# On Finding Roots Without Factoring and A Special Purpose Factoring Algorithm

Daniel R. L. Brown*

July 4, 2005

**Abstract**

For any integer $n$, some side information exists that allows roots of certain polynomials modulo $n$ to be found efficiently (in polynomial time). The quartics $q_{u,a,b}(x) = x^4 - 4ux^3 - 2ax^2 - (8b+4ua)x + a^2 - 4ub$, where $a$ and $b$ are some fixed integers, can be solved with probability approximately $\frac{1}{4}$ over integers $u$ chosen randomly from in $\{0, 1, \ldots, n-1\}$. The side information depends on $a$ and $b$, and is derivable from the factorization of $n$. The side information does not necessarily seem to reveal the factorization of $n$. For certain other polynomials, such as $p_u(x) = x^3 - u$, it is an important unsolved problem of theoretical cryptology whether there exists an algorithm for finding roots that does not also reveal the factorization of $n$. Cheng's special-purpose factoring algorithm is also reviewed and some extensions suggested.

## 1 Introduction

Given a composite $n$, it is well known that an elliptic curve $E : y^2 = x^3 + ax + b$ can be made to form group over the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. If $n$ is a product of distinct primes, such as $n = pq$, then, in terms of group structure:

$$E(\mathbb{Z}_n) \cong E(\mathbb{F}_p) \times E(\mathbb{F}_q), \tag{1}$$

which is seen by using the Chinese Remainder Theorem. These groups are used in the elliptic curve method (ECM) of factoring integers introduced by Lenstra [Len87]. This paper applies (1) in a slightly different way: to solve certain polynomial equation module a composite without knowing the factorization.

Similar techniques led to Cheng's special-purpose factoring algorithm [Che02]. Prime factors of the form $p = (4r - 1)(s^2 + s) + r$, where $r \in \{1, 3, 5, 11, 17, 41\}$ and $s$ is an integer, can be found efficiently (in polynomial-time) with Cheng's algorithm. It is unclear, however, if this algorithm can be made into a general-purpose factoring algorithm. Nevertheless, implementations of RSA that use private keys of special form should check that they are not vulnerable to this factoring algorithm or its variants.

Mathematically speaking, the two main ideas underlying these observations are:

- The function $\delta : E(\mathbb{Z}_n) \to E(\mathbb{Z}_n) : P \mapsto dP$ is invertible given $|E(\mathbb{Z}_n)|$. The function $\delta$ and its inverse can also be computed using the x-coordinate only.

*Certicom Research

- Complex multiplication can be used to find a curve over the rationals that has trace one when reduced modulo certain primes $p$.

The interpretations and implications to factoring and the RSA public key cryptosystem are why such trivialities may be interesting. Because of their triviality and lack of practical impact, it is highly likely that all or most of the ideas in this paper have been considered before. Indeed, it may have already proven that the factoring algorithm does not generalize or that the root-finding algorithm cannot be extended to the polynomials used in RSA.

## 2 On Finding Roots Without Factoring

In this section, a small amount of side information that allows certain classes of polynomials to be solved efficiently modulo a composite is shown to exist. The side information does not seem to reveal the factorization of the composite modulus. An unsolved theoretical problem in cryptology is whether there exists an algorithm for finding cube (or other odd degree) roots modulo a composite that cannot also be used to factor the composite. This section presents a solution to a variant of this problem, namely that of finding roots of certain other kinds of polynomials.

Suppose $|E(\mathbb{F}_p)| = r$ and $|E(\mathbb{F}_q)| = s$ for some primes $r$ and $s$ distinct from from $p$ and $q$. Let $m = rs$. The side information is $(m, a, b)$. Let $u \in \mathbb{Z}_n$. There is roughly a $\frac{1}{4}$ chance that $u$ is the x-coordinate of some point $P = (u, v)$ in $E(\mathbb{Z}_n)$. If $P$ exists, then there is a point $Q = (x, y)$ such that $2Q = P$. Given $x$, the point doubling formula gives $u$ as:

$$u = \lambda^2 - 2x = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x = \frac{(3x^2 + a)^2 - 8xy^2}{4y^2}$$
$$= \frac{9x^4 + 6ax^2 + a^2 - 8x^4 - 8ax^2 - 8bx}{4(x^3 + ax + b)} = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)} \quad (2)$$

The value of $u$ is a rational function of $x$, but $x$ may also be expressed as the solution to a quartic equation:

$$0 = q_u(x) = (x^4 - 2ax^2 - 8bx + a^2) - 4u(x^3 + ax + b)$$
$$= x^4 - 4ux^3 - 2ax^2 - (8b + 4ua)x + a^2 - 4ub. \quad (3)$$

On the other hand, $x$ can be computed from $u$ via the following computation. First observe that:

$$(x, y) = Q = (1/2 \mod m)P = (1/2 \mod m)(u, v). \quad (4)$$

The computation of $(1/2 \mod m)P$ is possible given the side information $(m, a, b)$ and $(u, v)$. As $v$ is not given in (3), the computation of $x$ in (4) should be done using Montgomery's exponentiation algorithm. (See §A.2.)

The relationship $P = 2Q$ can be replaced with $P = dQ$ for almost any integer $d$. This resulting polynomials have degree proportional to $d^2$, rather than being quartics.

Given the factorization of $n$, the group size $m$ can be determined from $(a, b)$ using the efficient Schoof-Elkies-Atkin (SEA) point-counting algorithm. Without the factorization, however, it seems to be harder problem, at least as hard as finding roots of polynomials such as (3). In fact, it is known that finding $m$ for random $(a, b)$ is as hard as factoring $n$, because for random $(a, b)$ and large smooth integers $s$, computing $sP$ reveals a factor $p$ of $n$ if $|E_{a,b}(\mathbb{F}_p)| \mid s$, which occurs non-negligible

probability. More generally, if $m$ can be factored, even if it is not smooth, then it may reveal the factorization of $n$. To avoid the the side information $(m, a, b)$ revealing the factorization of $n$, it must be chosen to avoid $|E_{a,b}(\mathbb{F}_p)|$ is not smooth for a factor $p$ of $n$ and preferably so that $m$ is not easy to factor. In this section, the property $m = rs$ avoids smoothness and helps to make factoring $m$ difficult.

### 2.1 Non-Triviality

The root solving algorithm in this section would be moot if the roots could be found by some trivial algorithm. For example, if roots could found among the rational numbers, then the problem could be regarded as trivial. Generally, however, the polynomials considered do not have rational roots.

For example, consider the elliptic curve $E : y^2 = x^3 - \frac{1}{4}$. Then (3) can be simplified to:

$$0 = q_u(x) = x^4 - 4ux^3 + 2x + u. \tag{5}$$

where $u$ is again an integer in $\{1, \ldots, n-1\}$. A rational root $x$ must be an integer dividing $u$. Therefore $u = cx$ for some integer $c$, and

$$x^4(1 - 4c) + x(2 + c) = 0. \tag{6}$$

Since $u \neq 0$, clearly $x$ can factored:

$$x^3 = \frac{c+2}{4c-1} \tag{7}$$

Since $x$ is an integer, $4c - 1 \mid c + 2$, which can only hold for $c \in \{-2, 0, 1\}$. More generally for (3), there are many $u$ such that $c = a^2 - 4ub$ is prime, so that a rational root must have $x \in \{-c, -1, 1, c\}$. Substitute each such choice of $x$ into $q_u(x) = 0$ to get an equation for $u$. The equation can be seen to be linear if $x \in \{-1, 1\}$ and quartic in $u$ if $x \in \{-c, c\}$. At most ten such $u$ can have $q_u(x)$ with a rational root. So, when $a^2 - 4ub$ is prime, then $q_u(x)$ has no rational roots, except in at most 10 cases, and should be non-trivial to find roots of modulo $n$.

### 2.2 Other Root Finding Algorithms

There also exist lattice-based algorithms to find roots of certain polynomials modulo a composite, such as the algorithms of Coppersmith [Cop96]. These algorithms also find nontrivial roots, in the sense the roots do not exist in the rational numbers, and they are also quite efficient. The lattice-based algorithms are more powerful than the algorithm in this section in a few respects:

- They only require the modulus $n$, so they do not require any side information.
- They can find roots of certain polynomials such as $x^3 - u$ that are of greater importance of the RSA cryptosystem.
- They extend, at least heuristically, to bivariate polynomials.

On the other, these algorithms are more limited than the algorithm of this section is two respects:

- They are limited to low-degree polynomials.
- They only find roots of low absolute value.

The two families special-purpose root-finding algorithms are somewhat incomparable. The most important difference is that the lattice-based algorithms actually lead to some attacks, albeit easily preventable ones. Both classes of algorithms suggest that the problem of finding roots of polynomials modulo a composite, especially inverting the RSA public function, is potentially an easier problem than factoring the composite.

### 2.3 On the Gap Between Finding Roots and Factoring

Algorithms for solving certain polynomial equations modulo a composite, such as finding square roots, are known to yield factoring algorithms. This is why the Rabin cryptosystem is as secure as factoring. For certain other kinds of polynomial equations, this is not known, such as computing cube roots when $\gcd(3, \phi(n)) = 1$. The polynomials $q_u$ introduced have not yet been widely studied in this context, so it is not yet clear which class of the two classes it would fall into.

A specific algorithm for finding cube roots modulo $n$ is known to reveal the factorization of $n$. The algorithm $x \mapsto x^d \mod n$ where $d \equiv 3^{-1} \mod \phi(n)$, or more specially the integer $d$, reveals the factorization of $n$. The idea is to write $3d = 2^e f$ where $f$ is odd, choose random $x$ and compute $y_0 \equiv x^f \mod n$. Then compute $y_i \equiv y_0^{2^i} \mod n$. The hope is that some $y_i \equiv 1 \mod p$ and $y_i \equiv -1 \mod q$. In theory, however, it is possible to present an algorithm that is an obfuscated version of $x \mapsto x^d \mod n$. Obfuscation may prevent $d$ from being revealed. Then it is not known how to use the algorithm as an oracle to factor $n$.

The algorithm for finding roots of $q_u(x)$ presented in this section can be regarded as giving a rational function $r(u)$ such that $q_u(r(u)) = 0$ for any $u$ corresponding to the x-coordinate of a point on the elliptic curve $E(\mathbb{F}_p)$. If the rational function could be expanded symbolically, then it may potentially lead to a factoring algorithm, much like how the symbolic expansion $x^d$ for finding cube roots reveals the factorization of $n$.

It may be the case that an oracle for finding roots of $q_u$ can be used to factor $n$. If so, any $(m, a, b)$ reveals the factorization of $n$, which slightly surprising if $m$ itself cannot be factored. If a $q_u$ root-finding oracle cannot be used to reveal the factorization of $n$, then there is a potential gap between the hardness of factoring and of finding roots of $q_u$: it is possible that the latter is easier. Generalizing, this suggests that finding roots polynomial modulo a composite is potentially easier problem than factoring. Just to be clear, however, this does not demonstrate that finding roots is easier, just that it could be easier.

The factor that $q_u(x)$ is a only quartic may have some significance in that quartics can be solved by radicals. Specifically, square roots, cube roots and rational operations can be used to solve any quartic. This suggests that, potentially, the quartic $q_u(x)$ can be arranged that its solution provides a cube root, namely the cube root that would be used to solve it. Even if this could work, it seems unlikely to be able to solve an arbitrary cube root.

## 3 Conclusion

A class of polynomial equations, some of whose roots can be found modulo a composite $n$ has been given. The roots do not exist in rationals, and are not small roots. The algorithm to find the roots uses some side information, an elliptic curve $E_{a,b}$ and its order $m = E_{a,b}(\mathbb{Z}_n)$ over $\mathbb{Z}_n$. Provided that $m$ is not easily factored, it is unclear if the side information can be used to factor $n$. This demonstrates that finding roots of certain polynomials can potentially be easier than factoring. (This was already known for small and rational roots.)

## References


[Che02] Q. Cheng, *A new class of unsafe primes*, ePrint, IACR, 2002, `http://eprint.iacr.org/2002/109`.

[Cop96] Don Coppersmith, *Finding a small root of a univariate modular equation*, Advances in Cryptology — EUROCRYPT '96 (Ueli Maurer, ed.), LNCS, no. 1070, IACR, Springer, May 1996, pp. 155–165.

[HMV04] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*, Springer, 2004.

[Len87] H. W. Lenstra, *Factoing integers with elliptic curves*, Annals of Mathematics **126** (1987), 649–673.

[Miy93] A. Miyaji, *Elliptic curves over $\mathbb{F}_p$ suitable for cryptosystems*, Advances in Cryptology: AUSCRYPT 92, LNCS, vol. 718, 1993, pp. 479–491.

[Sem98] I. A. Semaev, *Evaluation of discrete logarithms on some elliptic curves*, Math. Comp. **6** (1998), 353–356.


## A Cheng's Special-Purpose Factoring Algorithm

This section reviews Cheng's [Che02] factoring algorithm[1] The algorithm is highly specialized to find prime factors of a certain form quite quickly. The class of prime factors that can be found is so narrow that the algorithm is mainly of theoretical interest to cryptology. The two main points of interest are (a) whether it can be extended to a more general-purpose factoring algorithm, which seems unlikely, and (b) a new class of weak RSA keys that secure RSA key generation algorithms need to avoid with overwhelming probability, which is most important for special purpose RSA keys.

### A.1 How to Use Trace One Curves to Factor

The *trace* of an elliptic curve $E$ over a finite field $\mathbb{F}_p$ is the integer $t$ such that $|E(\mathbb{F}_p)| = p + 1 - t$. A trace one curve therefore has the property that

$$|E(\mathbb{F}_p)| = p. \tag{8}$$

Generally, for any prime $p$, there are integer coefficients $a$ and $b$ such that the curve $E = E_{a,b}$ : $y^2 = x^3 + ax + b$ has trace one over $\mathbb{F}_p$. More generally, there exist find rational numbers $a$ and $b$ and a certain class of primes of $p$, such that $E_{a,b}$ has trace one for half the $p$ in the class.

Consider the integer $n = pq$. Suppose an elliptic curve $E$ has trace one modulo $p$. Suppose also that $|E(\mathbb{F}_q)| \neq q$ and $p \nmid |E(\mathbb{F}_q)|$. Given any finite point $P$ on $E(\mathbb{Z}_n)$, the point $nP$ will be the point at infinity modulo $p$ and will be a finite point modulo $q$. The calculation of $nP$ will therefore involve a step of division by zero modulo $p$. When computing modulo $n$, the division by zero step will correspond to an Euclidean algorithm step for computing an inverse where the resulting GCD is $p$ instead of 1.

[1] Cheng's description uses division polynomials, while the description here uses Montgomery's algorithm, which are essentially the same.

Finding a finite point $P = (x, y)$ on $E(\mathbb{Z}_n)$ is nontrivial, because one has to solve a polynomial equation modulo a composite. However, using Montgomery's method (see [HMV04], for example), the x-coordinate of $nP$ can be efficiently computed given only the x-coordinate of $P$. For a random $x \in \{0, 1, \ldots, n-1\}$, there is approximately a $\frac{1}{4}$ chance that $x$ is the coordinate of a point on $E(\mathbb{Z}_n)$ because there is approximately a $\frac{1}{2}$ chance modulo each of $p$ and $q$.

### A.2 Example Algorithm

Some of the ideas are illustrated by providing an algorithm that finds a prime factor $p$ that is special in the sense that the elliptic curve $y^2 = x^3 - \frac{1}{4}$ has trace one over $\mathbb{F}_p$. (This includes primes of the form $p = 432s^2 + 108s + 7$.) Write the binary expansion $n = n_l 2^l + n_{l-1} 2^{l-1} + \cdots + n_0$ where $n_i \in \{0, 1\}$ and $n_l = 1$. (For simplicity, it is also assumed that $n$ is odd.)

1. Pick a random integer $x \in [0, n-1]$.
2. Set $p \leftarrow \gcd(n, 4x^3 - 1)$.
3. If $p = 1$, then
   (a) Set $(x_1, x_2) \leftarrow (x, \frac{x^4+2x}{4x^3-1} \mod n)$.
   (b) For $i$ from $l-1$ downto 0 do:
      i. Set $p \leftarrow \gcd(n, x_1 - x_2)$.
      ii. If $p = 1$ then
         A. If $n_i = 1$ then set $(x_1, x_2) \leftarrow (x_2, x_1)$.
         B. Set $(x_1, x_2) \leftarrow \left(\frac{x_1^4+2x_1}{4x_1^3-1} \mod n, \frac{2(x_1^3+x_2^3)-1}{(x_1-x_2)^2} - x - 2(x_1 + x_2) \mod n\right)$.
         C. If $n_i = 1$ then set $(x_1, x_2) \leftarrow (x_2, x_1)$.
4. If $p = 1$, go back to Step 1.
5. Output $p$.

This algorithm has been implemented in Maple. The implementation found the special factor $p$ of a 1017-bit number $pq$ in about 100 seconds.

### A.3 Constructions of Trace One Curves

Miyaji proposed [Miy93] using trace one elliptic curves for cryptography to avoid the MOV attacks, and gave some constructions using the complex multiplication (CM) method of Atkin and Morain. Semaev [Sem98] and various others then showed that using trace one curves in cryptography is insecure because the discrete logarithm problem (DLP) can be efficiently solved in these groups. Miyaji's construction of trace one curves was geared to the case where $p$ was known. In the context of factoring, of course, $p$ is unknown, which is an obstacle to the general construction. Some special cases of the construction work, however, as outlined below. Consider the ring

$$R_D = \mathbb{Z}\left[\frac{1 + \sqrt{-D}}{2}\right] \tag{9}$$

of algebraic integers. The parameter $D$ is often called the discriminant of the ring. An elliptic curve $E$ has complex multiplication by the ring $R_D$ if $\mathrm{End}(E) \cong R_D$, which is essentially equivalent

to there being a rational function $\theta : E \to E$ that has the same minimal equation as $\frac{1+\sqrt{-D}}{2}$. The type of complex multiplication can depend on the field being considered. When $p$ is known, then the field $\mathbb{F}_p$ is known. All elliptic curves over $\mathbb{F}_p$ have complex multiplication. When $p$ is unknown, however, one can still consider the field $\mathbb{Q}$ of rationals. Rarely do elliptic curves over $\mathbb{Q}$ have complex multiplication. One advantage of working over rationals, however, is that complex multiplication is usually inherited by the curve over any $\mathbb{F}_p$, even if $p$ is non known. Recall that the trace $t$ of elliptic curve $E$ over the field $\mathbb{F}_p$ is defined by $|E(\mathbb{F}_p)| = p + 1 - t$. When $E$ has complex multiplication by $R_D$, the trace satisfies:

$$4p = t^2 + Du^2 \tag{10}$$

for some integer $u$. The trace also satisfies $|t| < 2\sqrt{p}$. These conditions are enough to limit $t$ to a small set of values. In the ring $R_D$, the prime $p$ splits into two primes:

$$p = \left(\frac{t + u\sqrt{-D}}{2}\right)\left(\frac{t - u\sqrt{-D}}{2}\right) \tag{11}$$

If $D \in \{3, 11, 19, 43, 67, 163\}$, then $R_D$ has unique factorization, so the factorization (11) is unique up to units. For such $D$, the units of the ring $R_D$ are $\{1, -1\}$, except for the $R_3$ whose units are the sixth roots of unity. If

$$p = \frac{1 + Du^2}{4} \tag{12}$$

for some integer $u$, then the possible solutions for $t$ in (10) are $\{1, -1\}$ if $D \in \{11, 19, 43, 67, 163\}$. If $D = 3$, there are six solutions: $\{1, -1\}$ and four others corresponding to the other sixth roots of unity in $\mathbb{F}_p$. To summarize, an elliptic curve with complex multiplication by $R_D$ has its trace confined to a set of size two or six, including the critical case $t = 1$, when $D \in \{3, 11, 19, 43, 67, 163\}$.

Finding an elliptic curve with complex multiplication by $R_D$, without knowing $p$, can be done by working over $\mathbb{Q}$. The following elliptic curves have complex multiplication by $R_D$:

$$y^2 = x^3 + 1, \tag{13}$$
$$y^2 = x^3 - 264x + 1694, \tag{14}$$
$$y^2 = x^3 - 152x + 722, \tag{15}$$
$$y^2 = x^3 - 3440x + 77658, \tag{16}$$
$$y^2 = x^3 - 29480x + 1948226, \tag{17}$$
$$y^2 = x^3 - 8697680x + 9873093538, \tag{18}$$

for $D = 3, 11, 19, 43, 67, 163$, respectively. For random $p$ satisfying (12), the trace is one with probability about $\frac{1}{2}$ or $\frac{1}{6}$ if $D = 3$. If the trace is not one, however, the curve can modified into its twist to obtain a curve with trace one. If $D \neq 3$, a twist of $y^2 = x^3 + ax + b$ is the curve $y^2 = x^3 + ac^2x + bc^3$ for some $c$ such that $\left(\frac{c}{p}\right) = -1$. If $D = 3$, six curves form a collective twist, all of the form $y^2 = x^3 + b$. One of the curves has trace one, given (12). Setting $u = 2s + 1$ and $D = 4r - 1$ gives $r = 1, 3, 5, 11, 17, 41$, respectively, and (12) becomes $p = r + (4r - 1)(s^2 + s)$. When factoring $n = pq$, one therefore tries enough different $c$ until the trace is one modulo one factor but not the other factor. If $D \neq 3$, one can first compute $nP$ on the curve above. Either $nP$ reveals the factorization, or the trace is the same modulo $p$ and $q$, in which case one chooses a $c$ such that

$\left(\frac{c}{n}\right) = -1$ to make the traces opposite. If $D = 3$, then one just tries various $b$ until $nP$ reveals a factor. The average number of random $b$ that will be tried is about 3.6.

The ring $R_D$ has unique factorization for other values of $D$, but these do not admit trace one elliptic curves. When $R_D$ does not have unique factorization, if one knows $p$ one can construct an elliptic curve $E : y^2 = x^3 + ax + b$ with complex multiplication by $R_D$ by finding a root of the Hilbert class polynomial $H_D(t)$ over $\mathbb{F}_p$. The degree of $H_D(t)$ is the class number $h(D)$ of $R_D$, which is 1 if and only if $R_D$ has unique factorization. Given $n = pq$, one cannot find a root of $H_D(t)$ if the $h(D) > 1$, because that finding roots of nonlinear polynomials modulo a composite $n$ of unknown factorization is generally difficult. Perhaps a curve $E$ that has a complex multiplication by $R_D$ can be defined over the ring $\mathbb{Z}_n[t]/(H_D(t))$ instead of $\mathbb{Z}_n$. If so, then one would still need $p^{h(D)} = \left(1 + Du^2\right)/4$ for some $u$ to ensure a trace one curve, so the factoring algorithm will remain a very special-purpose algorithm.

### A.4 Conjectures and Generalizations

A general-purpose factoring algorithm would result from a better construction of trace one elliptic curves, that is if following can be solved:

**Problem 1.** *Find rational numbers $a$ and $b$ such that for a random prime $p$ the curve $E_{a,b} : y^2 = x^3 + ax + b$ has trace one over $\mathbb{F}_p$ with probability $\pi$ such that both $\pi$ and $1 - \pi$ are non-negligible.*

In practice, $a$ and $b$ also need to have small enough numerator and denominators to be manipulable and only primes $p$ of a size that one want to factor need to be considered. Theoretically, for any finite set of primes, one can use the CRT to find integers $a$ and $b$, albeit arbitrarily large integers, such that $E_{a,b}$ has trace one for any prime in the set.

More generally, one can try to construct hyperelliptic curves of genus $g$ whose Jacobians have $p^g$ points exactly. Indeed, one might try to generalize to other kinds of algebraic groups where the order has a chance of being a power of $p$. (Singular elliptic curves with additive reduction have order $p$, but do not help in factoring.)

This paper does not provide any justifiable speculation as to whether or not Problem 1, or its generalizations, are feasible. However, the trace satisfies $|t| < 2\sqrt{p}$ and it is not unreasonable to speculate that for most pairs $(a, b)$ that $t$ varies somewhat uniformly in this range. (Studies have shown that $t$ varies somewhat uniformly in this range when $p$ is fixed and $(a, b)$ is random.)

## B Insecure Variants of the RSA Public-Key Cryptosystem

Some insecure variants of RSA:

- Complement the public key $n$ with side information on an elliptic curve $E = E_{a,b}$ and its twist $E'$ including their orders. Create a ciphertext $\hat{x}$ from a plaintext $x$ by considering $x$ as the x-coordinate of a point $P$ on one of the elliptic curves and $\hat{x}$ computed as the x-coordinate of a scalar multiple $eP$ of $P$, where $e$ is a public parameter. A condition on $x$,

$$\left(\frac{x^3 + ax + b}{n}\right) = 1, \tag{19}$$

  ensures that $x$ corresponds to the one of the two elliptic curves. To determine whether $x$ belongs to the main curve or the twist, the encryptor can scalar multiply by the curve orders.

A message or symmetric key can be embedded in a valid plaintext by appropriately padding the message or key with various values until it is valid.

- Choose the public key $n = pq$ such that a certain elliptic curve over the rationals, such as $y^2 = x^3 - \frac{1}{4}$, has trace one over $p$. More generally, choose one or both of the primes in one of the special forms listed in §A.

These schemes are clearly insecure. The first scheme is insecure because the polynomial equation for the plaintext $x$ can be solved given the ciphertext $\hat{x}$, as shown in §2. The second scheme is insecure because $n$ can be factored, as shown in §A. These schemes are clearly artificial, however, so this work is mainly of theoretical interest to the security of RSA.