Elliptic Curve Point Multiplication

Alexander G. Rostovtsev and Elena B. Makhovenko

Department of Information Security of Computer Systems
St. Petersburg State Polytechnic University
Polytechnicheskaya st., 29, St. Petersburg, Russia
rostovtsev@ssl.stu.neva.ru helen@ssl.stu.neva.ru

Abstract

New type of elliptic curve point multiplication is proposed, where complex multiplication by $\sqrt{-2}$ or by $(1 \pm \sqrt{-7})/2$ is used instead of point duplication. This allows speeding up multiplication about 1.34 times. Using higher radix makes it possible to use one point duplication instead of two and to speed-up computation about 1.6 times. The method takes prime group order factorization: $r = \rho\bar{\rho}$ and integer exponent reduction modulo quadratic prime ρ in the Euclidean imaginary quadratic ring.

Key words: cryptography; elliptic curves; complex multiplication; fast algorithms.

1 Introduction

Elliptic curves over finite fields were proposed in [4] and are widely used in cryptography, because they are relatively fast and provide exponential strength. They allow building a wide range of cryptographic primitives (digital signatures, public-key encryption, key agreement, zero-knowledge proofs, oblivious transfer, etc.).

Elliptic curve points form Abelian group, which is cyclic or direct product of two cyclic groups [4]. Security of elliptic curve cryptosystems, such as ECDSS [1], public key encryption, Diffie — Hellman key agreement relies on the complexity of elliptic curve discrete logarithm problem (ECDLP): given elliptic curve $E(\mathbf{F}_q)$ over the field of $q = p^n$ elements, generator $Q \in E(\mathbf{F}_q)$ of prime order r and point $P \in \langle Q \rangle$ find an exponent l such that $P = lQ$.

Generalized Pollard's algorithm [6] of complexity $O(\sqrt{r})$ is the best known algorithm for solving ECDLP. If $E(\mathbf{F}_q)$ has efficiently counted non-trivial automorphism group, then this algorithm can be executed in two stages. The first one deals with orbits of the automorphism group and the second one refines logarithm with regard to the automorphism group [3]. Usually such automorphisms correspond to complex multiplication.

For example, elliptic curve $E(\mathbf{F}_q)$: $y^2 = x^3 + B$, $q \equiv 1 \pmod 6$, has automorphism: $\varphi(x, y) = (\omega x, -y)$, where $\omega^2 - \omega + 1 = 0$ in $\mathbf{F}_q$. If r^2 does not divide $\#E(\mathbf{F}_q)$, then φ acts in the cyclic subgroup of order r and $\varphi^6 \equiv 1 \pmod r$. Orbit cardinality of the affine points of this subgroup is equal to 6 for automorphism φ. Elements of the orbit have the same value x^3 (and y^2). There exists $\rho \in \mathbf{F}_r$ such that $\rho^6 = 1$. If l denotes discrete logarithm of an arbitrary element of the orbit, then $\rho^i l \pmod r$ is discrete logarithm of any other element of the orbit. This property allows decreasing ECDLP problem complexity about $\sqrt{6}$ times. Similarly, elliptic curve $E(\mathbf{F}_q)$: $y^2 = x^3 + Ax$, $q \equiv 1 \pmod 4$, has automorphism: $\varphi(x, y) = (-x, iy)$, where $i^2 = -1$ in $\mathbf{F}_q$. If r^2 does not divide $\#E(\mathbf{F}_q)$, then φ acts in the cyclic subgroup of order r and $\varphi^4 \equiv 1 \pmod r$. This property allows decreasing ECDLP problem complexity about 2 times.

ECDLP is hard if the following conditions hold:

- r is large prime (160 bits in ECDSS);
- there is no Weil pairing injective homomorphism [5] from $E(\mathbf{F}_q)$ to any group $\mathbf{F}_{q^n}^*$ for small exponents n;
- there is no surjective homomorphism from $E(\mathbf{F}_q)$ to $\mathbf{F}_p$ [8].

2 Elliptic curve with complex multiplication by $\sqrt{-2}$

Elliptic curve cryptosystem rate is dictated by the complexity of multiplication a point by a number. Usually this procedure is performed by duplications and additions [4]. For example, to compute $25Q$ we represent 25 in binary: $(11001)_2$ and then compute the chain: $2^3(2Q + Q) + Q$.

Point multiplication procedure allows further acceleration by higher radix exponent representation, combined with signed binary digits (0, 1, –1) [7].

Projective coordinates allow excluding inversion during duplication and addition; so inversion is needed only once, after all duplications and additions are done. Duplication (and addition) requires addition, subtraction and multiplication in $\mathbf{F}_q$. The first two operations are of linear complexity and multiplication is of quadratic complexity, so the rate of elliptic curve arithmetic depends on the number of multiplications. Duplication and addition need 12 and 15 field multiplications respectively [7].

Two types of curves: with $j = 0$ and $j = 1728$ possess complex multiplication as shown above. The exponent k for these curves can be represented as $k \equiv k_0 + wk_1 \pmod r$, where w is an eigenvalue of complex multiplication operator, and $|k_0| < \sqrt{r}$, $|k_1| < \sqrt{r}$. We can use common base of points Q, $2Q$, .., $2^{\lfloor \log_2 r/2 \rfloor}Q$ for k_0 and k_1. Point multiplication is performed in such a way: k_0Q, k_1Q, wk_1Q, $k_0Q + wk_1Q$. This allows increasing the rate of multiplication [7].

We introduce a large class of elliptic curves with fast complex multiplication instead of duplication and a simple algorithm, establishing bijection between the field $\mathbf{F}_r$ and a subset of polynomials of degree $\le r - 1$ over $\mathbf{F}_3 = \{–1, 0, 1\}$.

Elliptic curve $y^2 = x^3 + Ax^2 + Bx$ has isogeny of degree 2. Consider a curve $E(\mathbf{F}_p)$ over prime finite field with one parameter t:

$$y^2 = x^3 – 4tx^2 + 2t^2x. \tag{1}$$

It is known [2] that if

$$p = a^2 + 2b^2, \tag{2}$$

then

$$\#E(\mathbf{F}_p) = (a \pm 1)^2 + 2b^2. \tag{3}$$

The ring $\mathbf{Z}[\sqrt{-2}]$ is Euclidean and possesses unique factorization. So prime p has unique representation of form (2) if and only if –2 is quadratic residue modulo p. Note that if in (2) $a \equiv \pm 1 \pmod 6$ and $b \equiv 3 \pmod 6$ then $p \equiv 3 \pmod 4$ and $\#E(\mathbf{F}_p) \equiv 2 \pmod 4$ and it is possible to obtain $r = (p + 1 \pm 2a)/2$. Twisted curve is obtained by multiplying t by arbitrary quadratic non-residue modulo p, for example –1.

Assume that in (1) $r = \#E(\mathbf{F}_p)/2$. Isogeny of degree 2 acts on subgroup of r points as complex multiplication by $\sqrt{-2}$:

$$\sqrt{-2}(x, y) = (-y^2/(2x^2), (y(x^2 - 2t^2))/(2\sqrt{-2}x^2)).$$

So, given prime group order r, there exists $\sqrt{-2} \pmod r$ and there are positive integers c, d such that $r = c^2 + 2d^2$.

Elliptic curve (1), given in projective form $Y^2Z = X^3 – 4tX^2Z + 2t^2XZ^2$ for $t = 1/\sqrt{-2}$, has complex multiplication:

$$\sqrt{-2}(X, Y, Z) = (-Y^2Z, Y(X^2 + Z^2)/\sqrt{-2}, 2X^2Z). \tag{4}$$

Multiplication (4) is performed easier than duplication: only 7, instead of 12, modular multiplications are needed. So cryptographic algorithms become faster about 1.34 times.

Transformations $x \leftarrow x + 4t/3$, $t \leftarrow \pm(3/10)^{(p+1)/4}$ give "usual" Weierstrass equation for elliptic curve (1):

$$y^2 = x^3 + Ax + B, \tag{5}$$

where $A = 1$ if $p \equiv \pm 1 \pmod{10}$ and $A = -1$ if $p \equiv \pm 3 \pmod{10}$, $B = \pm(14/15)(2/15)^{(p+1)/4}$. Twisted curve is obtained by changing the sign of B.

Sometimes higher radix allows increasing the rate of point multiplication. For example if radix is 16 and we need to compute kQ, it is possible to precompute points $2Q$, $3Q$, …, $15Q$, to divide k (as binary vector) into 4-bit blocks: $k = k_0 + 16k_1 + \ldots + 16^m k_m$ and to execute procedure for $i = m, m-1, \ldots, 1$:

$$P_m = k_m Q,\ P_{i-1} = 16P_i + k_{i-1}Q. \tag{6}$$

One iteration in (6) takes four point duplications and one point addition. If we represent exponent k in δ-base notation with $\delta = \sqrt{-2} \pmod{r}$, then $\delta^4 = 2^2$, radix in (6) is 4 and one iteration takes only two duplications. Precomputation includes computation of points $\left(\sum_{i=0}^{3} c_i \delta^i\right) P$ for $c_i \in \{-1, 0, 1\}$. Vectors (c_3, c_2, c_1, c_0) are such that $(*, 1, *, 1) = (*, 0, *, -1)$, where * means arbitrary digit, so the base consists of 24 vectors (up to inverse): (0, 0, 0, 1), (0, 0, 1, 0), (0, 0, 1, 1), (0, 0, 1, –1), (0, 1, 0, 0), (0, 1, 0, –1), (0, 1, 1, 0), (0, 1, –1, 0), (0, 1, 1, –1), (0, 1, –1, 1), (0, 1, –1, –1), (1, 0, 0, 0), (1, 0, 0, 1), (1, 0, 0, –1), (1, 0, –1, 1), (1, 0, –1, 1), (1, 0, –1, –1), (1, 1, 0, 0), (1, –1, 0, 0), (1, 1, 0, –1), (1, 1, –1, 0), (1, 1, –1, –1), (1, –1, –1, 0), (1, –1, –1, 1).

Note that ECDSS takes point multiplication for fixed points, so the base can be computed independently. In this case for 4-digit radix the number of field multiplications is 1.61 times less.

3 $\sqrt{-2}$ -ary exponent representation

Each exponent admits of unique minimal $\sqrt{-2}$ -ary representation with the length $\log_2 r$ at most.

Let $K = \mathbf{Q}[\sqrt{-2}]$ and $O_K = \mathbf{Z}[\sqrt{-2}]$. Prime r in O_K is factored as $r = (c + \sqrt{-2}d)(c - \sqrt{-2}d) = \rho\overline{\rho}$. This factorization can be computed from (2), (3): $2r = (a \pm 1)^2 + 2b^2$, $r = b^2 + 2((a \pm 1)/2)^2$. One of these imaginary quadratic primes satisfies congruence: $\rho \equiv 0 \pmod{r}$ or $\overline{\rho} \equiv 0 \pmod{r}$ if we substitute $\sqrt{-2} \pmod{r}$. According to (4), transitions between ρ and its conjugate are obtained by changing sign in $\sqrt{-2} \pmod{p}$, so without loss of generality the first congruence will be considered.

Prime fields $\mathbf{F}_r$ and $O_K/\rho O_K$ are isomorphic. Exponent minimization is equivalent to reduction modulo ρ in O_K. Note that if $\sigma, \tau \in O_K$, then $\sigma + \tau\rho \equiv \alpha \pmod{\rho}$.

Define norm N of quadratic integer $s + t\sqrt{-2}$ as $N(s + t\sqrt{-2}) = s^2 + 2t^2$. Norm function is multiplicative, giving isomorphism from $(O_K/\rho O_K)^*$ to $\mathbf{F}_r^*$. Reduction $(k \in \mathbf{F}_r) \to (k \pmod{\rho} \in O_K/\rho O_K)$ can be computed by norm minimization. The following algorithm computes integer reduction modulo ρ.

Input: integer k; $\rho = c + d\sqrt{-2}$.

Output: $k \equiv k_0 + k_1\sqrt{-2} \pmod{\rho}$, where $|k_0| < \sqrt{r}$, $|k_1| < \sqrt{r}$.

Method:

1. Set $k_0 \leftarrow k$, $k_1 \leftarrow 0$, $\kappa \leftarrow k_0 + k_1\sqrt{-2}$.
2. Find optimal steps in real and imaginary directions: $n_r = \lfloor (ck_0 + 2dk_1)/r \rceil$, $n_i = \lfloor (ck_1 - dk_0)/r \rceil$ and norms $N_r = N(\kappa - n_r\rho)$, $N_i = N(\kappa - n_i\sqrt{-2}\rho)$. Square brackets mean the nearest integer.
3. If $n_i = n_r = 0$ then set $k \leftarrow \kappa$ else
   3.1. If $N_r < N_i$ then set $\kappa \leftarrow \kappa - n_r\rho$ else set $\kappa \leftarrow \kappa - n_i\sqrt{-2}\rho$.
   3.2. Go to step 2.
4. Return(k).

Algorithm finds representation $k \equiv k_0 + k_1\sqrt{-2} \pmod{\rho}$ with minimum norm, $N(k) < r$ and takes two iterations at most.

Algorithm can be illustrated geometrically in complex rectangular lattice with unit vectors $\{1, \sqrt{-2}\}$ as a process of successive approach to the origin. The process comes to a halt as soon as quadratic integer κ falls into a parallelogram with r integer points, disposed symmetrically within the ellipse $x^2 + 2y^2 = r$.

Algorithm can be transformed by analogy with usual Euclidean algorithm transformation to binary one. Here ρ can be represented as a vector over $\{-1, 0, 1\}$ and $k = \sum K_i 2^i$ as a vector $(\ldots, -K_3, 0, K_2, 0, -K_1, 0, K_0)$.

There is no known computable orbit of automorphism group for given point of order r. Note that if $\sqrt{-2}$ generates the whole group $\mathbf{F}_r^*$ or its large subgroup, then orbits attack has no advantages as compared to points attack. So there are no known algorithms for solving ECDLP faster than in $O(\sqrt{r})$ elliptic curve operations.

4 Elliptic curve with complex multiplication by $(1+\sqrt{-7})/2$

This approach is also suitable for elliptic curve $E(\mathbf{F}_p)$ with complex multiplication by $(1+\sqrt{-7})/2$. Then $p = a^2 + 7b^2$, where $a \equiv 0 \pmod 2$, $b \equiv 1 \pmod 2$ and $\#E(\mathbf{F}_p) = p + 1 \pm 2a \equiv 0 \pmod 4$.

Coefficients in (5) are: $A = \left(\frac{-7/5}{p}\right)$ (Jacobi symbol) and $B \equiv (2/5)(-7/5)^{(p+1)/4} \pmod p$. Twisted curve is obtained by changing the sign of B.

Let $\xi = (1+\sqrt{-7})/2$ in $\mathbf{F}_p$. Complex multiplication for the curve $Y^2Z = X^3 + tX^2Z + t^2\xi^6XZ^2/36$, where $t = -6/(2+\xi^2)$, is given by

$$((1+\sqrt{-7})/2)(X, Y, Z) = (Z(\alpha Y^2 + X^2), \gamma Y(X^2 + \delta Z^2), X^2Z),$$

where $\alpha = \xi^2/4$, $\gamma = -\xi^3/8$, $\delta = -\xi^6/36$. Complex multiplication takes 8 field multiplications.

Complex multiplication by $(1+\sqrt{-7})/2$ is given by conjugate coefficients α, γ, δ. Two complex multiplications by conjugates are equal to duplication, so radix can be represented by two or four digits from the set $\{-1, 0, 1\}$.

Formulas, determining complex multiplication given by isogeny of degree ≥ 3, are more complex than considered above, so these elliptic curves seem to be the fastest.

References

1. ANSI X9.62–1998, Public key cryptography for the financial industry: the elliptic curve digital signature algorithm (ECDSA).
2. A. O. Atkin. and F. Morain, "Elliptic curves and primality proving", *Mathematics of Computation*, 61 (1993), 29–68.
3. I. Dursma, P. Gaudry and F. Morain, "Speeding up the discrete log computation on curves with automorphisms", *LIX Research Report LIX/RR/99/03*.
4. N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, 48 (1987), 203–209.
5. A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in finite fields", *IEEE Transactions on Information Theory*, 39 (1993), 1639–1636.
6. J. M. Pollard, "Monte Carlo methods for index computation (mod *p*)", *Mathematics of Computation*, 32 (1978), 918–924.
7. A. Rostovtsev, V. Kuzmich and V. Belenko, "Process and method for fast scalar multiplication of elliptic curve point", *Claim for US patent 09/350,158*. July 9, 1999.
8. I. Semaev, "Evaluation of discrete logarithms in a group of *p*-torsion points of an elliptic curve in characteristic *p*", *Mathematics of Computation*, 67 (1998), 353–356.