Elliptic Curve Cryptography over Gaussian Integers

Elsayed Mohamed and Hassan Elkamchouchi
Alexandria University, Alexandria, Egypt

Summary
A new approach is used to implement elliptic curve cryptography (ECC) over prime finite fields. The new approach uses Gaussian integers instead of rational integers. It generates a much larger number of points under the same curve equation and the same prime p. The elliptic curve arithmetic is basically the same but works on complex numbers. The security of the proposed method is far higher. When compared to the original prime field, the new method requires double the space to store cryptographic keys represented by points but the security level, in terms of the group order, is roughly squared.

Key words:
Elliptic Curve Cryptography, Gaussian Integers

1. Introduction

- **Elliptic Curves**

Elliptic curves are known for their security. The common fields used for encryption are prime fields and characteristic 2 fields.

Elliptic curves over prime fields are on the form:
E: $y^2 = x^3 + ax + b \bmod p$
where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0 \bmod p$

The addition of two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ is calculated by:
$R(x_3, y_3) = P + Q$ where:
$x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = \lambda(x_1 - x_3) - y_1$,
$\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $P \neq Q$
$\lambda = (3x_1^2 + a)/2y_1$ if $P = Q$

The multiplication of points by a scalar is a series of doublings and additions of points. The multiplication by –1 converts P to $-P$ by negating the y coordinate of P, i.e., the negative of $P = (x, y)$ gives $-P = (x, -y)$

- **Gaussian Integers**

Gaussian integers are complex numbers on the form $a + bi$ where a and b are integers and $i = \sqrt{-1}$. The norm N of a Gaussian integer $a + bi$ is $a^2 + b^2$. A Gaussian prime is a Gaussian integer that cannot be expressed in the form of a product of other Gaussian integers. The ring of Gaussian integers is a unique factorization domain. Gaussian primes are Gaussian integers $z = a + bi$ satisfying one of the following properties:

1. If both a and b are nonzero then, $a + bi$ is a Gaussian prime iff $a^2 + b^2$ is an ordinary prime.
2. If $a = 0$, then bi is a Gaussian prime iff $|b|$ is an ordinary prime and $|b| = 3 \bmod 4$.
3. If $b = 0$, then a is a Gaussian prime iff $|a|$ is an ordinary prime and $|a| = 3 \bmod 4$.

2. Elliptic Curves over Gaussian Integers

In this version of elliptic curves, the elliptic curve points will have complex coordinates. This is equivalent to having two linked sets of points with each set on a separate Complex plane and the two Complex planes are linked by the elliptic curve equation.
As an example, the elliptic curve $y^2 = x^3 + 10x + 10 \bmod 11$ has 14 points under rational integers. Given that 11 is a also Gaussian prime, the same curve can be implemented in Gaussian integers. When implemented under Gaussian integers, it contains 140 points. The prime can also be a complex Gaussian prime with real and imaginary parts. If the same curve equation is applied under the Gaussian prime $p = 11 + 4i$, it results in a curve with 144 points. To show the idea and the distribution of points, a full enumeration of curve points has been done. The following figures show the points on both curves. The x and y coordinates are represented separately as each coordinate is complex.

- **Features of *x* and *y* Coordinates**

The x and y coordinate fall within the planar square limited by 0, p, ip and $(1 + i)p$. For $p = c + id$, the real part of x and y falls between c and $-d$. The imaginary part falls between 0 and $c + d$.

- **Point Counting and Hasse's Theorem**

Hasses's theorem states that the number of points on an elliptic curve over F_q is between $q + 1 - 2\sqrt{q}$ and $q + 1 + 2\sqrt{q}$. In the case of Gaussian integers, the characteristic q is the norm of the Gaussian prime number. For the example of $p = 11$, $q = p^2 = 121$ and the number of points is between $(121 + 1 - 2 \times 11)$ and $(121 + 1 + 2 \times 11)$, i.e. between 100 and 145. The actual number of points is 140, which falls in the indicated range. For the other example of $p = 11 + 4i$, $q = 11^2 + 4^2 = 137$ and the number of points is

between (137 + 1 – 2 × 12) and (137 + 1 + 2 × 12), i.e. between 114 and 162.

The actual number of points is 144, which falls again within the indicated range.

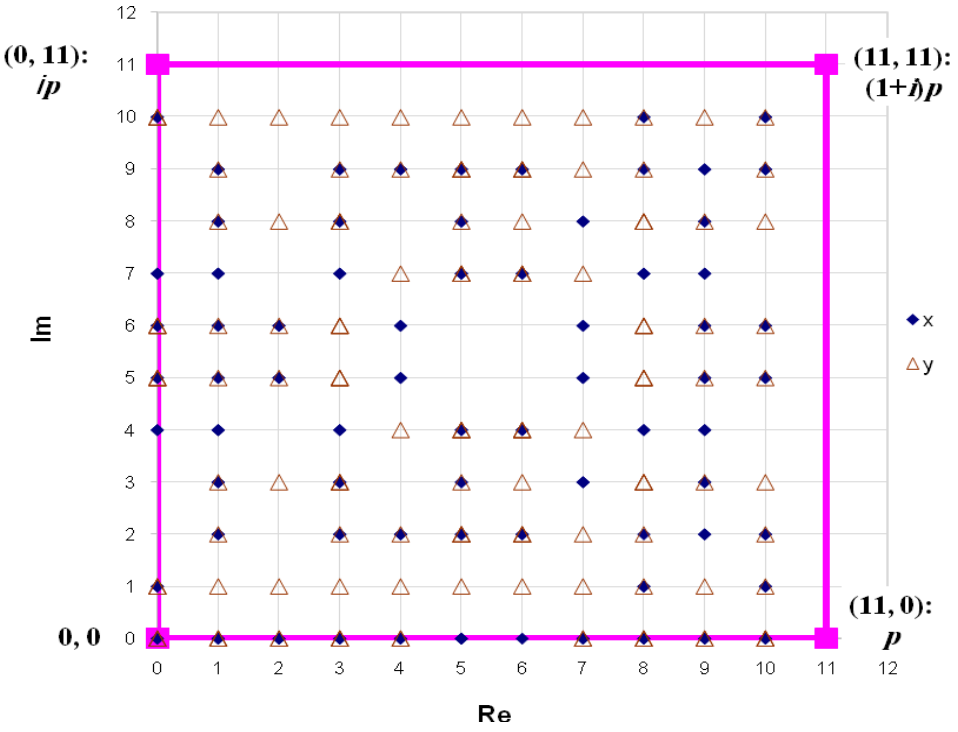

Figure 1:
x and y of $y^2 = x^3+10x+10$ mod 11 in complex plane

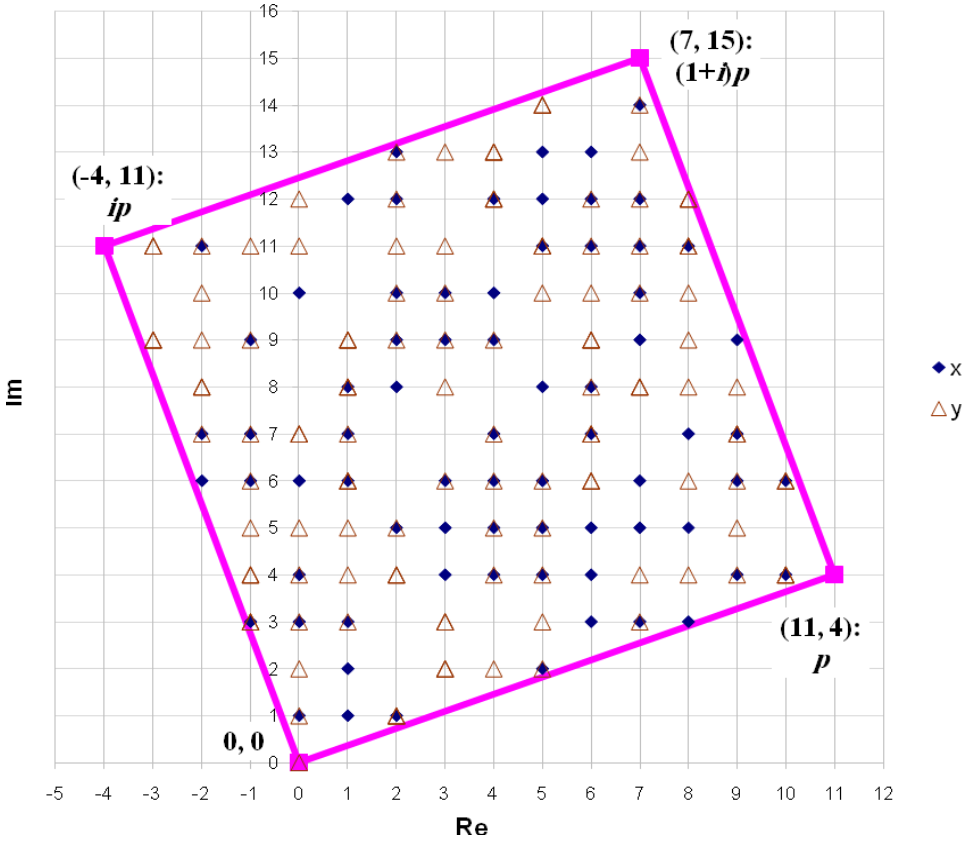

Figure 2:
x and y of $y^2 = x^3+10x+10$ mod 11 + $i4$ in complex plane

- **Elliptic Curve Arithmetic**

Negating, doubling and adding points are done the same way as in the rational integers case. Multiplication has two possible cases with implications for their use in cryptography. The two possibilities are explained below.

– ***Multiplication by Rational Integers***

The multiplication of a point by a rational integer is basically a series of doublings and additions: $kP = P + P +\ldots$ k times. This kind of multiplication is similar to the rational integer case and suitable for cryptographic purposes.

– ***Multiplication by i***

Multiplication of a point by the imaginary number i converts a point (x, y) to the point $(–x, iy)$. This results in a new point that is generally not on the original curve. If all the points on a curve are multiplied by i, this generates all the points that are on another curve. The equation of the other curve can be extracted by replacing x with $–x$ and y with iy in the original elliptic curve equation: $y^2 = x^3 + ax + b \bmod p$. This gives the new equation: $y^2 = x^3 + ax + (p–b) \bmod p$, which is the equation of another curve. Thus, multiplication by i introduces a shift that transforms the curve to another one. This makes multiplication of points by pure imaginary numbers or complex numbers unsuitable for cryptography.

3. ECC over Gaussian Integers

Discrete logarithm cryptographic protocols like Diffie-Hellman key exchange [1] and ElGamal encryption/signature [2] can be translated to their elliptic curve versions. The elliptic curves used can run over rational integers as well as Gaussian integers. However, there are certain features in the Gaussian case that are investigated below.

- **Complexity and Speed**

The number of digits involved in point operations over the Gaussian prime p is similar to the number of digits handled in point operations on the same elliptic curve over a rational prime on the order of p^2. However, complex arithmetic enables multipliers to compute the real and imaginary parts of the output independently. The multiplication of $(a + ib)$ times $(c + id)$ yields $(ac - bd)$ as the real part of the output and $(ad + bc)$ as the imaginary part. Both parts can be calculated independently. This leads to less complex implementation. The underlying modular arithmetic hardware implementation will require cheaper and less complex components because the required multipliers will need to work on inputs that are on the order of p rather than p^2. This implies that the used multipliers in case of Gaussian integers will need to handle a number of digits that is roughly half the number of digits needed to handle the larger integers on the order of p^2. The computational complexity of schoolbook long multiplication as an example is $O(n^2)$ where n is the number of digits in each of the two inputs. In case of rational primes on the order of p^2 that have n digits the complexity is $O(n^2)$ while the equivalent Gaussian integers with real and imaginary parts on the order of p each will have a complexity $O((n/2)^2) = O(n^2/4)$. We need double this time if a single multiplier is used to calculate the real part then the imaginary part of the output. If two multipliers are run in parallel to calculate the real and imaginary parts the total time complexity remains $O(n^2/4)$, which is 1/4 of the time needed in the rational integer case. Montgomery multiplication also has complexity $O(n^2)$ but it deals more efficiently with modular arithmetic [3]. Similar savings in computational complexity can be obtained if more efficient multiplication algorithms are used. Hardware manufacturers can implement the logic needed for the cryptographic operations with cheaper small-scale components without losing security strength at a speed considerably higher (four times higher in case of using the simple long multiplication algorithm).

- **Storage Requirements**

The new proposed method requires double the space and bandwidth used by the same curve equation over the same prime p due to the usage of complex keys represented by points. Point compression techniques can be used to decrease the memory space requirements.

- **Security**

An elliptic curve defined over Gaussian integers results in an elliptic curve group that is much larger than the group of the same curve over rational integers. In terms of the number of points, a curve becomes quadratically larger than the original curve under the same prime number and the same curve equation. The security is greatly improved as the group order (number of points) is squared. This enables system developers to reach a far higher level of security with a slight increase in storage. For systems with limited capacity like smart cards, a very high level of security can be achieved with low storage requirements. The attacks on ECC depend on the reduction of the elliptic curve discrete logarithm problem (ECDLP) to a discrete logarithm problem (DLP). Generally, the resulting DLP requires exponential time algorithms to solve, which makes it infeasible. However, the resulting DLP can be solved in sub–exponential time (or faster) if the original elliptic curve field satisfies certain conditions. The special classes of curves that satisfy these conditions are avoided

in cryptographic systems. The following parts discuss the feasibility of the those attacks for elliptic curves over Gaussian primes.

– ***Anomalous Curves Attack***

An elliptic curve E is anomalous over the rational prime p if the number of points on it equals p. The trace of Frobenius is –1. An isomorphism that converts $E(F_p)$ to F_p^+ can be efficiently computed for anomalous curves. The DLP in F_p^+ can be solved in linear time using the extended Euclidean algorithm [4]. The translation of this condition to curves over Gaussian primes is that the number of points on the curve equals q, the norm of p, which is the order of F_p when p is a Gaussian prime. Anomalous curves are a very small class of curves. Although computing the isomorphism and the extended Euclidean algorithm are computationally harder and more time–consuming in complex numbers, anomalous curves should be avoided in cryptographic applications.

– ***Supersingular Curves Attack***

Supersingular curves are curves for which p divides the trace of Frobenius. Curves that have their order equal to $p + 1$ are examples of this type. In the case of Gaussian integers, p is replaced by its norm in the condition. Using a Weil pairing on E, there is a polynomial time reduction of ECDLP to DLP [5]. These curves are exposed to the MOV attack that runs in sub–exponential time. Although the computations of the attack are longer with complex numbers and large group orders those curves should be avoided.

– ***General Attacks***

The general attacks do not require special properties in the curve. They depend on reducing the original elliptic curve problem to a discrete logarithm problem. For example, the complexity of the baby-step giant-step method is roughly $O(\sqrt{n})$ where n is the order of the group [6]. This estimate ignores the time to perform table lookups. The main problem with this method is that it requires the storage of $O(\sqrt{n})$ group elements. The other kinds of general attacks are also affected by the group order. As the curve order grows quadratically in the case of Gaussian prime curves (compared to the original rational prime field under the same prime), those attacks become much more time and space consuming.

Security Outcome:

The security of ECC is dependent on the curve order even for the weak classes of curves. The number of points contained in an elliptic curves over Gaussian primes is around the square number of points contained in the same curve under the same prime, assuming that it is prime in both Gaussian and rational integers. This increases the strength of the curve, especially if weak curves are avoided and the feasible attacks are only the general ones that require exponential or sub–exponential time.

4. Conclusion

The paper presented a new method to implement elliptic curve cryptography. The method utilizes Gaussian integers instead of rational integers. This requires double the space to store keys. The security of the new system is higher than the original curve over the same prime due to the quadratic increase in the number of points. In each arithmetic operation the underlying hardware/software is required to handle smaller integers at the scale of the real/imaginary part, which enables the designer to utilize two small size units working in parallel to double the processing speed at the same level of security. The method makes elliptic curve attacks more difficult and time consuming.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, vol. 22, 1976.

[2] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, vol. 31, 1985.

[3] Nigel Smart, "Cryptography: An Introduction", *McGraw-Hill*, 2003

[4] N. P. Smart, "The Discrete Logarithm Problem on Elliptic Curves of Trace One", *Journal of Cryptology*, vol. 12, 1999.

[5] Alfred J. Menezes, Tatsuaki Okamoto, Scott A. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", *IEEE Transactions on Information Theory*, vol. 39, 1993.

[6] Ian Blake, Gadiel Seroussi & Nigel Smart, "Elliptic Curves in Cryptography", *Cambridge University Press*, 1999.