ZETA FUNCTIONS, ONE–WAY FUNCTIONS, AND PSEUDORANDOM NUMBER GENERATORS

Michael Anshel
Department of Computer Sciences, City College of New York,
New York, NY 10031

Dorian Goldfeld
Department of Mathematics, Columbia University
New York, NY 10027

Abstract. New candidate one–way functions which arise from the intractable problem of determining a zeta function from its initial Dirichlet coefficients are presented. This intractable problem appears to be totally unrelated to the well known intractable problems of integer factorization and the computation of discrete logarithms. We introduce the feasible Selberg class of zeta functions and focus on three special subclasses: $\mathcal{Z}_{\text{Kronecker}}$ = Dirichlet L-functions with real characters, $\mathcal{Z}_{\text{Elliptic}}$ = L–functions of elliptic curves, and $\mathcal{Z}_{\text{Artin}}$ = Artin L-functions. It is shown that the reduction (mod 2) map on the Dirichlet coefficients of $\mathcal{Z}_{\text{Elliptic}}$ induces a map $\mathcal{Z}_{\text{Elliptic}} \to \mathcal{Z}_{\text{Artin}}$. The assumption that it is not feasible (in polynomial time) to determine an Artin L–function from its initial Dirichlet coefficients leads to a new pseudorandom number generator. These results are interpreted in various cryptographic settings by employing the Eisenstein–Jacobi law of cubic reciprocity.

Key Words: Zeta function, One–way function, Pseudorandom number generator, Elliptic curve, Frobenius element, Cubic reciprocity law, Feasible Selberg class.

§1. Introduction:

A central problem in cryptography is to establish the existence of one–way functions. Such a function would have the property that while it is computable in polynomial time, its inverse is not. One approach to this problem is to construct candidate one–way functions from seemingly intractable problems in number theory. We introduce a new intractable problem arising from the theory of zeta functions which leads to a new class of one–way functions based on the arithmetic theory of zeta functions. Moreover, there appears to be no relation between this problem and other intractable problems such as integer factorization and the computation of discrete logarithms where known attacks have emerged in recent years (see [22, 26]). At present the authors are unaware of any methods at all that would provide an attack on our candidate one–way functions.

It is a consequence of the main theorem of [12] that a 1–1 one–way function implies the existence of a pseudorandom number generator. The construction of such pseudorandom number generators, however, is computationally intensive. In our case we explicitly construct from a given elliptic curve a pseudorandom number generator $\mathrm{PNG}_{\mathrm{Elliptic}}$ which can be computed very efficiently and at low computational cost. Under the assumption that two different classes of zeta functions (the elliptic class and the Artin class, to be defined below) give rise to one–way functions, we prove that an elliptic curve satisfying certain hypotheses implies the existence of such a pseudorandom number generator. In this regard, the second author would like to take this opportunity to thank Fred Diamond for many helpful discussions concerning ℓ–adic representations.

§2. One–way Functions and the Feasible Selberg Class

Let $n \geq 0$ be an integer and define

$$d_2(n) = \begin{cases} \lfloor \log_2 n \rfloor + 1, & \text{if } n > 0 \\ 1, & \text{if } n = 0. \end{cases}$$

where for an arbitrary real number $x \geq 0$, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. We refer to $d_2(n)$ as the bit size of n. We extend this notion to non–negative integral vectors by defining the norm $||(n_1, n_2, \dots, n_t)||$ of a vector $(n_1, n_2, \dots, n_t) \in \mathbb{N}^t$ as

$$||(n_1, n_2, \dots, n_t)|| = \sum_{i=1}^{t} d_2(n_i).$$

Fix positive rational integers r, s. A function

$$f : \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

is a one–way function provided the following three conditions hold.

(2.1) *There exists an integer $k > 0$ such that*

$$||\vec{n}||^{\frac{1}{k}} \leq ||f(\vec{n})|| \leq ||\vec{n}||^k$$

for $\vec{n} = (n_1, n_2, \dots, n_r) \in \mathbb{N}^r$.

(2.2) *$f(\vec{n})$ can be computed in polynomial time in $||\vec{n}||$.*

(2.3) *Given $m \in \mathbb{N}^s$, there does not exist a polynomial time algorithm which either computes a vector $\vec{n} \in \mathbb{N}^r$ such that $f(\vec{n}) = \vec{m}$ or indicates that no such value exists.*

Condition (2.1) says that $f(\vec{n})$ is neither polynomially longer or shorter than $\vec{n}$. Currently, there is no guarantee that one–way functions exist even if $P \neq NP$. Certain candidate one–way functions associated with factorization, exponentiation modulo a prime, and discrete logarithms, etc. have been proposed. We introduce new candidate one–way functions based on a seemingly intractable problem in the theory of zeta functions. Our

candidate one–way functions arise from a very general class of zeta functions, the feasible Selberg class, which we now define.

In order to specify our intractable problem we axiomatically define a class, $\mathcal{Z}$, of zeta functions; the feasible Selberg class (defined from [23]). Every zeta function $Z(s) \in \mathcal{Z}$ is given by a Dirichlet series

$$Z(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}, \qquad a(n) \in \mathbb{C}$$

which is absolutely convergent in some half-plane $\mathrm{Re}(s) \gg 1$. We further assume that $Z(s)$ is a meromorphic function of a single complex variable s which satisfies the following hypotheses:

(2.4) *$a(n) = O(n^C)$ for some constant $C > 0$ independent of n.*

(2.5) *$\log \mathcal{Z}(s) = \sum_n b(n) \cdot n^{-s}$, where $b(n) = 0$ unless $n = p^r$, a positive prime power.*

(2.6) *Given a prime power p^r, $\exists$ an algorithm to compute $b(p^r)$ in polynomial time.*

(2.7) *There exist $A, k, b_i > 0, w \in \mathbb{C}$ with $|w| = 1$, and a polynomial $P(s)$ such that $Z(s)$ satisfies a functional equation of type:*

$$\Lambda(s) = A^s P(s) \left(\prod_i \Gamma(b_i s + d_i) \right) Z(s) = w \cdot \overline{\Lambda(k - \bar{s})}.$$

Selberg [23] introduced the class of zeta functions (now called the Selberg class) satisfying (2.4), (2.5), (2.7). The axiom (2.6) is new and justifies the term feasible Selberg class. It is precisely the axiom (2.6) which makes this class so interesting for cryptography. Note that axiom (2.6) is quite restrictive; zeta functions with transcendental coefficients cannot be in the feasible Selberg class.

The constant A in the functional equation is called the conductor of the zeta function. The Riemann hypothesis for any subfamily $\mathcal{Z}' \subset \mathcal{Z}$ is the statement that all zeros of $\Lambda(s)$ (corresponding to $Z(s) \in \mathcal{Z}'$) have $Re(s) = k/2$.

There are numerous well known special subfamilies of $\mathcal{Z}$. These include, Dedekind zeta functions of number fields [15] (among which is the famous Riemann zeta function), Dirichlet L-functions [8], and zeta functions associated to modular forms [20]. In contrast, the Hasse–Weil zeta function for algebraic varieties over a finite field may not satisfy axiom (2.6) (see [10]).

Definition: *We say a subfamily $\mathcal{Z}'$ of $\mathcal{Z}$ is abundant provided: for every $\epsilon > 0$, the number of distinct zeta functions in the subfamily for which the conductor A lies in an interval of length B is greater than $B^{1-\epsilon}$ as $B \to \infty$.*

With this definition, we introduce the motivating problem for this paper:

Problem[1]: *Let $\mathcal{Z}'$ be a fixed abundant subfamily of $\mathcal{Z}$. Given a list $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ of complex numbers, how difficult is it to determine whether or not there exists*

$$Z(s) = \sum_{n=1}^{\infty} a(n) \cdot n^{-s} \quad \in \quad \mathcal{Z}'$$

such that $a(n) = \alpha_n$ for $n = 1, 2, \ldots k$, and the conductor of $Z(s)$ lies in a given bounded interval. If such a zeta function exists, how difficult is it to construct one such zeta function?

The most general class of zeta functions which satisfy (2.4), (2.5), (2.6), (2.7), and for which there is a comprehensive arithmetic theory is the class of L-functions associated to automorphic representations of reductive groups in the sense of Jacquet–Langlands (see [14], [3]). We conjecture that problem[1] is intractable for abundant subfamilies of $\mathcal{Z}$ consisting of L–functions associated to *cuspidal* automorphic representations of reductive groups, and that this intractable problem provides the basis for constructing new one–way functions. As evidence for this conjecture, we will focus on three specific subclasses, $\mathcal{Z}_{\text{Kronecker}}$, $\mathcal{Z}_{\text{Elliptic}}$ and $\mathcal{Z}_{\text{Artin}}$.

§3. The classes $\mathcal{Z}_{\text{Kronecker}}$, $\mathcal{Z}_{\text{Elliptic}}$ and $\mathcal{Z}_{\text{Artin}}$

We define $\mathcal{Z}_{\text{Kronecker}}$ [8] to be the class of all Dirichlet L-series of the form

$$L_d(s) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \cdot n^{-s},$$

where $\left(\frac{d}{n}\right)$ denotes the Kronecker symbol and d is any product of relatively prime factors of the form

$$-4, \;\; 8, \;\; -8, \;\; (-1)^{\frac{1}{2}(p-1)}p \qquad (p \text{ a positive odd prime}).$$

Such integers d are called fundamental discriminants. A simple example of Problem[1] is the following:

Problem[2]: *Let B denote a large number. Set $b = (\log(B))^{\kappa}$ where $\kappa > 2$. Suppose we are given a list $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_b\}$ where each $\epsilon_j = \pm 1$ for $j = 1, 2, \ldots, b$. How difficult is it to decide if an L–function, $L_d(s) \in \mathcal{Z}_{\text{Kronecker}}$, with $B \leq |d| \leq 2B$, satisfies $\left(\frac{d}{n}\right) = \epsilon_n$ for $n = 1, 2, \ldots, b$? If such $L_d(s)$ exists, how difficult is it to construct one such fundamental discriminant d?*

Remarks: If we assume the Riemann hypothesis for the class $\mathcal{Z}_{\text{Kronecker}}$ then it can be shown (see [11]) there will be at most one such d. Problem[2] was first stated by Damgård [7] who was the first to suggest that the genuine hardness of this problem could be directly used to construct a cryptographically strong bit generator.

We now define the class $\mathcal{Z}_{\text{Elliptic}}$. An elliptic curve E over $\mathbb{Q}$ is specified by a pair of elements $a, b \in \mathbb{Q}$ for which the discriminant $\Delta_E = 4a^3 + 27b^2 \neq 0$. The set of $\mathbb{Q}$–rational

points of E is denoted $E(\mathbb{Q})$ and consists of all solutions $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ to the equation

$$y^2 = x^3 + ax + b,$$

together with the special point $\mathcal{O} = (\infty, \infty)$ at infinity. It is well known [28] that $E(\mathbb{Q})$ is a group with identity element $\mathcal{O}$. Two elliptic curves

$$E : y^2 = x^3 + ax + b, \qquad E' : y^2 = x^3 + a'x + b'$$

are isomorphic over $\mathbb{Q}$ if there exists a nonzero $u \in \mathbb{Q}$ for which $a' = u^4 a$ and $b' = u^6 b$. It follows that every elliptic curve over $\mathbb{Q}$ is isomorphic to an elliptic curve specified by a pair (a, b) where $a, b \in \mathbb{Z}$. We can make this choice canonical by requiring that the discriminant $4a^3 + 27b^2$ is minimized. Associated to E there is an L-function, $\mathrm{L}_E(s)$, defined by the Dirichlet series

$$\mathrm{L}_E(s) = \sum_{n=1}^{\infty} c_E(n) \cdot n^{-s},$$

where for a rational prime p (not dividing the discriminant),

$$c_E(p) = p + 1 - \#E(\mathbb{F}_p)$$

and $\#E(\mathbb{F}_p)$ denotes the number of integer solutions (x, y) of the congruence

$$y^2 = x^3 + ax + b \pmod{p} \qquad \text{with } 0 \le x, y \le p - 1,$$

plus 1. The plus one refers to the additional point $\mathcal{O}$ at infinity which also lies on the curve. This formula also holds for primes dividing the discriminant provided a more general Weierstrass minimal model is used (see [13]). For prime powers, we have the recurrence relation:

$$c_E(p^{r+1}) = c_E(p)c_E(p^r) - \delta_p \cdot p \cdot c_E(p^{r-1}) \qquad (r \ge 1)$$

where $c_E(1) = 1$, and

$$\delta_p = \begin{cases} 1 & \text{if } p \text{ doesn't divide } \Delta_E \\ 0 & \text{if } p \text{ divides } \Delta_E. \end{cases}$$

In general, if n factors into prime powers, $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, then $c_E(n)$ is defined by the formula

$$c_E(n) = \prod_{j=1}^{k} c_E(p_i^{e_i}).$$

The Riemann hypothesis for E was first proved by Hasse ([13], p. 243) and is equivalent to the bound

$$|c_E(n)| \le \sqrt{n} \cdot d(n),$$

where $d(n)$ denotes the number of positive integer divisors of n. The class $\mathcal{Z}_{\text{Elliptic}}$ consists of all L–functions

$$L_E(s) = \sum_{n=1}^{\infty} c_E(n) \cdot n^{-s}$$

associated to elliptic curves E defined over $\mathbb{Q}$.

Two elliptic curves

$$E : y^2 = x^3 + ax + b, \qquad E' : y^2 = x^3 + a'x + b'$$

defined over $\mathbb{Q}$ are isogenous if there exists a homomorphism from one into the other defined by rational functions [27]. For any fixed elliptic curve E defined over $\mathbb{Q}$ it is known [13], [25], that there are at most finitely many other non–isomorphic elliptic curves isogenous to it. Experimental evidence [6] suggests that on average the number of curves per isogeny class is approximately 2.08. It is known [27] that $\mathrm{L}_E(s) = \mathrm{L}_{E'}(s)$ if and only if E is isogenous to E'.

The Riemann hypothesis for elliptic curves implies that $\mathcal{Z}_{\mathrm{Elliptic}}$ satisfies condition (2.4) with $C > \frac{1}{2}$. From work of Schoof [21] it is known that $\mathcal{Z}_{\mathrm{Elliptic}}$ satisfies condition (2.6). Condition (2.7) was recently proved by Taylor–Wiles [31, 32] for semistable elliptic curves.

A second instance of Problem[1] can now be stated:

Problem[3]: *Let B denote a large number. Set $b = (\log(B))^\kappa$ where $\kappa > 2$. Suppose we are given a list $\{\gamma_1, \gamma_2, \dots, \gamma_b\}$ where each γ_j satisfies the Hasse bound $|\gamma_j| \leq \sqrt{j} \cdot d(j)$ for $j = 1, 2, \dots, b$. How difficult is it to determine whether or not there exists an L–function, $L_E(s) \in \mathcal{Z}_{\mathrm{Elliptic}}$, with $B \leq \Delta_E \leq 2B$, such that $\gamma_n = c_E(n)$ for $n = 1, 2, \dots, b$? If such an L–function exists how difficult is it to construct one such discriminant Δ_E?*

Remark: Again, the assumption of the Riemann hypothesis for the subclass $\mathcal{Z}_{\mathrm{Elliptic}}$ guarantees that there is at most one such E up to isogeny (see [11]).

In order to construct the pseudorandom number generator $\mathrm{PNG}_{\mathrm{Elliptic}}$ referred to in the beginning of the introduction, it is necessary to introduce yet a third class of zeta functions $\mathcal{Z}_{\mathrm{Artin}}$. To simplify the exposition we shall only deal with algebraic number fields which are finite Galois extensions of $\mathbb{Q}$.

Let K be an algebraic number field with finite Galois group

$$G = \mathrm{Gal}(K/\mathbb{Q}).$$

Set O_K to be the ring of integers of K. Let $p \in \mathbb{Q}$ be a prime number and let (p) denote the prime ideal $p\mathrm{O}_K$ in the ring of integers O_K. Let $\mathfrak{p}$ be a prime ideal of O_K lying above p (this simply means that $\mathfrak{p}|(p)$).

Consider the decomposition group $\mathrm{D}_\mathfrak{p}$ and the inertia group $\mathrm{I}_\mathfrak{p}$ defined by

$$\mathrm{D}_\mathfrak{p} = \{\sigma \in G \mid \sigma\mathfrak{p} = \mathfrak{p}\}$$
$$\mathrm{I}_\mathfrak{p} = \{\sigma \in \mathrm{D}_\mathfrak{p} \mid \sigma x = x \pmod{\mathfrak{p}}, \quad \forall x \in \mathrm{O}_K\}.$$

Let $K_\mathfrak{p}$ denote the completion of K with respect to the prime ideal $\mathfrak{p}$, and let $\mathbb{Q}_p$ denote the ordinary p–adic number field (completion of $\mathbb{Q}$ with respect to p). We have (see Tate [30])

$$\mathrm{D}_\mathfrak{p} = \mathrm{Gal}\,(K_\mathfrak{p}/\mathbb{Q}_p)$$

and there exists a group homomorphism

$$\mathrm{D}_{\mathfrak{p}} \longrightarrow \mathrm{Gal}\left(\mathrm{O}_K/\mathfrak{p}\Big/\mathbb{Z}/(p)\right)$$

with kernel $\mathrm{I}_{\mathfrak{p}}$. The quotient group $\mathrm{D}_{\mathfrak{p}}/\mathrm{I}_{\mathfrak{p}}$ is a finite cyclic group generated by the Frobenius element $\mathrm{Fr}_{\mathfrak{p}}$ which satisfies:

$$\mathrm{Fr}_{\mathfrak{p}}(x) \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{p}}, \qquad \forall x \in \mathrm{O}_K,$$

and N denotes the norm from K to $\mathbb{Q}$. If $\mathfrak{p}'$ denotes another prime ideal lying above p, then $\mathfrak{p}' = \sigma\mathfrak{p}$ for some $\sigma \in G$ and

$$\mathrm{D}_{\mathfrak{p}'} = \sigma \mathrm{D}_{\mathfrak{p}} \sigma^{-1}, \;\; \mathrm{I}_{\mathfrak{p}'} = \sigma \mathrm{I}_{\mathfrak{p}} \sigma^{-1}, \;\; \mathrm{Fr}_{\mathfrak{p}'} = \sigma \mathrm{Fr}_{\mathfrak{p}} \sigma^{-1}.$$

We will write Fr_p (with $p \in \mathbb{Q}$) to mean the Frobenius element determined up to conjugation.

Let

$$\psi : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}(2, \mathbb{C})$$

denote a representation of $G = \mathrm{Gal}(K/\mathbb{Q})$ into the group of 2×2 matrices with coefficients in $\mathbb{C}$. Then for any $\sigma \in G$, the trace and determinant of the matrix $\psi(\sigma)$ depend only on the conjugacy class in which σ lies. We define

$$\chi(\sigma) = \mathrm{trace}(\psi(\sigma))$$

for all $\sigma \in G$ to be the character of the representation ψ.

Now, consider a prime number $p \in \mathbb{Q}$. The principal ideal $(p) = p \cdot \mathrm{O}_K$ splits into a product of prime ideals of O_K (see [15])

$$(p) = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r)^e$$

where $efr = [K : \mathbb{Q}]$ (the degree of K over $\mathbb{Q}$) and f is the degree of the residue class field extension. The prime p is said to be ramified over K if $e > 1$. It is well known [15] that there are only finitely many ramified primes and that they must all divide the discriminant of the field extension $K/\mathbb{Q}$. Furthermore, p is unramified if and only if the inertia group I_p is trivial.

For $m = 1, 2, 3, \ldots$ define

$$\chi(p^m) = \frac{1}{e} \sum_{\tau \in \mathrm{I}_{\mathfrak{p}}} \chi\left(\mathrm{Fr}_{\mathfrak{p}}^m \cdot \tau\right).$$

This is well defined and independent of $\mathfrak{p}$ dividing p (see [15]). In the case that p is unramified over K, we have $\chi(p^m) = \chi(\mathrm{Fr}_p^m)$ for $m = 1, 2, 3, \ldots$

For a complex variable s with $Re(s) > 1$, the Artin L-function $\mathrm{L}(s, \chi)$ associated to the representation $\psi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{C})$ is defined by the absolutely convergent series

$$\log(\mathrm{L}(s, \chi)) = \sum_p \sum_{m=1}^{\infty} \frac{\chi(p^m)}{m\,(N(p))^{ms}},$$

where the outer sum goes over all rational primes p. Artin conjectured [1] that if χ is not the principal character then $\mathrm{L}(s, \chi)$ is an entire function of s which satisfies a functional equation of type

$$\begin{aligned}\Lambda(s, \chi) &= A(\chi)^s \Gamma\left(\frac{s}{2}\right)^{a(\chi)} \Gamma\left(\frac{s+1}{2}\right)^{b(\chi)} \mathrm{L}(s, \chi) \\ &= W(\chi)\Lambda(1 - s, \bar{\chi}),\end{aligned}$$

where $a(\chi), b(\chi)$ are positive integers, $A(\chi)$ is positive, and $W(\chi)$ is a complex number of absolute value one called the Artin root number. Further, we have that $A(\chi)$ (see [2], [24], [19]) is the product of non–negative integer powers of the ramified primes.

We define the class $\mathcal{Z}_{\mathrm{Artin}}$ to be the class of all Artin L-functions as defined above.

§4. Candidate One–Way Functions:

Consider an abundant class $\mathcal{Z}$ of zeta functions satisfying (2.4), (2.5), (2.6), (2.7). For sufficiently large $B \gg 0$, define the finite subclass $\mathcal{Z}^B$ by the condition that the conductor A (in the functional equation (2.7) lies in the interval $[B, 2B]$. For each such B, let k, m be integers satisfying:

$$k \geq ((\log B)^{\mu}), \qquad m \leq ((\log B)^{\nu}),$$

with $\mu, \nu > 0$, fixed and independent of B. The triple (B, k, m) defines a Fourier projection function $F = F_{B,k,m}$ where

$$F : \mathcal{Z}^B \to \mathbb{C}^k,$$

and where F is defined by the rule

$$F(Z(s)) = \{a(m), a(m+1), \ldots, a(m+k)\},$$

provided

$$Z(s) \;=\; \sum_{n=1}^{\infty} \frac{a(n)}{n^s} \;\in\; \mathcal{Z}^B.$$

Conjecture: *For the classes $\mathcal{Z}_{\mathrm{Kronecker}}$, $\mathcal{Z}_{\mathrm{Elliptic}}$, and $\mathcal{Z}_{\mathrm{Artin}}$ the associated Fourier projection function is a one–way function.*

Remarks: If we assume the generalized Riemann hypothesis for $\mathcal{Z}_{\mathrm{Kronecker}}$, $\mathcal{Z}_{\mathrm{Elliptic}}$, and we take

$$k \geq (\log B)^{\mu}, \qquad m \leq (\log B)^{\nu},$$

with $\mu > 2,\ \nu = 1$, then F will be a one–to–one function (see [11]), and, hence, by the results of [12] there will exist a pseudorandom number generator based on F. More generally, if $\mathcal{Z}^B$ is a finite set of zeta functions associated to a natural class of automorphic functions (e.g. zeta functions associated to modular forms on $GL(2)$) then we expect that the associated Fourier projection operator is a one–way function.

§5. An Algorithm to Compute $\mathrm{F}^{-1}_{\mathrm{Elliptic}}$:

Let $B \to \infty,\ k \leq (\log B), (\log B) \leq b \leq \sqrt{B},$ and $C \geq (\log B)/B$. Let

$$\big\{a(m), a(m+1), \ldots, a(m+k)\big\}$$

be any fixed vector of rational integers. We will present an algorithm which will determine if there exists an elliptic curve $E : y^2 = x^3 + ax + b$ defined over $\mathbb{Q}$ satisfying the conditions:

$$\begin{aligned} & c_E(p) = a(p) \qquad \forall \text{ primes } p, \quad m \leq p \leq m+k, \\ & B \leq \Delta_E \leq 2B \qquad 0 \leq |a|, |b| \leq C \cdot B. \end{aligned} \tag{5.1}$$

The algorithm will output a complete list $\mathcal{L}$ of all such elliptic curves, and its running time will be at least of the order $(C \cdot B)^{\frac{3}{2}+\epsilon}$. It follows from the abc–conjecture (see [16]) that all solutions a, b of

$$4a^3 + 27b^2 = \Delta_E$$

satisfy

$$|a| << \left(\prod_{p | \Delta_E} p \right)^{2+\epsilon}, \qquad |b| << \left(\prod_{p | \Delta_E} p \right)^{3+\epsilon}.$$

If this conjecture holds, then the algorithm will determine $\mathrm{F}^{-1}_{\mathrm{Elliptic}}$ provided we choose $C >> B^{2+\epsilon}$. The authors are unaware of any significantly faster algorithm to compute $\mathrm{F}^{-1}_{\mathrm{Elliptic}}$, which suggests that presently the cryptographic security of the candidate one–way function $\mathrm{F}_{\mathrm{Elliptic}}$ is probably superior to other known candidate one–way functions, such as those based on factoring or the computation of discrete logarithms.

In the course of describing this algorithm, we will prove the following theorem.

Theorem[4]: *Let* $B \to \infty,\ m \le (\log B),\ (\log B) \le k \le \sqrt{B},\ C \ge (\log B)/B$. *Then for any fixed vector*

$$v = \big\{a(m), a(m+1), \dots, a(m+k)\big\}$$

of coefficients (of some zeta function in $\mathrm{F}^{-1}_{\mathrm{Elliptic}}$*), and for every* $\epsilon > 0$, *the cardinality of the set* $\mathcal{L}$ *(defined by conditions (5.1)) will be bounded by* $\mathrm{O}\Big((C \cdot B)^{\frac{3}{2}+\epsilon}\Big)$, *where the implied constant depends at most on* ϵ.

Remark: If we restrict ourselves to the class of elliptic curves $y^2 = x^3 + ax + b$ with $a > 0$, and we choose $C = \sqrt{\frac{2}{27B}}$, it then follows from theorem[4] that the cardinality of $\mathrm{F}^{-1}_{\mathrm{Elliptic}}$ is bounded by $\mathrm{O}\Big(B^{\frac{3}{4}+\epsilon}\Big)$.

Algorithm to Compute $\mathrm{F}^{-1}_{\mathrm{Elliptic}}$**:** For each rational prime p there are $2p + \mathrm{O}(1)$ non–isomorphic elliptic curves E defined over $\mathbb{F}_p$, and the number of isomorphism classes of such curves $E/\mathbb{F}_p$ where $c_E(p)$ takes the value $a(p)$ is at most

$$\mathrm{O}\Big(\sqrt{p}\,(\log p)\,(\log\log p)^2\Big)$$

(see [18]). Since for any given elliptic curve over $\mathbb{F}_p$, there are at most $\frac{p-1}{2}$ elliptic curves isomorphic to it, it follows that there are at most

$$O\left(p^{\frac{3}{2}+\epsilon}\right)$$

pairs of integers $a, b \pmod p$ which give rise to elliptic curves $E : y^2 = x^3 + ax + b$ with $c_E(p) = a(p)$.

Step 1: For each prime $m \le p \le m + b$ make a list $\mathcal{E}_p$ of isomorphism classes of elliptic curves $E/\mathbb{F}_p$ where $c_E(p) = a(p)$. If $\mathrm{Card}(\mathcal{E}_p) = 0$, for some such p, then there will not be any elliptic curve defined over $\mathbb{Q}$ satisfying (5.1).

Step 2: (Induction) Let $p(1)$ be the smallest prime $\ge m$. We use the notation

$$m \le p(1) < p(2) < p(3) < \cdots$$

to denote successive primes. We define $\mathcal{E}(1) = \mathcal{E}_{p(1)}$ as in step 1. Given $\mathcal{E}(M)$ with $M \ge 1$, we now define $\mathcal{E}(M+1)$.

For every pair of elliptic curves $\{E, E'\} \in \mathcal{E}(M) \times \mathcal{E}_{p(M+1)}$ with

$$E : y^2 = x^3 + ax + b, \qquad E' : y^2 = x^3 + a'x + b',$$

use the Chinese remainder theorem to find all integers $\alpha, \beta \left(\mathrm{mod}\Big(\prod_{i=1}^{M+1} p(i)\Big)\right)$ satisfying

$$\alpha \equiv a, a' \left(\mathrm{mod}\left(\prod_{i=1}^{M+1} p(i)\right)\right), \qquad \beta \equiv b, b' \left(\mathrm{mod}\left(\prod_{i=1}^{M+1} p(i)\right)\right).$$

Then α, β, determine an elliptic curve $E^* : y^2 = x^3 + \alpha x + \beta$ satisfying

$$c_{E^*}(p(j)) = a(p(j))$$

for all $j \leq M+1$. Define $\mathcal{E}(M+1)$ to be the set of all such elliptic curves E^*.

Step 3: Choose an integer M_B so that $p(M_B)$ is the largest prime less than or equal to $m + \log(C \cdot B)$. (The reason for doing this is that the coefficients of any $E \in \mathcal{E}(M_B)$ will be automatically determined $\mod \Big(\prod_{1 \leq i \leq M_B} p(i)\Big)$ which is a number of size $\approx C \cdot B$.) Tabulate a list $\mathcal{L}(M_B)$ of all $E \in \mathcal{E}(M_B)$ with discriminant $B \leq \Delta_E \leq 2B$.

Step 4: For each $E \in \mathcal{L}(M_B)$ compute $c_E(q)$ for all primes q in the range $p(M_B) < q \leq m + k$. If $c_E((q) = a(q)$ for all such primes, then E must satisfy the conditions (5.1).

The total number of elliptic curves constructed by this algorithm is bounded by

$$\mathcal{P} = \prod_{m \leq p \leq m + (\log CB)} p^{\frac{3}{2}+\epsilon},$$

since for each prime p in the range $m \leq p \leq m + (\log CB)$ there are at most $p^{\frac{3}{2}+\epsilon}$ elliptic curves $E(\mod p)$ for which $c_E(p) = a(p)$. By the prime number theorem, [8], we have

$$\log \mathcal{P} = \sum_{m \leq p \leq m + (\log CB)} \left(\frac{3}{2} + \epsilon\right) \cdot (\log p) \quad \sim \quad \left(\frac{3}{2} + \epsilon\right) \cdot (\log CB),$$

as $B \to \infty$. It follows that $\mathcal{P} = \mathrm{O}\Big((C \cdot B)^{\frac{3}{2}+\epsilon}\Big)$ as $B \to \infty$.

§6. Applications to Cryptography:

The candidate one–way functions F_{Elliptic}, F_{Artin}, and $F_{\mathrm{Kronecker}}$ presented above provide the basis for numerous cryptographic applications. We shall describe a few.

[6.1] Authentication: A user's identity may be authenticated by employing the following procedure. The procedure assumes that $B \to \infty$ and m, b are polylogarithmic in B. Let Alice be the user and let Bob be the authenticator. We assume that each of them is in possession of an elliptic curve E with discriminant Δ_E where $B \leq \Delta_E \leq 2B$. Bob randomly chooses m, b and asks Alice to produce the vector

$$v = \{a(m), a(m+1), \ldots, a(M+b)\}$$

of Fourier coefficients (between m and $m+b$) of the zeta function associated to E. If Alice's list is correct then we have verified that Alice is an authenticated user. For large b, the probability of producing the correct list is very small. If someone is surveilling the system and records the vector v, this information will be of no help if in a future authentication

procedure, Bob chooses different m and b so that there is no overlap with any previous intervals. The effective lifespan of a particular elliptic curve used in such an authentication procedure will be logarithmic in B if one wants to insure high cryptographic security.

[6.2] Pseudorandom Number Generator: We adopt the notion of a pseudorandom generator suggested and developed by Blum and Micali [4] and Yao [33]. A pseudorandom number generator is a deterministic polynomial time algorithm that expands short seeds into longer bit sequences such that the output of the ensemble is polynomial–time indistinguishable from a target probability distribution. We shall present an algorithm for a cryptographically secure pseudorandom number generator which is based on the candidate one–way function for the class $\mathcal{Z}_{\text{Elliptic}}$ and $\mathcal{Z}_{\text{Artin}}$. We shall call this pseudorandom number generator $\text{PNG}_{\text{Elliptic}}$. It has the property that it transforms a short seed into a long binary string of zeros and ones with the target probability (1/3, 2/3), i.e. the probability of a zero appearing is 2/3 while the probability of a one is 1/3. The proof of these assertions is based on theorems [8] and [10] below.

Definition: *Let $\mathcal{P}$ be a set of primes having a certain property. We define the density of $\mathcal{P}$ to be*

$$\lim_{x\to\infty} \sum_{\substack{p\in\mathcal{P}\\ p\le x}} 1 \Bigg/ \sum_{p\le x} 1$$

provided the limit exists. If the limit does not exists then the density of $\mathcal{P}$ is not defined.

With this definition, we now state:

Theorem[5]: *Let $a, b \in \mathbb{Z}$, determine an elliptic curve $E : y^2 = x^3 + ax + b$. Define d to be the degree of the field obtained by adjoining the roots of the cubic equation $x^3 + ax + b = 0$ to $\mathbb{Q}$. If $d = 1, 2$ then $c_E(p)$ will be even for all except finitely many rational primes p. If $d = 3$ then the density of primes for which $c_E(p)$ is even is 1/3 while if $d = 6$, the density is 2/3.*

Proof of theorem[5]: Let F be any subfield of $\mathbb{C}$. We say that (x, y) is an F–solution of E if x, y satisfy the equation of E and $x, y \in F$. We let $E(F)$ denote the set of all F–solutions of E. There is a natural commutative group law on $E(F)$ with the point at infinity as identity element. If $P = (x, y) \in E(F)$, then $-P = (x, -y)$ (see [28]). If p is a rational prime number, let $E[p]$ denote the subgroup of points in $E(\bar{\mathbb{Q}})$ of order dividing p.

Now, let $P = (x, y)$ be a point of order two on $E(\bar{\mathbb{Q}})$. Then $2P = \text{O}$ or $P = -P$. Hence, $(x, y) = (x, -y)$ so $y = 0$. Consequently, $P = (x, y) \in E[2]$ if and only if either P is the identity or $P = (x, 0)$ where x is a root of the cubic equation $x^3 - ax - b = 0$. It follow that $E[2]$ is a group of four elements where each element has order 1 or 2, and, therefore, $E[2]$ must be the direct product of two cyclic groups of order two. Let $P_1 = (\alpha, 0)$, $P_2 = (\beta, 0)$ be generators for $E[2]$. Then every $P \in E[2]$ is of the form $rP_1 + sP_2$ with $r, s \in \mathbb{Z}/2\mathbb{Z}$.

Let $K = \mathbb{Q}(\alpha, \beta)$ be the algebraic number field obtained by adjoining the roots of

$x^3 - ax - b$ to $\mathbb{Q}$. Set $G = \mathrm{Gal}(K/\mathbb{Q})$. Then G acts on $E[2]$ by the rules

$$P_1^\sigma = (\alpha^\sigma, 0), \qquad P_2^\sigma = (\beta^\sigma, 0)$$

$$(rP_1 + sP_2)^\sigma = rP_1^\sigma + sP_2^\sigma$$

where $\sigma \in G$, $r, s \in \mathbb{Z}/2\mathbb{Z}$, and $\alpha^\sigma, \beta^\sigma$ denote the usual action of G on K. Since $P_1^\sigma, P_2^\sigma \in E[2]$, for any $\sigma \in G$, it follows that

$$P_1^\sigma = rP_1 + sP_2$$
$$P_2^\sigma = tP_1 + uP_2$$

for $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$. Thus we have a representation:

$$\psi : G \longrightarrow \mathrm{SL}(2, \mathbb{Z}/2\mathbb{Z}).$$

For a rational prime p, let $\mathrm{Fr}_p \in G$ denote the Frobenius element of K. We are interested in its image in $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$. It is known [25], [21], that for all but finitely many primes p that

$$\mathrm{trace}\big(\psi(\mathrm{Fr}_p)\big) \equiv p + 1 - \#E(\mathbb{F}_p) \pmod 2.$$

Since $p+1-\#E(\mathrm{Fr}_p) = c_E(p)$, we can complete the proof of theorem[5] if we can compute the density of primes p for which $\mathrm{trace}(\psi(\mathrm{Fr}_p)) = 0$. To accomplish this, we require the Chebotarev density theorem [17].

Theorem[6]: (Chebotarev) *Let K be a finite Galois extension of $\mathbb{Q}$ with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. For each subset $H \subset G$ stable under conjugation (i.e. $\sigma H \sigma^{-1} = H, \ \forall \sigma \in G$) let*

$$\mathcal{P}_H = \{p \in \mathbb{Q}, \ \text{prime} \mid \ \mathrm{Fr}_p \in H \text{ and } p \text{ unramified in } K\}.$$

Then $\mathcal{P}_H$ has density $|H|/|G|$, where $|H|, |G|$, denote the cardinalities of H, G, respectively.

The group $\mathrm{SL}(2, \mathbb{Z}/2\mathbb{Z})$ is generated by

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

where U is of order 3 and T is of order 2. If $d = [K : \mathbb{Q}] = 1, 2$, then the image of $G = \mathrm{Gal}(K/\mathbb{Q})$ in $\mathrm{SL}(2, \mathbb{Z}/2\mathbb{Z})$ is contained in the cyclic group of order two generated by T. Since $\mathrm{trace}(T) = 0$, it follows that all except finitely many $c_E(p)$ are even. In the case that $d = 3$, then the image is the cyclic group generated by U. Since $\mathrm{trace}(U) = \mathrm{trace}(U^2) = 1$, it follows from the Chebotarev density theorem that $2/3$ of the $c_E(p)'$s are odd. Finally, if $d = 6$, since only the two elements U, U^2, have trace 1, it follows from the Chebotarev density theorem that the density of primes p for which $c_E(p)$ is odd will be $2/3$. This completes the proof of theorem[5].

Theorem[7]: *Let E be an elliptic curve defined over $\mathbb{Q}$. Let K denote the field obtained by adjoining the 2–torsion points of E to $\mathbb{Q}$. Then there exists an entire Artin L-function*

$$L_K(s) = \sum_{n=1}^{\infty} b(n) \cdot n^{-s} \in \mathcal{Z}_{\text{Artin}}$$

of K with the property that

$$b(p) \equiv c_E(p) \pmod 2$$

for all except finitely many rational primes p.

Proof of theorem[7]: Recall that the group $\mathrm{SL}(2, \mathbb{Z}/2\mathbb{Z})$ is generated by

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

where U is of order 3 and T is of order 2. There exists a representation

$$\rho : \mathrm{SL}(2,\, \mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathrm{GL}(2,\, \mathbb{Z}[i])$$

which is defined on the generators U, T by

$$\rho(U) = \begin{pmatrix} -1 & i \\ i & 0 \end{pmatrix}, \qquad \rho(T) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

and satisfies

$$\begin{aligned} \mathrm{trace}(\rho(\sigma) &\equiv \mathrm{trace}(\sigma) \pmod 2 \\ \det(\rho(\sigma) &\equiv \det(\sigma) \pmod 2 \end{aligned}$$

for all $\sigma \in \mathrm{SL}(2,\, \mathbb{Z}/2\mathbb{Z})$. It follows that the representation $\rho \circ \psi : G \to \mathrm{GL}(2,\, \mathbb{Z}[i])$ determines an Artin L–function

$$\mathrm{L}_K(s) = \sum_{n=1}^{\infty} b(n) \cdot n^{-s}$$

of the field K where, $b(p) = \mathrm{trace}\Big(\rho(\psi(\mathrm{Fr}_p))\Big)$, for unramified p. Hence, if p is unramified, we have $b(p) \in \{0, 2\}$ if $c_E(p)$ is even and $b(p) = -1$ if $c_E(p)$ is odd. The Artin L–function is entire since $\mathrm{Gal}(K/\mathbb{Q}) \subseteq \mathrm{S}_3$ and Artin's conjecture is known for subgroups of S_3.

Assume we are presented with a sequence of bits, where the n^{th} bit is obtained by computing $c_E(p_n) \pmod 2$ for some elliptic curve E as above, and where p_n denotes the n^{th} prime. To be sure that we don't have a trivial sequence, we assume that the degree d of the field of 2-torsion points of E is 6. Theorem[5] then says that the bit sequence $c_E(p_n) \pmod 2$ for $n = 1, 2, 3, \ldots$ is pseudorandom with probability distribution (1/3, 2/3). We want to show that it is not possible in polynomial time to determine E from this sequence.

This follows immediately from theorem[7] if the Fourier projection operator F_{Artin} is a one–way function. It easily follows that the set of elliptic curves

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$ and discriminant $\Delta_E = 4a^3 + 27b^2$ in the range $B \leq \Delta_E \leq 2B$ which give rise to the same bit streams has cardinality at most $O\left(B^{\frac{1}{2}+\epsilon}\right)$ as $B \to \infty$.

Let E, E' be two elliptic curves defined over $\mathbb{Q}$ with discriminants $\Delta_E, \Delta_{E'}$, where $B \leq \Delta_E, \Delta_{E'} \leq 2B$. Set K, K' to be the field of 2-torsion points of E, E', respectively. Assume that K, K' are of degree six over $\mathbb{Q}$. Let $B \to \infty$ and let $b = (\log B)^\kappa$ for some $\kappa > 2$. If

$$c_E(p) \equiv c_{E'}(p) \pmod 2$$

for all primes $p < b$, then it appears very likely that $K = K'$ and the Artin L–functions $\mathrm{L}_K(s), \mathrm{L}_{K'}(s)$ are twists of each other by a quadratic character.

We now present the algorithm for $\text{PNG}_{\text{Elliptic}}$.

Step 1: Choose integers a, b such that the roots of the equation $x^3 + ax + b = 0$ generate a field of degree 6 over $\mathbb{Q}$. A simple test to determine whether the Galois group of this polynomial is S_3 (and hence, has order 6) is to simply check if the discriminant $-4a^3 - 27b^2$ is a perfect square of a rational number. If the discriminant is not a perfect square and the polynomial is irreducible, then the Galois group is S_3 . The integers a, b are taken to be the seed and determine an elliptic curve $E : y^2 = x^3 + ax + b$.

Step 2: For each prime p compute $\text{bit}(p) = c_E(p) \pmod 2$ which will have value either 0 or 1. Under the assumption that F_{Artin} is a one–way function, the binary stream

$$\{\text{bit}(3),\ \text{bit}(5),\ \text{bit}(7),\ \text{bit}(11),\ ...\}$$

running over odd primes will be a pseudorandom number sequence with probability distribution (1/3, 2/3).

Algorithm to compute $c_E(p) \pmod 2$**:** The following algorithm was suggested to us by Nikolaos Diamantis. Although the algorithm is classical, it is difficult to find in the literature, so we include it for clarity and completeness. When counting the number of solutions of the congruence

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

note that the solutions occur in pairs (x, y) and $(x, -y)$. Thus, since we are only interested in the number of solutions $\pmod 2$, it is enough to compute the number of solutions of $0 \equiv x^3 + ax + b \pmod p$. Let

$$\nu_p = \text{Card}\Big\{ x \,(\text{mod} p) \ \Big|\ 0 \equiv x^3 + ax + b \pmod p \Big\}.$$

Then we have

$$c_E(p) \equiv \nu_p \pmod 2.$$

Now ν_p can have the values 0, 1 or 3. Further, $\nu_p = 1$ if and only if the discriminant $-4a^3 - 27b^2$ is a quadratic non–residue (mod p). L.E. Dickson [9] showed that if $p > 3$, then $\nu_p = 0$ if and only if $-4a^3 - 27b^2 \equiv 81\mu^2 \pmod p$ and $\frac{1}{2}\left(-b + \mu\sqrt{-3}\right)$ is not congruent to a cube of any number of the form $x + y\sqrt{-3}$ with x, y rational integers. For efficient algorithms to compute quadratic residues and square roots (mod p), see [5], chapter 1. Dickson's last condition can be checked by computing the cubic residue symbol

$$\left(\frac{-b + \mu\sqrt{-3}}{p}\right)_3.$$

This symbol is defined as follows. Let $\omega = \frac{1}{2}(-1 - \sqrt{-3})$ be a cube root of unity. Consider the cubic field $\mathbb{Q}(\omega)$ with ring of integers $\mathbb{Z}[\omega]$. The primes of the ring $\mathbb{Z}[\omega]$ fall into three classes. The rational primes 2, 5, 11, 17, ... which are congruent to 2 (mod 3), the imaginary primes $a + b\omega$ (with $a, b \in \mathbb{Z}$) having norm $(a + b\omega) \cdot (a + b\omega^2) = a^2 - ab + b^2$ (which is equal to a rational prime congruent to (1 mod 3)), and the ramified primes $1 - \omega, 1 - \omega^2$ having norm 3. The units are $\pm 1, \pm\omega$, and $\pm\omega^2$. Let ρ be a prime in this ring and let $\alpha \in \mathbb{Z}[\omega]$ be coprime to ρ. We have the cubic extension of Fermat's theorem, viz.

$$\alpha^{N\rho - 1} \equiv 1 \pmod \rho,$$

where $N\rho$ denotes the norm of ρ. The cubic symbol symbol $\left(\frac{\alpha}{\rho}\right)_3$ is defined to be equal to ω^s where $s = 0, 1, 2$ according to whether

$$\alpha^{\frac{1}{3}(N\rho - 1)} \equiv \omega^s \pmod \rho.$$

Thus, $\left(\frac{\alpha}{\rho}\right)_3 = 1$ if and only if α is congruent to a cube (mod ρ). If $\alpha' \equiv \alpha \pmod \rho$, then we have

$$\left(\frac{\alpha'}{\rho}\right)_3 = \left(\frac{\alpha}{\rho}\right)_3.$$

This symbol may be extended to non–primes by defining

$$\left(\frac{\alpha}{\rho\rho'}\right)_3 = \left(\frac{\alpha}{\rho}\right)_3 \cdot \left(\frac{\alpha}{\rho'}\right)_3.$$

Further, if $\alpha = \mu \prod q_i^{e_i}$ is the prime factorization of α in the ring $\mathbb{Z}[\omega]$ (with μ a unit), then

$$\left(\frac{\alpha}{\rho}\right)_3 = \left(\frac{\mu}{\rho}\right)_3 \cdot \prod \left(\frac{q_i}{\rho}\right)_3^{e_i}.$$

Let $x + y\omega \in \mathbb{Z}[\omega]$ be not divisible by $1 - \omega$. Exactly one of the 3 pairs of numbers

$$\pm(x + y\omega), \quad \pm\omega(x + y\omega), \quad \pm\omega^2(x + y\omega),$$

will be congruent to $a+b\omega$ with $a \equiv \pm 1, b \equiv 0, \pmod 3$. We define $a+b\omega$ to be a primary number. It is easily seen that the product of two primary numbers is itself primary. The cubic symbol $\left(\frac{\alpha}{\rho}\right)_3$ can be computed in polynomial time in the number of digits of $N\rho$ by employing the Eisenstein–Jacobi reciprocity law, [29] viz.

$$\left(\frac{q}{\rho}\right)_3 = \left(\frac{\rho}{q}\right)_3,$$

which holds for all $\rho, q \in \mathbb{Z}[\omega]$ which are primary numbers. To compute $\left(\frac{\alpha}{\rho}\right)_3$ one first expresses α as a product of a unit u, a power of $1-\omega$, and a primary number q, i.e., $\alpha = u \cdot (1-\omega)^e \cdot q$. We can assume $Nq < N\rho$, by reducing (modρ). Thus

$$\left(\frac{\alpha}{\rho}\right)_3 = \left(\frac{u}{\rho}\right)_3 \cdot \left(\frac{1-\omega}{\rho}\right)_3^e \cdot \left(\frac{q}{\rho}\right)_3.$$

The symbols $\left(\frac{u}{\rho}\right)_3$ and $\left(\frac{1-\omega}{\rho}\right)_3$ can be computed very quickly. We have

$$\left(\frac{\omega}{\rho}\right)_3 = \omega^{\frac{1}{3}(N\rho-1)} = \omega^{m+n},$$
$$\left(\frac{1-\omega}{\rho}\right)_3 = \omega^{2m}$$

where the integers m, n are defined by the identity

$$\rho = 2m - 1 + 3n\omega.$$

To compute $\left(\frac{q}{\rho}\right)_3$ apply the reciprocity law and turn the symbol upside down. Let

$$\rho' \equiv \rho \pmod q$$

with $N\rho' < Nq$. Thus $\left(\frac{q}{\rho}\right)_3 = \left(\frac{\rho'}{q}\right)_3$. By iterating the previous procedure, the computation is reduced to computing symbols $\left(\frac{\mu}{\nu}\right)_3$ with primary numbers ν of small norm.

[6.3] Coin Flipping by telephone: Alice and Bob want to simulate a random coin toss over a telephone. The following algorithm provides a mechanism for accomplishing this task. The algorithm assumes that $B \to \infty$ and $m = (\log B)^\kappa$ for some constant $\kappa > 2$.

Step 1: Alice chooses integers a, b such that the roots of the equation $x^3 + ax + b = 0$ generate a field of degree 6 over $\mathbb{Q}$, and the discriminant $\Delta = 4a^3 + 27b^2$ lies in the interval $B \le \Delta \le 2B$. Alice then computes the vector v of the first m coefficients

$$v \;=\; \{a(1), a(2), \ldots, a(m)\}$$

of the zeta function associated to $E : y^2 = x^3 + ax + b$. Alice transmits v to Bob.

Step 2: Bob randomly chooses two prime numbers $p < p'$ with $p > m$.

Step 3: Alice computes $\text{trial}(p, p') = \Big(a(p) \pmod 2,\ \ a(p') \pmod 2\Big)$. If

$$\text{trial}(p, p') = (1, 0)$$

then the coin toss is heads. If

$$\text{trial}(p, p') = (0, 1),$$

then the coin toss is tails. If neither of these possibilities occur go back to step 2.

Step 4: Bob can verify the correctness of the coin flip when Alice announces the elliptic curve E. Otherwise it is not feasible for him to compute $\text{trial}(p, p')$.

Remark: The probability of either of the events: $\text{trial}(p, p') = (1, 0)$ or $(0, 1)$ is $2/9$, so they will occur with equal frequency.

For related applications, the reader may wish to consult [22].

REFERENCES

[1] E. ARTIN, *Zur Theorie der* L*–Reihen mit allgemeinen Gruppencharakteren*, Hamb. Abh. **8** (1930), 292–306, Collected Papers, No. 8.

[2] E. ARTIN, *Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahl–körper*, J. Reine angew. Math., **164** (1931), 1–11, Collected Papers, No. 9.

[3] A. BOREL, *Automorphic* **L***–functions*, in Automorphic Forms, Representations, and L-functions, Amer. Math. Soc., Proc. Symp. Pure Math. **33** (1979) part 2, 27–61.

[4] M. BLUM, S. MICALI, *How to generate cryptographically strong sequences of pseudo-random bits*, Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science, 1982, SIAM J. Comput, **13** (1984), 850–864.

[5] H. COHEN, A Course in Computational Number Theory, Springer Verlag, NY, (1993).

[6] J. CREMONA, Algorithms for Modular Elliptic Curves, Cambridge University Press, (1992).

[7] I.B. DAMGÅRD, *On the randomness of Legendre and Jacobi Sequences*, in Advances in Cryptology-Crypto '88, Lecture Notes in Computer Science 403, edited by S. Goldwasser, Springer–Verlag (1988), 163–172.

[8] H. DAVENPORT, Multiplicative Number Theory, Second Edition (revised by H. Montgomery), Springer-Verlag, (1980).

[9] L.E. DICKSON, History of the Theory of Numbers, Vol 1, Chelsea Publishing Co. New York, N.Y., (1971), 253–254.

[10] J. VON ZUR GATHEN, M. KARPINSKI, I. SHPARLINSKI, *Counting curves and their projections*, in Proceedings 25th Annual ACM, Symposium on the Theory of Computing (1993), 805–812.

[11] D. GOLDFELD, J. HOFFSTEIN, *On the number of Fourier coefficients that determine a modular form*, in Contemporary Math. **143**, A Tribute to Emil Grosswald: Number Theory and Related Analysis, Amer. Math. Soc. (1993), 385–393.

[12] O. GOLDREICH, H. KRAWCZYK, M. LUBY, *On the existence of pseudorandom generators*, SIAM J. Comput. Vol. 22, No. 6 (1993), 1163-1175.

[13] D. HUSEMOLLER, Elliptic Curves, Grad. Texts in Math., 111, Springer–Verlag, (1987).

[14] H. JACQUET, R. LANGLANDS, Automorphic forms on GL(2), Lecture Notes in Mathematics., vol 278, Springer–Verlag (1972).

[15] S. LANG, Algebraic Number Theory, Addison–Wesley Series in Mathematics, (1970).

[16] S. LANG, *Old and new conjectured diophantine inequalities,* Bulletin of the AMS, Volume 23, Number 1, (1990), 37–75.

[17] J.C. LAGARIAS, A.M. ODLYZKO, *Effective versions of the Chebotarev density theorem*, in Algebraic Number Fields, edited by A. Fröhlich, Academic Press (1977), 409–464.

[18] H.W. LENSTRA, Factoring integers with elliptic curves, Annals of Math., **126** (1987), 649–673.

[19] J. MARTINET, *Character theory and Artin* L*–functions*, in Algebraic Number Fields, edited by A. Fröhlich, Academic Press (1977), 1–87.

[20] A. OGG, Modular Forms and Dirichlet Series, W.A. Benjamin, Inc., (1969).

[21] R. SCHOOF, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. of Computation, Vol 44, Number 170 (1985), 483–494.

[22] B. SCHNEIER, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, John Wiley & Sons Inc., (1995).

[23] A. SELBERG, *Old and new conjectures and results about a class of Dirichlet series*, Collected Papers, Vol. 2, No. 44, Springer–Verlag (1991), 47–63.

[24] J.P. SERRE, Corps Locaux, Hermann, Paris (1962).

[25] J.P. SERRE, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Invent. Math. **15** (1972), 259-331, Collected Papers, no. 94.

[26] P. SHOR, *Algorithms for quantum computation: discrete logarithms, and factoring,* IEEE Symposium on Foundations of Computer Science, IEEE Computer Science Press, Los Alamitos, CA (1994), 124–134.

[27] J. SILVERMAN, The Arithmetic of Elliptic Curves, Graduate Texts in Math., 106, Springer–Verlag, (1986).

[28] J. SILVERMAN, J. TATE, Rational Points on Elliptic Curves, Undergraduate Texts in Math., Springer–Verlag, (1992).

[29] H.J.S. SMITH, Report on the Theory of Numbers, Chelsea Publishing Company, Bronx, N.Y. (1965), 88–92.

[30] J. TATE, *Global class field theory*, in Algebraic Number Theory, Edited by J.W.S. Cassels and A. Fröhlich, Thompson Book Company Inc., Washington D.C., (1967), 163–203.

[31] R. Taylor, A. Wiles, *Ring–theoretic properties of certain Hecke algebras,* Annals of Math., **141** (1995), 553–572.

[32] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem,* Annals of Math., **142**, (1995), 443–551.

[33] A.C. YAO, *Theory and applications of trapdoor functions*, Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science, (1982), 80-91.