Supersingular Abelian Varieties in Cryptology

Karl Rubin[1] * and Alice Silverberg[2] **

[1] Department of Mathematics
Stanford University
Stanford CA, USA
rubin@math.stanford.edu

[2] Department of Mathematics
Ohio State University
Columbus, OH, USA
silver@math.ohio-state.edu

Abstract. For certain security applications, including identity based encryption and short signature schemes, it is useful to have abelian varieties with security parameters that are neither too small nor too large. Supersingular abelian varieties are natural candidates for these applications. This paper determines exactly which values can occur as the security parameters of supersingular abelian varieties (in terms of the dimension of the abelian variety and the size of the finite field), and gives constructions of supersingular abelian varieties that are optimal for use in cryptography.

1 Introduction

The results of this paper show that it is the best of times and the worst of times for supersingular abelian varieties in cryptology. The results in Part 1 give the bad news. They state exactly how much security is possible using supersingular abelian varieties. Part 2 gives the good news, producing the optimal supersingular abelian varieties for use in cryptographic applications, and showing that it is sometimes possible to accomplish this with all computations taking place on an elliptic curve.

One-round tripartite Diffie-Hellman, identity based encryption, and short digital signatures are some problems for which good solutions have recently been found. These solutions make critical use of supersingular elliptic curves and Weil (or Tate) pairings. It was an open question whether or not these new schemes could be improved (more security for the same signature size or efficiency) using abelian varieties in place of elliptic curves. This paper answers the question in the affirmative. We construct families of examples of the "best" supersingular

* 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.

abelian varieties to use in these cryptographic applications (§§5–6), and determine exactly how much security can be achieved using supersingular abelian varieties (§§3–4).

Abelian varieties are higher dimensional generalizations of elliptic curves (elliptic curves are the one-dimensional abelian varieties). Weil and Tate pairings exist and have similar properties for abelian varieties that they have for elliptic curves. Supersingular abelian varieties are a special class of abelian varieties. For standard elliptic curve cryptography, supersingular elliptic curves are known to be weak. However, for some recent interesting cryptographic applications [18, 15, 2, 3, 22, 9], supersingular elliptic curves turn out to be very good. New schemes using supersingular elliptic curves and Weil or Tate pairings are being produced rapidly. The abelian varieties in this paper can be utilized in all these applications, to give better results (e.g., shorter signatures, or shorter ciphertexts) for the same security.

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 (DL) problem in the group of points. One of the advantages of using the group $A(\mathbf{F}_q)$ of an abelian variety in place of the multiplicative group $\mathbf{F}_q^*$ of a finite field $\mathbf{F}_q$ is that there is no known subexponential algorithm for computing discrete logarithms on general abelian varieties.

One of the attacks on the DL problem 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 $\mathbf{F}_{q^k}^*$, using the Weil or Tate pairing [17, 8, 7]. If this can be done for some small k, then the subexponential algorithm for the DL problem in $\mathbf{F}_{q^k}^*$ can be used to solve the DL problem in $A(\mathbf{F}_q)$. Thus, to have high security, $\#A(\mathbf{F}_q)$ should be divisible by a large prime that does not divide $\#\mathbf{F}_{q^k}^* = q^k - 1$ for any very small values of k.

On the other hand, for cryptographic applications that make use of the Weil or Tate pairing, it is important that $A(\mathbf{F}_q)$ (or the relevant large cyclic subgroup of $A(\mathbf{F}_q)$) *can* be mapped into $\mathbf{F}_{q^k}^*$ with k not too large, in order to be able to compute the pairing efficiently. Thus for these applications it is of interest to produce families of abelian varieties for which the security parameter $\frac{k}{g}$ is not too large, but not too small, where g is the dimension of the abelian variety. (In defining the security parameter, one takes the minimal k.) Taking supersingular elliptic curves (so $g = 1$), one can attain security parameter up to 6. However, it seems to be difficult to systematically produce elliptic curves with security parameter larger than 6 but not enormous. To obtain security parameters that are not too large but not too small, it is natural to consider supersingular abelian varieties.

In [9], 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 that do not decompose as products of lower dimensional abelian varieties.

In §4, we determine exactly which security parameters can occur, for simple supersingular abelian varieties. 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 corresponding entry in Table 1 (where $p = \mathrm{char}(\mathbf{F}_q)$), and each entry can be attained. The maximum of each column shows how these bounds compare with the bounds of Galbraith stated above, and how they improve on his bounds when $g \geq 3$. For

Table 1. Upper bounds on the cryptographic exponents

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	4	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

these bounds, see Theorems 11, 12, and 6 below. A '$*$' means that there are no simple supersingular abelian varieties of dimension g over $\mathbf{F}_q$.

In particular, we show that the highest security parameter for simple supersingular 4-dimensional abelian varieties is $7.5 = 30/4$, and this can be attained if and only if $p = 3$ and q is not a square. In particular, this answers in the affirmative an open question from [3] on whether one can use higher dimensional abelian varieties to obtain short signatures with higher security. When the dimension is 6 the highest security parameter is 7, and this can be attained if and only if $p = 3$ or 7 and q is not a square. In dimension 2 the highest security parameter is 6, which ties the elliptic curve case. However, these abelian surfaces are in characteristic 2, while the best supersingular elliptic curves occur only in characteristic 3. Therefore, there may be efficiency advantages in using abelian surfaces over binary fields.

In §§5–6 we find the best supersingular abelian varieties for use in cryptography. Theorem 17 gives an algorithm whose input is an elliptic curve and whose output is an abelian variety with higher security. The abelian variety is constructed as a subvariety of a Weil restriction of scalars of the elliptic curve (in the same way that the "XTR supergroup" [16] turns out to be the Weil restriction of scalars from $\mathbf{F}_{p^6}$ to $\mathbf{F}_p$ of the multiplicative group). The group of points of the abelian variety lies inside the group of points of the elliptic curve over a larger field, and thus all computations on the abelian variety can be done directly on the curve. We construct 4-dimensional abelian varieties with security parameter 7.5, thereby beating the security of supersingular elliptic curves, and construct abelian surfaces over binary fields with security parameter 6. We obtain efficient implementations of a variant of the BLS short signature scheme [3] using these abelian varieties (embedded in elliptic curves over larger fields). This gives the first practical application to cryptography of abelian varieties that are not known to be Jacobians of curves.

Theorem 20 gives a method for generating supersingular curves whose Jacobian varieties are good for use in cryptography. This result produces varieties in infinitely many characteristics. Example 21 gives families of examples of Jacobian varieties that are "best possible" in the sense that they achieve the upper bounds listed in the top row of Table 1.

Since $\frac{k}{\varphi(k)} \to \infty$ as $k \to \infty$ (where φ is Euler's φ-function), Theorems 11 and 12 imply that security parameters for simple supersingular abelian varieties are unbounded (as the dimension of the varieties grows). However, $\frac{k}{\varphi(k)}$ grows very slowly, and computational issues and security considerations preclude using high dimensional abelian varieties with high security parameters, at least at this time. We therefore restrict the examples in this paper to small dimensional cases.

The results in §4 rely on the theory of cyclotomic fields, Honda-Tate theory, and work of Zhu. The proof of Theorem 17 uses the theory of Weil restriction of scalars. The proof of Theorem 20 uses the theory of complex multiplication of abelian varieties, applied to Fermat curves.

Part 1: Bounds on the security

We begin with some preliminaries on abelian varieties.

Suppose A is an abelian variety over a finite field $\mathbf{F}_q$, where q is a power of a prime p. Then A is **simple** if it is not isogenous over $\mathbf{F}_q$ to a product of lower dimensional abelian varieties, and A is **supersingular** if A is isogenous over $\overline{\mathbf{F}}_q$ to a power of a supersingular elliptic curve. (An elliptic curve E is supersingular if $E(\overline{\mathbf{F}}_q)$ has no points of order p.) A **supersingular q-Weil number** is a complex number of the form $\sqrt{q}\zeta$ where ζ is a root of unity. (Throughout the paper, $\sqrt{q}$ denotes the positive square root.)

Theorem 1 ([13, 21, 24]) *Suppose A is a simple supersingular abelian variety over $\mathbf{F}_q$, where q is a power of a prime p, 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) the roots of G are supersingular q-Weil numbers;
(iii) $A(\mathbf{F}_q) \cong (\mathbf{Z}/G(1)\mathbf{Z})^e$ 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 $a + b = e$;

(iv) $\#A(\mathbf{F}_q) = P(1)$.

The roots of G are called the **q-Weil numbers for** A. For a given abelian variety, its q-Weil numbers are the Galois conjugates of a given one (under the action of the Galois group of $\bar{\mathbf{Q}}$ over $\mathbf{Q}$). We retain the notation of this section, including P, G, and e, throughout the paper. Note that

$$\dim(A) = \frac{\deg(P)}{2} = \frac{e\deg(G)}{2}.$$

Theorem 2 ([13, 21]) *The map that associates to a simple supersingular abelian variety over $\mathbf{F}_q$ one of its q-Weil numbers gives a one-to-one correspondence between the $\mathbf{F}_q$-isogeny classes of simple supersingular abelian varieties over $\mathbf{F}_q$ and Galois conjugacy classes of supersingular q-Weil numbers.*

2 Definition of the cryptographic exponent c_A

We introduce a useful new invariant, c_A, which we will call the cryptographic exponent. In the next section we show that c_A captures the MOV security [17] of the abelian variety.

Suppose A is a simple supersingular abelian variety over $\mathbf{F}_q$ and $\sqrt{q}\zeta$ is a q-Weil number for A. Let m denote the order of the root of unity ζ. Note that if $\sqrt{q}\zeta'$ is another q-Weil number for A, and m' is the order of ζ', then ζ^2 and $(\zeta')^2$ are Galois conjugate, and therefore have the same order, namely $\frac{m}{\gcd(2,m)} = \frac{m'}{\gcd(2,m')}$. If q is a square, then ζ and ζ' are Galois conjugate, and thus $m = m'$. Therefore when q is a square, m depends only on A.

Definition 3

$$c_A = \begin{cases} \frac{m}{2} & \textit{if } q \textit{ is a square,} \\ \frac{m}{\gcd(2,m)} & \textit{if } q \textit{ is not a square.} \end{cases}$$

We will call c_A the **cryptographic exponent** *of A. Let $\alpha_A = c_A/g$ and call it the* **security parameter** *of A.*

Roughly speaking, for a group G to have security parameter α means that the DL problem in G can be reduced to the DL problem in the multiplicative group of a field of size approximately $|G|^\alpha$. The group $G = A(\mathbf{F}_q)$ has order approximately q^g, and we will see in §3 below that q^{c_A} is the size of the smallest field F such that every cyclic subgroup of $A(\mathbf{F}_q)$ can be embedded in F^*.

When q is not a square, c_A is a natural number. When q is a square, c_A is either a natural number or half of a natural number.

If $\gcd(t, 2c_A) = 1$, then the cryptographic exponent for A over $\mathbf{F}_{q^t}$ is the same as the cryptographic exponent for A over $\mathbf{F}_q$.

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 $\deg(\Phi_k) = \varphi(k)$, where φ is Euler's φ-function.

Lemma 4 *Suppose that $\Phi_m(d)$ is divisible by a prime number ℓ, and $\ell \nmid m$. Then m is the smallest natural number k such that $d^k - 1$ is divisible by ℓ.*

Proof. The roots of Φ_m in $\overline{\mathbf{F}}_\ell$ are exactly the primitive m-th roots of unity, since $\ell \nmid m$. By assumption, d is a root of Φ_m in $\mathbf{F}_\ell$, and so m is the order of d in $\mathbf{F}_\ell^*$.

We include a useful closely related result.

Proposition 5 *If $m, d \in \mathbf{N}$, $d > 1$, and $(m, d) \neq (6, 2)$, then m is the smallest natural number k such that $d^k - 1$ is divisible by $\Phi_m(d)$.*

Proof. Since $x^m - 1 = \prod_{r|m} \Phi_r(x)$, we have that $\Phi_m(d)$ divides $d^m - 1$. The proposition is true if $m = 1$ or 2. If $m > 2$ and $(m, d) \neq (6, 2)$, it follows from an 1892 result of Zsigmondy (see Theorem 8.3, §IX of [14]) that $\Phi_m(d)$ has a prime divisor that does not divide m. The proposition now follows from Lemma 4.

In the exceptional case $(m, d) = (6, 2)$, we have $\Phi_m(d) = 3 = d^2 - 1$.

Theorem 6 *Suppose A is a simple supersingular abelian variety over $\mathbf{F}_q$.*

(i) If q is a square then the exponent of $A(\mathbf{F}_q)$ divides $\Phi_{2c_A}(\sqrt{q})$, which divides $\sqrt{q}^{2c_A} - 1$.
(ii) If q is not a square then the exponent of $A(\mathbf{F}_q)$ divides $\Phi_{c_A}(q)$, which divides $q^{c_A} - 1$.

Proof. By Theorem 1(iii), the exponent of $A(\mathbf{F}_q)$ divides $G(1)$. Let π be a q-Weil number for A. If q is a square, then $\Phi_{2c_A}(\frac{\pi}{\sqrt{q}}) = 0$. Thus, $G(x) = \sqrt{q}^{\varphi(2c_A)} \Phi_{2c_A}(\frac{x}{\sqrt{q}})$ and $G(1) = \sqrt{q}^{\varphi(2c_A)} \Phi_{2c_A}(\frac{1}{\sqrt{q}}) = \pm \Phi_{2c_A}(\sqrt{q})$. If q is not a square, then $\Phi_{c_A}(\frac{\pi^2}{q}) = 0$, so $G(x)$ divides $q^{\varphi(c_A)} \Phi_{c_A}(\frac{x^2}{q})$. Therefore $G(1)$ divides $q^{\varphi(c_A)} \Phi_{c_A}(\frac{1}{q}) = \pm \Phi_{c_A}(q)$. As in Proposition 5, $\Phi_m(d)$ divides $d^m - 1$.

3 The cryptographic exponent and MOV security

The next result shows that the cryptographic exponent c_A captures the MOV security of the abelian variety. In other words, if $A(\mathbf{F}_q)$ has a subgroup of large prime order ℓ, then q^{c_A} is the size of the smallest field of characteristic p containing a multiplicative subgroup of order ℓ. Recall $e \in \{1, 2\}$ from Theorem 1.

Theorem 7 *Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q$, $q = p^n$, $\ell > 5$ is a prime number, $\ell \mid \#A(\mathbf{F}_q)$, and $\ell > (1 + \sqrt{p})^{ng/e}$. Let r denote the smallest natural number k such that $\ell \mid p^k - 1$. Then $p^r = q^{c_A}$.*

Since the proof is rather technical, we do not give it here, but instead prove the following slightly weaker result.

Theorem 8 *Suppose A is a simple supersingular abelian variety over $\mathbf{F}_q$, ℓ is a prime number, $\ell \mid \#A(\mathbf{F}_q)$, and $\ell \nmid 2c_A$. Then c_A is the smallest half-integer k such that $q^k - 1$ is an integer divisible by ℓ.*

Proof. By Theorem 6, we have $\ell \mid \Phi_{2c_A}(\sqrt{q})$ if q is a square, and $\ell \mid \Phi_{c_A}(q)$ otherwise. The theorem now follows from Lemma 4.

Remark 9 *For purposes of cryptography we are only interested in the case where ℓ is large. If $\ell > 2g + 1$, then $\ell \nmid 2c_A$, so the condition $\ell \nmid 2c_A$ is not a problem. This follows since $2g = \deg(P) = e \deg(G)$, $\deg(G) = \varphi(2c_A)$ if q is a square, $\deg(G) = \varphi(c_A)$ or $2\varphi(c_A)$ if q is not a square, and $\varphi(M) \geq \ell - 1$ if $\ell \mid M$.*

4 Bounding the cryptographic exponent

Next we determine exactly which values can occur as cryptographic exponents for simple supersingular abelian varieties. Let

$$W_n = \{k \in \mathbf{N} : \varphi(k) = n\}.$$

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

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

Let k' denote the odd part of a natural number k. If p is a prime, define

$$X_p = \begin{cases} \{k \in \mathbf{N} : 4 \nmid k \text{ and 2 has odd order in } (\mathbf{Z}/k'\mathbf{Z})^*\} & \text{if } p = 2, \\ \{k \in \mathbf{N} : p \nmid k \text{ and } p \text{ has odd order in } (\mathbf{Z}/k\mathbf{Z})^*\} & \text{if } p \text{ is odd;} \end{cases}$$

$$V_p = \begin{cases} \{k \in \mathbf{N} : k \equiv 4 \pmod 8\} & \text{if } p = 2, \\ \{k \in \mathbf{N} : p \mid k \text{ and } k \equiv 2 \pmod 4\} & \text{if } p \equiv 3 \pmod 4, \\ \{k \in \mathbf{N} : p \mid k \text{ and } k \text{ is odd}\} & \text{if } p \equiv 1 \pmod 4; \end{cases}$$

$$K_g(p) = \begin{cases} (W_{2g} \cap V_p) \cup (W_g - V_p) & \text{if } g > 2, \\ (W_4 \cap V_p) \cup (W_2 - V_p) \cup \{1\} & \text{if } g = 2, \\ (W_2 \cap V_p) \cup (W_1 - V_p - \{1\}) & \text{if } g = 1. \end{cases}$$

The next result can be shown to follow from Proposition 3.3 of [24].

Proposition 10 ([24]) *Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q$.*

(i) If q is a square, then $e = 2$ if and only if $2c_A \in X_p$.
(ii) If q is not a square, then $e = 2$ if and only if $c_A = 1$ and $g = 2$.

Theorem 11 *Suppose g and n are natural numbers and n is even. Then $c = \frac{m}{2}$ occurs as the cryptographic exponent of a simple supersingular abelian variety of dimension g over $\mathbf{F}_{p^n}$ if and only if $m \in (W_g \cap X_p) \cup (W_{2g} - X_p)$.*

Proof. If ζ is a primitive m-th root of unity, then $\sqrt{p^n}\zeta$ corresponds by Theorem 2 to a simple supersingular abelian variety over $\mathbf{F}_{p^n}$ of dimension $d = e\deg(G)/2 = e\varphi(m)/2$. By Proposition 10(i), $d = g$ if and only if $m \in (W_g \cap X_p) \cup (W_{2g} - X_p)$.

Theorem 12 *Suppose g and n are natural numbers and n is odd. Then c occurs as the cryptographic exponent of a simple supersingular abelian variety of dimension g over $\mathbf{F}_{p^n}$ if and only if $c \in K_g(p)$.*

Proof. Suppose A is a simple supersingular abelian variety of dimension g over $\mathbf{F}_q = \mathbf{F}_{p^n}$ with a q-Weil number $\pi = \sqrt{q}\zeta$ with ζ a primitive m-th root of unity. Then $\varphi(c_A) = [\mathbf{Q}(\pi^2) : \mathbf{Q}]$. We have $2g = e[\mathbf{Q}(\pi) : \mathbf{Q}] = e[\mathbf{Q}(\pi) : \mathbf{Q}(\pi^2)][\mathbf{Q}(\pi^2) : \mathbf{Q}]$. It follows from Lemma 2.6 of [24] that $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^2)$ if and only if $c_A \in V_p$. It follows from Proposition 10(ii) that $c_A \in K_g(p)$. The converse follows by the same reasoning.

For any given g and q, it is easy to work out from Theorems 11 and 12 exactly which values can occur as cryptographic exponents c_A for g-dimensional simple supersingular abelian varieties A over $\mathbf{F}_q$, as is done in the following two corollaries.

Corollary 13 *If n is even, then the only possible cryptographic exponents c_A for simple supersingular abelian surfaces A over $\mathbf{F}_{p^n}$ are the numbers of the form $\frac{m}{2}$ with $m \in \{3, 4, 5, 6, 8, 10, 12\}$. For $m \in \{3, 4, 6\}$, $\frac{m}{2}$ occurs as a c_A if and only if $p \equiv 1 \pmod{m}$, and for $m \in \{5, 8, 10, 12\}$, $\frac{m}{2}$ occurs as a c_A if and only if $p \not\equiv 1 \pmod{m}$. An analogous statement holds for 4-dimensional varieties, with $\{3, 4, 6\}$ and $\{5, 8, 10, 12\}$ replaced by $\{5, 8, 10, 12\}$ and $\{15, 16, 20, 24, 30\}$, respectively.*

Corollary 14 *If n is odd, then the exact sets of cryptographic exponents c_A that occur for simple supersingular abelian varieties A of dimension g over $\mathbf{F}_{p^n}$ with $2 \le g \le 5$ are given below.*

(i) *Suppose $g = 2$.*

(a) $c_A \in \{1, 3, 4, 6\}$ if $p \ge 7$;
(b) $c_A \in \{1, 3, 4, 5, 6\}$ if $p = 5$;
(c) $c_A \in \{1, 3, 4\}$ if $p = 3$;
(d) $c_A \in \{1, 3, 6, 12\}$ if $p = 2$.

(ii) *Suppose $g = 3$.*

(a) There does not exist such an A if $p \ne 3, 7$;
(b) $c_A = 14$ if $p = 7$;
(c) $c_A = 18$ if $p = 3$.

(iii) *Suppose $g = 4$.*

(a) $c_A \in \{5, 8, 10, 12\}$ if $p \ge 7$;
(b) $c_A \in \{8, 10, 12, 15\}$ if $p = 5$;
(c) $c_A \in \{5, 8, 10, 12, 30\}$ if $p = 3$;
(d) $c_A \in \{5, 10, 20\}$ if $p = 2$.

(iv) *Suppose $g = 5$.*

(a) There does not exist such an A if $p \ne 11$;
(b) $c_A = 22$ if $p = 11$.

Corollary 15 *Suppose p is prime, n and g are odd natural numbers, and $g > 1$.*

(i) *If* $p \not\equiv 3 \pmod 4$*, then there does not exist a simple supersingular abelian variety of dimension* g *over* $\mathbf{F}_{p^n}$*.*
(ii) *If* $p \equiv 3 \pmod 4$*, and there exists a simple supersingular abelian variety of dimension* g *over* $\mathbf{F}_{p^n}$*, then* $g = p^{b-1}(p-1)/2$ *for some natural number* b*.*

Proof. Suppose there is a simple supersingular abelian variety A of dimension g over $\mathbf{F}_{p^n}$. Since $g > 1$ is odd, we conclude from Theorem 12 that $\varphi(c_A) = 2g \equiv 2 \pmod 4$ and $p \mid c_A$. This is only possible if $c_A = p^b$ or $2p^b$, and $p \equiv 3 \pmod 4$.

Part 2: Optimal supersingular abelian varieties

Definition 16 *Suppose* A *is a supersingular abelian variety of dimension* g *over* $\mathbf{F}_q$*. We say that* A *is* **optimal** *if* A *is simple, and* $c_A \geq c_B$ *for every simple supersingular abelian variety* B *of dimension* g *over* $\mathbf{F}_q$*.*

Optimal supersingular elliptic curves are well-known. The Jacobian of the genus 2 curve $y^2 + y = x^5 + x^3$ over $\mathbf{F}_2$ is optimal ($c_A = 12$), and was given in [9]. Recall that the genus of a curve is the same of the dimension of the Jacobian variety of the curve.

The next two sections give two different constructions of families of examples of optimal supersingular abelian varieties. The first comes from taking a piece of the Weil restriction of scalars of an elliptic curve. This construction has the advantage of producing abelian varieties of dimensions 2, 3, 4, and 6 with the largest security parameter possible for abelian varieties of that dimension, namely 6, 6, 7.5, and 7, respectively. The best such examples occur in characteristics 2 and 3, which gives a computational advantage. The second construction comes from Jacobian varieties of superelliptic curves, and has the advantage of giving a choice of infinitely many abelian varieties and characteristics.

5 A subvariety of the Weil restriction of scalars

If $\Bbbk \subset \Bbbk'$ are finite fields, E is an elliptic curve over $\Bbbk$, and $Q \in E(\Bbbk')$, write $\mathrm{Tr}_{\Bbbk'/\Bbbk} Q = \sum_{\sigma \in \mathrm{Gal}(\Bbbk'/\Bbbk)} \sigma(Q)$. See the appendix for a proof of a generalization of the following result.

Theorem 17 *Suppose* E *is a supersingular elliptic curve over* $\mathbf{F}_q$*,* π *is a* q*-Weil number for* E*, and* π *is not a rational number. Fix* $r \in \mathbf{N}$ *with* $\gcd(r, 2pc_E) = 1$*. Then there is a simple supersingular abelian variety* A *over* $\mathbf{F}_q$ *such that:*

(i) $\dim(A) = \varphi(r)$*;*
(ii) *for every primitive* r*-th root of unity* ζ*,* $\pi\zeta$ *is a* q*-Weil number for* A*;*
(iii) $c_A = rc_E$*;*
(iv) $\alpha_A = \frac{r}{\varphi(r)}\alpha_E$*;*
(v) *there is a natural identification of* $A(\mathbf{F}_q)$ *with the subgroup of* $E(\mathbf{F}_{q^r})$

$$\{Q \in E(\mathbf{F}_{q^r}) : \mathrm{Tr}_{\mathbf{F}_{q^r}/\mathbf{F}_{q^{r/\ell}}} Q = O \quad \textit{for every prime } \ell \mid r\}.$$

Abelian varieties of this form were considered by Frey in §3.2 of [6].

Remark 18 *By Theorem 17(iii), $A(\mathbf{F}_q)$ has the same MOV security as $E(\mathbf{F}_{q^r})$. By Theorem 17(v), computation in $A(\mathbf{F}_q)$ is as efficient as computation in $E(\mathbf{F}_{q^r})$. The advantage of using $A(\mathbf{F}_q)$ is that (by Theorem 17(iv)) its security parameter α_A is higher than that of $E(\mathbf{F}_{q^r})$ by a factor $r/\varphi(r)$, so (for example) it provides shorter signatures for the same security in the BLS short signature scheme [3].*

Using $E(\mathbf{F}_{q^r})$, a signature in the BLS scheme is the x-coordinate of a point on the elliptic curve, which is an element of $\mathbf{F}_{q^r}$ and therefore is $r\log_2(q)$ bits.

Fixing a basis for $\mathbf{F}_{q^r}$ over $\mathbf{F}_q$, an element of $\mathbf{F}_{q^r}$ can be viewed as a vector with r coordinates in $\mathbf{F}_q$. Using $A(\mathbf{F}_q)$ in the short signature scheme and identifying it with a subgroup of $E(\mathbf{F}_{q^r})$ as in Theorem 17(v), a signature will now be only the first $\varphi(r)$ coordinates *of the x-coordinate of a point in $E(\mathbf{F}_{q^r})$ (along with a few extra bits to resolve an ambiguity that may arise), so the signature is about $\varphi(r)\log_2(q)$ bits. Thus, for signature generation there is no additional computation required: just follow the algorithm in [3] to produce the x-coordinate of a point in $E(\mathbf{F}_{q^r})$, and drop the extra coordinates. However, for signature verification there is now an extra step: given a signature one must reconstruct the missing coordinates to get the x-coordinate of a point in our subgroup of $E(\mathbf{F}_{q^r})$, and then follow the verification algorithm in [3]. For more information on this extra verification step, see the examples below.*

Theorem 17 can be applied in particular to the low dimensional cases where the tuple $(\dim(A), p, r, c_A)$ is $(2,2,3,12)$, $(2, p>3, 3, 6)$, $(4,2,5,20)$, $(4,3,5,30)$, $(6,2,9,36)$, or $(6,3,7,42)$. Next we use Theorem 17 to give implementations in the cases $(4,3,5,30)$ and $(2,2,3,12)$.

5.1 $\dim(A) = 4$, $p = 3$

The largest security parameter for a 4-dimensional abelian variety is 7.5, and this occurs only in characteristic 3.

When $\gcd(n,6) = 1$ there are exactly 2 isogeny classes of elliptic curves over $\mathbf{F}_{3^n}$ with security parameter 6. Equations for a curve from each isogeny class, along with one of its Weil numbers and its characteristic polynomial of Frobenius, are given below, where $(\frac{3}{n})$ denotes the Jacobi symbol, which is $+1$ if $n \equiv \pm 1 \pmod{12}$, and -1 if $n \equiv \pm 5 \pmod{12}$.

curve	equation	Weil number	characteristic polynomial
E_n^+	$y^2 = x^3 - x + (\frac{3}{n})$	$\sqrt{3^n}e^{7\pi i/6}$	$G_n(x) = x^2 + 3^{\frac{n+1}{2}}x + 3^n$
E_n^-	$y^2 = x^3 - x - (\frac{3}{n})$	$\sqrt{3^n}e^{\pi i/6}$	$H_n(x) = x^2 - 3^{\frac{n+1}{2}}x + 3^n$

By Theorem 11 there is no elliptic curve over $\mathbf{F}_{3^n}$ with security parameter 6 when n is even. If n is an odd multiple of 3 then there are again two isogeny classes of curves with the same Weil numbers and characteristic polynomials as in the above table, but with different curves E_n^+ and E_n^-.

Applying Theorem 17 to the elliptic curves E_n^+ and E_n^- over $\mathbf{F}_{3^n}$ with $r = 5$ produces 4-dimensional abelian varieties A_n^+ and A_n^- over $\mathbf{F}_{3^n}$, described in the following table.

	Weil number	characteristic polynomial
A_n^+	$\sqrt{3^n}e^{\pi i/30}$	$H_{5n}(x^5)/G_n(x)$
A_n^-	$\sqrt{3^n}e^{17\pi i/30}$	$G_{5n}(x^5)/H_n(x)$

Write E for $E_n^\pm$ and A for $A_n^\pm$. By Theorem 17(iv), $\alpha_A = \frac{5}{4}\alpha_E = 7.5$. Using the characteristic polynomials to compute $\#A(\mathbf{F}_{3^n})$ for various n, we find the following sample values of n for which $\#A(\mathbf{F}_{3^n})$ is of a size suitable for cryptographic applications, and has a large prime factor. Here the signature length is $4\log_2(3^n)$ (see Remark 18), the DL security column contains $\log_2(\ell)$ where ℓ is the largest prime dividing $\#A(\mathbf{F}_{3^n})$, and the MOV security column contains $\log_2(q^{c_A}) = \log_2(3^{30n})$.

variety	n	signature length	DL security	MOV security
A_n^+	15	95	95	713
A_n^+	17	108	100	808
A_n^+	19	120	112	903
A_n^+	33	209	191	1569
A_n^+	43	273	265	2045

Let $\Bbbk = \mathbf{F}_{3^n}$ and $\Bbbk_1 = \mathbf{F}_{3^{5n}}$. As discussed in Remark 18, the extra computation required for signature verification amounts to solving the problem: given 4 of the 5 $\Bbbk$-coordinates of x, where $(x, y) \in E(\Bbbk_1)$ and $\mathrm{Tr}_{\Bbbk_1/\Bbbk}(x, y) = O$, compute the fifth.

We next give an algorithm to do this. Suppose $Q = (x, y) \in E(\Bbbk_1)$ and $\sum_{i=0}^{4} \sigma^i(Q) = O$ where σ generates $\mathrm{Gal}(\Bbbk_1/\Bbbk)$. Then there is a function $\mathcal{F}$ on E with zeros at the points $\sigma^i(Q)$ for $0 \le i \le 4$, a pole of order 5 at O, and no other zeros or poles. Let $g(z) = \prod_{i=0}^{4}(z - \sigma^i(x)) \in \Bbbk[z]$, and let X and Y denote the coordinate functions on E. Then $g(X)$ is a function on E with zeros at $\pm\sigma^i(Q)$ for $0 \le i \le 4$, a pole of order 10 at O, and no other zeros or poles. Thus $g(X) = \mathcal{F}\tilde{\mathcal{F}}$, where $\tilde{\mathcal{F}}$ is $\mathcal{F}$ composed with multiplication by -1 on E. Write $\mathcal{F} = f_1(X) + f_2(X)Y$ with $f_1(X), f_2(X) \in \Bbbk[X]$. Since X has a double pole at O and Y a triple pole, we have $\deg(f_1) \le 2$ and $\deg(f_2) = 1$. Setting $g(X) = f_1(X)^2 - Y^2 f_2(X)^2 = f_1(X)^2 - (X^3 - X \pm 1)f_2(X)^2$ gives equations relating the coefficients of g, f_1, and f_2.

Suppose we know 4 of the 5 coordinates of x with respect to some fixed basis of $\Bbbk_1$ over $\Bbbk$, and let $b \in \Bbbk$ denote the missing coordinate. The coefficients of g are polynomials in b with coefficients in $\Bbbk$. Solving the above system of equations for b reduces to computing the resultant of 2 polynomials in 2 variables, and then finding the roots of a degree 9 polynomial in $\Bbbk[z]$. (The extra bits in the signature are used here in case the polynomial has more than one root.) This extra verification step takes a few seconds on a desktop computer, using the number theory software package KASH to compute the resultant and find its roots, but this could be optimized by writing a dedicated program.

Remark 19 *$\Bbbk$-coordinates of x, An alternative way to generate a signature from the point Q above is to take 4 of the 5 symmetric functions of x and its conjugates (i.e., 4 of the 5 coefficients of the polynomial g), instead of taking 4 of the 5 $\Bbbk$-coordinates of x. It is computationally very fast to recover the missing coefficient of g using the algorithm above. Then x can be computed by factoring g over $\Bbbk_1$. In our experiments the method above, which works over $\Bbbk$ rather than $\Bbbk_1$, seems to be more efficient.*

One could alternatively apply Theorem 17 with $q = 3$ and $r = 5n$ and gain an additional factor of $n/\varphi(n)$ in the signature length. However, the verification problem becomes harder.

5.2 $\dim(A) = 2$, $p = 2$

The largest security parameter for an abelian surface is 6, and this occurs only in characteristic 2.

When n is odd there are exactly 2 isogeny classes of elliptic curves over $\mathbf{F}_{2^n}$ with $\alpha_E = 4$, namely those of $y^2 + y = x^3 + x + 1$ and $y^2 + y = x^3 + x$. Applying Theorem 17 with these curves and $r = 3$ produces two abelian surfaces $A_n^{\pm}$ over $\mathbf{F}_{2^n}$ with Weil number $\pm\sqrt{2^n}e^{\pi i/12}$ and characteristic polynomial of Frobenius

$$x^4 \mp 2^{\frac{n+1}{2}} x^3 + 2^n x^2 \mp 2^{\frac{3n+1}{2}} x + 2^{2n}.$$

(One of these abelian varieties was given in [9] as the Jacobian of a hyperelliptic curve.)

By Theorem 17(iv) (or directly from the definition), $\alpha_{A_n^{\pm}} = 6$. Using the characteristic polynomials to compute $\#A_n^{\pm}(\mathbf{F}_{2^n})$ for various n, we find the following sample values of n that are suitable for cryptographic applications. Here the signature length is $2n$.

variety	n	signature length	DL security	MOV security
A_+	43	86	82	516
A_-	53	106	93	636
A_+	79	158	141	948
A_+	87	174	167	1044
A_-	87	174	156	1044
A_-	103	206	192	1236
A_-	121	242	220	1452

As discussed in Remark 18, there is no extra computation required to generate short signatures using $A_n^{\pm}$, and the extra computation required for signature verification amounts to solving the following problem: given two of the three $\mathbf{F}_{2^n}$-coordinates of a point in the subgroup of $E_n^{\pm}(\mathbf{F}_{2^{3n}})$ corresponding to $A_n^{\pm}(\mathbf{F}_{2^n})$ under Theorem 17(v), find the third coordinate. Using the method described above in the case of $p = 3$, $g = 4$, and $r = 5$, in the present case the computation reduces to taking one square root in $\mathbf{F}_{2^n}$ and solving one quadratic polynomial over $\mathbf{F}_{2^n}$. Taking square roots in a field of characteristic 2 is just a single exponentiation, and solving a quadratic equation is not much harder. Neither of these operations took measurable time on a desktop computer with the field $\mathbf{F}_{2^{103}}$.

6 Jacobian varieties that are optimal when q is a square

The next result gives families of examples of Jacobian varieties that are optimal. They have the advantage of giving a choice of infinitely many field characteristics.

Theorem 20 *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 $\gamma \in F^*$, 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 the dimension of A_γ is $\varphi(n)/2$ and A_γ is supersingular. If in addition γ generates F^* modulo n-th powers, then A_γ is simple, $c_{A_\gamma} = n$, and $A_\gamma(F)$ is cyclic.

Proof. The dimension of A_γ is the genus of C_γ. The genus g of C_γ being $\varphi(n)/2$ follows from the fact that g is independent of γ, and the formula for the genus of $C_{\pm 1}$ given on p. 55 of [4].

Since $q \equiv -1 \pmod{n}$, Theorem 20.15 of [19] 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

$$\begin{array}{ccc} C_1 & \xrightarrow{\phi_1} & C_1 \\ {\scriptstyle\lambda}\big\downarrow & & \big\downarrow{\scriptstyle\lambda'} \\ C_\gamma & \xrightarrow{\phi_\gamma} & C_\gamma \end{array}$$

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^* 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 $P(x)$. Therefore A_γ is simple and $c_A = n$. By Theorem 1, $A_\gamma(F)$ is cyclic.

Example 21 *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, $1 \le \alpha, \beta \le \ell-1$, 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^* modulo n-th powers. Let C be the curve $y^n = \gamma x^a(1-x)^b$ and A its Jacobian variety. Then by Theorem 20, A is simple and supersingular, $\operatorname{genus}(C) = \dim(A) = g$, $c_A = n$, $A(F)$ is cyclic, and $2n$ is the smallest integer k such that $\#A(F)$ divides $q^k - 1$. In the table, 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 element of W_{2g}, so A is optimal. Optimal examples with $g = 1$ and 5 are obtained 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.

7 Security

Proofs of security for cryptosystems based on elliptic curves rely on the difficulty of some problem (EC Diffie-Hellman and/or Weil Diffie-Hellman, for the systems in [18, 15, 2, 3, 22]). These hard problems generalize to abelian varieties, where they are also believed to be hard. However, we note some additional security considerations.

Allowing the cryptographic exponent c_A to take half-integer values when q is a square means that c_A correctly captures the MOV security of the variety. For example, for every prime p there is a supersingular elliptic curve E over $\mathbf{F}_{p^2}$ such that $c_A = \frac{1}{2}$, by Theorem 11. By Theorem 1, $E(\mathbf{F}_{p^2}) \cong (\mathbf{Z}/(p-1)\mathbf{Z})^2$, and the smallest field in which the Weil and Tate pairings take their values is $\mathbf{F}_p$. Therefore, solving the DL problem in $\mathbf{F}_p^*$ will break cryptographic schemes that base their security on the difficulty of solving the DL problem in a subgroup of $E(\mathbf{F}_{p^2})$. In other words, the MOV security here really comes from $\mathbf{F}_p$, and not $\mathbf{F}_q$. Theorem 7 says that in general the MOV security comes from a field of size q^{c_A}.

It follows from Theorem 8 that in the special case where A is an elliptic curve, q is not a square, and Q is a point in $A(\mathbf{F}_q)$ of large order, the cryptographic exponent c_A coincides with the "security multiplier" for Q that was defined in [3].

Abelian varieties that are Jacobians of hyperelliptic curves over a finite field whose size is small compared to the curve's genus are considered to be weak for use in cryptography, due to attacks in [1, 11]. The examples coming from §5 do not appear in general to be Jacobians of curves. The examples in §6 are Jacobians, but outside of the cases equivalent to the $a = b = 1$ case they do not appear to be Jacobians of hyperelliptic curves. In any case, these attacks do not apply to abelian varieties of small dimension.

Weil descent attacks [12, 10] have been carried out for certain elliptic curves over binary fields. In these attacks one starts with an elliptic curve over $\mathbf{F}_{q^r}$ and takes its Weil restriction of scalars down to $\mathbf{F}_q$. This is an abelian variety B of dimension r over $\mathbf{F}_q$. The attack proceeds by looking for a hyperelliptic curve whose Jacobian variety is related to B, solving the DL problem for this Jacobian variety, and using it to solve the DL problem for the original elliptic curve. For an abelian variety A produced by Theorem 17 from an elliptic curve E, we have $A(\mathbf{F}_q) \subseteq E(\mathbf{F}_{q^r})$. It is tempting to try to break the associated cryptosystems by solving the DL problem on $E(\mathbf{F}_{q^r})$ using Weil descent. However, the Weil descent attack replaces (the subfield curve) E by its Weil restriction of scalars from $\mathbf{F}_{q^r}$ to $\mathbf{F}_q$, which has A as a large simple factor, so we are back where we started. In addition, it is not known how to carry out Weil descent attacks except when $p = 2$ and $\dim(A) \geq 4$, and the most important applications of Theorem 17 (the examples in §5) have either $p = 3$ and $\dim(A) = 4$, or $p = 2$ and $\dim(A) = 2$. For these examples, one could ask whether there is an efficient way to find hyperelliptic curves, if they exist, whose Jacobians are related to the given abelian variety in a helpful way. This is likely to be a hard problem in general. Its analogue in characteristic zero would solve a long-standing problem by producing a sequence of elliptic curves of unbounded rank.

Acknowledgments. The authors thank Steven Galbraith for his observations and Dan Boneh for helpful conversations.

References

1. L. Adleman, J. DeMarrais and M-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields, in Algorithmic number theory. Lecture Notes in Computer Science, Vol. 877. Springer-Verlag (1994) 28–40.
2. D. Boneh and M. Franklin. Identity based encryption from the Weil pairing, in Advances in Cryptology — Crypto 2001. Lecture Notes in Computer Science, Vol. 2139. Springer-Verlag (2001) 213–229.
3. D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing, in Advances in Cryptology — Asiacrypt 2001. *Lect. Notes in Comp. Sci.* **2248** (2001), Springer-Verlag, 514–532.
4. R. Coleman and W. McCallum, Stable reduction of Fermat curves and Jacobi sum Hecke characters. *J. Reine Angew. Math.* **385** (1988) 41–101.
5. D. Cox, J. Little and D. O'Shea. Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. Springer-Verlag (1997).
6. G. Frey. Applications of arithmetical geometry to cryptographic constructions, in Finite fields and applications (Augsburg, 1999). Springer-Verlag (2001) 128–161.
7. G. Frey, M. Müller and H-G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory* **45** (1999) 1717–1719.

8. G. Frey and 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.
9. S. Galbraith. Supersingular curves in cryptography, in Advances in Cryptology — Asiacrypt 2001. Lecture Notes in Computer Science, Vol. 2248. Springer-Verlag (2001) 495–513.
10. S. Galbraith, F. Hess and N. P. Smart. Extending the GHS Weil descent attack, in Advances in Cryptology — Eurocrypt 2002. Lecture Notes in Computer Science, Vol. 2332. Springer-Verlag (2002) 29–44.
11. P. Gaudry. A variant of the Adleman–DeMarrais–Huang algorithm and its application to small genera, in Advances in Cryptology — Eurocrypt 2000. Lecture Notes in Computer Science, Vol. 1807. Springer-Verlag (2000) 19–34.
12. P. Gaudry, F. Hess and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology* **15** (2002) 19–46.
13. T. Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan* **20** (1968) 83–95.
14. B. Huppert and N. Blackburn. Finite groups II. Springer-Verlag (1982).
15. A. Joux. A one round protocol for tripartite Diffie-Hellman, in Algorithmic Number Theory (ANTS-IV), Leiden, The Netherlands, July 2–7, 2000, Lecture Notes in Computer Science, Vol. 1838. Springer-Verlag (2000) 385–394.
16. A. K. Lenstra and E. R. Verheul. *The XTR public key system*, in Advances in Cryptology — Crypto 2000. Lecture Notes in Computer Science, Vol. 1880. Springer-Verlag (2000) 1–19.
17. A. J. Menezes, T. Okamoto and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory* **39** (1993) 1639–1646.
18. R. Sakai, K. Ohgishi and M. Kasahara, Cryptosystems based on pairing. SCIS2000 (The 2000 Symposium on Cryptography and Information Security), Okinawa, Japan, January 26–28, 2000, C20.
19. G. Shimura. Abelian varieties with complex multiplication and modular functions. Princeton Univ. Press, Princeton, NJ (1998).
20. J. Silverman. The arithmetic of elliptic curves. Springer-Verlag (1986).
21. J. Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), in Séminaire Bourbaki, 1968/69, Soc. Math. France, Paris (1968) 95–110.
22. E. R. Verheul. Self-blindable credential certificates from the Weil pairing, in Advances in Cryptology — Asiacrypt 2001, Lecture Notes in Computer Science, Vol. 2248. Springer-Verlag (2001) 533–551.
23. A. Weil. Adeles and algebraic groups. Progress in Math. **23**, Birkhäuser, Boston (1982).
24. H. J. Zhu. Group structures of elementary supersingular abelian varieties over finite fields. *J. Number Theory* **81** (2000) 292–309.

Appendix

In this appendix we will state and prove a more general version (Theorem 24 below) of Theorem 17.

Write $\mathrm{Res}(f, g)$ for the resultant of two polynomials f and g.

Lemma 22 *Suppose a, b, c are pairwise relatively prime integers. Then there are $g_1(x), g_2(x) \in \mathbf{Z}[x]$ such that*

$$g_1(x) \prod_{a|d|abc} \Phi_d(x) + g_2(x) \prod_{b|d|abc} \Phi_d(x) = \prod_{ab|d|abc} \Phi_d(x).$$

Proof. Let $f_1(x) = \prod_{a|d|abc, b\nmid d} \Phi_d(x)$ and $f_2(x) = \prod_{b|d|abc, a\nmid d} \Phi_d(x)$. If η_i is a root of f_i for $i = 1$ and 2, then η_1/η_2 is a root of unity of order divisible by both a prime divisor of a and a prime divisor of b. Hence $\eta_1/\eta_2 - 1$ is a (cyclotomic) unit in the ring of algebraic integers. Therefore $\mathrm{Res}(f_1, f_2)$, an integer which is the product of the differences of the roots of f_1 and the roots of f_2, is ± 1. By Proposition 9 in §3.5 of [5], there are $g_1, g_2 \in \mathbf{Z}[x]$ such that $g_1(x)f_1(x) + g_2(x)f_2(x) = \mathrm{Res}(f_1, f_2)$.

Lemma 23 *Suppose M is a square matrix over a field F with characteristic polynomial f_M, and $g(x) \in F[x]$. Then $\det(g(M)) = \mathrm{Res}(g, f_M)$.*

Proof. This is clear if M is upper-triangular. To obtain the general case, replace F by its algebraic closure and upper-triangularize M.

Recall the notation e from Theorem 1.

Theorem 24 *Suppose $\mathcal{E}$ is a supersingular abelian variety over $\mathbf{F}_q$ with $e = 1$. Fix $r \in \mathbf{N}$ such that $\gcd(r, 2pc_{\mathcal{E}}) = 1$. Then there is a simple supersingular abelian variety A over $\mathbf{F}_q$ such that:*

(i) $\dim(A) = \varphi(r)\dim(\mathcal{E})$;
(ii) if π is a q-Weil number for $\mathcal{E}$, then $\pi\zeta$ is a q-Weil number for A for every primitive r-th root of unity ζ;
(iii) $c_A = rc_{\mathcal{E}}$;
(iv) $\alpha_A = \frac{r}{\varphi(r)}\alpha_{\mathcal{E}}$;
(v) there is a natural identification of $A(\mathbf{F}_q)$ with the subgroup of $\mathcal{E}(\mathbf{F}_{q^r})$

$$\{Q \in \mathcal{E}(\mathbf{F}_{q^r}) : \mathrm{Tr}_{\mathbf{F}_{q^r}/\mathbf{F}_{q^{r/\ell}}} Q = O \quad \textit{for every prime } \ell \mid r\}.$$

Proof. Let Ω be the set of q-Weil numbers for $\mathcal{E}$, and $d = \dim(\mathcal{E})$. Since $e = 1$, the characteristic polynomial of the Frobenius endomorphism $\phi_{\mathcal{E}}$ on $\mathcal{E}$ is $P_{\mathcal{E}}(x) = \prod_{\pi\in\Omega}(x - \pi)$.

Let $\Bbbk = \mathbf{F}_q$ and $\Bbbk_1 = \mathbf{F}_{q^r}$, and let B denote the Weil restriction of scalars (§1.3 of [23]) of $\mathcal{E}$ from $\Bbbk_1$ to $\Bbbk$. Then B is an rd-dimensional abelian variety defined over $\Bbbk$, there is a natural isomorphism

$$B(\Bbbk) \cong \mathcal{E}(\Bbbk_1), \tag{1}$$

and $P_B(x) = \prod_{\pi\in\Omega}(x^r - \pi^r)$ is the characteristic polynomial of the Frobenius endomorphism on B over $\Bbbk$. Fix a $\pi \in \Omega$ and a primitive r-th root of unity ζ. Then $P_B(\pi\zeta) = 0$, so B has a simple supersingular abelian subvariety A with $\pi\zeta$ as a q-Weil number. We will show that the conclusions of the theorem hold for A.

Assertion (iii) holds by Definition 3. By Proposition 10 and the fact that $p \nmid r$, $e = 1$ for A. Thus, $2\dim(A) = [\mathbf{Q}(\pi\zeta) : \mathbf{Q}]$. Since $\gcd(r, 2pc_{\mathcal{E}}) = 1$ we have $\mathbf{Q}(\zeta) \cap \mathbf{Q}(\pi) = \mathbf{Q}$, so $[\mathbf{Q}(\pi\zeta) : \mathbf{Q}] = [\mathbf{Q}(\pi) : \mathbf{Q}][\mathbf{Q}(\zeta) : \mathbf{Q}] = 2\dim(\mathcal{E})\varphi(r)$. This proves (i), and (ii) and (iv) follow. The isomorphism (1) identifies $A(\Bbbk)$ with a subgroup of $\mathcal{E}(\Bbbk_1)$, and it remains only to determine this subgroup.

If ℓ is a prime divisor of r, write $r = \ell^i m$ with $\ell \nmid m$, let $\Bbbk_\ell = \mathbf{F}_{q^{r/\ell}}$, and let $h_\ell(x) = \prod_{d|m} \Phi_{\ell^i d}(x) = (x^r - 1)/(x^{r/\ell} - 1)$. Let

$$T = \{Q \in \mathcal{E}(\Bbbk_1) : \mathrm{Tr}_{\Bbbk_1/\Bbbk_\ell} Q = O \text{ for every prime } \ell \mid r\} = \cap_{\ell|r} \ker(h_\ell(\phi_\mathcal{E})).$$

Applying Lemma 22 inductively one can show that there are $\gamma_\ell(x) \in \mathbf{Z}[x]$ such that $\sum_{\ell|r} \gamma_\ell(x) h_\ell(x) = \Phi_r(x)$. It follows that $T = \ker(\Phi_r(\phi_\mathcal{E}))$. Since $\phi_\mathcal{E}$ is (purely) inseparable (see Proposition II.2.11 of [20]), it follows that $\Phi_r(\phi_\mathcal{E})$ is separable (its action on the space of differential forms on $\mathcal{E}$ is $\Phi_r(0) \not\equiv 0 \pmod{p}$; see Proposition II.4.2(c) of [20]). By Theorem III.4.10(c) of [20], $\#T$ is the degree of the endomorphism $\Phi_r(\phi_\mathcal{E})$.

Applying Lemma 23 to the matrix $M_\mathcal{E}$ giving the action of $\phi_\mathcal{E}$ on the ℓ-adic Tate module of $\mathcal{E}$ for some prime $\ell \neq p$ shows that

$$\begin{aligned}\#T = \deg(\Phi_r(\phi_\mathcal{E})) &= \det(\Phi_r(M_\mathcal{E})) \\ &= \mathrm{Res}(\Phi_r, P_\mathcal{E}) = \prod_{\Phi_r(\eta)=0} P_\mathcal{E}(\eta) = P_A(1) = \#A(\Bbbk).\end{aligned}$$

If $\mathcal{E}(\Bbbk_1)$ is cyclic, it follows that the isomorphism (1) identifies $A(\Bbbk)$ with T. In the special cases where $\mathcal{E}(\Bbbk_1)$ is not cyclic (Theorem 1(iii)) one can show that $\#A(\Bbbk) = P_A(1)$ is odd, and since the odd part of $\mathcal{E}(\Bbbk_1)$ is always cyclic, (1) identifies $A(\Bbbk)$ with T in this case also.