THE BEST AND WORST OF SUPERSINGULAR ABELIAN VARIETIES IN CRYPTOLOGY

KARL RUBIN AND ALICE SILVERBERG

Abstract. For certain cryptography applications, including identity based encryption schemes [1] and short signatures [2], it is important to have simple abelian varieties with security parameters that are neither too small nor too large. Simple supersingular abelian varieties are natural candidates for these applications. This paper gives improvements on the upper bounds of Galbraith [6] for the security parameters of simple supersingular abelian varieties, and constructs several families of curves whose jacobians achieve these upper bounds.

1. Introduction

Abelian varieties are higher-dimensional generalizations of elliptic curves (elliptic curves are the one-dimensional abelian varieties). Supersingular abelian varieties are a very special class of abelian varieties. Supersingular abelian varieties are bad for some purposes [9, 5, 4]. However, for some recent interesting cryptographic applications [11, 7, 1, 2, 14, 6], supersingular abelian varieties turn out to be very good. This paper gives families of examples of the "best" supersingular abelian varieties to use in these cryptographic applications, and gives strong upper bounds on how good supersingular abelian varieties can be for use in cryptography.

The group of points on an abelian variety over a finite field can be used in cryptography in the same way one uses the multiplicative group of a finite field. The security of the system relies on the difficulty of the discrete logarithm problem (DLP) in the group of points. One of the advantages of using the group $A(\mathbf{F}_q)$ of an abelian variety in place of $\mathbf{F}_q^\times$ is that there is no known subexponential algorithm for computing discrete logarithms on general abelian varieties.

One of the attacks on the DLP in $A(\mathbf{F}_q)$ is to map $A(\mathbf{F}_q)$ (or the relevant large cyclic subgroup of $A(\mathbf{F}_q)$) into a multiplicative group $\mathbf{F}_{q^k}^\times$, using the

Date: December 2001.

Key words and phrases. abelian varieties, supersingular, elliptic curves.

Rubin was partially supported by NSF grant DMS-9800881. Silverberg was partially supported by Xerox PARC and by NSF grant DMS-9988869. Some of this work was conducted while she was a visiting researcher at Xerox PARC.

Weil or Tate pairing [9, 5, 4]. If this can be done for some small k, then the subexponential algorithm for the DLP in $\mathbf{F}_{q^k}^\times$ can be used to solve the DLP in $A(\mathbf{F}_q)$. Thus, to have high security, $\#A(\mathbf{F}_q)$ should be divisible by a large prime which does not divide $\#(\mathbf{F}_{q^k}^\times) = q^k - 1$ for any very small values of k.

On the other hand, for certain cryptographic applications which make use of the Weil or Tate pairing [11, 7, 1, 2, 14, 6], it is important that $A(\mathbf{F}_q)$ (or the relevant large cyclic subgroup of $A(\mathbf{F}_q)$) *can* be mapped into $\mathbf{F}_{q^k}^\times$ with k not too large, in order to compute the pairing efficiently. For these applications it is of interest to produce families of abelian varieties for which this "security multiplier" k (see §6) is not too large, but not too small. It is known how to produce families of elliptic curves with security multiplier up to 6, namely supersingular elliptic curves. However, it seems to be difficult to systematically produce elliptic curves with security multiplier larger than 6 but not enormous. To obtain security multipliers that are not too large but not too small, it is natural to consider supersingular abelian varieties.

In [6], Galbraith defined a certain function $k(g)$ and showed that if A is a supersingular abelian variety of dimension g over a finite field $\mathbf{F}_q$, then there exists an integer $k \leq k(g)$ such that the exponent of $A(\mathbf{F}_q)$ divides $q^k - 1$. For example, $k(1) = 6$, $k(2) = 12$, $k(3) = 30$, $k(4) = 60$, $k(5) = 120$, and $k(6) = 210$.

Note that, since cryptographic security is based on the cyclic subgroups of $A(\mathbf{F}_q)$, for purposes of cryptology it is only necessary to consider simple abelian varieties, i.e., abelian varieties which do not decompose as products of lower-dimensional abelian varieties.

Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q$ and q is a square. In Theorem 8 we show that if we are not in the case where $g \leq 2$ and $q = 4$, then the smallest positive integer k such that the exponent of $A(\mathbf{F}_q)$ divides $q^{k/2} - 1$ satisfies $\varphi(k) \in \{g, 2g\}$, where φ is Euler's φ-function. Theorem 8 is a refinement of Theorem 3 of [6], and uses some of the same ideas (see also Theorem 4.2 of [10]), along with a new idea (Proposition 2) that relies on [8]. Theorem 9 gives results in the case where q is not a square, and uses algebraic number theory and cyclotomic fields.

For example, we show that if A is a simple supersingular abelian variety over $\mathbf{F}_q$ of dimension g, then the exponent of $A(\mathbf{F}_q)$ divides $q^k - 1$ for some positive integer k less than or equal to the entry in the following table (where $p = \mathrm{char}(\mathbf{F}_q)$). The maximum of each column shows how our bounds compare with the bounds of Galbraith stated above, and how they improve on his bounds when $g \geq 3$.

g	1	2	3	4	5	6
q a square	3	6	9	15	11	21
q not a square, $p > 11$	2	6	$*$	12	$*$	18
q not a square, $p = 2$	4	12	$*$	20	$*$	36
q not a square, $p = 3$	6	6	18	30	$*$	42
q not a square, $p = 5$	2	6	$*$	15	$*$	18
q not a square, $p = 7$	2	6	14	12	$*$	42
q not a square, $p = 11$	2	6	$*$	12	22	18

(A '$*$' means that there are no simple supersingular abelian varieties of dimension g over $\mathbf{F}_q$. See Corollary 10 below.)

In Theorem 13 we obtain a method for generating good supersingular curves for use in cryptography. Example 14 gives families of examples which are "best possible", in the sense that their jacobians are simple abelian varieties which achieve the upper bounds listed in the top row of the table above. Our main tools come from the theory of complex multiplication of abelian varieties, especially when applied to Fermat curves.

In §4 we introduce a useful new invariant, the cryptographic exponent of an abelian variety. Our results are phrased in terms of this invariant. In Theorem 11 we show that the security multiplier (defined in [2]) attached to a point of large order coincides with either the cryptographic exponent of the variety, or, in certain cases, half the cryptographic exponent.

2. Cyclotomy

Let $\mathbf{N}$ denote the set of natural numbers. If $k \in \mathbf{N}$ write $\Phi_k(x)$ for the k-th cyclotomic polynomial $\prod_\zeta (x - \zeta)$, where the product is over the primitive k-th roots of unity ζ. Note that $\deg(\Phi_k) = \varphi(k)$.

Lemma 1. (i) *For all $k \in \mathbf{N}$, $x^k - 1 = \prod_{d|k} \Phi_d(x)$.*

(ii) *$\Phi_k(x) = x^{\varphi(k)}\Phi_k(1/x)$ if $k > 1$, and $\Phi_1(x) = -x\Phi_1(1/x)$.*

(iii) *If $k, q \in \mathbf{N}$ then $\Phi_k(q)$ divides $q^k - 1$.*

Proof. The first two assertions are straightforward, and (iii) follows from (i). □

Proposition 2. *Suppose $w, q \in \mathbf{N}$, and $\Phi_k(q)$ divides $q^w - 1$. Then either $w \geq k$, or $(k, q) = (6, 4)$.*

Proof. Suppose $w < k$. Since $\Phi_k(q) \mid q^k - 1$ and the gcd $(q^w - 1, q^k - 1) = q^{(k,w)} - 1$, we may assume that $w \mid k$. Let $m = k/w > 1$, and consider the polynomial identity

$$\frac{x^k - 1}{x^w - 1} = x^{(m-1)w} + x^{(m-2)w} + \cdots + 1 \equiv m \pmod{x^w - 1}.$$

Since $\Phi_k(x)$ divides the left-hand side, evaluating this identity at q shows that $\Phi_k(q) \mid m$. But when $(k, q) \neq (6, 4)$, it follows from (29) and (35) of [8] that $\Phi_k(q)$ has a prime divisor which does not divide k. This contradiction shows that we cannot have $w < k$. (In the exceptional case $(k, q) = (6, 4)$, we have $\Phi_k(q) = 3$ which divides $q - 1$.) □

3. Simple supersingular abelian varieties

Suppose A is an abelian variety over the finite field $\mathbf{F}_q$, where q is a power of a prime p. A is **supersingular** if A is isogenous over $\overline{\mathbf{F}}_q$ to a power of a supersingular elliptic curve. (An elliptic curve is supersingular if $E(\overline{\mathbf{F}}_q)$ has no points of order p.) A is **simple** if it is not isogenous over $\mathbf{F}_q$ to a product of lower-dimensional abelian varieties.

Theorem 3 (Zhu [15])**.** *Suppose A is a simple supersingular abelian variety over $\mathbf{F}_q$, and $P(x)$ is the characteristic polynomial of the Frobenius endomorphism of A. Then:*

(i) *$P(x) = G(x)^e$, where $G(x) \in \mathbf{Z}[x]$ is a monic irreducible polynomial and $e = 1$ or 2;*

(ii) *$A(\mathbf{F}_q) \cong (\mathbf{Z}/G(1)\mathbf{Z})^e$ unless q is not a square and either*

  (a) *$p \equiv 3 \pmod 4$, $\dim(A) = 1$, and $G(x) = x^2 + q$, or*

  (b) *$p \equiv 1 \pmod 4$, $\dim(A) = 2$, and $G(x) = x^2 - q$.*

  In these exceptional cases, $A(\mathbf{F}_q) \cong (\mathbf{Z}/G(1)\mathbf{Z})^a \times (\mathbf{Z}/\frac{G(1)}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})^b$ with non-negative integers a and b such that $a + b = e$.

Remark 4. Note that in the two exceptional cases in Theorem 3, the exponent of $A(\mathbf{F}_q)$ is either $|G(1)|$ or $|G(1)|/2$. Otherwise, the exponent of $A(\mathbf{F}_q)$ is exactly $|G(1)|$. Always, $\#A(\mathbf{F}_q) = P(1)$.

4. The cryptographic exponent k_A

Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q$. We will associate to A (for fixed q) a positive integer k_A, which we will call the **cryptographic exponent** of A. We retain the notation G and e from Theorem 3. Let

$$G_1(x) = \frac{G(\sqrt{q}x)}{q^{g/e}} \in \mathbf{Q}(\sqrt{q})[x].$$

Proposition 5. *Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q$.*

(i) *Suppose q is a square. Then there is a unique positive integer k_A such that $G_1(x) = \Phi_{k_A}(x)$. Further, $\varphi(k_A) = 2g/e$ and $G(1) = \pm\Phi_{k_A}(\sqrt{q})$.*

(ii) *Suppose q is not a square, and $G_1(x) \in \mathbf{Q}[x]$. Then there is a unique positive integer k_A such that $G_1(x) = \Phi_{k_A}(x^2)$. Further, $\varphi(k_A) = g/e$ and $G(1) = \pm\Phi_{k_A}(q)$.*

(iii) *Suppose q is not a square, and $G_1(x) \notin \mathbf{Q}[x]$. Then there is a unique positive integer k_A such that $G_1(x)G_1(-x) = \Phi_{k_A}(x^2)$. Further, we have $\varphi(k_A) = 2g/e$ and $G(1)G(-1) = \pm\Phi_{k_A}(q)$.*

Proof. Note that G_1 is monic. Since A is supersingular, the roots of G_1 are roots of unity by p. 142 of [13].

Suppose first that q is a square. Then $G_1 \in \mathbf{Q}[x]$, and G_1 is irreducible in $\mathbf{Q}[x]$ because G is. Hence G_1 is a cyclotomic polynomial, so there is a (unique) k_A such that $G_1 = \Phi_{k_A}$. We have $\varphi(k) = \deg(G_1) = \deg(G) = 2g/e$, and by Lemma 1(ii), $G(1) = q^{g/e}G_1(1/\sqrt{q}) = \pm\Phi_{k_A}(\sqrt{q})$. This proves (i).

Now suppose that q is not a square, and that $G_1(x) \in \mathbf{Q}[x]$. Then $G_1(x)$ is a polynomial in x^2, say $G_1(x) = h(x^2)$ with $h(x) \in \mathbf{Z}[x]$. Since G is irreducible, so is h, and so h is a cyclotomic polynomial Φ_{k_A}. We have $\varphi(k_A) = \deg(\Phi_{k_A}) = \deg(G_1)/2 = \deg(G)/2 = g/e$, and (again using Lemma 1(ii))

$$G(1) = q^{g/e}G_1(1/\sqrt{q}) = q^{g/e}\Phi_{k_A}(1/q) = \pm\Phi_{k_A}(q).$$

Finally, suppose that $G_1(x) \notin \mathbf{Q}[x]$. Then $G_1(-x) = \overline{G}_1(x) \in \mathbf{Q}(\sqrt{q})[x]$, where the bar denotes the nontrivial automorphism of $\mathbf{Q}(\sqrt{q})$, and we have $G_1(x)G_1(-x) = G_1(x)\overline{G}_1(x) = h(x^2)$ with $h \in \mathbf{Q}[x]$. Since G is irreducible and $G_1(x) \notin \mathbf{Q}[x]$, h is irreducible. The roots of h are roots of unity, so h is a cyclotomic polynomial Φ_{k_A}. We have $\varphi(k_A) = \deg(\Phi_{k_A}) = \deg(G_1\overline{G}_1)/2 = \deg(G) = 2g/e$, and

$$G(1)G(-1) = q^{2g/e}G_1(1/\sqrt{q})G_1(-1/\sqrt{q}) = q^{2g/e}\Phi_{k_A}(1/q) = \pm\Phi_{k_A}(q). \qquad \square$$

Definition 6. The **cryptographic exponent** of A is the integer k_A given by Proposition 5.

Theorem 7.

(i) *If q is a square then the exponent of $A(\mathbf{F}_q)$ divides $\Phi_{k_A}(\sqrt{q})$, which divides $\sqrt{q}^{k_A} - 1$.*

(ii) *If q is not a square then the exponent of $A(\mathbf{F}_q)$ divides $\Phi_{k_A}(q)$, which divides $q^{k_A} - 1$.*

Proof. Apply Remark 4, Proposition 5, and Lemma 1(iii). □

5. Bounds on the cryptographic exponent

Theorem 8. *Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q$ and q is a square. Then:*

(i) *$\varphi(k_A) \in \{g, 2g\}$;*

(ii) *if we are not in the case where $g \leq 2$, $q = 4$, and $k_A = 6$, then k_A is the smallest positive integer k such that the exponent of $A(\mathbf{F}_q)$ divides $\sqrt{q}^k - 1$.*

Proof. The first assertion is part of Proposition 5(i). By Theorem 3, the exponent of $A(\mathbf{F}_q)$ is $G(1)$. By Proposition 5(i), $G(1) = \pm\Phi_{k_A}(\sqrt{q})$. The result now follows from Lemma 1(iii) and Proposition 2. □

If g is a positive integer and p is a prime, define finite sets

$$W_n = \{k \in \mathbf{N} : k \geq 2,\ \varphi(k) = n\}$$

and

$$K_g(p) = \begin{cases} W_g \cup \{k \in W_{2g} : k \equiv 4 \pmod 8\} & \text{if } p = 2, \\ W_g \cup \{k \in W_{2g} : p \mid k \text{ and } k \text{ is odd}\} & \text{if } p \equiv 1 \pmod 4, \\ W_g \cup \{k \in W_{2g} : p \mid k \text{ and } k \equiv 2 \pmod 4\} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

For example, $W_1 = \{2\}$, $W_n = \emptyset$ if n is odd and $n > 1$,

$$W_2 = \{3, 4, 6\}, \quad W_4 = \{5, 8, 10, 12\}, \quad W_6 = \{7, 9, 14, 18\},$$

$K_g(p) = W_g \cup$

$p:$ 2	3	5	7	11	13	> 13	if $g =$
$\{4\}$	$\{6\}$						1
$\{12\}$		$\{5\}$					2
	$\{18\}$		$\{14\}$				3
$\{20\}$	$\{30\}$	$\{15\}$					4
				$\{22\}$			5
$\{28, 36\}$	$\{42\}$		$\{42\}$		$\{13\}$		6

Theorem 9. *Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q$ and q is not a square. Let $p = \mathrm{char}(\mathbf{F}_q)$. Then either $k_A \in K_g(p)$, or else $g = 2$ and $k_A = 1$.*

Proof. Suppose $G_1(x) \in \mathbf{Q}[x]$. By Proposition 3.3 of [15], if $e = 2$ then $G_1(x) = x^2 - 1$, so $k_A = 1$ and $g = 2$. If $e = 1$, then $k_A \in W_g$ by Proposition 5(ii).

Suppose $G_1(x) \notin \mathbf{Q}[x]$. By Proposition 5(iii), $G_1(x)G_1(-x) = \Phi_{k_A}(x^2)$ and $k_A \in W_g \cup W_{2g}$. Thus the roots of G_1 (and therefore also the coefficients) lie in the cyclotomic field $\mathbf{Q}(\zeta_{2k_A})$. Thus $\sqrt{p} \in \mathbf{Q}(\zeta_{2k_A})$, and it follows that p divides k_A. If k_A is odd, then the primes p such that $\mathbf{Q}(\sqrt{p}) \subseteq \mathbf{Q}(\zeta_{2k_A})$ are exactly the primes dividing k_A that are congruent to $1 \pmod 4$. In particular, if $p = 2$ or $p \equiv 3 \pmod 4$ then k_A is even.

Suppose that k_A is even. Then $\Phi_{k_A}(x^2) = \Phi_{2k_A}(x)$. Let Δ denote the Galois group of $\mathbf{Q}(\zeta_{2k_A})$ over $\mathbf{Q}(\sqrt{p})$. Identifying Δ with a subgroup of $(\mathbf{Z}/2k_A\mathbf{Z})^\times$, then Δ is the reduction modulo $2k_A$ of the set

$$D = \{d \in \mathbf{Z} : (d, 2k_A) = 1 \text{ and } \left(\frac{p}{d}\right) = 1\}$$

where $(\frac{p}{d})$ is the Jacobi symbol. Since G_1 is stable under Δ, we can write $G_1(x) = \prod_{\delta\in\Delta}(x - \zeta^\delta)$ where ζ is a primitive $2k_A$-th root of unity. Since $\Phi_{2k_A}(x)$ has no multiple roots, $G_1(x)$ and $G_1(-x)$ are relatively prime, so $\zeta^d \neq -\zeta$ for every $d \in D$. In particular since $\zeta^{k_A+1} = -\zeta$, it follows that $k_A + 1 \notin D$. Combining the definition of D with quadratic reciprocity we obtain

$$-1 = \left(\frac{p}{k_A+1}\right) = \begin{cases} (-1)^{\frac{p-1}{2}\frac{k_A}{2}}\left(\frac{k_A+1}{p}\right) = (-1)^{\frac{p-1}{2}\frac{k_A}{2}} & \text{if } p \text{ is odd,}\\ (-1)^{\frac{(k_A+1)^2-1}{8}} & \text{if } p = 2.\end{cases}$$

If p is odd we conclude that $p \equiv 3 \pmod 4$ and $k_A \equiv 2 \pmod 4$. If $p = 2$, then $4|k_A$ (since $\sqrt{2} \in \mathbf{Q}(\zeta_{2k_A})$), so $k_A \equiv 4 \pmod 8$. □

Corollary 10. *Suppose p is prime, s and g are odd positive integers, and $g > 1$.*

(i) *If $p \not\equiv 3 \pmod 4$, then there does not exist a simple supersingular abelian variety A of dimension g over $\mathbf{F}_{p^s}$.*

(ii) *If $p \equiv 3 \pmod 4$, and there exists a simple supersingular abelian variety A of dimension g over $\mathbf{F}_{p^s}$, then $g = p^{b-1}(p-1)/2$ for some positive integer b.*

Proof. Suppose there is a simple supersingular abelian variety A of dimension g over $\mathbf{F}_{p^s}$. Since $g > 1$ is odd, we conclude from Theorem 9 that $\varphi(k_A) = 2g$ and $p \mid k_A$. This is only possible if $k_A = p^b$ or $2p^b$, and $p \equiv 3 \pmod 4$. □

The table in the introduction follows from Theorems 8, 9, and 7 and Corollary 10.

6. The security multiplier α

As in [2], define the **security multiplier** α as follows. If A is an abelian variety over $\mathbf{F}_q$ and $P \in A(\mathbf{F}_q)$ is a point of prime order ℓ, let α denote the order of $q \pmod \ell$. Equivalently, α is the smallest positive integer a such that $\mathbf{F}_{q^a}$ contains non-trivial ℓ-th roots of unity.

For purposes of cryptography we are only interested in the case where ℓ is large. Since $\varphi(k_A) \leq 2g$, the cryptographic exponent k_A is small, so the condition that $\ell \nmid k_A$ in the following result is not a problem.

Theorem 11. *Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q$, α is the security multiplier for some point in $A(\mathbf{F}_q)$ of prime order ℓ, and $\ell \nmid k_A$. Then $\alpha = k_A$, unless q is a square and k_A is even, in which case $\alpha = k_A/2$. Thus, $\varphi(\alpha) \in \{\frac{g}{2}, g, 2g\}$ (in particular, if g is odd then either $g = 1$ and $\alpha = 2$, or $\varphi(\alpha) = 2g$).*

Proof. Note that ℓ divides the exponent of $A(\mathbf{F}_q)$. Since A is supersingular, $\ell \nmid q$. The roots of Φ_{k_A} in $\overline{\mathbf{F}}_\ell$ are exactly the primitive k_A-th roots of unity, since $\ell \nmid k_A$.

Suppose first that q is a square. By Theorem 7(i), we have $\ell \mid \Phi_{k_A}(\sqrt{q})$, so $\sqrt{q}$ has order k_A in $\mathbf{F}_\ell^\times$. Thus $\alpha = k_A$ if k_A is odd and $\alpha = k_A/2$ if k_A is even.

Now suppose that q is not a square. By Theorem 7(ii), we have $\ell \mid \Phi_{k_A}(q)$, so q has order k_A in $\mathbf{F}_\ell^\times$. Thus $\alpha = k_A$. □

7. The best supersingular abelian varieties

Definition 12. Suppose A is a supersingular abelian variety of dimension g over $\mathbf{F}_q$. We say that A is **optimal** if

(i) A is simple, and
(ii) $k_A \geq k_B$ for every simple supersingular abelian variety B of dimension g over $\mathbf{F}_q$.

Note that if A is simple, to prove than A is optimal it suffices to show that k_A is the largest k with $\varphi(k) = 2g$ if q is a square (Theorem 8(i)), or that k_A is the largest element of $K_g(p)$ if q is an odd power of a prime p (Theorem 9).

In this section we give families of examples of optimal supersingular abelian varieties A and compute their cryptographic exponents k_A. These include examples with $g = 3, 4, 5$, and 6, for infinitely many prime powers q.

Theorem 13. *Suppose that $a, b, n \in \mathbf{N}$ have no common divisor greater than 1, n is odd, and $n + 2 - ((n, a) + (n, b) + (n, a + b)) = \varphi(n)$. Let q be a prime power congruent to $-1 \pmod{n}$, and let $F = \mathbf{F}_{q^2}$. For $\gamma \in F^\times$ let C_γ be the curve*

$$y^n = \gamma x^a (1 - x)^b$$

over F and write A_γ for its jacobian variety. Then

(i) *C_γ has genus $\varphi(n)/2$,*
(ii) *A_γ is supersingular.*

If in addition γ generates $F^\times$ modulo n-th powers, then

(iii) *A_γ is simple,*
(iv) *$k_{A_\gamma} = 2n$,*
(v) *$A_\gamma(F)$ is cyclic,*
(vi) *if $(n, q) \neq (3, 4)$ then n is the smallest positive integer k such that $\#A_\gamma(F)$ divides $q^k - 1$.*

Proof. The genus g of C_γ is independent of γ, so assertion (i) follows from the formula for the genus of $C_{\pm 1}$ given on p. 55 of [3].

Since $q \equiv -1 \pmod{n}$, Theorem 20.15 of [12] shows that the Frobenius endomorphism of A_1 is multiplication by $-q$. In particular, the characteristic polynomial of Frobenius is $(x+q)^{2g}$, and A_1 is supersingular. Since every A_γ is isomorphic to A_1 over the algebraic closure $\bar{F}$, every A_γ is supersingular.

The endomorphism ring $\mathrm{End}(A_\gamma)$ contains the group of n-th roots of unity $\boldsymbol{\mu}_n$, where $\xi \in \boldsymbol{\mu}_n$ acts on C_γ by sending (x,y) to $(x, \xi y)$.

Fix an n-th root δ of γ. Then δ^{q^2} is also an n-th root of γ. Let $\zeta = \gamma^{(q^2-1)/n} = \delta^{q^2-1}$. Then $\zeta^n = 1$, so we can view $\zeta \in \boldsymbol{\mu}_n \subset \mathrm{End}(A_\gamma)$. We have a commutative diagram

$$\begin{tikzcd}
C_1 \arrow[r, "\phi_1"] \arrow[d, "\lambda"'] & C_1 \arrow[d, "\lambda'"] \\
C_\gamma \arrow[r, "\phi_\gamma"] & C_\gamma
\end{tikzcd}$$

where ϕ_1, ϕ_γ are the q^2-power maps $(x,y) \mapsto (x^{q^2}, y^{q^2})$ of C_1 and C_γ, respectively, and $\lambda, \lambda' : C_1 \to C_\gamma$ are the isomorphisms $(x,y) \mapsto (x, \delta y)$, $(x,y) \mapsto (x, \delta^{q^2} y)$. Writing $[\phi_\gamma]$, $[\lambda']$, etc. for the induced maps on A_1 and A_γ, we noted above that $[\phi_1] = -q$, and so the Frobenius endomorphism of A_γ is

$$[\phi_\gamma] = [\lambda' \circ \phi_1 \circ \lambda^{-1}] = [\lambda^{-1}] \circ [\phi_1] \circ [\lambda'] = [\lambda^{-1}] \circ (-q) \circ [\lambda'] = -q \circ [\lambda' \circ \lambda^{-1}] = -\zeta q.$$

Suppose now that γ generates $F^\times$ modulo n-th powers. Then ζ is a primitive n-th root of unity, and since n is odd, $-\zeta$ is a primitive $2n$-th root of unity. The characteristic polynomial $P(x)$ of Frobenius on A_γ has degree $2g = \varphi(n) = \varphi(2n)$, and has $-\zeta q$ as a root, so $P(x) = \prod_\xi (x - \xi q)$, product over primitive $2n$-th roots of unity ξ. Thus $P(x) = q^{\varphi(2n)} \Phi_{2n}(x/q)$.

Since $\Phi_{2n}(x)$ is irreducible, so is $P(x)$. Assertion (iii) follows from this, (iv) is immediate from the definition of k_A (Theorem 5(i)), and (v) follows from Theorem 3. The final assertion follows from Theorem 8. □

The following examples are easily deduced from Theorem 13.

Example 14. Suppose (g, n, a, b) is one of the following 4-tuples:

g	n	a	b
3	9	3	1
4	15	5	3
6	21	7	3
9	27	9	1
10	33	11	3
$\frac{\ell-1}{2}$	ℓ	α	β

where in the last row ℓ is a prime, $1 \leq \alpha, \beta \leq \ell - 1$, and $\alpha + \beta \neq \ell$. Let q be a prime power congruent to $-1 \pmod{n}$, $F = \mathbf{F}_{q^2}$, and γ a generator of $F^\times$ modulo n-th powers. Let C be the curve $y^n = \gamma x^a (1-x)^b$ and A its jacobian. Then by Theorem 13, A is simple and supersingular, $\mathrm{genus}(C) = \dim(A) = g$,

$k_A = 2n$, $A(F)$ is cyclic, and n is the smallest integer k such that $\#A(F)$ divides $q^k - 1$.

In the table above, if $g = 3, 4, 6, 9, 10$, or if $g > 3$ and g is a prime of the form $(\ell - 1)/2$, then $2n$ is the largest integer k such that $\varphi(k) = 2g$, so A is optimal (in the sense of Definition 12).

Remark 15. Example 14 gives optimal examples with $g = 1$ and 5 by taking $\ell = 3$ and 11 in the last row, and non-optimal examples with $g = 2$ and 3 by taking $\ell = 5$ and 7 in the last row. The example $y^2 + y = x^5 + x^3$ over $\mathbf{F}_2$ satisfies $k_A = 12$ and $g = 2$ (i.e., is optimal), and was given in [6]. Example 14 gives many optimal examples over $\mathbf{F}_q$ when q is a square. One would like additional optimal examples when q is not a square.

8. Conclusion

For certain security applications it is useful to have simple abelian varieties with security parameters that are neither too small nor too large. Simple supersingular abelian varieties are natural candidates for these applications. This paper gives strong upper bounds for the security parameters of simple supersingular abelian varieties (in terms of the dimension of the abelian variety and the size of the finite field), and gives constructions of several families of curves over fields of square order whose jacobians achieve these upper bounds.

Acknowledgments. The authors thank Steven Galbraith for his observations.

References

[1] D. Boneh, M. Franklin, *Identity based encryption from the Weil pairing*, in Advances in Cryptology — Crypto 2001, Lect. Notes in Comp. Sci. **2139** (2001), Springer, 213–229.

[2] D. Boneh, B. Lynn, H. Shacham, *Short signatures from the Weil pairing*, in Advances in Cryptology — Asiacrypt 2001, Lect. Notes in Comp. Sci. **2248** (2001), Springer, 514–532.

[3] R. Coleman, W. McCallum, *Stable reduction of Fermat curves and Jacobi sum Hecke characters*, J. Reine Angew. Math. **385** (1988), 41–101.

[4] G. Frey, M. Müller, H-G. Rück, *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Trans. Inform. Theory **45** (1999), 1717–1719.

[5] G. Frey, H-G. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), 865–874.

[6] S. Galbraith, *Supersingular curves in cryptography*, in Advances in Cryptology — Asiacrypt 2001, Lect. Notes in Comp. Sci. **2248** (2001), Springer, 495–513.

[7] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, in Algorithmic Number Theory (ANTS-IV), Leiden, The Netherlands, July 2–7, 2000, Lect. Notes in Comp. Sci. **1838** (2000), Springer, 385–394.

[8] H-J. Kanold, *Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme. I*, J. Reine Angew. Math. **187** (1950), 169–182.

[9] A. J. Menezes, T. Okamoto, S. A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inform. Theory **39** (1993), 1639–1646.

[10] F. Oort, *Subvarieties of moduli spaces*, Invent. Math. **24** (1974), 95–119.

[11] R. Sakai, K. Ohgishi, M. Kasahara, Cryptosystems based on pairing, SCIS2000 (The 2000 Symposium on Cryptography and Information Security), Okinawa, Japan, January 26–28, 2000, C20.

[12] G. Shimura, Abelian varieties with complex multiplication and modular functions, Princeton Univ. Press, Princeton, NJ, 1998.

[13] H. Stichtenoth, C. Xing, *On the structure of the divisor class group of a class of curves over finite fields*, Arch. Math. **65** (1995), 141–150.

[14] E. R. Verheul, *Self-blindable credential certificates from the Weil pairing*, in Advances in Cryptology — Asiacrypt 2001, Lect. Notes in Comp. Sci. **2248** (2001), Springer, 533–551.

[15] H. J. Zhu, *Group structures of elementary supersingular abelian varieties over finite fields*, J. Number Theory **81** (2000), 292–309.

Department of Mathematics, Stanford University, Stanford CA 94305, USA
E-mail address: rubin@math.stanford.edu

Department of Mathematics, Ohio State University, Columbus OH 43210, USA
E-mail address: silver@math.ohio-state.edu