J. Cryptology (1989) 1: 139–150

Journal of Cryptology

Hyperelliptic Cryptosystems[1]

Neal Koblitz
Department of Mathematics GN-50, University of Washington,
Seattle, WA 98195, U.S.A.

Abstract. In this paper we discuss a source of finite abelian groups suitable for cryptosystems based on the presumed intractability of the discrete logarithm problem for these groups. They are the jacobians of hyperelliptic curves defined over finite fields. Special attention is given to curves defined over the field of two elements. Explicit formulas and examples are given, and the problem of finding groups of almost prime order is discussed.

Key words. Cryptosystem, Public key, Discrete logarithm, Hyperelliptic curve, Jacobian.

1. Introduction

In a finite abelian group, if an element was obtained as a multiple of another known element (the "base"), the discrete logarithm problem consists in finding the integer that was multiplied by the base to get the element. Whenever we have a finite abelian group for which the discrete log problem appears to be intractable, we can construct various public key cryptosystems in which taking large multiples of a group element is the trapdoor function. Such cryptosystems were first constructed from the multiplicative group of a finite field. However, because certain special techniques are available for attacking the discrete log problem in that case (especially when the field has characteristic 2, see [13]), it is worthwhile to study other sources of finite abelian groups.

In [8] we described how the group of points on an elliptic curve can be used to construct public key cryptosystems. The purpose of the present article is to discuss the more general class of groups obtained from the jacobians of hyperelliptic curves. These jacobian varieties seem to be a rich source of finite abelian groups for which, so far as is known, the discrete log problem is intractable. We pay special attention to the case when the ground field has characteristic 2, because arithmetic over such fields is particularly amenable to efficient implementation, and because it is in that case that the multiplicative group of the field does not provide secure cryptosystems unless the size of the field is extremely large, as explained in [13].

After giving the basic definitions of the group elements and the group addition in Section 2, we describe an algorithm for addition in Section 3. In Sections 2 and

[1] Date received: February 4, 1988. Date revised: September 28, 1988.

3 we follow [2], with the addition of some minor modifications and clarifications. In particular, we treat a more general equation for the hyperelliptic curve, which enables us to include the case of characteristic 2. We next describe how to determine the number of $\mathbf{F}_{q^n}$-points on the jacobian for varying n, and discuss the problem of finding n for which the group has "almost prime" order. If the jacobian has a certain irreducibility property, the latter problem is a natural analog of the Mersenne number problem of elementary number theory. For groups of "almost prime" order we expect the discrete log problem to be intractable.

In Section 5 we describe how such public key cryptosystems as the Diffie–Hellman key exchange can be carried over to these jacobians. We briefly discuss the generation of the random group elements that are needed in such cryptosystems. Finally, we give a procedure which in many cases simplifies the computation of large multiples of group elements.

2. The Groups

Let K be an arbitrary field, and let $\bar{K}$ denote its algebraic closure. We define a *hyperelliptic curve C of genus g* over K to be an equation of the form $v^2 + h(u)v = f(u)$, where $h(u)$ is a polynomial of degree at most g and $f(u)$ is a monic polynomial of degree $2g + 1$. Here f and h have coefficients in K, and we require that the curve have no singular points (u, v), i.e., that there be no values $u, v \in \bar{K}$ which satisfy $v^2 + h(u)v = f(u)$ and also both of the partial derivative equations $2v + h(u) = 0$ and $h'(u)v - f'(u) = 0$ (where the derivative of a polynomial is defined over an arbitrary field by means of the usual formulas). Throughout this section we assume that the curve C has been fixed.

Let L be a field containing K. By an *L-point* $P \in C$ we mean either the symbol ∞ or else a solution $u = x \in L$, $v = y \in L$ of the equation $v^2 + h(u)v = f(u)$. The latter is called a "finite" point and is denoted $P_{x,y}$. If σ is an automorphism of L over K, we let P^σ denote $P_{\sigma(x),\sigma(y)}$ and set $\infty^\sigma = \infty$.

We now introduce the *jacobian* of the curve C, using the notion of a "divisor" on C. The reader interested only in the algorithms may skip to the beginning of Section 3, at which point we regard a divisor explicitly as merely a pair of polynomials. On the other hand, the reader who wants a treatment of the theory of algebraic curves that is more thorough than the discussion below is referred to [5].

A *divisor* is a finite formal sum of $\bar{K}$-points $D = \sum m_i P_i$. We define the *degree* of D to be the integer $\sum m_i$. The divisors form an additive group $\mathbf{D}$, in which the divisors of degree 0 form a subgroup $\mathbf{D}^0$. Given $D = \sum m_i P_i \in \mathbf{D}$, we define $D^+ = \sum_{m_i > 0} m_i P_i$ (the "positive part" of D), we say that $D \geq 0$ if $D = D^+$, and we set $D^0 = D - (\deg D)\infty$. Thus, $D^+ \geq 0$ and $D^0 \in \mathbf{D}^0$. Given two divisors $D_1 = \sum m_i P_i$ and $D_2 = \sum n_i P_i$ in $\mathbf{D}^0$, we define g.c.d. $(D_1, D_2) \in \mathbf{D}^0$ to be $(\sum \min(m_i, n_i)P_i)^0$, i.e., $\sum \min(m_i, n_i)P_i - (\sum \min(m_i, n_i))\infty$.

Given a finite point $P = P_{x,y} \in C$, we define its "opposite" $\tilde{P}$ to be $\tilde{P} = (x, -y - h(x))$, i.e., the unique other point with the same u-coordinate x. If $P = \infty$, then we define $\tilde{P} = \infty$.

Let $p(u, v)$ be a polynomial with coefficients in $\bar{K}$, considered as a function on C.

Since $v^2 = f(u) - h(u)v$ on C, we may replace higher powers of v by lower powers to obtain an equivalent "reduced" polynomial of the form $\bar{p}(u, v) = a(u) - b(u)v$. We define the *order* of $p(u, v)$ at a point $P \in C$, denoted $\mathrm{ord}_P\, p$, as follows:

(1) Assume $P = P_{x,y}$ is a finite point. Write $\bar{p}$ in the form $(u - x)^{r_0}(a_0(u) - b_0(u)v)$, where $(u - x)$ does not divide both a_0 and b_0; let $r = r_0$ if $P \neq \tilde{P}$ and $r = 2r_0$ if $P = \tilde{P}$. Then $\mathrm{ord}_{P_{x,y}}\, p$ is equal to r if $a_0(x) - b_0(x)y \neq 0$, and if $a_0(x) - b_0(x)y = 0$ it is equal to r plus the exponent of the highest power of $(u - x)$ which divides $a_0(u)^2 + h(u)a_0(u)b_0(u) - f(u)b_0(u)^2$.

(2) If $P = \infty$, then $\mathrm{ord}_\infty\, p = -\max(2 \deg a, 2g + 1 + 2 \deg b)$.

Here in (1) (assume with $r_0 = 0$) the idea is that with $v = a(u)/b(u)$ the value $u = x$ should be an ($\mathrm{ord}_{P_{x,y}}\, p$)-th root of $v^2 + h(u)v - f(u) = (a^2 + hab - fb^2)/b^2$. In (2), if we think of u as approaching ∞ "with order 2," then v approaches ∞ "with order $2g + 1$" (since $v^2 = u^{2g+1}$ + lower-order terms), and $|\mathrm{ord}_\infty\, p|$ is the order at which $a(u) - b(u)v$ approaches ∞; thus, we say that the order of vanishing of p at infinity is the negative of this value.

To any $p(u, v)$ such that $\bar{p} \neq 0$ (i.e., $p(u, v)$ is not divisible by $v^2 + hv - f$ as polynomials in u and v), we associate the divisor $(p) = \sum(\mathrm{ord}_P\, p)P$. Here the summation is over all points P on the curve (including ∞) where p has nonzero order. This sum is clearly finite. We can also verify that $(p) \in \mathbf{D}^0$. As an example, if $p(u, v) = u - x$, then $(u - x) = P_{x,y} + \tilde{P}_{x,y} - 2\infty$, where y is one of the two solutions of $y^2 + h(x)y = f(x)$.

By a *rational function* on C we mean a ratio of the form $p(u, v)/q(u, v)$ with $\bar{q} \neq 0$. To such a rational function we associate the divisor $(p/q) = (p) - (q) \in \mathbf{D}^0$. A divisor of the form $(p) - (q)$ is called *principal*; such divisors form a subgroup $\mathbf{P}$ of $\mathbf{D}^0$. The quotient group $\mathbf{D}^0/\mathbf{P}$ is called the *jacobian* $\mathbf{J}$ of the curve C. If $D_1, D_2 \in \mathbf{D}^0$, we write $D_1 \sim D_2$ if $D_1 - D_2 \in \mathbf{P}$, i.e., if D_1 and D_2 are equal when considered as elements of $\mathbf{J}$.

For example, for any $\bar{K}$-point P we have $P - \infty \sim -(\tilde{P} - \infty)$, since $P + \tilde{P} - 2\infty = (u - x)$ (where x is the u-coordinate of P). In particular, in the case when $P = \tilde{P}$ we have $2P \sim 2\infty$. It then follows that any $D \in \mathbf{D}^0$ can be modified by a principal divisor to obtain an equivalent $D_1 \sim D$ of the form $\sum m_i P_i - (\sum m_i)\infty$, where the $m_i \geq 0$ and the P_i are finite points such that when P_i occurs in the sum, $\tilde{P}_i$ does not occur, unless $\tilde{P}_i = P_i$, in which case the corresponding m_i is at most 1. We say that a divisor D is "semireduced" when it is brought to the form D_1.

If K is a perfect field (e.g., a finite field), we say that a divisor $D = \sum m_i P_i$ is *defined over K* (or is a "K-divisor") if $D^\sigma = \sum m_i P_i^\sigma$ is equal to D for all automorphisms σ of $\bar{K}$ over K. Notice that this does not mean that each P_i^σ is equal to P_i; σ may permute the points. We can show that a principal divisor is defined over K if and only if it is the divisor of a rational function that has coefficients in K.

It follows from the Riemann–Roch theorem (see [5]) that every $D \in \mathbf{D}^0$ can be uniquely represented as an element of $\mathbf{J}$ (i.e., modulo $\mathbf{P}$) by a semireduced divisor $D_1 = \sum m_i P_i - (\sum m_i)\infty$ for which $\sum m_i \leq g$. A divisor D_1 with this property is called *reduced*.

A semireduced divisor $D = \sum m_i P_{x_i, y_i} - (\sum m_i)\infty$ can be uniquely represented as the g.c.d. of two principal divisors of functions of the form $a(u)$ and $b(u) - v$ (that is, $D = \text{g.c.d.}\ ((a(u)), (b(u) - v)))$, where $a(u) = \prod(u - x_i)^{m_i}$ and $b(u)$ is the unique polynomial of degree $< \deg a$ such that $b(x_i) = y_i$ for each i and $b(u)^2 + h(u)b(u) - f(u)$ is divisible by $a(u)$. (If $a(u)$ happens to have distinct roots, i.e., if all $m_i = 1$, then the latter condition is redundant.) A divisor D represented in the form $\text{g.c.d.}\ ((a(u)), (b(u) - v))$ is abbreviated $D = \text{div}(a, b)$. D is reduced if and only if $\deg a \le g$.

For example, the divisor $D = P_{x,y} - \infty$ is equal to $\text{div}(a, b)$ with $a(u) = u - x$ and $b(u) = y$. If $h(u) = 0$ (which is possible only if char $K \neq 2$) and if $y \neq 0$, then for the divisor $D = 2P_{x,y} - 2\infty$ we have $a(u) = (u - x)^2$ and $b(u) = (\bar{f} + y^2)/2y$, where $\bar{f}$ denotes the remainder of $f(u)$ modulo $(u - x)^2$.

3. The Algorithm

From now on, a divisor D will be regarded simply as a pair of polynomials $D = \text{div}(a, b)$ such that $\deg b < \deg a$ and $b^2 + hb - f$ is divisible by a (here a, b, h, and f are polynomials in u). Such a divisor is called "semireduced." An element of our group **J** is an equivalence class of divisors. Every divisor is equivalent to a unique "reduced" divisor, by which we mean a semireduced $D = \text{div}(a, b)$ for which $\deg a \le g$.

If a, b, and c are three polynomials in u, then the notation $b = c \pmod a$ means that b is equal to the residue of c modulo a, i.e., it is the unique polynomial b of degree $< \deg a$ such that a divides $c - b$.

The algorithm for adding divisors $D \in \mathbf{J}$ consists of two stages. Given $D_1 = \text{div}(a_1, b_1)$ and $D_2 = \text{div}(a_2, b_2)$, we first find a semireduced divisor $D = \text{div}(a, b)$ such that $D \sim D_1 + D_2$. Next, we "reduce" D, i.e., we find $a'(u)$ and $b'(u)$ such that $\deg a' \le g$, $\deg b' < \deg a'$, and $D \sim \text{div}(a', b')$. Our description of the two stages of the algorithm follows [2], except that we are working without the assumption in [2] that $h(u) = 0$ and char $K \neq 2$. We omit the proof of correctness of the algorithm, which is virtually identical to the proof in [2].

Thus, we wish to find the sum of $\text{div}(a_1, b_1)$ and $\text{div}(a_2, b_2)$ on the jacobian of the curve $v^2 + hv = f$, where a_1, a_2, b_1, b_2, h, and f are all polynomials in u. (Here h and f have coefficients in K, and a_1, a_2, b_1, and b_2 may have coefficients in an extension field of K.)

Stage 1. Let $d = d(u)$ be the g.c.d. of the three polynomials $a_1(u)$, $a_2(u)$, and $b_1(u) + b_2(u) + h(u)$; and choose $s_1(u)$, $s_2(u)$, and $s_3(u)$ to be polynomials in u such that

$$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h). \tag{1}$$

Set

$$a = a_1 a_2 / d^2$$

and

$$b = (s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f))/d \pmod a. \tag{2}$$

We easily verify that d divides $s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f)$, so that this expression makes sense. We further derive the following identity of polynomials in u, v:

$$(b_1+b_2+h)(b-v)=(b_1-v)(b_2-v)+s_1a_1(b_2^2+hb_2-f)/d+s_2a_2(b_1^2+hb_1-f)/d,$$

from which the correctness of the definition is proved, as in [2].

Special Cases. 1. If a_1 and a_2 have no common factor, then $d = 1$, we can take $s_3 = 0$, and so $a = a_1a_2$, $b = s_1a_1b_2 + s_2a_2b_1 \pmod{a}$.

2. When $a_2 = a_1$ and $b_2 = b_1$ (i.e., we are doubling an element of **J**), we can take $s_2 = 0$.

(a) Assume char $K = 2$ and $h(u) = 1$. Then $d = 1$, $s_1 = s_2 = 0$, $s_3 = 1$, and $a = a_1^2$, $b = b_1^2 + f \pmod{a}$.

(b) Assume char $K = 2$ and $h(u) = u$. Also assume that u does not divide $a(u)$, which in this situation is equivalent to requiring that none of the P_i occurring in $\operatorname{div}(a_1, b_1) = \sum m_iP_i - (\sum m_i)\infty$ is equal to its opposite $\tilde{P}_i$. (If $P_i = \tilde{P}_i$, then $2P_i \sim 2\infty$, as we saw.) Then $d = 1$, $s_1 = (a_1(0))^{-1}$, $s_2 = 0$, $s_3 = (a_1(u)/a_1(0) + 1)/u$, and $a = a_1^2$, $b = (a_1b_1 + (a_1(u) + a_1(0))(b_1^2 + f)/u)/a_1(0) \pmod{a}$. For example, if $D = P_{x,y} - \infty = \operatorname{div}(u - x, y)$ (here x and y are constants), then $2D = \operatorname{div}(a, b)$ with $a = u^2 + x^2$ and $b = (\bar{f} + yu + xy + y^2)/x$, where $\bar{f}$ is the linear polynomial in u that is obtained from f by replacing u^2 by x^2.

Stage 2. Given $D = \operatorname{div}(a, b)$ with $\deg a > g$, the following procedure replaces D with an equivalent divisor $D' = \operatorname{div}(a', b')$ for which $\deg a' < \deg a$. By successively applying the procedure, we eventually obtain $D'' = \operatorname{div}(a'', b'')$ for which $D \sim D''$ and $\deg a'' \leq g$.

We set

$$a' = (f - hb - b^2)/a \tag{3}$$

and then

$$b' = -h - b \pmod{a'}. \tag{4}$$

We then show that $\operatorname{div}(a', b') \sim \operatorname{div}(a, b)$ and $\deg a' < \deg a$ (see [2]). This concludes the description of the algorithm.

Remarks. 1. This algorithm is analogous to the procedure for adding classes of quadratic forms. For instance, in Stage 2 with $h = 0$, the reduction formulas (3) and (4) are similar to the following formulas for finding a quadratic form $a'X^2 + 2b'XY + c'Y^2$ equivalent to the form $aX^2 + 2bXY + cY^2$ of discriminant $4f = 4(b^2 - ac)$. Assuming $a > b$, we replace $\begin{pmatrix} X \\ Y \end{pmatrix}$ by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$ to get $aY^2 - 2b(X + jY)Y + c(X + jY)^2$, i.e., $a' = c = (b^2 - f)/a$, $b' = -b + jc = -b \pmod{c}$ with j chosen so that b' is the least nonnegative residue modulo $c = a'$.

2. In the case $g = 1$ (elliptic curves), the reduced divisors $D = \operatorname{div}(u - x, y)$ are in one-to-one correspondence with the points $P_{x,y} \in C$. The above algorithm is then easily seen to reduce to the usual formulas for the addition of points on an elliptic curve (see, e.g., [6]).

Examples. Let $K = \mathbf{F}_2$ be the field of two elements. For $P \in C$ we let $P^{(j)}$ denote P^{σ^j}, where σ^j is the automorphism of $\bar{\mathbf{F}}_2$ given by $x \mapsto x^{2^j}$. In certain cases there are simple formulas expressing $2^k P$ in terms of $P^{(j)}$ which give a short-cut in computing multiples of $D = \sum m_i P_i - (\sum m_i)\infty$. The formulas below all follow by repeated application of Stage 1 (special case 2(a)) and then Stage 2 of the algorithm.

1. C is given by $v^2 + v = u^{2g+1}$. Then:

(a) for $g = 1$,
$$2P = -P^{(2)};$$
(b) for $g = 2$,
$$4P = -P^{(4)};$$
(c) for $g = 3$,
$$8P = 2P^{(3)} - P^{(6)};$$
(d) for $g = 4$,
$$8P = -P^{(6)}.$$

2. C is given by $v^2 + v = u^{2g+1} + u$. Then:

(a) for $g = 1$,
$$4P = -P^{(4)};$$
(b) for $g = 2$,
$$16P = P^{(8)};$$
(c) for $g = 4$,
$$64P = -P^{(12)}.$$

3. C is given by $v^2 + v = u^5 + u^3$, $g = 2$. Then
$$64P = -P^{(12)}.$$

4. C is given by $v^2 + v = u^5 + u^3 + u$, $g = 2$. Then
$$8P = P^{(6)}.$$

Remark. In Section 5 we give a general method for reducing the calculation of mP for m large to the computation of linear combinations of $P^{(j)}$ with small coefficients.

4. Number of Points

Let $\mathbf{J}$ be the jacobian of the hyperelliptic curve C given by an equation $v^2 + h(u)v = f(u)$ with coefficients in K. Assume that K is a perfect field, and let L be an algebraic field extension of K. We let $\mathbf{J}(L)$ denote the set of *L-points* of $\mathbf{J}$, i.e., the divisors D such that $D^\sigma = D$ for all automorphisms σ of $\bar{K}$ over L. Since this invariance property is preserved under addition, $\mathbf{J}(L)$ is a subgroup of $\mathbf{J} = \mathbf{J}(\bar{K})$. In terms of the explicit representation of divisors in the form $\operatorname{div}(a, b)$ which we used in Section 3, an L-point of $\mathbf{J}$ is simply an element $\operatorname{div}(a, b)$ for which the polynomials a and b have coefficients in L.

We assume that $K = \mathbf{F}_q$ is a finite field with q elements. It is easy to see that the abelian group $\mathbf{J}(L)$ is finite for any finite extension $L = \mathbf{F}_{q^n}$. We set

$$N_n = \#(\mathbf{J}(\mathbf{F}_{q^n})).$$

A basic fact about the N_n is that there is a simple method for determining the sequence $N_1, N_2, \ldots$ by counting the number of $\mathbf{F}_{q^n}$-solutions of the equation of C for the first g values $n = 1, \ldots, g$. We now describe this method.

Let $M_n = \#(C(\mathbf{F}_{q^n})) - q^n$, where $\#(C(\mathbf{F}_{q^n}))$ is the number of solutions $u, v \in \mathbf{F}_{q^n}$ of the equation $v^2 + h(u)v = f(u)$. Associated with the curve C is a polynomial $Z(T)$ of degree $2g$ with integer coefficients having the form

$$\begin{aligned} Z(T) &= T^{2g} + a_1 T^{2g-1} + \cdots + a_{g-1} T^{g+1} + a_g T^g \\ &\quad + q a_{g-1} T^{g-1} + q^2 a_{g-2} T^{g-2} + \cdots + q^{g-1} a_1 T + q^g \\ &= \prod_{j=1}^{g} ((T - \alpha_j)(T - \overline{\alpha_j})), \end{aligned} \tag{5}$$

where $a_1, \ldots, a_g \in \mathbf{Z}$ and where $\overline{\alpha_j} = q/\alpha_j$ (i.e., the roots are complex numbers of absolute value $\sqrt{q}$). The relationship between $Z(T)$ and $\{M_n\}$ is the following power series identity (where $\tilde{Z}(T)$ denotes the reciprocal polynomial $T^{2g}Z(1/T)$):

$$\log(\tilde{Z}(T)) = \sum_{n=1}^{\infty} \frac{M_n}{n} T^n.$$

Note that the first g values $M_1, \ldots, M_g$ are enough to determine the coefficients of $Z(T)$.

Once $Z(T)$ has been found, N_n can be determined from the formula

$$N_n = \prod_{j=1}^{g} |1 - \alpha_j^n|^2, \tag{6}$$

where $|\,|$ denotes the usual complex absolute value. In particular, $N_1 = Z(1)$. Also observe from (6) that $(q^{n/2} - 1)^{2g} \le N_n \le (q^{n/2} + 1)^{2g}$, i.e., N_n is asymptotically of magnitude q^{ng}.

Here are the explicit formulas in the simplest cases $g = 1$ and $g = 2$.

$g = 1$. If α is a root of $T^2 + M_1 T + q$, then $N_n = |1 - \alpha^n|^2$.

$g = 2$. We first find the number of $\mathbf{F}_q$- and $\mathbf{F}_{q^2}$-solutions of $v^2 + h(u)v = f(u)$, thereby determining M_1 and M_2. The coefficients of $Z(T)$ are given by $a_1 = M_1$, $a_2 = (M_1^2 + M_2)/2$. Next, let γ_1 and γ_2 be the two roots of the quadratic equation $X^2 + a_1 X + (a_2 - 2q) = 0$. Then α_j for $j = 1, 2$ is a root of the quadratic equation $X^2 - \gamma_j X + q = 0$. Finally, $N_n = |1 - \alpha_1^n|^2 |1 - \alpha_2^n|^2$.

Examples. 1. Let $K = \mathbf{F}_2$ and let C be given by $v^2 + v = u^5 + u^3$ (see Example 3 of Section 3). We find that the four roots of $Z(T)$ are

$$(1 \pm i)\left(\frac{-1 \pm i\sqrt{3}}{2}\right).$$

For n not divisible by 2 or 3 this leads to the formula

$$N_n = 2^{2n} + 2^n + 1 + (-1)^{[(n+1)/4]} 2^{(n+1)/2}(2^n + 1) \tag{7}$$

(here [ ] denotes the greatest integer function), while if n is divisible by 2 or 3, then N_n is a perfect square. For example, if n is divisible by 12, then $N_n = ((2i)^{n/2} - 1)^4$.

Similarly, for the curve $v^2 + v = u^5 + u^3 + 1$ over $\mathbf{F}_2$ the roots of $Z(T)$ are given by $(1 \pm i)((1 \pm i\sqrt{3})/2)$ and N_n (n not divisible by 2 or 3) is given by

$$N_n = 2^{2n} + 2^n + 1 - (-1)^{[(n+1)/4]} 2^{(n+1)/2}(2^n + 1). \tag{8}$$

2. Let $K = \mathbf{F}_2$ and C be given by $v^2 + v = u^5 + u^3 + u$ (see Example 4 of Section 3). A similar computation leads to the formula

$$N_n = 2^{2n} - 2^n + 1 \tag{9}$$

if n is prime to 6. If n is divisible by 2 but not by 3, then $N_n = (2^n + 2^{n/2} + 1)^2$; if n is divisible by 3 but not by 2, then $N_n = (2^n - 1)^2$; and if n is divisible by 6, then $N_n = (2^{n/2} - 1)^4$.

Remark. From the formula in Example 3 of Section 3 it follows that all $\mathbf{F}_{2^{12}}$-points on the jacobian of $v^2 + v = u^5 + u^3$ have order dividing 65. Thus, this group is isomorphic to $(\mathbf{Z}/65\mathbf{Z})^4$. Similarly, it follows from the formula in Example 4 of Section 3 that the group of $\mathbf{F}_{2^6}$-points on the jacobian of $v^2 + v = u^5 + u^3 + u$ is isomorphic to $(\mathbf{Z}/7\mathbf{Z})^4$.

For cryptographic purposes (see Section 5) it is desirable for $N_n = \#(\mathbf{J}(\mathbf{F}_{q^n}))$ to be divisible by a large prime number. The best possibility in this direction is for N_n itself to be prime. However, this rarely happens, because $\mathbf{J}(\mathbf{F}_{q^d})$ is a subgroup of $\mathbf{J}(\mathbf{F}_{q^n})$ for any divisor d of n, and so $N_d | N_n$.

Definition. We say that N_n is *almost prime* if N_n divided by the least common multiple of N_d $(1 \leq d < n, d|n)$ is prime. In particular, for n prime we say that N_n is almost prime if N_n/N_1 is prime.

We now assume that n is prime. By (6), we have

$$N_n/N_1 = \prod_{j=1}^{g} |(1 - \alpha_j^n)/(1 - \alpha_j)|^2. \tag{10}$$

If the α_j are not all conjugates, i.e., if the polynomial $Z(T)$ factors over the rationals, then even for n prime the value N_n/N_1 in (10) has a corresponding factorization.

Example. For C given by $v^2 + v = u^5$ over $\mathbf{F}_2$, $g = 2$, we have $Z(T) = T^4 + 4 = (T^2 + 2T + 2)(T^2 - 2T + 2)$ with roots $\pm 1 \pm i$; for n odd, N_n is given by $N_n = (2^n + 2^{(n+1)/2} + 1)(2^n - 2^{(n+1)/2} + 1)$.

On the other hand, if all of the α_j are conjugates, then $N_n/N_1 = \mathbf{N}((\alpha_1^n - 1)/(\alpha_1 - 1))$, where $\mathbf{N}$ denotes the absolute norm of an algebraic number. The question of primality of these norms is a natural generalization of the general Mersenne problem of studying when numbers of the form $(a^n - 1)/(a - 1)$ (n prime) are prime (see [1] and [14]).

Table 1. Genus two curves over $\mathbf{F}_2$ with irreducible $Z(T)$.

Equation of C	$Z(T)$
$v^2 + v = u^5 + u^3$	$T^4 + 2T^3 + 2T^2 + 4T + 4$
$v^2 + v = u^5 + u^3 + 1$	$T^4 - 2T^3 + 2T^2 - 4T + 4$
$v^2 + v = u^5 + u^3 + u$	$T^4 + 2T^2 + 4$
$v^2 + uv = u^5 + 1$	$T^4 + T^3 + 2T + 4$
$v^2 + uv = u^5 + u^2 + 1$	$T^4 - T^3 - 2T + 4$

Table 2. Almost prime values of $\#(\mathbf{J}(\mathbf{F}_{2^n}))$ for prime $n < 50$ for C given by $v^2 + v = u^5 + u^3 + u$.

n	$2^{2n} - 2^n + 1$
5	$3 \cdot 331$
7	$3 \cdot 5419$
13	$3 \cdot 22366891$
29	$3 \cdot 96076791871613611$

Table 3. Almost prime values of $\#(\mathbf{J}(\mathbf{F}_{2^n}))$ for prime $n < 50$ for C given by $v^2 + v = u^5 + u^3$.

n	$2^{2n} + 2^n + 1 + (-1)^{[(n+1)/4]}2^{(n+1)/2}(2^n + 1)$
5	$13 \cdot 61$
7	$13 \cdot 1429$
11	$13 \cdot 312709$
17	$13 \cdot 1326700741$
23	$13 \cdot 5415624023749$
29	$13 \cdot 22170214192500421$
37	$13 \cdot 1453030298001690873541$

Table 4. Prime values of $\#(\mathbf{J}(\mathbf{F}_{2^n}))$ for prime $n < 50$ for C given by $v^2 + v = u^5 + u^3 + 1$.

n	$2^{2n} + 2^n + 1 - (-1)^{[(n+1)/4]}2^{(n+1)/2}(2^n + 1)$
5	1321
7	14449
11	4327489
19	275415303169
23	70334392823809
31	4611545283086450689
43	5951631966296685834686149

Examples. Among all genus two curves defined over $\mathbf{F}_2$, there are five cases of irreducible $Z(T)$, given in Table 1. In the first three cases, the formulas for N_n, given in (7)–(9) above, are algebraic factors of $2^{6n} + 1$ or $2^{3n} + 1$, and so the question of almost primality can be determined from the factorization tables of $2^n + 1$ in [1]. Tables 2–4 list in each of those three cases all primes $n < 50$ for which N_n is almost prime. Note that for C given by $v^2 + v = u^5 + u^3 + 1$ we have $N_1 = 1$, and so in that case the groups $\mathbf{J}(\mathbf{F}_{2^n})$ actually have prime order for the tabulated values of n.

5. Cryptosystems

Whenever we have a finite abelian group for which the discrete logarithm problem appears to be intractable, we can construct various public key cryptosystems in which taking large multiples of a group element is the trapdoor function.

In the case of the group of $\mathbf{F}_{q^n}$-points of the jacobian $\mathbf{J}$ of a hyperelliptic curve C defined over $\mathbf{F}_q$, the discrete log problem takes the following form, in the notation of Section 2.

Definition. The *discrete logarithm problem* on $\mathbf{J}(\mathbf{F}_{q^n})$ is the problem, given two divisors D_1 and D_2 defined over $\mathbf{F}_{q^n}$, of determining an integer $m \in \mathbf{Z}$ such that $D_2 \sim mD_1$ if such m exists.

Thus, the Diffie–Hellman key exchange [3] in the context of $\mathbf{J}(\mathbf{F}_{q^n})$ works as follows. The finite field $\mathbf{F}_{q^n}$ and the equation of C are publicly known, as is a fixed element $D_0 \in \mathbf{J}(\mathbf{F}_{q^n})$. Each user A chooses a large integer m_A, which is kept secret, and computes and makes public the divisor $m_A D_0$. When two users A and B wish to have a key for use in some other cryptosystem, they use the divisor $m_A m_B D_0 \in \mathbf{J}(\mathbf{F}_{q^n})$. Here divisors are reduced to the form $\operatorname{div}(a, b)$ with $\deg b < \deg a \leq g$, and some standard way is agreed upon, using the coefficients of a and b, to associate to $\operatorname{div}(a, b)$ an integer which serves as the key.

Similarly, the Massey–Omura and ElGamal systems can be adapted for the group $\mathbf{J}(\mathbf{F}_{q^n})$ just as they were for elliptic curves in [8]. Now, of course, we are taking multiples of divisors rather than simply points.

In cryptosystems of this sort, we need to have a method of generating a "random" element of the group. In our case this means a divisor $D \in \mathbf{J}(\mathbf{F}_{q^n})$. It suffices to show how to find a "random" point P on C with coordinates in $\mathbf{F}_{q^n}$, after which we can generate $D = \sum m_i P_i - (\sum m_i)\infty$ with $m_i \geq 0$ and $\sum m_i \leq g$ by choosing points P with $\mathbf{F}_{q^{kn}}$-coordinates for small ($\leq g$) values of k and then setting D equal to a sum of divisors of the form $\sum_{\sigma \in \operatorname{Gal}(\mathbf{F}_q{}^{kn}/\mathbf{F}_q{}^{n})} P^\sigma - k\infty$.

Without loss of generality we may assume $n = 1$, i.e., we may regard C as defined over $\mathbf{F}_{q^n}$ and replace q^n by q. Let C have equation $v^2 + h(u)v = f(u)$, as before. Choose the coordinate $u = x \in \mathbf{F}_q$ at random and attempt to solve $v^2 + h(x)v = f(x)$ for v.

Case (i). q is odd. Then the problem reduces to taking a square root in a finite field. There is approximately a 50% chance that a solution $v = y$ exists, in which case it can be found, for example, by Shanks' probabilistic method (see pp. 47–48 of [7]). If no solution exists, then we choose another random $u = x \in \mathbf{F}_q$ and repeat the procedure.

Case (ii). q is even. Then $h(x) \neq 0$, and the change of variables $z = v/h(x)$ leads to the equation $z^2 + z = a$, where $a = f(x)/h(x)^2$. It is easy to see that this equation has a solution $z \in \mathbf{F}_q$ if $\operatorname{Tr}_{\mathbf{F}_q/\mathbf{F}_2} a = 0$ and does not have a solution if this trace is 1. In the latter case, we must choose another $u = x \in \mathbf{F}_q$ and start again. In the former case we can find z as follows. If $q = 2^n$ is an odd power of 2, simply set $z = \sum_{j=0}^{(n-1)/2} a^{2^{2j}}$. For even n, we can proceed as in [11, p. 80]: first choose γ such that $\operatorname{Tr}_{\mathbf{F}_q/\mathbf{F}_2} \gamma = 1$. Next, set $\delta_j = a + a^2 + a^4 + \cdots + a^{2^{j-1}}$ for $j = 1, 2, \ldots, n$. Finally, take $z = \sum_{j=1}^{n} \delta_j \gamma^{2^{j-1}}$.

Thus, there exist efficient probabilistic algorithms for selecting random $D \in \mathbf{J}(\mathbf{F}_{q^n})$. It is not known whether there exist deterministic polynomial-time algorithms for this.

Computing Multiples of Divisors. A central ingredient in cryptosystems based on the discrete log problem in an abelian group A is an efficient process for computing mD for $D \in A$ and for large integers m. Suppose that the group law in A is given explicitly by an algorithm taking time $O(\log^r(\# A))$. Then the repeated-doubling method enables us to compute mD in $O(\log m \log^r(\# A))$ bit operations.

Assume $A = \mathbf{J}(\mathbf{F}_{q^n})$ is the jacobian of a curve C defined over $\mathbf{F}_q$. We regard q and C as fixed, and n as varying. It is easy to see that the algorithm in Section 2 takes $O(n^2)$ bit operations. Since mD depends only upon m modulo $\# A$ (here we are assuming $\# A$ to be known), it follows that we may assume that $m < \# A = O(q^{gn})$. Thus, mD can be computed in time $O(n^3)$.

In practice, rather than using the pure repeated doubling method, in some cases it is more efficient to combine it with a procedure which replaces mD by a linear combination with small integer coefficients of the divisors D^{σ^j} (where $\sigma\colon x \mapsto x^q$ is the Frobenius automorphism of $\mathbf{F}_{q^n}$). This sometimes reduces the total number of additions of divisors that must be performed in order to compute mD. We now describe this procedure.

Proposition. *Let* $\mathbf{J}$ *be the jacobian of a genus* g *curve* C *defined over* $\mathbf{F}_q$. *Suppose that* n_0 *is large enough so that*

$$(1 + q^{-n_0/2})^{2g} < 2. \tag{11}$$

Then there exists a polynomial-time (in n *and* $\log m$*) algorithm which for any* m *and* n *gives an expression for* mD, $D \in \mathbf{J}(\mathbf{F}_{q^n})$, *in the form* $\sum_{j=0}^{n-1} a_j D^{\sigma^j}$ *in which the integers* a_j *satisfy* $|a_j| < q^{n_0 g}$.

Proof. Let $G = \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) = \{\sigma^j\}_{j \in \mathbf{Z}/n\mathbf{Z}}$. The group ring $\mathbf{Z}[G]$ acts on $\mathbf{J}(\mathbf{F}_{q^n})$ in the obvious way: $(\sum a_j \sigma^j) \sum m_i P_i = \sum_{i,j} m_i a_j P_i^{\sigma^j}$. If $Z(T)$ is the polynomial (5), then it is known (see, e.g., [16]) that $Z(\sigma) \in \mathbf{Z}[G]$ annihilates every $D \in \mathbf{J}(\mathbf{F}_{q^n})$. Now for any n_0, the polynomial $Z_{n_0}(T)$ defined by

$$Z_{n_0}(T) = \prod_{j=1}^{g} (T - \alpha_j^{n_0})(T - \bar{\alpha}_j^{n_0})$$

has the property that $Z_{n_0}(T^{n_0})$ is divisible by $Z(T)$, and hence $Z_{n_0}(\sigma^{n_0})$ also annihilates $\mathbf{J}(\mathbf{F}_{q^n})$. We claim that the condition (11) ensures that the constant term $q^{n_0 g}$ of $Z_{n_0}(T)$ is greater than the sum of the absolute values of all other coefficients. To see this, note that, since $|\alpha_j| = \sqrt{q}$, it follows that the sum of the absolute values of all coefficients of $Z_{n_0}(T)$ is at most

$$\prod_{j=1}^{g} (1 + |\alpha_j^{n_0}|)^2 = (1 + q^{n_0/2})^{2g} < 2q^{n_0 g},$$

by (11). This proves the claim. To prove the proposition, it now suffices to observe that for any $D \in \mathbf{J}(\mathbf{F}_{q^n})$ we have

$$q^{n_0 g} D = -(Z_{n_0}(\sigma^{n_0}) - q^{n_0 g})D,$$

where the sum of the absolute values of the coefficients of the element of $\mathbf{Z}[G]$ on the right is $< q^{n_0 g}$. This gives an inductive procedure for expressing any element of $\mathbf{Z}[G]$ modulo $Z(\sigma)$ in the form $\sum_{j=0}^{n-1} a_j \sigma^j$ with $|a_j| < q^{n_0 g}$. In particular, any $m \in \mathbf{Z} \subset \mathbf{Z}[G]$ can be so expressed. □

Example. For C given by $v^2 + v = u^5 + u^3$ over $\mathbf{F}_2$, the constant term $4 = Z(0)$ is not greater than the sum of the other coefficients (see Table 1). However, for $n_0 \geq 5$ we have (11). Let $n_0 = 6$. Then $Z_6(T^6) = (T^{12} + 64)^2$. Since $Z(T)$ divides $(T^{12} + 64)^2$ and has no multiple factors, it actually divides $T^{12} + 64$, and so we have $64D = -D^{\sigma^{12}}$. (See Example 3 at the end of Section 3.) Now assume, for instance, that $D \in \mathbf{J}(\mathbf{F}_{2^{37}})$ (see Table 3) and $m \approx 10^{23}$ is a large positive integer. We write m to the base 64: $m = \sum_{j=0}^{13} m_j 64^j$, $0 \leq m_j < 64$. Then

$$mD = \sum_{j=0}^{13} (-1)^j m_j D^{\sigma^{12j}},$$

where we can replace $12j$ in the exponent of σ by its least nonnegative residue modulo 37.

References

[1] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorization of $b^n \pm 1, b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers*, American Mathematical Society, Providence, RI, 1983.

[2] D. Cantor, Computing in the jacobian of a hyperelliptic curve, *Math. Comp.*, **48** (1987), 95–101.

[3] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory*, **22** (1976), 644–654.

[4] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theory*, **31** (1985), 469–472.

[5] W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969.

[6] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.

[7] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.

[8] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.* **48** (1987), 203–209.

[9] N. Koblitz, Primality of the number of points on an elliptic curve over a finite field, *Pacific J. Math.*, **131** (1988), 157–165.

[10] S. Lang, *Introduction to Algebraic Geometry*, Interscience, New York, 1958.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.

[12] V. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology–Crypto '85*, Springer-Verlag, New York, 1986, pp. 417–426.

[13] A. M. Odlyzko, Discrete logarithms and their cryptographic significance, *Advances in Cryptography: Proceedings of Eurocrypt 84*, Springer-Verlag, New York, 1985, pp. 224–314.

[14] E. Seah and H. C. Williams, Some primes of the form $(a^n - 1)/(a - 1)$, *Math. Comp.*, **33** (1979), 1337–1342.

[15] D. Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd edn., Chelsea, New York, 1985.

[16] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* (4), **2** (1969), 521–560.