Constructive and destructive facets of torus-based cryptography

David R. Kohel

School of Mathematics and Statistics
University of Sydney, NSW 2006, Australia
kohel@maths.usyd.edu.au

Abstract. We introduce a constructive model for algebraic tori based on reduced divisors on singular curves. By using a singular hyperelliptic model, this provides an alternative representation, and computational model, for groups of rational points on an algebraic tori [4]. We obtain a represention of elements on certain tori of dimension r in compact representation using $r+1$ elements. By embedding the ElGamal discrete logarithm of a composite degree field in an algebraic torus, we obtain an attack on the discrete logarithm problem based on index calculus in the generalized Jacobian of a hyperelliptic curve.

Key words: Torus-based cryptography, ElGamal discrete logarithms

1 Introduction

The Jacobian of a nonsingular curve is an abelian variety, whose set of rational points is equipped with the structure of an abelian group. In the simplest nontrivial case, that of an elliptic curve, the group of rational points is represented by defining equations for the abelian variety, which is canonically identified with the curve itself. Curves of genus two are represented by an equation of a hyperelliptic curve $C : y^2 = f(x)$, where $f(x)$ is of degree 5 or 6. Rational points on the Jacobian J, an abelian variety of dimension two, are represented by reduced divisors on the curve, identifying the rational points of J with reduced divisors on C. The Cantor reduction algorithm [1] provides an effective model for computation in the Jacobian of a hyperelliptic curve using reduced divisors. Analogous algorithms have been worked out for representing elements of the Jacobians of curves in other families, such as superelliptic and C_{ab} curves.

Often with little or no modification, the algorithmic models for representing elements of the Jacobian carry over to singular curves in the respective families – hyperelliptic, superelliptic, or C_{ab} curves. The geometric object modelled by the divisor groups is a generalized Jacobian [3].

This geometric object is still a group scheme, but will be of mixed type, with simple quotients isomorphic to affine space, algebraic tori, or abelian varieties. Following [4], we denote by $T_n/\mathbb{F}_q$ the simple algebraic torus of dimension $\varphi(n)$, with $|T_n(\mathbb{F}_{q^r})| = \Phi_n(q^r)$, for any extension degree r coprime to n, where $\Phi_n(x)$ is the n-th cyclotomic polynomial of degree $\varphi(n)$. As a first case, we describe the basic arithmetic properties of degenerate elliptic curves. We then present a more general model for tori in terms of singular hyperelliptic curves, for which the generalized Jacobians are pure algebraic tori, whose factors are of the form T_n. As a consequence, we are able to carry over both the explicit constructive theory of hyperelliptic curves to the setting of algebraic tori, but also to apply the destructive potential of subexponential hyperelliptic curve algorithms for large genus curves.

2 Degenerate Elliptic Curves

The singular elliptic curve $E/\mathbb{F}_q : v^2 = u^2(u+\delta)$, where $\delta \neq 0$, provides the first nontrivial example of a singular curve whose generalized Jacobian gives a algebraic torus. The nonsingular points – those other than $(0,0)$ – form a group with the point O at infinity as the identity. The standard addition law on an elliptic curve determines the group law:

$$[2](u,v) = \Big(\frac{u^2}{4(u+\delta)}, \frac{(u^3-2\delta)uv}{8(u+\delta)^2}\Big)$$

and $(u_1,v_1)+(u_2,v_2) = (u_3,v_3)$, where

$$u_3 = \frac{(u_1u_2(u_1+u_2+2\delta) - 2v_1v_2)}{(u_1-u_2)^2},$$
$$v_3 = \frac{(u_1+3u_2)u_1^2v_2 - (3u_1+u_2)u_2^2v_1 + 2\delta(u_1v_2-u_2v_1)(u_1+u_2)}{(u_1-u_2)^3}.$$

Cantor reduction for curves of hyperelliptic type determines the same group law on the nonsingular points $E(\mathbb{F}_q)\backslash\{(0,0)\}$. This group maps injectively to the unit group $\mathbb{F}_q[\gamma]^*$, where γ is a square root of δ, by the map

$$(u,v) \longmapsto \frac{v-\gamma u}{v+\gamma u}. \tag{1}$$

This map is a homomorphism of groups, with image $\mathbb{F}_q^*$ when δ is a square, or surjects on the cyclic subgroup of order $q+1$ in $\mathbb{F}_q[\gamma]^*$ consisting of elements of norm 1. The generalized Jacobian J of E is a torus canonically

identified with the open subscheme $E\backslash\{(0,0)\}$ of nonsingular points on E together with the point at infinity as identity. In the notation of Rubin and Silverberg, this torus is $J = T_1$ when δ is a square in $\mathbb{F}_q^*$, and $J = T_2$ otherwise.

Note that in either case, the torus is of dimension 1, and we have achieved a representation of J as a curve of arithmetic genus 1, for which points are specified using two coefficients u, v. A rational model for this curve would achieve the desired goal of Rubin and Silverberg [4] of representing the torus of dimension one with exactly one coefficient. In this case we can achieve this minimal representation, using the inclusion of the coordinate ring in its integral closure:

$$\frac{\mathbb{F}_q[u,v]}{(v^2 - u^3 - \delta u^2)} \subseteq \mathbb{F}_q[z], \tag{2}$$

where $z = v/u$, so that $(u,v) = (z^2 - \delta, z(z^2 - \delta))$. Thus there is a bijective correspondence between points (u,v) in $E\backslash\{(0,0)\}$ and z with $z^2 \neq \delta$.

In the section which follows, we generalize this construction to reduced divisors on singular hyperelliptic curves of arithmetic genus $r+1$ in order to represent certain torus of dimension r by $2r+2$ coefficients in a standard model, and $r+1$ coefficients in compact form. Thus we are able to achieve a model for these algebraic tori which is near the optimal representation achieved by a birational map to $\mathbb{A}^r$.

3 Hyperelliptic Models for Tori

In this section we propose singular hyperelliptic curves as a computational model for representing algebraic tori. The algorithms for Cantor reduction [1] and arithmetic of reduced divisors on hyperelliptic curves is well-developed and composition and divisor reduction carry over essentially unmodified to singular hyperelliptic curves. Thus we obtain efficient models for arithmetic on algebraic tori using existing computational machinery.

We propose using reduced divisors on singular hyperelliptic curves of geometric genus 0 of the form

$$C : y^2 = cxf(x)^2, \tag{3}$$

for c in $\mathbb{F}_q$ and $f(x)$ squarefree in $\mathbb{F}_q[x]$ as a model for algebraic tori. The generalized Jacobian J of C is then a torus of dimension equal to $n = \deg(f(x))$. A point on J is represented by a reduced divisor, determined

by an ideal $(a(x), y - b(x))$, where $a(x)$ is a monic polynomial of degree n and $b(x)$ is a polynomial of degree less than that of $a(x)$. Thus we need $2n$ coefficients to specify a point on the torus of dimension n in this representation.

If $f(x)$ factors as $f_1(x)f_2(x)$, we note that we obtain quotients to the curves C_i given by

$$C_i : y_i^2 = cxf_i(x)^2,$$

by taking $(x, y) \mapsto (x, y/f_{3-i}(x))$. The induced maps on divisors imply that the generalized Jacobian is isogenous over $\mathbb{F}_q$ to the product $J_1 \times J_2$ of generalized Jacobians of C_1 and C_2. In particular, J is not simple.

If we apply the same principle over a splitting field $\mathbb{F}_{q^n}$ for $f(x)$, we obtain an isomorphism of J with the Weil restriction of $\mathbb{G}_m = T_1/\mathbb{F}_{q^n}$ or $T_2/\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, as we now explain. Explicitly we proceed as above and reduce to the case of the degenerate elliptic curve. Let δ be a root of $f(x)$ in $\mathbb{F}_{q^n}$, and write $f(x) = (x-\delta)g(x)$. Then C has a map to the degenerate elliptic curve

$$E_\delta : v_\delta^2 = cu^2(u + \delta), \tag{4}$$

given by

$$(x, y) \mapsto (u, v) = (x + \delta, y/g(x + \delta)).$$

As in the previous section we find that E_δ is isomorphic to either $T_1/\mathbb{F}_{q^n}$ or $T_2/\mathbb{F}_{q^n}$, depending on whether or not $c\delta$ is a square in $\mathbb{F}_{q^n}$. By descending back to $\mathbb{F}_q$, we conclude that J is isomorphic to the Weil restriction of $T_1/\mathbb{F}_{q^n}$ or $T_2/\mathbb{F}_{q^n}$, and we therefore find the splitting

$$J \sim \prod_{m|n} T_m \text{ or } J \sim \prod_{m|n} T_{2m}$$

up to isogeny. If n is odd, then for each fixed $f(x)$, the class of c in $\mathbb{F}_q^*/\mathbb{F}_q^{*2}$ determines which of the two cases occurs. We summarise this result in the following theorem.

Theorem 1. *For n odd and coprime to q, the algebraic tori T_n and T_{2n} can be represented as subschemes of the generalized Jacobians of the singular hyperelliptic curves*

$$C : y^2 = cxf(x)^2,$$

for irreducible polynomials $f(x)$ of degree n in $\mathbb{F}_q[x]$. The codimension of T_n or T_{2n} in J is $n - \varphi(n)$.

In particular for n an odd prime, the tori T_n and T_{2n} can be represented as subschemes of codimension 1 in some generalized Jacobians.

Example 1. The 2-dimensional torus $T_6/\mathbb{F}_{13}$ embeds in the 3-dimensional generalized Jacobian of the curve

$$C_1 : y^2 = x(x^3 + x + 5)^2.$$

One checks that the group $J(\mathbb{F}_{13})$ is a cyclic group of order $13^3 + 1$. The image of $T_6(\mathbb{F}_{13})$ determines a subgroup of order $157 = 13^2 - 13 + 1$, for which the reduced divisor

$$(x^3 + 2x^2 + 4x + 3, y - x^2 - x + 2)$$

is a generator. Using this divisor representation, each point is specified by 6 coefficients, as would be necessary for the embedding in $\mathbb{F}^*_{13^6}$.

The arithmetic of the generalized Jacobian carries over to curves which are not absolutely irreducible. For $f(x)$ of odd degree, Cantor reduction can be extended to irreducible curves C of the form $y^2 = cf(x)^2$, despite the fact that C splits into a union of two curves over a quadratic extension.

Example 2. The 2-dimension torus $T_6/\mathbb{F}_{13}$ can be represented more compactly as the generalized Jacobian of the absolutely reducible curve

$$C_2 : y^2 = 2(x^3 + x + 5)^2.$$

Since C_2 itself has no rational points over $\mathbb{F}_{13}$, every reduced divisor is of the form $(a(x), y - b(x))$ where $a(x)$ is an irreducible polynomial of degree 2 and $b(x)$ has degree 1, a typical example being the divisor

$$(x^2 + 3x + 6, y - x - 1),$$

which generates the group $J(\mathbb{F}_{13})$ of order 157. With this model only 4 coefficients are necessary to specify a point.

While the latter construction is more efficient in the hyperelliptic divisor representation, it fails to yield the more compact form of the next section, so we will not pursue this representation further. However, we do note that for any reduced divisor $(a(x), y - b(x))$ in this model, the factorizations of $a(x)$ have the interesting property of consisting only of even degree polynomials. This property may have relevance to the subexponential attacks of the final section.

4 Compact Divisor Representations

In this section we make use of the integral closure, analogous to (2), in order to find a compact representation for points on J. The integral closure of the coordinate ring of the curve (3) is a polynomial ring:

$$\frac{\mathbb{F}_q[x,y]}{(y^2 - cxf(x)^2)} \subseteq \mathbb{F}_q[z]$$

where $x = z^2/c$ and $y = f(x)z$. A reduced divisor $(a(x), y - b(x))$ in J will be coprime to $f(x)$, and is determined by a unique monic polynomial of degree at most n in z. This gives a rational model for the generalized Jacobian J, and when n is prime, a torus T isomorphic to T_n or T_{2n} embeds as a subscheme of codimension 1. As a result, points are thus specified by $n = \dim(T) + 1$ coefficients, which is near the optimal which would be achieved by a rational representation of T itself.

5 Attacks by Weil Descent to Tori

The reduction of a generalized Jacobian to the singular elliptic curve (4), followed by the map (1) to a multiplicative group can be applied in reverse, to pull back a discrete logarithm problem in a finite field extension to an algebraic torus over a subfield. The isomorphic discrete logarithm problem may then be attacked by subexponential algorithms.

We indicate, by way of example, how the discrete logarithm problem on a torus represented in terms of singular hyperelliptic divisors is open to such an attack. For this purpose the arithmetic of singular hyperelliptic curves, their generalized Jacobians, and index calculus attacks were implemented in Magma [2].

Example 3. Let $C/\mathbb{F}_{17}$ be the singular hyperelliptic curve given by the Weierstrass equation:

$$y^2 = x(x^7 + 11x^4 + 14x^3 + 15x^2 + 16x + 10)^2.$$

The generalized Jacobian J of C is isogenous to $T_2 \times T_{14}$, where T_2 is the nontrivial quadratic twist of $\mathbb{G}_m$ with

$$T_2(\mathbb{F}_{17}) \cong \{x \in \mathbb{F}_{17^2}^* | \mathrm{N}(x) = 1\},$$

and T_{14} is a Galois twist of $\mathbb{G}_m^6$ such that $T_{14}(\mathbb{F}_{17})$ is isomorphic to the cyclic subgroup of $\mathbb{F}_{17^{14}}^*$ of prime order

$$\Phi_{14}(p) = p^6 - p^5 + p^4 - p^3 + p^2 - p + 1 = 22796593.$$

Conventional wisdom would suggest that the best subexponential attacks on the discrete logarithm in $T_{14}(\mathbb{F}_{17})$ are obtained by embedding the DLP in $\mathbb{F}^*_{17^{14}}$, a group of order

$$17^{14} - 1 = 168377826559400928,$$

thus the security of the DLP should be judged in terms of naïve square root attacks on a group of order $O(p^6)$ or subexponential attacks on a group of order $O(p^{14})$. However, using the native representation of T_{14} in J, the nine points

$$\{(0,0),(1,1),(2,3),(4,3),(8,6),(9,1),(13,1),(15,5),(16,3)\},$$

on C give rise to a factor basis of reduced degree one divisors on J, over which we can attempt to find smooth relations among the reduced divisors of degree 7. This yields the relation matrix:

$$\begin{bmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 5 & 3 & 0 & 1 & -1 & 4 \\
1 & 3 & 1 & 2 & 4 & 4 & -3 & -2 & -1 \\
1 & 6 & 0 & 4 & -4 & 1 & -4 & 5 & -2 \\
0 & 5 & -5 & -3 & 1 & 3 & 7 & 2 & -2 \\
0 & 2 & 1 & 4 & 3 & -4 & 4 & 0 & -8 \\
1 & 3 & 3 & 0 & 6 & -2 & -2 & 9 & 3 \\
0 & 3 & -4 & -3 & -3 & -3 & -1 & -9 & 8 \\
0 & 3 & 23 & 3 & -9 & 5 & 8 & -4 & 2
\end{bmatrix}$$

much more readily than would the corresponding factor basis of degree one polynomials among the degree 13 representatives for $\mathbb{F}^*_{17^{14}}$. We note that in this example, we made use of auxilliary divisors of degree two which were subsequently eliminated.

Note that the torus T_{14} of dimension six can also be represented in terms of reduced divisors on the absolutely reducible curve:

$$y^2 = c(x^7 + 11x^4 + 14x^3 + 15x^2 + 16x + 10)^2,$$

where c is any nonsquare in $\mathbb{F}^*_{17}$. There exist no rational points on this curve over any odd degree extension, thus the only possible smooth elements over which we can factor divisors have even degree.

6 Torus-based Cryptanalysis

We have shown that certain algebraic tori have a representation which is both practical for efficient implementations, and, in large dimension, ammenable to subexponential attacks. In general the probability of finding smooth divisors in these representations of algebraic tori may be lower than for finite field extensions, due to the relative lack of degree one elements. However the existence of a native subexponential attack on certain algebraic tori suggests that the minimal dimension $r = \varphi(n)$ of a torus in which a group G embeds, not the dimension n of the field $\mathbb{F}_q^n$ into which G can be mapped, is a more conservative measure of the security of G against subexponential attacks. We are careful to point out that the cryptanalytic potential for toric cryptography is asymptotic in the dimension, and that for any fixed dimension, the best asymptotic attacks will be fully exponential. One might, however, reassess the security against attacks on XTR, torus cryptography in T_6, or an MOV reduction to $\mathbb{F}_{p^6}^*$ as giving comparable security as the analogous subgroups of $\mathbb{F}_{p^3}^*$. A more significant case to reconsider is the level of security conferred when a discrete logarithm problem in G embeds in a large degree extension $\mathbb{F}_{p^n}^*$ of the prime field.

References

1. D. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.*, **48** (1987), 95-101.
2. Magma Handbook, J. Cannon and W. Bosma, eds., `http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`.
3. M. Rosenlicht, Generalized Jacobian varieties. *Ann. of Math.* (2) **59**, (1954). 505–530.
4. K. Rubin and A. Silverberg, Torus-based cryptography, 349–365, *Advances in Cryptology – CRYPTO 2003*, Lecture Notes in Computer Science, **2729**, 2003.