Computing the Order of Points on an Elliptic Curve Modulo $N$ is as Difficult as Factoring $N$

S. MARTÍN
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya, Barcelona, Spain
smartin@ma2.upc.es

P. MORILLO AND J. L. VILLAR
Departamento de Matemática Aplicada y Telemática
Universitat Politècnica de Catalunya, Barcelona, Spain
jvillar@mat.upc.es

(Received February 2000; accepted March 2000)

Communicated by J. Lagarias

Abstract—Given a square-free integer $N$, the group of points on an elliptic curve over the ring $\mathbb{Z}_N$ is defined in the natural way. We prove that computing the order of points on elliptic curves over $\mathbb{Z}_N$ is as difficult as factoring $N$, in the sense of randomly polynomial time reduction. Therefore, cryptosystems based on the difficulty of computing the order of points on elliptic curves over the ring $\mathbb{Z}_N$ will be at least as robust as those based on the difficulty of factoring $N$. © 2001 Elsevier Science Ltd. All rights reserved.

Keywords—Public-key cryptography, Elliptic curves, Costly computational problems.

1. INTRODUCTION

Factorization of large integers is an extensively studied problem, due to its cryptographic applications. In fact, the security of some cryptosystems as RSA [1] is believed to lie on the difficulty of factoring a certain integer $N = pq$.

On the other hand, elliptic curves have become more and more used in cryptography in the last decade, directly for designing new cryptosystems [2], as well as in the design of factorization algorithms [3] and primality tests [4,5].

In most cryptographic applications of elliptic curves, knowing the order of the group of points or the order of some points on the elliptic curve is required. Schoof's algorithm [6], and its improvements [7], are the known methods to solve this problem for elliptic curves over the field $\mathbb{F}_p$. Nevertheless, the above algorithms are useless if the elliptic curve is defined over the ring $\mathbb{Z}_N$, where $N$ is a composite integer.

In this letter, the definition of elliptic curve over $\mathbb{Z}_N$, where $N$ is square-free, is given. We show that $N$ can be easily factored with high probability, with an oracle providing the order of any point on such a curve. Therefore, cryptosystems based on the difficulty of computing the
order of points on elliptic curves over the ring $\mathbb{Z}_N$ will be at least as robust as those based on the difficulty of factoring $N$.

2. ELLIPTIC CURVES

2.1. Elliptic Curves Modulo $p$

**Definition 1.** Let $p$ be a prime number, $p \neq 2, 3$, and $\mathbb{Z}_p$ the field of the integers modulo $p$. An elliptic curve over $\mathbb{Z}_p$, denoted as $E_p(a, b)$, where $a, b \in \mathbb{Z}_p$ and $4a^3 + 27b^2 \neq 0 \pmod{p}$, is defined to be the set of affine points $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $y^2 = x^3 + ax + b$, and one additional point $O$, called the point at infinity.

An elliptic curve can be seen as an additive Abelian group whose zero element is $O$. The $k$th multiple of a point $P$ is denoted by $k \cdot P$. The order of the elliptic curve, that is, the number of points on it including $O$, will be denoted as $\#E_p(a, b)$ and the order of a point, $P$, on that curve will be denoted by $o(P)$.

There is another equivalent definition of elliptic curve in projective coordinates $E_p(a,b) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{Z}_p) \mid y^2z = x^3 + axz^2 + bz^3\}$. Here, the affine point $(x, y)$ is mapped onto $(x : y : 1)$, and $O$ is mapped onto $(0 : 1 : 0)$.

The formulas for computing multiples and adding points, as well as more detailed information on elliptic curves can be found in [8].

2.2. Elliptic Curves Modulo a Square-Free Integer $N$

**Definition 2.** Let $N = 6N' + 1$ be a square-free integer. An elliptic curve over $\mathbb{Z}_N$, denoted as $E_N(a, b)$, where $a, b \in \mathbb{Z}_N$ and $\gcd(4a^3 + 27b^2, N) = 1$, is defined to be the set of points $(x : y : z) \in \mathbb{P}^2(\mathbb{Z}_N)$ such that $y^2z = x^3 + axz^2 + bz^3$ and $\gcd(x, y, z, N) = 1$.

The points $(x : y : z) \in E_N(a, b) - \{(0 : 1 : 0)\}$ such that $\gcd(z, N)$ is a nontrivial factor of $N$ will be called factor-revealing points.

Let us consider $N = p_1 \cdots p_r$, where $p_1 < \cdots < p_r$ are prime numbers. If projective coordinates are considered, the projections $P = (x : y : z) \mapsto x_i \pmod{p_i}$ map $E_N(a, b)$ onto $E_{p_i}(a, b)$. Then, using the Chinese Remainder Theorem, the bijection $\pi = (\pi_1, \ldots, \pi_r): E_N(a, b) \rightarrow E_{p_1}(a, b) \times \cdots \times E_{p_r}(a, b)$ defines group structure in $E_N(a, b)$. Now, the order of a point $P \in E_N(a, b)$, can be computed as the least common multiple of the orders of $\pi_i(P)$ in $E_{p_i}(a, b)$, for $i = 1, \ldots, r$, that is, $o(P) = \text{lcm}(o(P_1), \ldots, o(P_r))$. The factor-revealing points can be characterized in terms of $\pi_i$ as the points $P$ such that some but not all projections $\pi_i(P) = O$.

Note that the above definition for the group of points of the elliptic curve $E_N(a, b)$ could be directly extended to any integer, $N = 6N' + 1$, if the definition of elliptic curve over the ring $\mathbb{Z}_q$, where $q$ is a prime power, were given.

If the factorization of $N$ must be kept secret, only the affine points on $E_N(a, b)$ might be considered. Since the formulas for computing multiples and adding points on $E_p(a, b)$, $p$ prime, are rational expressions of the coordinates, they are also valid if applied to affine points on $E_N(a, b)$, in most cases. Namely, the formulas can compute $(x_1 : y_1 : 1) + (x_2 : y_2 : 1)$ when $x_1 - x_2 \in \mathbb{Z}_N^*$ or when $x_1 = x_2$ and $y_1 + y_2 \in \mathbb{Z}_N^*$. Thus, if the classical formulas fail, a nontrivial factor of $N$ is easily obtained.

3. FACTORING $N$ GIVEN AN ORACLE OF $o(P)$

Although any factor-revealing point (see the previous section) will reveal a nontrivial factor of $N$, the probability of finding a such point at random is very small when the primes $p_i$ are large enough. In this section, we show how factor-revealing points can be found by using the oracle $\mathcal{O}$ defined as follows.
INPUT: A square-free integer $N$, an elliptic curve $E_N(a, b)$ such that $\gcd(4a^3 + 27b^2, N) = 1$, and an affine point $P = (x : y : 1)$ on this curve.

OUTPUT: The order $o(P)$ on $E_N(a, b)$.

**Theorem 1.** Let $E_N(a, b)$ be an elliptic curve with even order and $P \in E_N(a, b)$ a point with even order such that $o(P_i) = 2^s \alpha_i$, where $i = 1, \ldots, r$, and all $\alpha_i$ are odd.

Then, $Q = (o(P)/2)\#P$ is a factor-revealing point if and only if $\exists i \neq j$ s.t. $s_i \neq s_j$.

**Proof.** Since $o(P) = \text{lcm}(o(P_1), \ldots, o(P_r)) = 2^s \alpha$, where $\alpha$ is odd and $s = \max(s_1, \ldots, s_r)$, then,

$$o(P_i) \mid o(P) \iff o(P_i) = O \iff \exists j \text{ s.t. } s_i < s_j.$$

Thus, if all $s_i$ are equal, $\pi_i(Q) \neq O$ for all $i$, and $Q$ is an affine point. Otherwise, there exist some (but not all) $i = 1, \ldots, r$ such that $\pi_i(Q) = O$, that is, $Q$ is a factor-revealing point.

Actually, during the computation of $Q$, one of the additions of points involved could fail. As seen in Section 2.2, in such case, a nontrivial factor of $N$ is also found.

**Corollary 1.** Let $E_N(a, b)$ be an elliptic curve such that $\#E_{p_i}(a, b)$ is odd for some $i = 1, \ldots, r$ and $P \in E_N(a, b)$ a point with even order. Then, $(o(P)/2)\#P$ is a factor-revealing point.

**Proof.** Since $\#E_{p_i}(a, b)$ is odd, then $s_i = 0$, but since $o(P)$ is even, then $\exists j$ such that $s_j > 0$, therefore, Theorem 1 applies.

**Algorithm**

Since the factorization of $N$ is unknown, it seems that there is no deterministic way to build elliptic curves and points fulfilling the conditions of Corollary 1 to obtain a nontrivial factor of $N$. Then, the following random algorithm is proposed.

1. Generate $(x, y, a)$ at random, uniformly distributed on $\mathbb{Z}_N \times \mathbb{Z}_N \times \mathbb{Z}_N$.
   - Let $b = y^2 - x^3 - ax$ (mod $N$).
   - Let $g = \gcd(4a^3 + 27b^2, N)$.
   - If $g = N$, go to 1.
   - Else if $g \neq 1$, $g$ is a nontrivial factor of $N$. Exit.
2. Let $P = (x : y : 1)$.
   - Obtain $o(P)$ from the oracle $O$.
   - If $o(P)$ is odd, go to 1.
3. Compute $Q = (o(P)/2)\#P$, using the classical formulas.
   - If the computation fails, a nontrivial factor of $N$ is found. Exit.
   - Else if $Q$ is an affine point, go to 1.
   - Else, $Q$ is a factor-revealing point. Exit.

**Proposition 1.** For $(x, y, a)$ uniformly distributed on $\mathbb{Z}_N \times \mathbb{Z}_N \times \mathbb{Z}_N$, the probability that, in one round, the above algorithm reveals a nontrivial factor of $N$ is greater than $41/225$.

**Proof.** Since the proof is very technical, it has been placed in the Appendix.

**Theorem 2.** Let $N = 6N' \pm 1$ be a square-free composite integer. There is a random polynomial time algorithm for factoring $N$, using the oracle $O$.

**Proof.** Since, as seen in Proposition 1, each round of the proposed algorithm obtains a nontrivial factor of $N$ in polynomial time with a probability greater than a positive constant, then $N$ is factorized in random polynomial time.
4. CONCLUSIONS

In this letter, a definition for the group of points on an elliptic curve modulo a square-free integer \( N = 6N' + 1 \) is given. From this definition, it is shown that if \( N \) is composite, the problem of finding the order of a point on an elliptic curve modulo \( N \) is at least as difficult as factoring \( N \). Therefore, any cryptosystem based on the difficulty of computing such orders is as robust as the well-known RSA cryptosystem, as well as any other cryptosystem based on the difficulty of the factorization problem. The results obtained here could be directly extended to the general case (i.e., nonsquare-free integers) if a definition of elliptic curve over the ring \( \mathbb{Z}_q \), where \( q \) is a prime power, were given.

In [9], Kunihiro and Koyama show the equivalence between counting the number of points on elliptic curves over the ring \( \mathbb{Z}_N \) and factoring \( N \), for any square-free integer \( N \). Although this result is related to the main result in our paper, it is not equivalent.

It is not known how to use an oracle for \( \#E_N(a, b) \) to compute the order of a given point \( P \in E_N(a, b) \). On the other hand, an oracle of the form in this paper can be used to get information on \( \#E_N(a, b) \). Instead of using our oracle \( O \) as a “front end” for the random polynomial time reduction used in [9], a direct reduction is given in this letter. The use of irreducible polynomials makes possible to get a lower bound of the probability of factoring \( N \) in each round of the algorithm, without any assumption about the probability distribution of \( \#E_p(a, b) \) on the Hasse interval.

APPENDIX

The aim of this Appendix is to prove Proposition 1. Let \( p \) be a prime number greater than 3.

**Lemma 1.** \( \#E_p(a, b) \) is odd if and only if the polynomial \( X^3 + aX + b \) is irreducible in \( \mathbb{Z}_p \).

**Proof.** \( \#E_p(a, b) \) is even if and only if there exists a point with order two on the curve. From the definition of 2#P in an elliptic curve modulo \( p \) [8], a point \( (x, y) \in E_p(a, b) \) has order 2 if and only if \( y = 0 \) and, then \( x^3 + ax + b = 0 \). Finally, observe that \( X^3 + aX + b \) is irreducible if and only if it has no roots.

**Lemma 2.** There are exactly \((p^2 - 1)/3\) polynomials \( X^3 + aX + b \) irreducibles in \( \mathbb{Z}_p \).

**Proof.** The polynomials \( X^3 + aX + b \) can be seen as a canonical representation of the set of polynomials \( X^3 + c_2X^2 + c_1X + c_0 \in \mathbb{Z}_p[X] \) modulo translations (i.e., \( X \mapsto X - \mu, \mu \in \mathbb{Z}_p \)). Note that all classes in the quotient set have exactly \( p \) polynomials. Since the above transformations preserve the irreducibility of the polynomials, and there are \((p^3 - p)/3\) irreducible polynomials of degree 3 over \( \mathbb{Z}_p \) (see [10]), then there are \((p^3 - 1)/3\) classes of irreducible polynomials.

Let \( \tilde{E}_p(a, b) = E_p(a, b) - \{O\} \) be the set of affine points on \( E_p(a, b) \). For any \( \alpha \in \mathbb{Z}_p^* \), the transformation \( E_p(a, b) \mapsto E_p(\alpha^2a, \alpha^3b) \) is a bijection on the set of elliptic curves over \( \mathbb{Z}_p \). It is known that if \( \alpha \) is a nonquadratic residue modulo \( p \), then \( \#E_p(a, b) + \#E_p(\alpha^2a, \alpha^3b) = 2p \).

**Lemma 3.** Let \( I = \{(a, b) \in \mathbb{Z}_p^2 : X^3 + aX + b \text{ irreducible}\} \) and \( D = \{(a, b) \in \mathbb{Z}_p^2 : 4a^3 + 27b^2 \neq 0\} \). Then,

\[
\sum_{(a, b) \in I} \#\tilde{E}_p(a, b) = \frac{p^3 - p}{3} \quad \text{and} \quad \sum_{(a, b) \in D} \#\tilde{E}_p(a, b) = p^3 - p^2.
\]

**Proof.** Let \( \alpha \) be a nonquadratic residue modulo \( p \).

From Lemma 2, \(|I| = (p^2 - 1)/3\). Since \( \#E_p(a, b) \) and \( \#E_p(\alpha^2a, \alpha^3b) \) have the same parity, then \( X^3 + aX + b \) is irreducible if and only if \( X^3 + \alpha^2aX + \alpha^3b \) is. Therefore,

\[
\sum_{(a, b) \in I} \#\tilde{E}_p(a, b) = \frac{1}{2} \sum_{(a, b) \in I} \left[ \#E_p(a, b) + \#E_p(\alpha^2a, \alpha^3b) \right] = \frac{1}{2} \frac{p^3 - 1}{3} = \frac{p^3 - p}{3}.
\]
There are exactly \( p \) solutions \((a, b)\) of the equation \( 4a^3 + 27b^2 \equiv 0 \pmod{p} \), corresponding to the \( p \) polynomials \( X^3 + aX + b \) with a double or a triple root in \( \mathbb{Z}_p \). Thus, \( |D| = p^2 - p \). Since the condition \( 4a^3 + 27b^2 = 0 \) holds for \((a, b)\) if and only if it holds for \((a^2a, a^3b)\), then

\[
\sum_{(a, b) \in D} \#E_p(a, b) = \frac{1}{2} \sum_{(a, b) \in D} \left[ \#E_p(a, b) + \#E_p(a^2a, a^3b) \right] = \frac{1}{2} 2p (p^2 - p) = p^3 - p^2.
\]

**Proof of Proposition 1.** Let us find a lower bound of the probability \( S \) that a nontrivial factor of \( N \) is found in a given round of the algorithm, that is, for one choice of \( x, y, \) and \( a \).

Following the algorithm, if \( \Delta = 4a^3 + 27b^2 \not\equiv Z_p^* \), then \( \Delta \) is a nontrivial factor of \( N \), unless \( \Delta = 0 \). Otherwise, if conditions in Corollary 1 hold for \( P \) and \( E_N(a, b) \) (i.e., \( o(P) \) is even and \( \exists \) \( i \) such that \( \#E_p(a, b) \) is odd), the nontrivial factor of \( N \) is surely found.

Then, one round of the algorithm can fail to find a nontrivial factor of \( N \) only if \( \Delta = 0 \) or if \( \Delta \in Z_N^* \) and conditions in Corollary 1 do not hold for \( P \) and \( E_N(a, b) \). Therefore,

\[
S \geq 1 - \Pr\{\Delta = 0\} - \Pr\{o(P) \text{ odd } \cup \#E_p(a, b) \text{ even } \forall i \mid \Delta \in Z_N^*\} \Pr\{\Delta \in Z_N^*\}
\]

\[
= 1 - \Pr\{\Delta = 0\} - \Pr\{o(P) \text{ odd } \mid \Delta \in Z_N^*\} + \Pr\{\#E_p(a, b) \text{ even } \forall i \mid \Delta \in Z_N^*\}
\]

\[
- \Pr\{o(P) \text{ odd } \cap \#E_p(a, b) \text{ even } \forall i \mid \Delta \in Z_N^*\} \Pr\{\Delta \in Z_N^*\}.
\]

Note that, according to the Chinese Remainder Theorem, choosing \((x, y, a)\) uniformly distributed on \( Z_N \times Z_N \times Z_N \) is equivalent to independently choosing \((x_i, y_i, a_i)\) uniformly distributed on \( Z_{p_i} \times Z_{p_i} \times Z_{p_i} \), for \( i = 1, \ldots, r \).

Let \( \Delta_i = \Delta \pmod{p_i} \), \( G_i = \Pr\{\Delta_i = 0\} \), \( E_i = \Pr\{\#E_p(a, b) \text{ even } \mid \Delta_i \neq 0\} \), and \( F_i = \Pr\{o(P_i) \text{ odd } \mid \#E_p(a, b) \text{ even } \cap \Delta_i \neq 0\} \). Then,

\[
S \geq 1 - \prod_{i=1}^r \Pr\{\Delta_i = 0\} - \left[ \prod_{i=1}^r \Pr\{o(P_i) \text{ odd } \mid \Delta_i \neq 0\} + \prod_{i=1}^r \Pr\{\#E_p(a, b) \text{ even } \mid \Delta_i \neq 0\} \right] \prod_{i=1}^r \Pr\{\Delta_i \neq 0\}
\]

\[
= 1 - \prod_{i=1}^r G_i - \left[ \prod_{i=1}^r (1 - E_i) + E_i F_i \right] + \prod_{i=1}^r E_i - \prod_{i=1}^r E_i F_i \prod_{i=1}^r (1 - G_i),
\]

where, in the last equality, \( \Pr\{o(P_i) \text{ odd } \mid \Delta_i \neq 0\} \) has been calculated as follows:

\[
\Pr\{o(P_i) \text{ odd } \mid \Delta_i \neq 0\} = \Pr\{\#E_p(a, b) \text{ odd } \mid \Delta_i \neq 0\}
\]

\[
+ \Pr\{o(P_i) \text{ odd } \cap \#E_p(a, b) \text{ even } \mid \Delta_i \neq 0\}
\]

\[
= (1 - E_i) + E_i F_i.
\]

Since \( F_i \leq 1/2 \forall i \), and expression (*) is decreasing in \( F_i \forall i \), we can take 1/2 as an upper bound on the \( F_i \), and

\[
S \geq 1 - \prod_{i=1}^r G_i - \left[ \prod_{i=1}^r (1 - E_i) + \left( 1 - \frac{1}{2} \right) \prod_{i=1}^r E_i \right] \prod_{i=1}^r (1 - G_i).
\]

Using Lemma 3,

\[
E_i = 1 - \frac{|\{(x, y, a) \mid X^3 + aX + b \text{ irreducible in } Z_{p_i}\}|}{|\{(x, y, a) \mid \Delta_i \neq 0\}|} = 1 - \frac{p_i^3 - p_i}{3(p_i^3 - p_i^2)} = \frac{2}{3} \left( 1 - \frac{1}{2p_i} \right)
\]

and

\[
G_i = 1 - \frac{|\{(x, y, a) \mid \Delta_i \neq 0\}|}{p_i^3} = 1 - \frac{p_i^3 - p_i^2}{p_i^3} = \frac{1}{p_i}.
\]
Then,

\[ S \geq 1 - \prod_{i=1}^{r} \frac{1}{p_i} - \left( \frac{2}{3} \right)^r \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right) \left[ \prod_{i=1}^{r} \left( 1 + \frac{1}{4p_i} \right) + \left( 1 - \frac{1}{2r} \right) \prod_{i=1}^{r} \left( 1 - \frac{1}{2p_i} \right) \right] \]

\[ = 1 - \prod_{i=1}^{r} \frac{1}{p_i} - \left( \frac{2}{3} \right)^r \left[ \prod_{i=1}^{r} \left( 1 - \frac{3}{4p_i} \right) + \left( 1 - \frac{1}{2r} \right) \prod_{i=1}^{r} \left( 1 - \frac{1}{2p_i} \right) \left( 1 - \frac{1}{p_i} \right) \right] \]

\[ > 1 - \prod_{i=1}^{r} \frac{1}{p_i} - \left( \frac{2}{3} \right)^r \left( 2 - \frac{1}{2r} \right) \cdot \]

Finally, since \( r \geq 2 \) and \( p_i \geq 5 \),

\[ S > 1 - \frac{1}{5^2} - \left( \frac{2}{3} \right)^2 \left( 2 - \frac{1}{2^2} \right) = \frac{41}{225}. \]

REFERENCES