PRIME NUMBERS AND CRYPTOSYSTEMS BASED ON DISCRETE LOGARITHMS

Maciej Grześkowiak

Adam Mickiewicz University Faculty of Mathematics and Computer Science
Umultowska 87, 61-614 Poznań, Poland.
maciejg@amu.edu.pl

Abstract. In this paper, we give a short overview of algorithms of generating primes to a DL systems. The algorithms are probabilistic and works in a polynomial time.

Keywords: Torus-based cryptography, Elliptic and hyperelliptic curve cryptography

1. Introduction

Let $(G, \cdot)$ be an abelian group, and let $|G| = N$ be the order of G. The Discrete Logarithm Problem (DLP) is: given $g, h \in G$ find $x \in \mathbb{N}$, if it exists, such that $h = g^x$. The security of a discrete logarithm (DL) system depend on the assumption that discrete logarithms in G are hard to compute. In practice a DL system is based on a cyclic subgroup of G of a prime order q. Let q be the largest prime divisor of N. It is well known that the DLP in G is as hard as the DLP in the subgroup of order q [20]. For this reason it is essential to choose G such that $q \mid N$ and q is a large prime. From the security point of view it is reasonable to assume that $q \approx 2^{160}$. For the complexity of algorithms depending on N we define the function

$$L_N(\alpha, c) = \exp((c + o(1))(\log N)^{\alpha}(\log \log N)^{1-\alpha}).$$

with $a, c \in \mathbb{R}$, $0 \leq a \leq 1$ and $c > 0$ [6]. If the second parameter is omitted, it is understood that is equal $1/2$. Let $G = \mathbb{F}_{p^n}^*$ be a multiplicative group of finite fields. The DLP in $\mathbb{F}_{p^n}^*$ can be computed in subexponential time $L_{p^n}(1/3)$ [1], [10], [15], [16]. For finite fields of small characteristic, this problem can be solved with heuristic complexity $L_{p^n}(1/4)$ [14]. The above shows that one should take p^n at least 1024 bits in order to have the DLP intractable to solve. So to efficiently implement a DL system in G one need to find primes p, q of appropriate size such that

$$q \mid p^n - 1.$$

The author was partially supported by the grant no. 2013/11/B/ST1/02799 from National Science Centre.

Fix $n = 1$. In many a DL systems a generator g of G is required. No polynomial-time algorithm is known for finding generators, or even for testing whether an element is a generator of G if the factorization of is unknown. There is a special kind of prime for which it is easy. Namely, let $p = 2q + 1$, where q is also a prime. In order to find a generator of G one select randomly $g \in G$ such that $g^2 \not\equiv 1 \pmod{p}$ and $g^q \not\equiv 1 \pmod{p}$. For $p \approx 2^{1024}$ the algorithm works well in practice. On the other hand, theoretical estimation of the algorithms running time becomes a problem. We do not know if there exist infinitely many primes p of the above form. This is an extremely hard, still unproven mathematical problem. However, there are some conjectures related to this problem [13]. To overcome this problem, we consider the second approach for generating a generator g of G. Let $x \in \mathbb{R}$ be a sufficiently large number. Fix a prime $q \in [x, 2x]$. The algorithm randomly selects a positive integer $k \in [0, cq(\log q)^{20}]$, where $c > 0$ is a constant. Next it computes $p = qk + 1$ and checks if p is a prime. If it is a prime then the algorithm returns the prime p and k. Otherwise, it randomly finds k and the above mentioned steps are repeated. Let $\lambda \geq 1$. The above algorithm finds a prime $p \leq cq^2(\log q)^{20}$ with probability greater than or equal to $1 - e^{-\lambda}$ after repeating $[c_0\lambda(\log x)]$ steps with the possible exception of at most $O(x(\log x)^{-2})$ values of q, where $c_0 > 0$ is a constant [12]. Since $p-1 = kq$, the factorization of $p-1$ can be obtained by factoring k. However, we cannot exclude the possibility that the number of steps we need to factor k is exponential. On the other hand, given p, q, one can easily find an element $g \in G$ of order q and implement a DL system in the subgroup generated by g. We define the parameter

$$\rho(G) = \frac{\log N}{\log q},$$

which measures the group G size N relative to the size of the prime order q subgroup of G. For sufficiently large x the above algorithm finds primes p and q with $\rho(\mathbb{F}_p^*) = 2 + o(1)$. An interesting problem in this area is the following: Construct a polynomial-time algorithm that finds primes p, q such that $q \mid p^n - 1$ with

$$\rho(\mathbb{F}_{p^n}^*) = n + o(1).$$

Let n be a positive integer, and let $\Phi_n(x)$ be the nth cyclotomic polynomial. Let p be a prime and let $\mathbb{F}_{p^n}^*$ be a multiplicative group of finite field $\mathbb{F}_{p^n}$. It is well known that

$$|\mathbb{F}_{p^n}^*| = p^n - 1 = \prod_{d|n} \Phi_d(p).$$

Let G be a subgroup of $\mathbb{F}_{p^n}^*$ of a prime order $q > n$, and let q divides $\Phi_n(p)$. Then $\mathbb{F}_{p^n}$ is the smallest extension of $\mathbb{F}_p$ that contains G [18]. In recent years, there have been several proposal DL systems based on the G with $q < \Phi_n(p)$ [19], [25]. Rubin and Silverberg [22] generalise the above cryptosystems using the algebraic torus $T_n(\mathbb{F}_p)$ which is isomorphic to the G with $q = \Phi_n(p)$. Techniques used in the above mentioned DL systems allow to represent an element of G with less coefficients than a general element of $\mathbb{F}_{p^n}$ needs. Such an approach leads to substantial savings both in the computational complexity of algorithms performing arithmetic operations in $\mathbb{F}_{p^n}$ and transmission elements of $\mathbb{F}_{p^n}$, without compromising security. We introduce the following definition [12].

Definition 1. A prime q is relatively n-cyclotomic to a prime p if q divides $\Phi_n(p)$.

Algorithms for generating primes p and q such that q is relatively n-cyclotomic to a prime p are utilized for computing key parameters in DL systems based on G. From the security point of view it is essential to find a prime p such that $\Phi_n(p)$ has a large prime factor q having at least 160 bits to make DLP in G intractable. On the other hand, one should find a prime p such that $n \log p \approx 1024$ in order to have the DLP unfeasible to solve by applying an index calculus method. In [12] a polynomial time algorithm generating of two primes p and q such that q is relatively n-cyclotomic to p is proposed. The algorithm is probabilistic and finds such primes with

$$\rho(\mathbb{F}_{p^n}^*) = n + o(1).$$

For cryptographic purposes one can replace $\mathbb{F}_{p^n}^*$ by the group of rational points of $E(\mathbb{F}_{p^n})$ on an elliptic curve. Let $G = E(\mathbb{F}_p)$. The most efficient way to solve DLP in G is the Pollard's rho method [21]. It takes $O(\sqrt{N})$ group operations. On the other hand Hasse's theorem shows that $N = p + 1 - t$, where $|t| \leq 2\sqrt{p}$. So in practice it is recommended to generate a prime $p \approx 2^{200}$. Now, we introduce the following definition [11].

Definition 2. Let p, q be a pair of primes and $\Delta < 0$. The primes p, q are defined to be CM-primes with respect to Δ if there exist integers f and t such that

$$|t| \leq 2\sqrt{p}, \quad q \mid p + 1 - t, \quad 4p - t^2 = \Delta f^2.$$

To construct a DL system based on G it is essential to find CM-primes p and q with respect to Δ of appropriate order of magnitude. Given such primes, an elliptic curve E over $\mathbb{F}_p$ can be constructed by applying the

complex multiplication (CM) method [4], [7]. Given current computational power, the method can construct curves over $\mathbb{F}_p$ when $|\Delta| \leq 10^{12}$. For this reason Δ should be sufficiently small to make the CM method work effectively in practice. In [11] a polynomial time construction of CM primes with respect to Δ is proposed. The algorithm is probabilistic and finds such primes with

$$\rho(E(\mathbb{F}_p)) = \frac{5}{2} + o(1).$$

Let C be a hyperelliptic curve of genius g defined over finite prime field $\mathbb{F}_p$. We denote the group of $\mathbb{F}_p$-rational points of the Jacobian of C by $J_C(\mathbb{F}_p)$. Koblitz [11] proposed the DLP in groups of the form $G = J_C(\mathbb{F}_p)$. For general hyperelliptic curves of genus $g \leq 2$ the DLP in $J_C(\mathbb{F}_p)$ is thought to be hard [2], [8], [9], [26]. To make the DLP in $J_C(\mathbb{F}_p)$ intractable, it is essential to generate a large prime p, and a curve C defined over $\mathbb{F}_p$, such that $|J_C(\mathbb{F}_p)|$ has a large prime factor q. To construct a genus 2 curve over $\mathbb{F}_p$ with the above properties one can use the genus 2 CM method [27]. This method generates curves for which a prime p and $|J_C(\mathbb{F}_p)|$ are known in advance. In practice, to the above mentioned method works efficiently, K must have a small discriminant. A field K is called a CM field if it is a totally imaginary quadratic extension of a totally real algebraic number field. Let K, $[K : \mathbb{Q}] = 2t$ be a CM field with the corresponding ring of integers $\mathcal{O}_K$. We say that π is a Weil q-number if $\pi \in \mathcal{O}_K$, and for every complex embedding $\sigma : K \to \mathbb{C}$ we have $|\sigma(\pi)| = \sqrt{q}$. There is a connection between $|J_C(\mathbb{F}_p)|$ and a Weil p-number. Namely, if $K = \mathbb{Q}(\pi)$ then

$$N_{K/\mathbb{Q}}(\pi) = p^t, \quad |J_C(\mathbb{F}_p)| = N_{K/\mathbb{Q}}(\pi - 1).$$

Now, we introduce the following definition

Definition 3. Let K be a CM field, and let p, q be a pair of primes. The primes p, q are defined to be CM-primes with respect to K if there exist $\pi \in \mathcal{O}_K$ such that π is a Weil p-number, and

$$p = \pi\overline{\pi}, \quad q \mid N_{K/\mathbb{Q}}(\pi - 1).$$

Let K be a quartic CM field. To implement a DL system based on G of appropriate order of magnitude CM primes p, q with respect to K are required. In [27] a probabilistic method for generating CM primes with respect to K is presented. However, an analysis of computational complexity of the algorithm were not given there. An interesting open problem is the

following: Construct a polynomial-time algorithm generating CM primes p, q with respect to K.

In the present paper, we give a survey of certain algorithms generating primes to DL systems. We focus attention on the algorithms that works in polynomial time. The remaining part of the paper is organized as follows. In Section 2 we describe an algorithm for generating of finding two primes p, q such that q is relatively n-cyclotomic to a prime p. An algorithm for CM-primes with respect to Δ is given in Section 3.

2. Relatively n-cyclotomic primes

Fix $n \in \mathbb{N}$. In the present section, we show a general method of finding two primes p, q such that q is relatively n-cyclotomic to a prime p [12]. Before we describe the algorithm, we introduce some notation. Given a primitive nth root of unity ω, $K = \mathbb{Q}(\omega)$ denotes the nth cyclotomic field with the ring of integers

$$\mathcal{O}_K = \{a_1 + a_2\omega + \ldots + a_{\varphi(n)}\omega^{\varphi(n)-1}, \quad a_i \in \mathbb{Z}, \quad i = 1, \ldots, \varphi(n)\}.$$

Let $\alpha \in \mathcal{O}_K$, we write

$$\alpha\omega^{i-1} = \sum_{j=1}^{\varphi(n)} a_{ij}\omega^{j-1}, \quad a_{ij} \in \mathbb{Z}, \quad a_{1j} = a_j. \tag{2.1}$$

The determinant $\det[a_{ij}]$ of the matrix $A(\alpha) = [a_{ij}]$ of (2.1) is the norm of the element $\alpha \in \mathcal{O}_K$ relative to the $K/\mathbb{Q}$ [5, Definition, p. 400]. So, if $\alpha \in \mathcal{O}_K$ is given then $N(\alpha) = \det(A(\alpha))$. The main algorithm consists of the following three procedures. We start with a procedure which generates $\alpha \in \mathcal{O}_K$ such that $N(\alpha) \equiv 1 \pmod{n}$ is a prime.

Procedure 1 (n). Fix $n \in \mathbb{Z}$, $n > 1$ and let ω be a primitive nth root of unity. Fix $K = \mathbb{Q}(\omega)$, $[K : \mathbb{Q}] = 2t$, where t is the number of complex embeddings of K into $\mathbb{C}$. Let $\varepsilon_1, \ldots, \varepsilon_r$, be a system of fundamental units of K, where $r = t-1$, and let $\sigma_1, \overline{\sigma_1} \ldots, \sigma_t, \overline{\sigma_t}$ be embeddings of $K = \mathbb{Q}(\omega)$ into $\mathbb{C}$. We define

$$M = M(n) = \max_{1 \le i \le r}\{\log|\sigma_j(\varepsilon_i)|, \quad j = 1, \ldots, t\}.$$

Let $\omega_1 = \omega, \omega_2, \ldots \omega_{\varphi(n)}$ be the conjugates of ω and we define

$$C = C(n) = \max\{|v_{i,j}|, \quad i = 1, \ldots, \varphi(n), \quad j = 1, \ldots, \varphi(n)\}. \tag{2.2}$$

where

$$\begin{bmatrix} 1 & \omega_1 & \cdots & \omega_1^{\varphi(n)-1} \\ 1 & \omega_2 & \cdots & \omega_2^{\varphi(n)-1} \\ \vdots & \vdots & \ddots & \cdots \\ 1 & \omega_{\varphi(n)} & \cdots & \omega_{\varphi(n)}^{\varphi(n)-1} \end{bmatrix}^{-1} = \begin{bmatrix} \upsilon_{1,1} & \upsilon_{1,2} & \cdots & \upsilon_{1,\varphi(n)} \\ \upsilon_{2,1} & \upsilon_{2,2} & \cdots & \upsilon_{2,\varphi(n)} \\ \vdots & \vdots & \ddots & \cdots \\ \upsilon_{\varphi(n),1} & \upsilon_{\varphi(n),2} & \cdots & \upsilon_{\varphi(n),\varphi(n)} \end{bmatrix}$$

The procedure finds $\alpha = \sum_{i=1}^{\varphi(n)} a_i \omega^{i-1} \in \mathcal{O}_K$ such that $N(\alpha) \equiv 1 \pmod{n}$ is a prime, $x \leq N(\alpha) \leq 2x$ and $|a_i| < C\varphi(n)e^{rM}(2x)^{1/\varphi(n)}$.

step 1.: For $i = 1, \ldots, \varphi(n)$, choose $a_i \in \mathbb{Z}$ such that $|a_i| < C\varphi(n)e^{rM}(2x)^{1/\varphi(n)}$ at random in $\mathbb{Z}$. Write $\alpha = a_1 + a_2\omega + \ldots + a_{\varphi(n)}\omega^{\varphi(n)-1} \in \mathcal{O}_K$.

step 3.: Compute $q = N(\alpha)$. If $q < x$ or $q > 2x$, then go to step 1.

step 4.: If q is a prime, then terminate the procedure. Otherwise go to step 1.

step 5.: Return $a_1, \ldots, a_{\varphi(n)}$, q and $A(\alpha)$ such that $\det(A(\alpha)) = q$.

Let m be a positive integer. We denote by $\mathcal{PT}$ the number of bit operations necessary to carry out the deterministic primality test [3]. For simplicity, assume that $\mathcal{PT}$ takes at least $O(\log^3 m)$ bit operations.

Theorem 2. *Given $n \in \mathbb{Z}$, $n > 2$, there exist two constants $c_0 > 0$ and x_0 such that for every $x \geq x_0$ and an arbitrary real $\lambda \geq 1$, Procedure 1 finds*

$$\alpha = \sum_{i=1}^{\varphi(n)} a_i \omega^{i-1} \in \mathcal{O}_K, \quad |a_i| < C\varphi(n)e^{rM}(2x)^{1/\varphi(n)}$$

such that

$$N(\alpha) \equiv 1 \pmod{n}, \quad x \leq N(\alpha) \leq 2x,$$

is a prime, with probability greater than or equal to $1 - e^{-\lambda}$ after repeating $[c_0\lambda(\log x)]$ steps of the procedure. Every step of the procedure takes at most $\mathcal{PT}$ bit operations.

Proof. See [12]. □

Now, we introduce the deterministic procedure of finding roots of irreducible polynomials $\Phi_n(x) \pmod{q}$ that works effectively in polynomial time and may be an alternative to the random algorithms.

Procedure 3 $(\alpha, A(\alpha), q)$. Fix $n \in \mathbb{Z}$, $n \geq 1$. Given $\alpha \in \mathcal{O}_K$ and a prime q such that $N(\alpha) = q \equiv 1 \pmod{n}$, where $N(\alpha) = \det(A(\alpha))$, this procedure computes a root of $\Phi_n(x) \pmod{q}$.

step 1.: Determine the matrix $M = [A(\alpha)^T | C]_{\varphi(n)\times\varphi(n)+1}$ which is a matrix obtained by appending the columns of $A(\alpha)^T$ and the vector C, where $C^T = [y, -1, 0, \ldots, 0]_{1\times\varphi(n)}$.

step 2.: Applying Gaussian Elimination algorithm over $\mathbb{F}_q$ transform the matrix M into the upper triangular form

$$M' = \left[\begin{array}{cccc|c} a'_{1,1} & a'_{2,1} & \cdots & a'_{\varphi(n),1} & c'_1 \\ 0 & a'_{2,2} & \cdots & a'_{\varphi(n),2} & c'_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a'_{\varphi(n),\varphi(n)} & c'_{\varphi(n)} \end{array}\right],$$

where $c'_i = c'_i(y)$ are polynomials of degree no greater than 1.

step 3.: For each $i = \varphi(n), \ldots, 1$

(1) Write

$$b_i = \frac{1}{a'_{ii}}\left(c'_i(y) - \sum_{j=i+1}^{\varphi(n)} a'_{ij}b_j\right) = \frac{r_i y + s_i}{t_i}, \quad \text{where} \quad q|t_i$$

(2) If $(r_i, q) = 1$ then compute $y \equiv -s_i r_i^{-1} \pmod q$ and go to Step 4. Otherwise go to Step 3

step 4.: Return $y \pmod q$.

Theorem 4. *Fix $n > 2$, and let $\Phi_n(x)$ be the nth cyclotomic polynomial. Given $\alpha \in \mathcal{O}_K$, a matrix $A(\alpha)$ and a prime q such that $q = N(\alpha) \equiv 1 \pmod n$, where $N(\alpha) = \det(A(\alpha))$, Procedure 3 is deterministic and finds a root of $\Phi_n(x) \pmod q$ using $O(\varphi(n)^3 \log^3 q)$ bit operations.*

Proof. See [12]. □

Procedure 5 (r, q). Given a prime q and $r < q$, the procedure finds a prime $p \equiv r \pmod q$.

step 1.: Choose randomly $k \in \mathbb{N}$ such that

$$k \in [10, ((2^{40}q^2(\log 2^{20}q)^{20}) - r)q^{-1}].$$

step 2.: Compute $p = qk + r$. If p is not a prime, then go to step 1.

step 3.: Return p.

Theorem 6. *Let a prime $q \in [x, 2x]$ be the output of Procedure 3, and let $r < q$. For sufficiently large $q \geq 2^{32}$ and an arbitrary real $\lambda \geq 1$, Procedure 5 finds $k \in \mathbb{N}$ and a prime $p = qk + r$ such that*

$$k \in [0, ((2^{40}q^2(\log 2^{20}q)^{20}) - r)q^{-1}], \quad q \leq p \leq 2^{40}q^2(\log 2^{20}q)^{20}$$

with probability greater than or equal to $1 - e^{-\lambda}$ after repeating $[\lambda 8 \log(2^{20}q)]$ steps of the procedure with the possible exception of at most $O(x(\log x)^{-2})$ values of q. Every step of the procedure takes at most $\mathcal{PT}$ bit operations.

Proof. See [12]. □

We are now in a position to introduce the main algorithm.

Algorithm 7. (n)
step 1.: $\alpha, A(\alpha), q :=$ Procedure 1 (n)
step 2.: $y :=$ Procedure 3 $(\alpha, A(\alpha), q)$
step 3.: $p :=$ Procedure 5 (y, q)
step 4.: Return p, q;

Theorem 8. *Algorithm 7 finds two primes p and q such that q is relatively n-cyclotomic to a prime p.*

Proof. See [12]. □

An interesting open problem is the following: Construct a polynomial-time algorithm that finds CM-primes p, q such that

$$\rho(E(\mathbb{F}^*_{p^n})) = \frac{n}{\varphi(n)} + o(1).$$

3. CM primes with respect to Δ

Throughout this section, $\Delta < 0$ is a square-free rational integer, $K = \mathbb{Q}(\sqrt{\Delta})$ is the quadratic field with the corresponding ring of integers

$$\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\},$$

and $\mathcal{O}_f = [1, f\omega]$, $f \in \mathbb{Z}$ is any order of K, where

$$\omega = \frac{1 + \sqrt{\Delta}}{2} \qquad \text{if} \quad \Delta \equiv 1 \pmod 4,$$
$$\omega = \sqrt{\Delta} \qquad \text{if} \quad \Delta \equiv 2, 3 \pmod 4.$$

By $N(\alpha) = \alpha\overline{\alpha} = (a + b\omega)(a + b\overline{\omega})$ we denote the norm of an element $\alpha = a + b\omega \in \mathcal{O}_K$ with respect to $\mathbb{Q}$. That is

$$N(\alpha) = a^2 + ab + \frac{1-\Delta}{4}b^2 \qquad \text{if} \quad \Delta \equiv 1 \pmod 4,$$
$$N(\alpha) = a^2 - \Delta b^2 \qquad \text{if} \quad \Delta \equiv 2, 3 \pmod 4.$$

In this section we describe a probabilistic algorithm which generates CM-primes q and p with respect to Δ that executes in polynomial time [11]. The algorithm consists of the following two procedures.

Procedure 9 (n, Δ, x, γ) Given $n, m \in \mathbb{N}$, $(m, n) = 1$, a square-free $\Delta \in \mathbb{Z}$, $\Delta < 0$, and a sufficiently large $x \in \mathbb{R}$. Fix $K = \mathbb{Q}(\sqrt{\Delta})$ with the corresponding ring of integers $\mathcal{O}_K$. Let $\gamma = f + g\omega \in \mathcal{O}_K$ be such that $|f|, |g| \leq n$, $N(\gamma) \equiv m \pmod n$; this procedure finds $\alpha = a + b\omega \in \mathcal{O}_K$, $N(\alpha) \equiv m \pmod n$, such that $N(\alpha) = q$ is a prime with $x \leq q \leq 2x$.

step 1.: Choose u, v at random in $\mathbb{Z}$ such that

$$|u| \leq \left(\frac{\sqrt{1-\Delta}}{\sqrt{-\Delta}}(2x)^{1/2} - f\right)n^{-1}, \quad |v| \leq \left(\frac{2}{\sqrt{-\Delta}}(2x)^{1/2} - g\right)n^{-1}$$
if $\Delta \equiv 1 \pmod 4$,
$$|u| \leq ((2x)^{1/2} - f)n^{-1}, \qquad |v| \leq \left(\frac{1}{\sqrt{-\Delta}}(2x)^{1/2} - g\right)n^{-1}$$
if $\Delta \equiv 2, 3 \pmod 4$.

step 2.: Compute $a = nu + f$ and $b = nv + g$

step 3.: Compute

$$q = a^2 + ab + \frac{1-\Delta}{4}b^2 \quad \text{if} \quad \Delta \equiv 1 \pmod 4,$$
$$q = a^2 - \Delta b^2 \quad \text{if} \quad \Delta \equiv 2, 3 \pmod 4.$$

If $q < x$ or $q > 2x$, then go to step 1.

step 4.: If q is a prime, then terminate the procedure. Otherwise, go to step 1.

step 5.: Return $\alpha = a + b\omega$, q.

Let $\mathfrak{f}$ be an ideal of $\mathcal{O}_K$. Let $H^*_{\mathfrak{f}}(K)$ be the group of narrow ray classes $\pmod{\mathfrak{f}}$, and let $h^*_{\mathfrak{f}}(K)$ be the number of elements in $H^*_{\mathfrak{f}}(K)$. In the notation above we have the following theorem.

Theorem 10. *Given $n, m \in \mathbb{N}$, $(m, n) = 1$, and a square-free integer $\Delta < 0$. Fix $K = \mathbb{Q}(\sqrt{\Delta})$ with the corresponding ring of integers $\mathcal{O}_K$, and let $\mathfrak{f} = n\mathcal{O}_K$. There exists $x_0 > 0$ such that for every $x \geq x_0$ and an arbitrary real $\lambda \geq 1$, Procedure 9 finds $\alpha = a + b\omega \in \mathcal{O}_K$ such that $N(\alpha) \equiv m \pmod{n}$ is a prime, $x \leq N(\alpha) \leq 2x$, where*

$$|a| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-\Delta}}(2x)^{\frac{1}{2}}, \quad |b| \leq \frac{2}{\sqrt{-\Delta}}(2x)^{\frac{1}{2}} \quad \text{if } \Delta \equiv 1 \pmod 4,$$
$$|a| \leq (2x)^{\frac{1}{2}}, \qquad\qquad |b| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{\frac{1}{2}} \quad \text{if } \Delta \equiv 2, 3 \pmod 4.$$

with probability greater than or equal to $1 - e^{-\lambda}$ after repeating $[c_1\lambda(\log x)]$ steps of the procedure, where

$$c_1 = \frac{16\sqrt{1-\Delta}h^*_{\mathfrak{f}}(K)}{-\Delta n^2} \quad \text{if} \quad \Delta \equiv 1 \pmod 4,$$
$$c_1 = \frac{16h^*_{\mathfrak{f}}(K)}{\sqrt{-\Delta}n^2} \quad \text{if} \quad \Delta \equiv 2, 3 \pmod 4.$$

Every step of the procedure takes no more than $\mathcal{PT}$ bit operations.

Proof. See [11]. □

Procedure 11 (α, q, Δ, x). Fix $0 < \varepsilon < 2/5$, and fix $K = \mathbb{Q}(\sqrt{\Delta})$ with the corresponding ring of integers $\mathcal{O}_K$. Given $\alpha = a + b\omega \in \mathcal{O}_K$ such that $q = N(\alpha) \equiv m \pmod n$, $(m, n) = 1$, is a prime, $x \leq q \leq 2x$; this procedure finds $\beta \in \mathcal{O}_K$ such that $\beta \equiv 1 \pmod{\alpha\mathcal{O}_K}$ and $N(\beta)$ is a prime.

step 1.: Choose s, t at random in $\mathbb{Z}$.

If $\Delta \equiv 1 \pmod 4$,

$$|s| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{2}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}.$$

If $\Delta \equiv 2, 3 \pmod 4$

$$|s| \leq (2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}$$

step 2.: Compute

$$c = as - \frac{1-\Delta}{4}bt + 1, \quad d = bs + (a+b)t \quad \text{if } \Delta \equiv 1 \pmod 4,$$
$$c = as + \Delta bt + 1, \qquad d = bs + at \qquad \text{if } \Delta \equiv 2, 3 \pmod 4.$$

step 3.: Compute

$$p = c^2 + cd + \frac{1-\Delta}{4}d^2 \quad \text{if} \quad \Delta \equiv 1 \pmod 4,$$
$$p = c^2 - \Delta d^2 \quad \text{if} \quad \Delta \equiv 2, 3 \pmod 4.$$

If $p < x$ or $p > (2x)^{5/(2-5\varepsilon)}$, then go to step 1.

step 4.: If p is a prime, then terminate the procedure. Otherwise, go to step 1.

step 5.: Return $\beta = c + d\omega$, p.

Theorem 12. *Let $\Delta < 0$ be a square-free integer. Fix $K = \mathbb{Q}(\sqrt{\Delta})$ with the corresponding ring of integers $\mathcal{O}_K$, and fix $0 < \varepsilon < \frac{2}{5}$. Let $\alpha \in \mathcal{O}_K$ and $x \le q \le 2x$ be the output of Procedure 9. Procedure 11 with the input consisting of α, q and Δ, has the following properties: there exists $x_0 > 0$ such that for every $x \ge x_0$, and for an arbitrary real $\lambda \ge 1$, and for any constant $A > 2$, the procedure finds $\beta \in \mathcal{O}_K$ such that,*

$$\beta = c + d\omega, \quad p = N(\beta) \text{ is a prime}, \quad x \le N(\beta) \le (2x)^{5/(2-5\varepsilon)},$$

with probability greater than or equal to $1 - e^{-\lambda}$ after repeating $[c_2\lambda(\log 2x)]$ steps of the procedure, where

$$c_2 = \frac{80h(K)\sqrt{1-\Delta}}{-(2-5\varepsilon)w(K)\Delta} \quad \text{if} \quad \Delta \equiv 1 \pmod 4,$$
$$c_2 = \frac{40h(K)}{(2-5\varepsilon)w(K)\sqrt{-\Delta}} \quad \text{if} \quad \Delta \equiv 2, 3 \pmod 4.$$

for almost all α with the possible exception of at most $O(x(\log x)^{-A})$ values of α. Every step of the procedure takes no more than $\mathcal{PT}$ bit operations.

Proof. See [11]. □

We are now in a position to introduce our main algorithm.

Algorithm 13. (n, Δ, x, γ)

step 1.: $\alpha, q :=$ Procedure 9 (n, Δ, x, γ).

step 2.: $\beta, p :=$ Procedure 11 (α, q, Δ, x).

step 3.: Return p, q, α, β.

Theorem 14. *Given $n, m \in \mathbb{N}$, $(m, n) = 1$, and a square-free integer $\Delta < 0$. Fix $K = \mathbb{Q}(\sqrt{\Delta})$ with the corresponding ring of integers $\mathcal{O}_K$. If Algorithm 13 terminates, then the output is a pair $\alpha, \beta \in \mathcal{O}_K$, $\beta = c + d\omega$ such that $q = N(\alpha) \equiv m \pmod{n}$, $N(\beta) = p$ are CM-primes.*

Proof. See [11]. □

Remark 15. Let $n \in \mathbb{N}$, and let $\Delta < 0$ be a square-free integer. Fix $K = \mathbb{Q}(\sqrt{\Delta})$ with the corresponding ring of integers $\mathcal{O}_K$. Given CM-primes $q = N(\alpha)$, $p = N(\beta)$, where $\alpha = a + b\omega$, $\beta = c + d\omega \in \mathcal{O}_K$. There exists an elliptic curve E over $\mathbb{F}_p$ with complex multiplication by an order $\mathcal{O}_d = [1, d\omega] \subseteq K$ such that q divides

$$\begin{aligned} |E(\mathbb{F}_p)| &= p + 1 - 2c - d \quad \text{if} \quad \Delta \equiv 1 \pmod 4, \\ |E(\mathbb{F}_p)| &= p + 1 - 2c \qquad\ \ \text{if} \quad \Delta \equiv 2, 3 \pmod 4. \end{aligned}$$

Let $c > 0$ be a constant, and let $\Delta = O((\log p)^c)$. For any $\epsilon > 0$ constructing E over $\mathbb{F}_p$ via the CM method takes $O((\log p)^{c(1+\epsilon)/2})$ arithmetic operations in $\mathbb{F}_p$.

An interesting open problem is the following: Construct a polynomial-time algorithm that finds CM-primes p, q such that

$$\rho(E(\mathbb{F}_p)) \leq 2.$$

References

[1] L. Adleman, *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, The 20th Annual Symposium on Foundations of Computer Science (Washington, DC, USA), SFCS '79, IEEE Computer Society, 1979, pp. 55–60.

[2] L. Adleman, J. DeMarrais, and M. Huang, *A subexponential algorithm for discrete logarithmsover the rational subgroup of the jacobians of large genus hyperelliptic curves over fnite felds*, Algorithmic Number Theory, LNCS 877, 1994, pp. 28–40.

[3] M. Agrawal, N. Kayal, and N. Saxena, *Primes is in p*, Ann. of Math. **160** (2004), no. 2, 781–793.

[4] A. Atkin and F. Morain, *Elliptic curves and primality proving*, Tech. report, Projet ICSLA RR-1256, INRIA, 1990.

[5] Z. Borevich and I. Shafarevich, *Number theory*, Academic Press, 1966.

[6] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography, second edition*, 2nd ed., Chapman & Hall/CRC, 2012.

[7] R. Dupont, A. Enge, and F. Morain, *Building curves with arbitrary small mov degree over fnite prime felds*, J. Cryptology **18** (2005), no. 2, 79–89.

[8] P. Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology - EUROCRYPT 2000, LNCS 1807, 2000, pp. 19–34.

[9] P. Gaudry, E. Thom´e, N. Th´eriault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, IACR Cryptology ePrint Archive (2004), 153.

[10] D. Gordon, Discrete logarithms in $gf(p)$ using the number feld sieve, SIAM J. Discret. Math. **6** (1993), no. 1, 124–138.

[11] M. Grześkowiak, *An algorithmic construction of fnite elliptic curves of order divisible by a large prime*, Fund. Inform.,to appear.

[12] M. Grześkowiak, *Algorithms for relatively cyclotomic primes*, Fund. Inform. **125** (2013), no. 2, 161–181.

[13] G. H. Hardy and J. E. Littlewood, *Some problems of partition numerorum iii: On the ex- pression of a number as a sum of primes*, Acta Math. **44** (1922), 1–70.

[14] A. Joux, *A new index calculus algorithm with complexity* $l(1/4+o(1))$ *in very small characteristic*, 2013.

[15] A. Joux and R. Lercier, *The function feld sieve in the medium prime case*, Advances in Cryptology - EUROCRYPT 2006, LNCS 4004 (Serge Vaudenay, ed.), Springer Berlin Heidelberg, 2006, pp. 254–270 (English).

[16] A. Joux, R. Lercier, N. Smart, and F.Vercauteren, *The number feld sieve in the medium prime case*, Advances in Cryptology - CRYPTO 2006, LNCS 4117, Springer Berlin Heidelberg, 2006, pp. 326–344.

[17] N. Koblitz, *Hyperelliptic cryptosystems*, Journal of Cryptology **1** (1989), no. 3, 139–150 (English).

[18] A. Lenstra, *Using cyclotomic polynomials to construct efcient discrete logarithm cryptosystems over fnite felds.*

[19] A. Lenstra and E. Verheul, *The xtr public key system*, Advances in Cryptology CRYPTO 2000, LNCS 1880, 2000, pp. 1–19.

[20] S. Pohlig and M. Hellman, *An improved algorithm for computing logarithms over and its cryptographic signifcance (corresp.)*, IEEE Trans. Inf. Theor. **24** (2006), no. 1, 106–110.
[21] J. Pollard, *Monte Carlo methods for index computation* (mod p), Mathematics of Computation 32 (1978), 918–924.
[22] K. Rubin and A. Silverberg, *Torus-based cryptography*, Advances in Cryptology - CRYPTO 2003, LNCS 2729, 2003, pp. 349–365.
[23] K. Rubin and A. Silverberg, *Using primitive subgroups to do more with fewer bits*, Algorithmic Number Theory 6th International Symposium, ANTS-VI, LNCS 3076, 2004, pp. 18–41.
[24] E. Savaş, T.A. Schmidt, and C. K. Koç, *Generating elliptic curves of prime order*, Cryptographic Hardware and Embedded Systems CHES 2001, LNCS 2162, 2001, pp. 145–161.
[25] P. Smith and C. Skinner, *A public-key cryptosystem and a digital signature system based on the lucas function analogue to discrete logarithms*, In Advances in Cryptology ASIACRYPT 1995, LNCS 917, 1995, pp. 357–364.
[26] N. Thériault, *Index calculus attack for hyperelliptic curves of small genus*, Advances in Cryptology - ASIACRYPT 2003, LNCS 2894, 2003, pp. 75–92.
[27] A. Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comput. **72** (2003), no. 241, 435–458.

LICZBY PIERWSZE I KRYPTOSYSTEMY OPARTE NA LOGARYTMACH DYSKRETNYCH

Streszczenie. W pracy przedstawiamy algorytmy, które generują liczby pierwsze do kryptosystemów opartych na logarytmach dyskretnych. Zaprezentowane algorytmy są probabilistyczne i działają w wielomianowym czasie.

Słowa kluczowe: Kryptosystemy oparte na torusie, kryptosystemy eliptyczne i hipereliptyczne.