 \mod 4, (3a^2 + 1)^2 + 3(q-3)a^4 \equiv 0 + 3 \equiv 2 \mod 4 \]
which is contradictory. So \( b \) is odd and \( a \) is even. Let \( a = 2r \), where \( r \) is a non-negative integer. Then
\[ (12r^2 + 1)^2 + 48(q-3)r^4 = b^2 \quad (16) \]
Let \( r = 6s^2 + 1 \) be prime, where \( s \) is non-negative odd. There is \( q = 2r + 3 \), hence (16) is equivalent to
\[ 12^2r^4 + 24rt^2 + 1 + 96rt^4 = b^2 \]
\[ \Rightarrow (b + 12r^2 + 1)(b - 12r^2 - 1) = 96rt^4 \]
Let \( k = \gcd(b + 12r^2 + 1, b - 12r^2 - 1) \), then \( 2 \mid k \), \( 2 \mid b, b \) are odd, \( 24r^2 + 2 \). If \( k > 2 \), let \( p_i \) denote one prime divisor of \( \frac{k}{2} \), then \( p_i \mid b, p_i \mid 12r^2 + 1 \), and \( p_i \mid 96rt^4 \). By
\[ \gcd(12r^2 + 1, 96rt^4) = \gcd(12r^2 + 1, r) \]
We know $p_1 | r$, so $p_1 = r$, and $r | b, r | 12r^2 + 1$, as well as $r$ and $96$ can’t be divided by $r$, but $r^2 | 96r^4$, it is a contradiction. So $p_1 = 1$, i.e. $k = 2$.

Let $t = fg$, $\gcd(f, g) = 1$, then we can denote
\[ b + 12r^2 + 1 = \frac{2^3 \cdot 3r}{c} f^4, \quad b - 12r^2 - 1 = cg^4 \]
where $c = 2, 6, 16, 48, 2r, 6r, 48r$.

If $c = 2$, then $b = 24rf^4 + g^4$, $12r^2 + 1 = 24rf^4 - g^4$.
Because $3$ can’t divide $12r^2 + 1$, so $3$ don’t divide $g$, hence
\[ 1 = 12r^2 + 1 = 24rf^4 - g^4 \equiv -1 \pmod{3} \]
which is contradictory.

If $c = 6$, then $b = 8rf^4 + 3g^4$, $12r^2 + 1 = 8rf^4 - 3g^4$.
Because of $t = fg$, so the second equation of the above is equivalent to the following
\[ 12f^2g^2 + 1 = 8rf^4 - 3g^4 \]
\[ (2r + 3)(2f^2)^2 - 3(2f^2 + g^2)^2 = 1 \]
Because of $r = 6s^2 + 1$, the above equation is equivalent to the following
\[ (12s^2 + 5)(2f^2)^2 - 3(2f^2 + g^2)^2 = 1 \]
we can get the equation
\[ (12s^2 + 5)x^2 - 3y^2 = 1 \]
has integer point $(x, y) = (2f^2, 2f^2 + g^2)$. But
\[ 1 = (12s^2 + 5)x^2 - 3y^2 \equiv 5x^2 \equiv 0 \quad \text{or} \quad 2 \pmod{3} \]
It is contradictory.

If $c = 16$, then $b = 3rf^4 + 8g^4$, $12r^2 + 1 = 3rf^4 - 8g^4$.
By the second equation of the above, we know $f$ is odd, so
\[ 0 \equiv 12r^2 + 8g^4 = 3rf^4 - 1 \equiv 2 \pmod{4} \]
which is contradictory.

If $c = 48$, then $b = rf^4 + 24g^4$, $12r^2 + 1 = rf^4 - 24g^4$.
By the second equation of the above, it is easy to verify $f$ can’t be divided by $3$ and $f$ is odd. Because $s$ is odd, so
\[ 0 \equiv 12r^2 + 24g^4 = rf^4 - 1 = (6s^2 + 1)f^4 - 1 \equiv (6 + 1)f^4 - 1 = 6or2 \pmod{12} \]
which is contradictory.

If $c = 16$, then $b = 8f^4 + 3rg^4$, $12r^2 + 1 = 8f^4 - 3rg^4$.
By the second equation of the above, it is easy to verify $g$ is odd, so
\[ 0 \equiv 24rf^4 - 12r^2 = 1 + rg^4 \equiv 1 + g^4 = 2or4 \pmod{6} \]
which is contradictory.

If $c = 6r$, then $b = 8f^4 + 3rg^4$, $12r^2 + 1 = 8f^4 - 3rg^4$.
so $g$ is odd. If $f$ is odd, then
\[ 4 \equiv 8f^4 - 12r^2 = 1 + 3rg^4 \equiv -2 \pmod{8} \]
It is a contradiction. If $f$ is even, because of $t = fg$, we has
\[ 0 \equiv f^4 - 12r^2 = 1 + 3rg^4 \equiv -2 \pmod{8} \]
It is contradictory.

If $c = 16r$, then $b = 3f^4 + 8rg^4$, $12r^2 + 1 = 3f^4 - 8rg^4$.
It is easy to verify that \( f \) is odd, and \( 1 = 12r^2 + 1 = 3f^4 - 8rg^4 \equiv 3 \mod 4 \), which is contradictory.

If \( c = 48r \), then

\[
b = f^4 + 24rg^4, \quad 12r^2 + 1 = f^4 - 24rg^4
\]

so \( f \) is odd, \( f^4 \equiv 1 \mod 12 \Rightarrow f^2 = 1 \mod 12 \), \( f^2 = 1 \mod 24 \), and \( t = fg \) is even, i.e. \( g \) is even. By the second equation of the above we can get

\[
(f^2 - 6g^2)^2 - 12(2r + 3)g^4 = 1
\]

Because of \( r = 6s^2 + 1 \), then the above is equivalent to the follows

\[
(f^2 - 6g^2)^2 - 12(12s^2 + 5)g^4 = 1
\]

so \((f^2 - 6g^2, g)\) is a set of integer solution of the equation

\[
X^2 - (144s^2 + 60)Y^2 = 1
\]

By lemma 2 we know the above equation has two set of non-negative integer solution at most, so (13) has no more than two solutions in addition to \((0, 0)\). And \((f^2 - 6g^2, g^2)\) is one solution of the equation

\[
X^2 - (144s^2 + 60)Y^2 = 1
\]

By theorem 1, we know the equation \( X^2 - 12qY^2 = 1 \), where \( q = 12s^2 + 5 \) is prime has the structure \((6qd^2 + 1, d\sqrt{3qd^2 + 1})\) of the non-negative integer solution, where \( d \) is any non-negative integer such that \( 3qd^2 + 1 \) is square, so there is some integer \( d \) such that

\[
[f^2 - 6g^2] = 6qd^2 + 1, \quad g^2 = d\sqrt{3qd^2 + 1}
\]

Because of

\[
1 = [f^2 - 6g^2] = 6qd^2 + 1 = 6d^2 + 1 \mod 12, \quad \gcd(d, 3qd^2 + 1) = 1, \quad g^2 = d\sqrt{3qd^2 + 1}
\]

so \( d \) is square which can be divided by 4.

By the above analysis, we know if the elliptic curve

\[
y^2 = x^3 + (p - 4)x - 2p
\]

has other non-negative integer point except of \((2, 0)\), then it has two set of non-negative integer solution at most, and it’s solution is \((x, y) = (3u^2 + 2, 3uab)\), where \( u = 2fg, b = f^4 + 24rg^4 \). \( f \) is odd, \( g \) is even which satisfy : \( f^2 \equiv 1 \mod 12 \), and \((f^2 - 6g^2, g^2)\) is one solution of the elliptic curve

\[
X^2 - (144s^2 + 60)Y^2 = 1
\]

i.e. there is a square integer \( d \) which can be divide by 4 such that \([f^2 - 6g^2, g^2] = (6qd^2 + 1, d\sqrt{3qd^2 + 1})\), and \( 3qd^2 + 1 \) is a fourth power integer.

3. CONCLUSIONS

For theorem 1, we gave the following example to describe it was feasible for solving the equation (7).

Example 1 If \( q = 113 \), we could find only one value 2453 for \( a \) in \((0, 10^4)\), and the (7)’s solution is

\[
(4946145799, 121987690)
\]

For theorem 2, it was easy to prove that \( r = 6s^2 + 1, q = 12s^2 + 5, p = 36s^2 + 7 \) were primes when \( s \) taken the following 40 values

\[
1 \quad 24 \quad 79 \quad 164 \quad 276 \quad 284 \quad 649 \quad 814 \quad 836 \quad 1314 \quad 1369 \quad 1864 \quad 2231 \quad 2441 \quad 2664 \quad 2924 \quad 3386 \quad 3631 \quad 3684 \quad 3929 \quad 4296 \quad 4434 \quad 4461 \quad 4741 \quad 4911 \quad 5036 \quad 5799 \quad 6346 \quad 6534 \quad 6589 \quad 7194 \quad 8041 \quad 8391 \quad 8899 \quad 9341 \quad 9406 \quad 9571 \quad 9921 \quad 10246 \quad 10789
\]

and there 20 values of the above were odd.

Example 2 If \( s = 1 \), then \( r = 6s^2 + 1 = 7, q = 12s^2 + 5 = 17, p = 36s^2 + 7 = 43 \) are prime, we could find eight values of \( d \) such as

\[
7, 700, 69993, 6998600, 77974401, 84973001, 91971601, 98970201 \quad \text{in } (0, 10^8) \text{ such that } 3qd^2 + 1 \text{ are square}. \text{ For the first fourth values of } d, \text{ we could give the (7)’s solutions}
\]

214
and

\[(4999,350), (49980001,3499300), (499700044999,34986001050),\]
\[(4996000999920001,349790034998600)\]

It was easy to verify that

\[49980001 + 3499300\sqrt{204} = (4999 + 350\sqrt{204})^2\]
\[499700044999 + 34986001050\sqrt{204} = (4999 + 350\sqrt{204})^3\]
\[4996000999920001 + 349790034998600\sqrt{204} = (4999 + 350\sqrt{204})^4\]

But \((4999,350)\) wasn’t the \((7)’s\) basic solution.

Between in this values of \(d\),only \(700,698600\) could be divided by \(4\) but which were not square. So there wasn’t square integer \(d\) in \((0,10^8)\) which can be divided by \(4\) such that

\[\left(\left|f^2 - 6g^2\right|, g^2\right) = \left(6qd^2 + 1, d\sqrt{3q} + 1\right)\]

i.e. we can’t find \((13)’ integer point for \(d\) in \((0,10^8)\), or in other words, the equation \((13)\) had no integer points in \((0,10^{24})\).

Example 2 showed that if the elliptic curve \((13)\) has a solution had one integer solution, then the integer was very large when we take large enough prime number prime \(q\) which satisfied the given condition. And it was relatively safe if the solution of the elliptic curve was taken as the key of password. On the other hand, because of the scarcity of the elliptic curve \((13)’ solution, it is not feasible to use the form of \((13)\) to factor integer.

Acknowledgements
This work was supported by the key projects of Provincial Natural Science Research of Anhui Province(No. KJ2014A144).

REFERENCES