J. Cryptology (1991) 3: 187–199

Journal of Cryptology

One-Way Permutations on Elliptic Curves[1]

Burton S. Kaliski, Jr.
RSA Data Security Inc., 10 Twin Dolphin Drive,
Redwood City, CA 94065, U.S.A.
burt@rsa.com

Abstract. In recent years one-way functions have been shown to have important applications in cryptography, especially one-way functions that are also permutations. But even with the generality of this research, no function is known to be one-way and the few specific permutations believed to be one-way are all invertible in subexponential time. Elliptic curves offer new permutations that appear to require exponential time for inversion. The permutations are essentially generalizations of discrete exponentiation that rely on newly demonstrated correspondences between elements of elliptic curves and the integers.

Key words. Cryptography, Discrete logarithms, Elliptic curves, One-way functions.

1. Introduction

One-way functions have been shown in recent years to have important applications in cryptography, including various cryptosystems and secure pseudorandom number generators. Indeed, modern cryptography is based on the assumption that one-way functions exist [9]. For example, Impagliazzo *et al.* have shown [13], following work by a number of researchers [5], [29], [20], [6], [10], [11], that if there is a one-way function, then there is a secure pseudorandom number generator, and conversely. One-way functions that are also permutations are of particular interest [14].

As far as specific permutations believed to be one-way are concerned, however, there are relatively few, among them discrete exponentiation modulo a prime, squaring modulo a Blum integer [25], [4], and the RSA function [26]. All three functions can be inverted in probabilistic subexponential time: discrete exponentiation by methods of Adleman [1] and others [8], [24]; squaring and RSA by integer factorization methods [19], [18], [24].

[1] Date received: March 22, 1989. Date revised: August 20, 1990. Support for this research was provided in part by the National Science Foundation under Contract Number MCS-8006938. A preliminary version appeared as part of an MIT Ph.D. thesis [16]. Part of this work was done while the author was visiting Rochester Institute of Technology.

Given that the permutations are all invertible in probabilistic subexponential time, a natural question arises: *Are there permutations that are not invertible in subexponential time?*

Progress toward an answer was made in 1985 by Miller [22], who argued that the elliptic curve analog of discrete exponentiation mod p is not vulnerable to an analog of Adleman's subexponential-time algorithm, and consequently that the most efficient algorithm yet known for inverting it is just D. Shanks' generic "baby-step giant-step" method. Shanks' method can be applied to any finite commutative group and has time complexity $O(n^{1/2+o(1)})$ where n is the order of the group. In general this is exponential in $\log n$. Pohlig and Hellman's improvement based on factoring the order n can also be applied [23], but the running time is still exponential in general.

This paper presents further progress by constructing a permutation based on elliptic curves that is at least as hard to invert as elliptic curve exponentiation. As a result, assuming Miller's arguments, the answer to the question is yes: there are permutations that cannot be inverted in subexponential time.

As this paper was going to production, Menezes and Vanstone announced a subexponential-time algorithm for inverting the permutations involving one elliptic curve described in Section 3 [21]. Their algorithm is based on a reduction from inverting elliptic curve exponentiation to inverting exponentiation in a finite field. The permutations on two elliptic curves described in Section 4 still appear to require exponential time to invert, however, as the finite field in Menezes and Vanstone's method has an exponentially large extension degree in general.

1.1. *Related Work*

Elliptic curves have received a great deal of attention among computer scientists since Lenstra's discovery in 1985 of a factorization algorithm based on elliptic curves [19]. At about the same time Schoof gave a deterministic polynomial-time algorithm for computing the order of an elliptic curve [27]. Miller [22] and Koblitz [17] then independently proposed elliptic curve analogs of cryptosystems based on discrete exponentiation, and Chudnovsky and Chudnovsky gave, among other things, some particularly efficient implementations of elliptic curve operations [7].

In 1986 Goldwasser and Kilian showed how to use elliptic curves to obtain in expected polynomial time a proof of primality for almost any given prime number p [12]. This suprising application is in contrast with previous algorithms that obtain proofs of compositeness. Adleman and Huang subsequently improved Goldwasser and Kilian's result using hyperelliptic curves, showing how to obtain a proof of primality for *any* prime [2].

My interest in elliptic curves was to generalize Blum and Micali's pseudorandom number generator [5] to elliptic curves [15], [16]. In the process I found that I had in fact constructed a new candidate one-way permutation. The one-way permutation implies the pseudorandom number generator, so the permutation appears to be the important result.

Many of these applications of elliptic curves are described in a forthcoming survey [18].

1.2. *Organization*

This article consists of six sections: the introduction; Section 2, elliptic curves; Section 3, permutations involving one elliptic curve; Section 4, permutations involving two elliptic curves; Section 5, on finding cyclic elliptic curves and elements of maximum order; and Section 6, conclusion.

2. Elliptic Curves

The following can be found in Silverman's textbook [28].

2.1. *Definition*

An *ellitpic curve* mod p is defined by a congruence

$$y^2 \equiv x^3 + ax + b \mod p,$$

where p is a prime, $p > 3$, and $4a^3 + 27b^2 \not\equiv 0 \bmod p$. (For $p = 2$ or 3 the congruence takes a different form.) The *elements* of the elliptic curve are the solutions (x, y) to the congruence together with an identity element O.

2.2. *Composition, Exponentiation, and Logarithm*

The elements of an elliptic curve form a commutative group under a composition operation called "chords and tangents." Consider the line connecting two elements (x_1, y_1) and (x_2, y_2). If the elements are distinct, then the line is a chord with slope $m = (y_2 - y_1)/(x_2 - x_1)$; if the elements are identical, it is a tangent with slope $m = (3x_1^2 + a)/(2y_1)$. If the slope of the line is finite, then there is a third element (x_3, y_3) also on this line, where the coordinates x_3 and y_3 satisfy

$$x_3 = m^2 - x_1 - x_2,$$

$$y_3 = y_1 + m(x_3 - x_1).$$

The reflection across the x-axis of this third element, i.e., $(x_3, -y_3)$, is the composition of (x_1, y_1) and (x_2, y_2). If the slope of the line is infinite, then the composition of (x_1, y_1) and (x_2, y_2) is the identity and the elements are inverses.

Exponentiation is just repeated composition. The ith power (or multiple) of an element G is denoted by $[i]\,G$. *Logarithm* is the inverse of exponentiation.

Without fast arithmetic algorithms, the time complexity of composition is $O((\log p)^2)$ bit operations and the time complexity of exponentiation is $O((\log p)^2 \log i)$ bit operations. Both can be improved by a constant factor in a projective coordinate system, since composition can be performed in such a system without mod p division. Chudnovsky and Chudnovsky discuss this in more detail [7].

2.3. *Order and Group Structure*

By a theorem of Hasse, the *order* or number of elements n of an elliptic curve mod p satisfies the inequality

$$|n - (p + 1)| \leq 2p^{1/2}.$$

An elliptic curve mod p is isomorphic either to the additive group $(\mathbf{Z}/n\mathbf{Z})$ (in which case it is cyclic) or to the product of two additive groups $(\mathbf{Z}/n_1\mathbf{Z})(\mathbf{Z}/n_2\mathbf{Z})$ where n_2 divides n_1 (in which case it is noncyclic). In the noncyclic case, n_2 also divides $p - 1$.

The 2-primary component of an elliptic curve is of particular interest. Since an element has order 2 if and only if its y-coordinate is 0, the number of such elements equals the number of solutions to the congruence

$$x^3 + ax + b \equiv 0 \mod p.$$

The 2-primary component is thus null, cyclic, or noncyclic, depending on whether the congruence has 0, 1, or 3 solutions.

3. Permutations Involving One Elliptic Curve

The permutations involving one elliptic curve are based on a generalization of elliptic curve exponentiation and a one-to-one correspondence l between elements and integers. The permutations take the form

$$f(i) = l([i]G),$$

where G is an element of an elliptic curve. The following conditions are sufficient for such a function f to be a permutation on the set $\{0, \ldots, n - 1\}$, where n is the order of the elliptic curve:

- the elliptic curve is cyclic;
- the element G has maximum order; and
- the function l is one-to-one from the elliptic curve to the set $\{0, \ldots, n - 1\}$.

The difficult part is finding a one-to-one function l that can be computed efficiently. In two cases of elliptic curve, this can be done in a straightforward manner. The cases are

1. $y^2 \equiv x^3 + b \mod p$ for $p \equiv 2 \mod 3$; and
2. $y^2 \equiv x^3 + ax \mod p$ for $p \equiv 3 \mod 4$ and $(a/p) = 1$.

Inverting the permutation f is at least as hard as inverting exponentiation, assuming l can be computed efficiently, since

$$f^{-1}(l(X)) = \log_G X.$$

The correspondences l defined in this section have the additional property of being efficiently (and deterministically) invertible. As such they can be used to embed messages in elements of elliptic curves in any of the elliptic curve cryptosystems discussed by Miller [22] and Koblitz [17].

3.1. *The Case* $y^2 \equiv x^3 + b \mod p$, $p \equiv 2 \mod 3$

In this case of multiplicative group mod p has the following property which is essential to a straightforward construction:

Cube roots mod p exist and are unique when $p \equiv 2 \mod 3$.

This property leads to the following three lemmas about the elliptic curves.

Lemma 3.1. *The order of the elliptic curve* $y^2 \equiv x^3 + b \bmod p$ *where* $p \equiv 2 \bmod 3$ *is* $p + 1$.

Proof. Since cube roots exist and are unique, every value y determines exactly one solution $((y^2 - b)^{1/3}, y)$ to the congruence. Thus there are p solutions and $p + 1$ elements including the element O. □

Lemma 3.2. *The elliptic curve* $y^2 \equiv x^3 + b \bmod p$ *where* $p \equiv 2 \bmod 3$ *is cyclic.*

Proof. Suppose the elliptic curve were noncyclic. Then the l-primary component of the elliptic curve, for some l, would be noncyclic. By the group structure properties of elliptic curves, such an l would divide both $p - 1$ and the order $p + 1$ of the elliptic curve, so it would be 2. But the 2-primary component is cyclic, as the congruence $x^3 + b \equiv 0 \bmod p$ has only one solution, $x \equiv -b^{1/3}$. Thus the elliptic curve is cyclic. □

Lemma 3.3. *The function* l *defined as*

$$l((x, y)) = y,$$
$$l(O) = p$$

is one-to-one from the elliptic curve $y^2 \equiv x^3 + b \bmod p$ *where* $p \equiv 2 \bmod 3$ *to the set* $\{0, \ldots, p\}$.

Proof. Since every value y determines exactly one solution, the inverse of l is well defined:

$$l^{-1}(w) = ((w^2 - b)^{1/3}, w) \qquad \text{if} \quad 0 \le w < p,$$
$$l^{-1}(p) = O.$$

Thus l is one-to-one. □

(The inverse of l can be computed deterministically using the relationship

$$(w^2 - b)^{1/3} \equiv (w^2 - b)^{(2p-1)/3} \mod p,$$

since $(2p - 1)/3$ is an integer for $p \equiv 2 \bmod 3$.)

Lemmas 3.1–3.3 lead to the following theorem.

Theorem 1. *Let* p *be a prime congruent to* 2 mod 3, *let* b *be an integer between* 1 *and* $p - 1$, *and let* G *be an element of maximum order on the elliptic curve*

$$y^2 \equiv x^3 + b \mod p.$$

Then the function

$$f(i) = l([i]G),$$

where

$$l((x, y)) = y,$$

$$l(O) = p$$

is a permutation on the set $\{0, \ldots, p\}$.

Proof. By Lemma 3.1 the order of the elliptic curve is $p + 1$. The conditions sufficient for the function f to be a permutation are satisfied as follows:

- by Lemma 3.2, the elliptic curve is cyclic;
- by assumption, the element G has maximum order; and
- by Lemma 3.3, the function l is one-to-one. □

3.2. *The Case* $y^2 \equiv x^3 + ax \bmod p$, $p \equiv 3 \bmod 4$, $(a/p) = 1$

In this case, the following property is essential:

The element -1 is a quadratic nonresidue mod p when $p \equiv 3 \bmod 4$.

This property leads to the following three lemmas.

Lemma 3.4. *The order of the elliptic curve* $y^2 \equiv x^3 + ax \bmod p$ *where* $p \equiv 3 \bmod 4$ *and* $(a/p) = 1$ *is* $p + 1$.

Proof. Since -1 is a quadratic nonresidue, every pair of nonzero values x and $-x$ determines exactly two solutions: either

- $(x, (x^3 + ax)^{1/2})$ and $(x, -(x^3 + ax)^{1/2})$ if $((x^3 + ax)/p) = 1$; or
- $(-x, (-x^3 - ax)^{1/2})$ and $(-x, -(-x^3 - ax)^{1/2})$ if $((x^3 + ax)/p) = -1$.

The congruence $x^3 + ax \equiv 0 \bmod p$ has only one solution, $x \equiv 0$, since a is a quadratic residue and $-a$ is thus a quadratic nonresidue. Thus the value $x = 0$ determines exactly one solution $(0, 0)$. The number of solutions to the congruence is p and the number of elements is $p + 1$. □

Lemma 3.5. *The elliptic curve* $y^2 \equiv x^3 + ax \bmod p$ *where* $p \equiv 3 \bmod 4$ *and* $(a/p) = 1$ *is cyclic.*

Proof. As in Lemma 3.2, if the elliptic curve were noncyclic, then the 2-primary component would be noncyclic. But the 2-primary component is cyclic, as the congruence $x^3 + ax \equiv 0 \bmod p$ has only one solution, $x \equiv 0$. Thus the elliptic curve is cyclic. □

Lemma 3.6. *The function* l *defined as*

$$l((x, y)) = x \quad \text{if} \quad y > 0,^2$$

$$l((x, y)) = -x \quad \text{if} \quad y < 0,$$

$$l((0, 0)) = 0,$$

[2] Read "$y > 0$" as "$0 < y \leq (p - 1)/2$" and "$y < 0$" as "$(p + 1)/2 \leq y \leq p - 1$."

and

$$l(O) = p$$

is one-to-one from the elliptic curve $y^2 \equiv x^3 + ax \bmod p$ *where* $p \equiv 3 \bmod 4$ *and* $(a/p) = 1$ *to the set* $\{0, \ldots, p\}$.[3]

Proof. Since every pair of nonzero values x and $-x$ determines exactly two solutions, the inverse of l is well defined:

$$l^{-1}(w) = (w, (w^3 + aw))^{1/2} \quad \text{if} \quad ((w^3 + aw)/p) = 1, \quad 0 < w < p,$$

$$l^{-1}(w) = (-w, -(w^3 + aw))^{1/2} \quad \text{if} \quad ((w^3 + aw)/p) = -1, \quad 0 < w < p,$$

$$l^{-1}(0) = (0, 0),$$

and

$$l^{-1}(p) = O.$$

(Here $(w^3 + aw)^{1/2}$ is the "positive" square root of $w^3 + aw$.) Thus l is one-to-one. □

(The inverse of l can be computed deterministically using the relationship

$$(w^3 + aw)^{1/2} \equiv (w^3 + aw)^{(p+1)/4} \bmod p,$$

since $(p + 1)/4$ is an integer for $p \equiv 3 \bmod 4$.)

Lemmas 3.4–3.6 lead to the following theorem.

Theorem 2. *Let* p *be a prime congruent to* 3 mod 4, *let* a *be an integer between* 1 *and* $p - 1$ *with Legendre symbol* $(a/p) = 1$, *and let* G *be an element of maximum order on the elliptic curve*

$$y^2 \equiv x^3 + ax \bmod p.$$

Then the function

$$f(i) = l([i]G),$$

where

$$l((x, y)) = x \quad \text{if} \quad y > 0,$$

$$l((x, y)) = -x \quad \text{if} \quad y < 0,$$

$$l((0, 0)) = 0,$$

and

$$l(O) = p$$

is a permutation on the set $\{0, \ldots, p\}$.

---

[3] P. G. Anderson suggests another definition:

$$l((x, y)) = x \quad \text{if} \quad (y/p) = 1,$$

$$l((x, y)) = -x \quad \text{if} \quad (y/p) = -1,$$

$$l((0, 0)) = 0,$$

and

$$l(O) = p.$$

Proof. By Lemma 3.4, the order of the elliptic curve is $p + 1$. The conditions sufficient for the function f to be a permutation are satisfied as follows:

- by Lemma 3.5, the elliptic curve is cyclic;
- by assumption, the element G has maximum order; and
- by Lemma 3.6, the function l is one-to-one. □

4. Permutations Involving Two Elliptic Curves

In cases of elliptic curve other than those considered in Section 3, there does not seem to be a straightforward correspondence between only one elliptic curve and the integers. Permutations in general involve one-to-one correspondences l and l' between elements of *two* elliptic curves and integers. The two elliptic curves are related by *twisting*: they are isomorphic over a quadratic extension of mod p, though not over mod p itself. Specifically, the permutations take the form

$$f(i) = l([i]G) \quad \text{if} \quad 0 \le i < n,$$
$$f(i) = l'([i]G') \quad \text{if} \quad n \le i < n + n',$$

where G is an element on one elliptic curve, G' is an element on the other, and n and n' are the orders of the elliptic curves.

The following conditions are sufficient for the function f to be a permutation on the set $\{0, \ldots, n + n' - 1\}$:

- both elliptic curves are cyclic;
- both elements G and G' have maximum order on their respective elliptic curves; and
- both functions l and l' are one-to-one from their respective elliptic curves to the set $\{0, \ldots, n + n' - 1\}$, and their ranges are nonintersecting.

Inverting the permutation f is at least as hard as inverting exponentiation on one of the elliptic curves, since

$$f^{-1}(l(X)) = \log_G X$$

and

$$f^{-1}(l'(X')) \bmod n' = \log_{G'} X'.$$

The following two lemmas show the properties of elliptic curves related through twisting.

Lemma 4.1. *The elliptic curves*

$$E: \quad y^2 \equiv x^3 + ax + b \mod p,$$
$$E': \quad y^2 \equiv x^3 + au^2x + bu^3 \mod p,$$

where u is a quadratic nonresidue mod p, *together have order* $2p + 2$.

Proof. Since u is a quadratic nonresidue mod p, every pair of values x and ux determine exactly two solutions, total, to the congruences E and E': either

- $(x, (x^3 + ax + b)^{1/2})$ and $(x, -(x^3 + ax + b)^{1/2})$ on E if $((x^3 + ax + b)/p) = 1$; or
- $(x, 0)$ on E and $(ux, 0)$ on E' if $((x^3 + ax + b)/p) = 0$; or
- $(ux, (u^3(x^3 + ax + b))^{1/2})$ and $(ux, -(u^3(x^3 + ax + b))^{1/2})$ on E' if $((x^3 + ax + b)/p) = -1$.

Thus there are $2p$ solutions, total, and $2p + 2$ elements. □

Lemma 4.2. *The function l defined as*

$$l((x, y)) = (ux \bmod p) \quad \text{if} \quad y \geq 0,$$

$$l((x\ y)) = (ux \bmod p) + p + 1 \quad \text{if} \quad y < 0,$$

$$l(O) = p$$

is one-to-one from the elliptic curve

$$E: \quad y^2 \equiv x^3 + ax + b \mod p$$

to the set $\{0, \ldots, 2p + 1\}$, the function l' defined as

$$l'((x', y')) = x' \quad \text{if} \quad y' > 0,$$

$$l'((x', y')) = x' + p + 1 \quad \text{if} \quad y' \leq 0,$$

$$l'(O') = 2p + 1$$

is one-to-one from the elliptic curve

$$E': \quad y^2 \equiv x^3 + au^2x + bu^3 \mod p,$$

where u is a quadratic nonresidue mod p *to the set $\{0, \ldots, 2p + 1\}$, and the ranges of the functions are nonintersecting.*

Proof. The functions l and l' are clearly one-to-one. Suppose their ranges intersected. Then there would be elements (x, y) on E and (x', y') on E' such that $l((x, y)) = l'((x', y'))$. By definition of l and l', ux would equal x' mod p, and y and y' would not both be zero. Thus by definition of the elliptic curves, u^3y^2 would equal $(y')^2$, so u^3 would be a quadratic residue. But u^3 is not a quadratic residue. Thus the ranges of l and l' are nonintersecting. □

Lemmas 4.1 and 4.2 lead to the following theorem, stated without proof.

Theorem 3. *Let p be a prime, let a and b be integers between 0 and $p - 1$ such that $4a^3 + 27b^2 \not\equiv 0 \bmod p$, let u be an integer between 1 and $p - 1$ with Legendre symbol $(u/p) = -1$, let G be an element of maximum order on the elliptic curve*

$$E: \quad y^2 \equiv x^3 + ax + b \mod p,$$

and let G' be an element of maximum order on the elliptic curve

$$E': \quad y^2 \equiv x^3 + au^2x + bu^3 \mod p.$$

If both elliptic curves E and E' are cyclic, then the function

$$f(i) = l([i]G) \quad \text{if} \quad 0 \leq i < n,$$

$$f(i) = l'([i]G') \quad \text{if} \quad n \leq i < 2p + 2,$$

where

$$l((x, y)) = (ux \bmod p) \quad \text{if} \quad y \geq 0,$$
$$l((x, y)) = (ux \bmod p) + p + 1 \quad \text{if} \quad y < 0,$$
$$l(O) = p$$

and

$$l'((x', y')) = x' \quad \text{if} \quad y' > 0,$$
$$l'((x', y')) = x' + p + 1 \quad \text{if} \quad y' \leq 0,$$
$$l'(O) = 2p + 1$$

is a permutation on the set $\{0, \ldots, 2p + 1\}$.

5. On Finding Cyclic Elliptic Curves and Elements of Maximum Order

A very important issue related to the permutations on elliptic curves is finding cyclic elliptic curves and elements of maximum order efficiently. There seem to be at least three methods for this:

1. Choose only elliptic curves that are always cyclic and whose order is trivially determined, and apply a generalization of Blum and Micali's algorithm [5] for finding primes and elements of maximum order in a multiplicative group. Briefly, their algorithm uses a result of Bach [3] to select a factored integer n at random, a standard primality test to determine whether $p = n + 1$ is prime, and then a standard order-computation algorithm to determine whether an element selected at random has maximum order. The algorithm is easily generalized to the two cases of elliptic curve in Section 3 (setting $p = n - 1$).
2. Choose only elliptic curves whose order is prime or the product of a large prime and a small square free integer (such elliptic curves are always cyclic), and use a standard order-computation algorithm to determine whether an element selected at random has maximum order. This is essentially the approach Miller [22] and Koblitz [17] take. Such elliptic curves are not hard to find if the prime p is selected uniformly at random. However, it is not clear that pairs of such elliptic curves related by twisting are easy to find unless one makes assumptions on the distribution of prime numbers. Moreover, the orders of the elliptic curves are in general not trivially determined, and the fastest algorithm known for computing order [27], although polynomial time, is not very practical.
3. Choose any elliptic curve and use a partial factorization of the order n to determine (possibly incorrectly) whether an element selected at random has order n, thereby showing that the element has maximum order and that the elliptic curve is cyclic. This is also effective for pairs of elliptic curves related by twisting. However, since the orders of elliptic curves are in general not trivially determined, the method is again not very practical. The importance of this method is its generality. This is the approach taken in [16].

The third method is based on the observation that the standard algorithm for computing order, if given only a partial factorization of the order n of a cyclic group, would still be correct for many elements. In particular, each unknown prime factor l of n affects a fraction at most $1/l$ of the elements. Thus if all prime factors of n up to a bound b could somehow be determined, then the fraction of elements whose order would not be computed correctly would be at most $(\log_b n)/b$, since there would be at most $\log_b n$ unknown factors.

The bound b is also important in determining whether the elliptic curve is cyclic. If any l-primary component of the elliptic curve were noncyclic but the prime factor l were unknown, then the standard algorithm for computing order, given a partial factorization, would be incorrect for many elements. However, the fraction of elliptic curves mod p whose l-primary component is noncyclic has been shown by Lenstra [19] (in proving something else) to be

$$\begin{cases} 1/l(l^2-1) + O(p^{-1/2}) & \text{if } p-1 \text{ is divisible by } l; \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

If all prime factors of the order of an elliptic curve mod p up to a bound b could somehow be determined, then the fraction of elliptic curves with an unknown noncyclic primary component would be at most $(\log_b p)/(b(b^2-1)) + O((\log_b p)p^{-1/2})$.

How large can be bound b be made in polynomial time? Trial-and-error factorization of the order n is not practical since the number of operations is proportional to the bound. An alternative, but one which is really still impractical, is Lenstra's algorithm [19], which has the property that the number of operations depends primarily on the prime factor and not on the number being factored. This property has been used to speed up other factorization methods [24]. Under reasonable assumptions Lenstra's algorithm can find small prime factors much faster than trial and error. Nevertheless, there may be some factors that Lenstra's algorithm cannot find, which would increase the probability of falsely accepting a noncyclic elliptic curve or an element not of maximum order.

Finally, even if the methods described are efficient and correct, are there enough cyclic elliptic curves and elements of maximum order? Blum and Micali's observation [5] that the fraction of elements of maximum order in a cyclic group of order n is $1/O(\log \log n)$ provides part of the answer. The other part is provided by the following lemma and corollary.

Lemma 5.1. *The fraction of elliptic curves* mod p *that are cyclic is at least* $0.7785 - o(1)$.

Proof. The fraction of elliptic curves mod p that are noncyclic is at most the sum over all primes l of the fraction of curves whose l-primary component is noncyclic. Applying equation (1) and observing that $p-1$ has at most $\log p$ prime factors, the fraction is at most

$$\left(\sum_{l \text{ prime}} 1/l(l^2-1)\right) + O((\log p)p^{-1/2}) \approx 0.2214 + o(1).$$

The result follows. □

Corollary. *The fraction of pairs of elliptic curves* mod *p related by twisting, both of which are cyclic, is at least* $0.5570 - o(1)$.

Proof. This follows from a straightforward counting argument. □

6. Conclusion

New permutations on elliptic curves which appear to require probabilistic exponential time to invert have been constructed.

Some open problems remain:

- Are there permutations other than those given that involve only one elliptic curve?
- Are there algorithms for finding pairs of cyclic elliptic curves related by twisting, and elements of maximum order, that are more efficient than the one given in Section 5? Perhaps Atkin's improvement to Goldwasser and Kilian's method of proving primality would be helpful here (see [18]).
- Are there permutations that require probabilistic exponential time to invert but only quadratic time to compute? This is of particular interest because without fast arithmetic algorithms the time complexity of the permutations on elliptic curves is cubic, so for a given number of operations required to invert a permutation, other permutations (e.g., squaring modulo a Blum integer) may require fewer operations to compute.

Acknowledgments

I wish to thank R. L. Rivest, S. Goldwasser, and S. Micali for their supervision and reading of the Ph.D thesis that led to these results; V. Miller for his many suggestions, including the twisting isomorphism; B. Chor and O. Goldreich for motivating discussions; and the referees for helpful criticism. I also wish to thank R. S. Czernikowski of Rochester Institute of Technology and J. Bidzos of RSA Data Security for their support. Finally, I consider all my work in relation to the following exhortation: "Whatever you do, do all to the glory of God" (I Cor. 10:31).

References

[1] L. Adleman, A subexponential algorithm for the discrete logarithm problem with applications to cryptography, *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, IEEE, New York, 1979, pp. 55–60.

[2] L. Adleman and M. Huang, Recognizing primes in random polynomial time, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, ACM, New York, 1987, pp. 462–470.

[3] E. Bach, How to generate factored random numbers, *SIAM Journal on Computing*, vol. 17 (1988), pp. 179–193. Previously appeared in *Proceedings of the 15th Annual ACM Symposium on Theory of Computing*, ACM, New York, 1983, pp. 184–188.

[4] M. Blum, Coin flipping by telephone, *Proceedings of IEEE Spring COMPCON*, 1982, pp. 133–137.

[5] M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudo-random bits, *SIAM Journal on Computing*, vol. 13 (1984), pp. 850–864. Previously appeared in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, IEEE, New York, 1982, pp. 112–117.

[6] R. Boppana and R. Hirschfeld, Pseudorandom generators and compexity classes, *Advances in Computing Research*, vol. 5 (1989), pp. 1–26.

[7] D. V. Chudnovsky and G. V. Chudnovsky, Sequences of numbers generated by additions in formal groups and new primality and factorization tests, *Advances in Applied Mathematics*, vol. 7 (1986), pp. 385–434.

[8] D. Coppersmith, A. M. Odlyzko, and R. Schroeppel, Discrete logarithms in GF(p), *Algorithmica*, vol. 1 (1986), pp. 1–15.

[9] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, vol. 22 (1976), pp. 644–654.

[10] O. Goldreich, H. Krawczyk, and M. Luby, On the existence of pseudorandom generators, *Proceedings of the 29th Annual Symposium on Foundations of Computer Science*, IEEE, New York, 1988, pp. 12–24.

[11] O. Goldreich and L. Levin, A hard-core predicate for all one-way functions, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, ACM, New York, 1989, pp. 25–32.

[12] S. Goldwasser and J. Kilian, Almost all primes can be quickly certified, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, ACM, New York, 1986, pp. 316–329.

[13] R. Impagliazzo, L. Levin, and M. Luby, Pseudo-random generation from one-way functions, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, ACM, New York, 1989, pp. 12–24.

[14] R. Impagliazzo and S. Rudich, Limits on the provable consequences of one-way permutations, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, ACM, New York, 1989, pp. 44–61.

[15] B. S. Kaliski Jr., A pseudo-random bit generator based on elliptic logarithms, *Advances in Cryptology: Proceedings of Crypto '86* (Lecture Notes in Computer Science, vol. 263), Springer-Verlag, New York, 1987, pp. 84–103.

[16] B. S. Kaliski, Jr., Elliptic Curves and Cryptography: A Pseudorandom Bit Generator and Other Tools, Ph.D. thesis, MIT/LCS/TR-411, Department of EECS, MIT, Cambridge, MA, 1988.

[17] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, vol. 48 (1987), pp. 203–209.

[18] A. K. Lenstra and H. W. Lenstra, Jr., Algorithms in number theory, in J. van Leeuwen, ed., *Handbook of Theoretical Computer Science*, vol. A, *Algorithms and Complexity*, Elsevier, Amsterdam, and MIT Press, Cambridge, MA, 1990, pp. 673–715.

[19] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Annual of Mathematics*, vol. 126 (1987), pp. 649–673.

[20] L. Levin, One-way functions and pseudorandom generators, *Combinatorica*, vol. 7 (1987), pp. 357–363. Previously appeared in *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, ACM, New York, 1985, pp. 363–365.

[21] A. Menezes and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, talk presented at Crypto '90 (Santa Barbara, CA, August 12–15, 1990).

[22] V. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology: Proceedings of Crypto '85* (Lecture Notes in Computer Science, vol. 218), Springer-Verlag, New York, 1986, pp. 417–426.

[23] S. C. Pohlig and M. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, *IEEE Transactions on Information Theory*, vol. 24 (1978), pp. 106–110.

[24] C. Pomerance, Fast, rigorous factorization and discrete logarithm algorithms, in D. S. Johnson *et al.*, eds., *Discrete Algorithms and Complexity (Kyoto, 1986)* (Perspectives in Computing, vol. 15), Academic Press, Boston, 1987, pp. 119–143.

[25] M. O. Rabin, Digital Signatures and Public Key Functions as Intractable as Factorization, MIT/LCS/TR-212, MIT, Cambridge, MA, 1979.

[26] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol. 21 (1978), pp. 120–126.

[27] R. J. Schoof, Elliptic curves over finite fields and the computation of square roots and mod p, *Mathematics of Computation*, vol. 44 (1985), pp. 483–494.

[28] J. Silverman, *The Arithmetic of Elliptic Curves* (Graduate Texts in Mathematics, vol. 106), Springer-Verlag, New York, 1986.

[29] A. Yao, Theory and applications of trapdoor functions, in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, IEEE, New York, 1982, pp. 80–91.