USING ABELIAN VARIETIES TO IMPROVE PAIRING-BASED CRYPTOGRAPHY

K. RUBIN AND A. SILVERBERG

Abstract. We show that supersingular abelian varieties can be used to obtain higher MOV security per bit, in all characteristics, than supersingular elliptic curves. We give a point compression/decompression algorithm for primitive subgroups associated with elliptic curves, that gives shorter signatures, ciphertexts, or keys for the same security while using the arithmetic on supersingular elliptic curves. We determine precisely which embedding degrees are possible for simple supersingular abelian varieties over finite fields, and define some invariants that are better measures of cryptographic security than the embedding degree. We construct examples of good supersingular abelian varieties to use in pairing-based cryptography.

1. Introduction

In this paper we show that supersingular abelian varieties can be used to obtain higher MOV security per bit, in all characteristics, than supersingular elliptic curves. We also give a point compression/decompression algorithm that allows one to take advantage of elliptic curve algorithms and software while obtaining shorter transmissions, signatures, ciphertexts, and keys. We also define the "cryptographic exponent" and "security parameter" for supersingular abelian varieties, and prove that they are closely related to the embedding degree but are better measures of cryptographic security. We determine precisely which embedding degrees are possible for simple supersingular abelian varieties over finite fields. We also construct optimal supersingular abelian varieties to use in pairing-based cryptography.

For pairing-based cryptography, it is useful to have abelian varieties with embedding degrees that are neither too small (which would lead to poor security) nor too large (which would make computations prohibitive). Supersingular abelian varieties are a natural source of varieties for these applications.

Elliptic curves are useful in cryptography because they are algebraic groups (also known as group varieties). This implies that they, their group law, and inverse map are all defined by polynomials, and therefore are amenable to efficient computer computation, and the group structure gives a discrete logarithm problem on cyclic subgroups. Abelian varieties are exactly the connected projective algebraic groups. Elliptic curves are exactly the one-dimensional abelian varieties. One of the advantages of using the group $A(\mathbb{F}_q)$ of an abelian variety in place of the multiplicative group $\mathbb{F}_q^\times$ of a finite field $\mathbb{F}_q$ is that there is no known subexponential algorithm for computing discrete logarithms on general abelian varieties or elliptic curves. While subexponential algorithms exist for abelian varieties (and elliptic curves) of

Preliminary versions of parts of this paper appeared in the proceedings of Crypto 2002 [38], ANTS VI [40] and the Daewoo Workshop on Cryptography [46].

Key words and phrases. elliptic curves, pairing-based cryptography, elliptic curve cryptography, abelian varieties, compression.

small embedding degree, such varieties nevertheless have been found to be useful for pairing-based cryptography.

Section 2 below gives some background on abelian varieties. In §3 we discuss pairings on abelian varieties and generalize an elliptic curve result of Balasubramanian and Koblitz. In §4 we define useful invariants for elementary supersingular abelian varieties, the cryptographic exponent $c_{A,q}$ and the security parameter $\alpha(A,q)$. In §6 we relate $c_{A,q}$ to the embedding degree, and show that $c_{A,q}$ is a finer and more accurate measure of the cryptographic security. If a prime ℓ divides $|A(\mathbb{F}_q)|$, then the embedding degree of A over $\mathbb{F}_q$ with respect to ℓ is defined as the multiplicative order of q modulo ℓ, and (for ℓ sufficiently large and for A elementary and supersingular) is $c_{A,q}$ if $c_{A,q} \in \mathbb{Z}$ and is $2c_{A,q}$ otherwise. The security parameter $\alpha(A,q)$, which measures MOV security per bit, is $c_{A,q}/g$, where g is the dimension of the abelian variety. This allows us to compare security among abelian varieties of different dimension. Theorem 6.3 below is stronger than Theorem 7 of [38] (except for the harmless $\ell > 7$ condition) which was stated there without proof. Our setting is that of elementary abelian varieties, which is more general than the setting of simple abelian varieties in [38].

Galbraith [20] gave upper bounds on the embedding degrees (and therefore on the security parameters) for supersingular Jacobian varieties of curves, and asked whether his bounds can be improved. Inspired by and building on [20], and making use of results of Zhu, in §7 we determine exactly which values can occur as the security parameters of simple supersingular abelian varieties. In particular, we significantly improve on Galbraith's bounds when the dimension is more than two. Note that, since cryptographic security is based on the cyclic subgroups of $A(\mathbb{F}_q)$, for purposes of cryptology it suffices to consider simple abelian varieties A, i.e., abelian varieties that do not decompose as products of lower dimensional abelian varieties. Our results in §7 imply that if A is a simple supersingular abelian variety over $\mathbb{F}_q$ of dimension g, then the security parameter $\alpha(A,q)$ is at most the corresponding entry in Table 1 (where $p = \mathrm{char}(\mathbb{F}_q)$), and each entry can be attained. A '$*$' means that there are no simple supersingular abelian varieties of dimension g over $\mathbb{F}_q$.

Table 1. Upper bounds on the security parameters $\alpha(A,q)$

g	1	2	3	4	5	6
q a square	3	3	3	3.75	2.2	3.5
q not a square, $p > 11$	2	3	$*$	3	$*$	3
q not a square, $p = 2$	4	6	$*$	5	$*$	6
q not a square, $p = 3$	6	2	6	7.5	$*$	7
q not a square, $p = 5$	2	3	$*$	3.75	$*$	3
q not a square, $p = 7$	2	3	$4\frac{2}{3}$	3	$*$	7
q not a square, $p = 11$	2	3	$*$	3	4.4	3

Our results imply that security parameters for simple supersingular abelian varieties are unbounded (as the dimension of the varieties grows). However, large security parameters require very large dimension. This, computational issues, and possibly 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. Our results show that over every finite field, one can attain higher MOV security using four-dimensional simple supersingular abelian varieties than using supersingular elliptic curves, and supersingular abelian surfaces attain higher MOV security per bit than supersingular elliptic curves over every finite field of non-square size in characteristic $\neq 3$. This answers in the affirmative the open question from [6] on whether one can use higher dimensional abelian varieties to obtain higher security per bit than [6]'s BLS short signature scheme. In fact, we show that higher security per bit can be attained using only elliptic curve arithmetic, by using our compression algorithm on primitive subgroups associated with elliptic curves. Supersingular abelian surfaces in large characteristic (especially those that are primitive subgroups coming from elliptic curves) seem especially promising for pairing-based cryptography.

In §8 we discuss the "primitive" subgroups of the restrictions of scalars of abelian varieties. In §9 we obtain results on the cryptographic security of primitive subgroups in the supersingular case. Corollary 9.4 gives an algorithm whose inputs are a supersingular elliptic curve E over $\mathbb{F}_q$ and a "suitable" prime r and whose output is an abelian variety E_r (the r-th "primitive" subgroup) over $\mathbb{F}_q$ whose MOV security per bit is higher by a factor of $r/(r-1)$. We have $E_r(\mathbb{F}_q) \cong A_0 \subseteq E(\mathbb{F}_{q^r})$, where A_0 is the trace zero subgroup of $E(\mathbb{F}_{q^r})$. It has been pointed out that Theorem 9.2 also shows that only $\varphi(r)/r$ of the bits in Boneh-Lynn-Shacham signatures over fields of the form $\mathbb{F}_{q^r}$ contribute to the security.

In §10 we present a compression/decompression algorithm for the points in the trace zero subgroups of elliptic curves over $\mathbb{F}_{q^r}$, which compresses by a factor of $r/(r-1)$. We can make decompression practical when $r = 3$ or 5. The (de)compression algorithm applied to the examples of §12 can be used to improve the bandwidth efficiency of any pairing-based cryptosystem, giving shorter transmissions for the same MOV security, while using only elliptic curve arithmetic. In [3] it is shown that for optimized pairing implementations in the supersingular characteristic two case, using our compression on E_3 in general outperforms Jacobians of genus two curves.

Our (de)compression algorithm is analogous to what Lucas-based cryptosystems [35, 47, 48], XTR [31], the $\mathbb{T}_2$-cryptosystem and CEILIDH [39] accomplish for the multiplicative group of a finite field (see [40]). The restriction of scalars from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ of an elliptic curve E over $\mathbb{F}_q$ splits (up to isogeny) into a direct sum $\oplus_{d|r}E_d$ where each primitive subgroup E_d is an abelian variety over $\mathbb{F}_q$ of dimension $\varphi(d)$. Thus, doing cryptography in $E(\mathbb{F}_{q^r})$ reduces to doing cryptography in each $E_d(\mathbb{F}_q)$. For greatest efficiency, one would like to represent elements of $E_d(\mathbb{F}_q)$ in $\mathbb{F}_q^{\varphi(d)}$, i.e., one would like a low degree "compression" map $E_d \to \mathbb{A}^{\varphi(d)}$, where $\mathbb{A}^m$ is affine m-space, with a computable decompression function. A compression map of degree b allows one to represent elements of $E_d(\mathbb{F}_q)$ in $\mathbb{F}_q^{\varphi(d)} \times \{0,1\}^{\lceil \log_2 b \rceil}$, since the extra $\lceil \log_2 b \rceil$ bits determine which inverse image to choose. Our compression/decompression algorithm is efficient when $d = 3$ and 5, with morphisms $E_d - O \to \mathbb{A}^{\varphi(d)}$ of degree 8 and 54, respectively. Note that for $d = 1$ we have $E_1 = E$, and the usual elliptic curve point compression $(x, y) \mapsto x$ gives a degree 2 map $E_1 - O \to \mathbb{A}^1$, while for $d = 2$ in odd characteristic, writing $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{D})$ and writing $s \in \mathbb{F}_{q^2}$ as $s_0 + s_1\sqrt{D}$ with $s_0, s_1 \in \mathbb{F}_q$, the map $(s, t) \mapsto s_0$ from $E(\mathbb{F}_{q^2}) - O$ to $\mathbb{F}_q$ induces a degree 2 compression map $E_2 - O \to \mathbb{A}^1$, for which decompression is easy since $s_1 = 0$ for points (s, t) in the trace zero subgroup of $E(\mathbb{F}_{q^2})$. Note that E_2 is the quadratic twist of E. We leave it as an open question to find efficient (i.e., low degree) dominant maps $E_d - O \to \mathbb{A}^{\varphi(d)}$ with efficiently computable decompression maps when $d > 5$. For the $\mathbb{T}_2$-cryptosystem one can work directly with compressed elements; it is an open problem to find efficient arithmetic for working directly with compressed elements of $E_3(\mathbb{F}_q)$ or $E_5(\mathbb{F}_q)$.

Pairing-based cryptography originated in papers of Joux [27] and Sakai-Ohgishi-Kasahara [42], and has numerous applications (see [2]), including tripartite Diffie-Hellman [27], identity-based cryptography [4], and short signatures [6]. We use short signatures as an illustrative example. In [6], Boneh, Lynn, and Shacham used pairings associated with supersingular elliptic curves, and asked whether abelian varieties can be used instead to obtain shorter signatures. We answer this question in the affirmative in §11. Our modification of the BLS signature scheme multiplies the MOV security of BLS signatures (for supersingular elliptic curves) by r while multiplying the signature size by $\varphi(r)$, thus shortening BLS signatures over $\mathbb{F}_{q^r}$ by a factor of $r/\varphi(r)$ (if $\gcd(r, 2qc_{E,q}) = 1$). While we arrived at our method for compressing BLS signatures by studying the arithmetic of abelian varieties, our algorithm can be performed entirely using elliptic curve arithmetic, without needing to know anything about higher dimensional abelian varieties. We also give a novel application of primitive subgroups to obtain new instantiations of composite order bilinear groups.

In §12 we construct good supersingular abelian varieties to use in cryptography, in both large and small characteristic. In §13 we discuss some security considerations that arise for the abelian varieties E_r.

We note that primitive and trace zero subgroups were studied by Frey, Lange, Naumann (who did a compression/decompression algorithm for E_3), Weimerskirch, and Diem; we thank Tanja Lange for drawing our attention to [30, 17, 37, 12, 53].

We thank Dan Boneh for asking the question that led to Theorem 3.1 and Corollary 3.2. We thank Steven Galbraith for drawing our attention to [3].

Rubin thanks NSF for support, and Silverberg thanks NSF, NSA, Xerox PARC, and IPAM. Partial support was provided by NSF grant DMS-0457481 and NSA grants H98230-05-1-0044 and H98230-07-1-0039.

1.1. **Notation.** Let $\mathbb{F}_q$ denote the finite field with q elements. Let $\mathbb{N}$ denote the set of positive integers. If $r \in \mathbb{N}$, write $\Phi_r(x)$ for the r-th cyclotomic polynomial $\prod_\zeta (x - \zeta)$, where the product is over the primitive r-th roots of unity ζ. Note that $\Phi_r(x) \in \mathbb{Z}[x]$ and $\deg(\Phi_r) = \varphi(r)$, where φ is Euler's φ-function. The positive square root of q is denoted $\sqrt{q}$. If K is a field, $\bar{K}$ denotes an algebraic closure. If G is an abelian group, let $|G|$ denote the number of elements and let $G[m]$ denote the subgroup of elements of order dividing m.

2. Abelian varieties

An abelian variety over a field K is a connected projective group variety over K. The one-dimensional abelian varieties are the elliptic curves. It is a theorem that the group law on every abelian variety is abelian. From now on, when we say abelian variety we mean abelian variety of dimension ≥ 1.

Definition 2.1. *Suppose A and B are abelian varieties over the same field K. A* **homomorphism** *$f : A \to B$ is a morphism that is also a group homomorphism. A homomorphism $f : A \to B$ is an* **isogeny** *over K if f is surjective and defined over K and* $\dim(A) = \dim(B)$. *If an isogeny between A and B exists we say A and B are* **isogenous** *over K. If A is an abelian variety over K, A is called* **simple**

(over K) if it is not isogenous over K to a product of lower dimensional abelian varieties, and A is called **elementary** *(over K) if it is isogenous over K to a power of a simple abelian variety over K (this is sometimes called isotypic).*

Definition 2.2. *An elliptic curve E over a finite field $\mathbb{F}_q$ of characteristic p is* **supersingular** *if $E(\overline{\mathbb{F}}_q)$ has no points of order p. If A is an abelian variety over $\mathbb{F}_q$, then A is* **supersingular** *if A is isogenous over $\overline{\mathbb{F}}_q$ to a power of a supersingular elliptic curve.*

Definition 2.3. *If A is an abelian variety over $\mathbb{F}_q$, let $F_A(x)$ (or $F_{A,q}(x)$ if necessary) denote the characteristic polynomial of the Frobenius endomorphism of A over $\mathbb{F}_q$. The* **q-Weil numbers for** *A are the roots of $F_A(x)$.*

Definition 2.4. *If q is a prime power, then a* **supersingular q-Weil number** *is a complex number of the form $\sqrt{q}\zeta$ where ζ is a root of unity.*

Next we gather some important well-known results concerning abelian varieties over finite fields, due to Weil, Deuring, and others (see [51]), that we will use later.

Theorem 2.5. *If A is an abelian variety over $\mathbb{F}_q$, then:*

(i) $F_A(x) \in \mathbb{Z}[x]$;
(ii) $\deg(F_A) = 2\dim(A)$;
(iii) $|A(\mathbb{F}_q)| = F_A(1)$;
(iv) *if A is supersingular, then all the roots of F_A are supersingular q-Weil numbers;*
(v) *if all the roots of F_A are supersingular q-Weil numbers, then A is supersingular.*

We will also make use of the following results.

Theorem 2.6 (Tate [49])**.** *Two abelian varieties A and B over $\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if $F_A(x) = F_B(x)$.*

Theorem 2.7 (Honda-Tate [26, 50])**.** (i) *If ω is a supersingular q-Weil number, then there is a simple supersingular abelian variety A such that ω is a q-Weil number for A.*
(ii) *The map that associates to a simple supersingular abelian variety over $\mathbb{F}_q$ one of its q-Weil numbers gives a one-to-one correspondence between the $\mathbb{F}_q$-isogeny classes of simple supersingular abelian varieties over $\mathbb{F}_q$ and the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes of supersingular q-Weil numbers.*
(iii) *A supersingular abelian variety A over $\mathbb{F}_q$ is elementary over $\mathbb{F}_q$ if and only if $F_A(x) = G_A(x)^{f_A}$ for some monic irreducible polynomial $G_A(x) \in \mathbb{Z}[x]$ and some $f_A \in \mathbb{N}$.*

Theorem 2.8 (Zhu [54])**.** *Suppose A is an elementary supersingular abelian variety over $\mathbb{F}_q$. Let $p = \mathrm{char}(\mathbb{F}_q)$. Then with G_A and f_A as in Theorem 2.7(iii), we have:*

(i) *$A(\mathbb{F}_q) \cong (\mathbb{Z}/G_A(1)\mathbb{Z})^{f_A}$ unless q is not a square and either*
(a) *$p \equiv 3 \pmod 4$ and A is $\mathbb{F}_q$-isogenous to a power of a supersingular elliptic curve E with $G_E(x) = x^2 + q$, or*
(b) *$p \equiv 1 \pmod 4$ and A is $\mathbb{F}_q$-isogenous to a power of a supersingular abelian surface E with $G_E(x) = x^2 - q$,*
in which case $A(\mathbb{F}_q) \cong (\mathbb{Z}/G_A(1)\mathbb{Z})^a \times (\mathbb{Z}/\frac{G_A(1)}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^b$ with nonnegative integers a and b such that $a + b = f_A$;

(ii) *if A is simple over $\mathbb{F}_q$ then $f_A = 1$ or 2.*

In (only) the next section, we mention dual abelian varieties and polarizations. For definitions of dual abelian variety and the Weil pairing, see for example [36]. For a definition of polarization, see for example [44]. An abelian variety is isogenous to its dual. A polarization gives an isogeny from the abelian variety to its dual; a polarization is principal if this isogeny is an isomorphism. The degree of a polarization is the degree of the isogeny (and this degree is one if and only if the polarization is "principal"). All elliptic curves, Jacobian varieties of curves, and products of principally polarized abelian varieties are principally polarized abelian varieties.

3. Non-degenerate pairings

We show that having an abelian variety over $\mathbb{F}_q$ with a prescribed embedding degree k is sufficient to give a non-degenerate Weil pairing over $\mathbb{F}_{q^k}$ (assuming a condition on the multiplicity of 1 as an eigenvalue of Frobenius). This answers a question asked of us by Dan Boneh, generalizes an elliptic curve result of Balasubramanian and Koblitz, and is important for scaling pairing-based cryptography to higher security levels.

Theorem 1 of [1] shows that if A is an elliptic curve over $\mathbb{F}_q$, ℓ is a prime, $\ell \nmid q(q-1)$, $O \neq P \in A(\mathbb{F}_q)[\ell]$, and k is the order of q modulo ℓ, then $A[\ell] \subseteq A(\mathbb{F}_{q^k})$ (and thus $e_\ell(P,Q) \neq 1$ for some $Q \in A(\mathbb{F}_{q^k})[\ell]$, where e_ℓ is the Weil pairing). We generalize this to abelian varieties with a polarization of degree prime to ℓ, generalizing the condition $\ell \nmid (q-1)$ to a condition on the multiplicity of 1 as an eigenvalue of Frobenius. As shown in [1], some such condition is necessary. Our main conclusion (Corollary 3.2) is that there is a $Q \in A(\mathbb{F}_{q^k})[\ell]$ that pairs nontrivially with P under the pairing induced by the Weil pairing and the polarization.

If ℓ is a prime and A is an abelian variety over a field K whose characteristic is not ℓ, then the Weil pairing is a non-degenerate Galois-equivariant pairing from $A[\ell] \times A'[\ell]$ to $\boldsymbol{\mu}_\ell$, where A' is the dual abelian variety, $\boldsymbol{\mu}_\ell$ is the group of ℓ-th roots of unity in $\bar{K}$, and $A[\ell] := A(\bar{K})[\ell]$. Every polarization on A defined over K gives a K-isogeny between A and A', so if a polarization has degree relatively prime to ℓ it induces a non-degenerate Galois-equivariant pairing

$$e_\ell : A[\ell] \times A[\ell] \to \boldsymbol{\mu}_\ell.$$

Frey and Rück (Proposition 2.5 of [19]; see also [43]) proved that if A is the Jacobian of a curve over $\mathbb{F}_q$, ℓ is a prime not dividing q, k is the order of q modulo ℓ, $\sigma : x \mapsto x^q$ is the Frobenius automorphism of $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$, and U is the kernel of $\sigma - q$ in $A[\ell]$, then there is a non-degenerate Tate pairing

$$t_m : U \times A(\mathbb{F}_q)/\ell A(\mathbb{F}_q) \to \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^\ell.$$

Theorem 3.1 below is an analogue for the Weil pairing.

If e is a Tate or Weil pairing, $P \in A(\mathbb{F}_q)[\ell]$, k is the order of q mod ℓ, $Q \in A(\mathbb{F}_{q^k})[\ell]$, and $e(P,Q) \neq 1$, then the map from $\langle P \rangle$ to $\mathbb{F}_{q^k}^\times$ defined by $R \mapsto e(R,Q)$ is injective, where $\langle P \rangle$ denotes the group (of order ℓ) generated by P. Thus, as shown in [33, 19], the discrete log problem in $\langle P \rangle$ reduces to the discrete log problem in $\mathbb{F}_{q^k}^\times$. The "MOV security" of $\langle P \rangle$ is the discrete log security of $\mathbb{F}_{q^k}^\times$.

If $e : V \times V \to \boldsymbol{\mu}_\ell$ is a pairing, a subspace W of V is *isotropic* with respect to e if $e(P,Q) = 1$ for all $P, Q \in W$.

Theorem 3.1. *Suppose A is an abelian variety over $\mathbb{F}_q$, ℓ is a prime not dividing q, and A has a polarization over $\mathbb{F}_q$ of degree prime to ℓ. Let k denote the order of q modulo ℓ, let $e_\ell : A[\ell] \times A[\ell] \to \boldsymbol{\mu}_\ell$ denote the pairing induced by the Weil pairing and the polarization, let $V = A(\mathbb{F}_q)[\ell]$, let $d = \dim_{\mathbb{F}_\ell}(V)$, let $\sigma : x \mapsto x^q$ denote the Frobenius automorphism of $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$, let F denote the characteristic polynomial of σ acting on $A[\ell]$, and let U denote the kernel of $\sigma - q$ in $A[\ell]$. Suppose 1 occurs as a root of F with multiplicity exactly d. Then*

(i) $U \subseteq A(\mathbb{F}_{q^k})$,
(ii) $e_\ell : V \times U \to \boldsymbol{\mu}_\ell$ *is non-degenerate,*
(iii) $\dim_{\mathbb{F}_\ell}(U) = \dim_{\mathbb{F}_\ell}(V) = d$,
(iv) *if* $\ell \nmid (q-1)$, *then* $U \cap V = 0$ *and* V *is isotropic with respect to* e_ℓ,
(v) *if* $\ell \mid (q-1)$ *and* $V \neq 0$, *then* V *is not isotropic with respect to* e_ℓ.

Proof. If $Q \in U$, then $\sigma^k(Q) = q^k Q = Q$ (by the definition of U and the fact that $q^k \equiv 1 \pmod{\ell}$), so $Q \in A(\mathbb{F}_{q^k})$ and we have (i). The roots of F occur in pairs a, q/a. Thus q is a root of F with multiplicity d. Write $F(x) = (x-q)^d g(x)$, let $W = \ker(g(\sigma))$, and let $U_d = \ker((\sigma - q)^d) \supseteq U$. Then $\gcd((x-q)^d, g(x)) = 1$, U_d and W are σ-invariant subspaces of $A[\ell]$, $A[\ell] = U_d \oplus W$, and $\dim(U_d) = d$. Since q is not an eigenvalue for the action of σ on W, $\sigma - q$ is an isomorphism on W. Thus, $W = (\sigma - q)W$. If $P \in V$ and $T \in A[\ell]$, then

$$e_\ell(P, (\sigma - q)T) = e_\ell(P, \sigma(T))/e_\ell(P, qT) = \sigma(e_\ell(P,T))/e_\ell(P,T)^q = 1.$$

Thus, $e_\ell(P, R) = 1$ for all $R \in W$. Since e_ℓ is non-degenerate, either $V = 0$ or there is a $Q \in U_d$ such that $e_\ell(P, Q) \neq 1$. In either case, it follows that the σ-equivariant homomorphism $f : V \to \operatorname{Hom}(U_d, \boldsymbol{\mu}_\ell)$ defined by $f(P)(Q) = e_\ell(P, Q)$ is injective. Since $\dim(V) = \dim(U_d)$, f is an isomorphism, as is the corresponding map $U_d \to \operatorname{Hom}(V, \boldsymbol{\mu}_\ell)$. Thus the restriction of e_ℓ to $V \times U_d$ is non-degenerate. Since σ is the identity on V and acts via q on $\boldsymbol{\mu}_\ell$, $\sigma - q$ kills $\operatorname{Hom}(V, \boldsymbol{\mu}_\ell)$, and thus kills U_d. Thus $U_d \subseteq U$. So $U_d = U$, giving (ii) and (iii).

We have $q \equiv 1 \pmod{\ell}$ if and only if $U = V$. If $U = V \neq 0$, then (ii) implies V is not isotropic, and we have (v).

If V is not isotropic, then the restriction of e_ℓ to $V \times V$ is non-trivial, but takes values in $\boldsymbol{\mu}_\ell(\mathbb{F}_q)$ (since $V \subseteq A(\mathbb{F}_q)$). Thus $\boldsymbol{\mu}_\ell(\mathbb{F}_q) \neq 1$, so $\ell \mid (q-1)$. So if $\ell \nmid (q-1)$, then V is isotropic, and then (ii) implies $U \cap V = 0$. □

Corollary 3.2. *Suppose A is an abelian variety over $\mathbb{F}_q$, ℓ is a prime not dividing q, $O \neq P \in A(\mathbb{F}_q)[\ell]$, 1 occurs with multiplicity one as a root of the characteristic polynomial of Frobenius σ acting on $A[\ell]$, and A has a polarization of degree relatively prime to ℓ. Let $e_\ell : A[\ell] \times A[\ell] \to \boldsymbol{\mu}_\ell$ denote the pairing induced by the Weil pairing and the polarization, let k denote the order of q modulo ℓ, and let $U = \ker(\sigma - q) \subseteq A[\ell]$. Then $\dim_{\mathbb{F}_\ell}(U) = 1$, and for all $O \neq Q \in U$ we have $Q \in A(\mathbb{F}_{q^k})$ and $e_\ell(P, Q) \neq 1$.*

Proof. Since 1 occurs with multiplicity one as an eigenvalue of σ, $A(\mathbb{F}_q)[\ell]$ has dimension one over $\mathbb{F}_\ell$. Now apply (i-iii) of Theorem 3.1 with $d = 1$. □

The hypotheses in Corollary 3.2 imply that $\ell \nmid (q-1)$, since the pair 1 and q occur as eigenvalues of Frobenius, but 1 occurs with multiplicity exactly one.

4. The cryptographic exponent $c_{A,q}$

We begin by giving definitions of the cryptographic exponent $c_{A,q}$ and security parameter $\alpha(A,q)$ (we originally gave these definitions in [38]). The security parameter $\alpha(A,q)$ is $c_{A,q}/g$, where $g = \dim(A)$. It measures MOV security per bit, and is the relevant measure for comparing security among supersingular abelian varieties of different dimension. Roughly speaking, for a group G to have security parameter α means that the discrete logarithm problem in G can be reduced to the discrete logarithm problem in the multiplicative group of a field of size approximately $|G|^\alpha$. The group $G = A(\mathbb{F}_q)$ has order approximately q^g. We will relate $q^{c_{A,q}}$ to the size of the smallest field F such that every cyclic subgroup of $A(\mathbb{F}_q)$ can be embedded in $F^\times$.

Definition 4.1. *If A is an elementary supersingular abelian variety over $\mathbb{F}_q$, define its* **cryptographic exponent** $c_{A,q}$ *to be*

$$c_{A,q} := \begin{cases} \frac{m}{2} & \text{if } q \text{ is a square,} \\ \frac{m}{\gcd(2,m)} & \text{if } q \text{ is not a square,} \end{cases}$$

where $\sqrt{q}\zeta$ is a q-Weil number for A with ζ a primitive m-th root of unity.

Lemma 4.2. *The number $c_{A,q}$ is well-defined.*

Proof. 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, so $m = m'$. □

Remark 4.3. (i) When q is not a square, $c_{A,q} \in \mathbb{N}$.

(ii) When q is a square, $c_{A,q} \in \frac{1}{2}\mathbb{N} = \{\frac{s}{2} : s \in \mathbb{N}\}$.

Lemma 4.4. *If $\gcd(t, 2c_{A,q}) = 1$, then $c_{A,q^t} = c_{A,q}$.*

Proof. If $\omega = \sqrt{q}\zeta$ is a q-Weil number for A over $\mathbb{F}_q$, then $\omega^t = \sqrt{q^t}\zeta^t$ is a q^t-Weil number for A over $\mathbb{F}_{q^t}$. If ζ is a primitive m-th root of unity and $\gcd(t,m) = 1$, then ζ^t is a primitive m-th root of unity. The lemma now follows from the definitions of c_{A,q^t} and $c_{A,q}$. □

The next definition builds on the definition of "security multiplier" for elliptic curves in [7], extending it to measure security per bit for higher-dimensional abelian varieties.

Definition 4.5. *If A is an elementary supersingular abelian variety over $\mathbb{F}_q$, define its* **security parameter** $\alpha(A,q)$ *to be*

$$\alpha(A,q) := \frac{c_{A,q}}{\dim(A)}.$$

Recall the notation G_A and f_A from Theorem 2.7(iii). Recall that the exponent of a finite abelian group H is the smallest positive integer N such that $NH = 0$ (with the group law written additively). See Proposition 3.1 of [55] for a version of the following result that gives more information.

Theorem 4.6 ([55])**.** *Suppose A is an elementary supersingular abelian variety over $\mathbb{F}_q$.*

(i) *If q is a square, then:*

  (a) *$G_A(x) = \sqrt{q}^{\varphi(2c_{A,q})}\Phi_{2c_{A,q}}(\frac{x}{\sqrt{q}})$, and*
  (b) *the exponent of $A(\mathbb{F}_q)$ divides $\Phi_{2c_{A,q}}(\sqrt{q})$, which divides $q^{c_{A,q}} - 1$.*

(ii) *If q is not a square then:*
  (a) *$G_A(x)$ divides $q^{\varphi(c_{A,q})}\Phi_{c_{A,q}}(\frac{x^2}{q})$, and*
  (b) *the exponent of $A(\mathbb{F}_q)$ divides $\Phi_{c_{A,q}}(q)$, which divides $q^{c_{A,q}} - 1$.*

Proof. Part (i)(a) is part of Proposition 3.1(I) of [55]. Thus if q is a square, $G_A(1) = \sqrt{q}^{\varphi(2c_{A,q})}\Phi_{2c_{A,q}}(\frac{1}{\sqrt{q}}) = \pm\Phi_{2c_{A,q}}(\sqrt{q})$. If q is not a square and ω is a q-Weil number for A, then $\Phi_{c_{A,q}}(\frac{\omega^2}{q}) = 0$, so $G_A(x)$ divides $q^{\varphi(c_{A,q})}\Phi_{c_{A,q}}(\frac{x^2}{q})$, so $G_A(1)$ divides $q^{\varphi(c_{A,q})}\Phi_{c_{A,q}}(\frac{1}{q}) = \pm\Phi_{c_{A,q}}(q)$. By Theorem 2.8(i), the exponent of $A(\mathbb{F}_q)$ divides $G_A(1)$. Since $\Phi_m(x)$ divides $x^m - 1$, the result follows. □

Lemma 4.7. *Suppose A is an elementary supersingular abelian variety over $\mathbb{F}_q$, and ω is a q-Weil number for A. Then:*

(i) $2\dim(A)/f_A = \deg(G_A) = [\mathbb{Q}(\omega) : \mathbb{Q}]$;
(ii) *if q is a square, then* $\deg(G_A) = \varphi(2c_{A,q})$;
(iii) *if q is not a square, then* $\deg(G_A) = \varphi(c_{A,q})$ *or* $2\varphi(c_{A,q})$, *and* $\varphi(c_{A,q}) = [\mathbb{Q}(\omega^2) : \mathbb{Q}]$;
(iv) *if ℓ is a prime divisor of $2c_{A,q}$, then $\ell \leq 2\dim(A) + 1$.*

Proof. Part (i) follows from Theorems 2.5(ii) and 2.7(iii) and the definitions of G_A and ω. Let $c = c_{A,q}$, $g = \dim(A)$, and $\omega = \sqrt{q}\zeta_m$. If q is a square, then $[\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) = \varphi(2c)$, giving (ii). If q is not a square, then $[\mathbb{Q}(\zeta_m^2) : \mathbb{Q}] = \varphi(c)$ and $\deg(G_A) = [\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}(\omega^2)]\varphi(c) = \varphi(c)$ or $2\varphi(c)$, and (iii) follows. Suppose ℓ is a prime divisor of $2c$. If q is a square then by (i,ii) we have $2g \geq \deg(G_A) = \varphi(2c) \geq \ell - 1$, while if q is not a square then by (i,iii) we have $2g \geq \deg(G_A) \geq \varphi(c) \geq \ell - 1$, giving (iv). □

5. Lemmas

To prove Theorems 6.1 and 6.3 below, we begin with some lemmas.

Lemma 5.1. *Suppose that $\Phi_m(d)$ is divisible by a prime number ℓ, and $\ell \nmid m$. Then m is the order of d modulo ℓ.*

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

Lemma 5.2. *For all positive integers n and r,*

$$\Phi_n(x^r) = \prod_{\substack{d \mid r \\ (d,n)=1}} \Phi_{\frac{r}{d}n}(x).$$

Proof. We induct on the number of prime divisors of r (with multiplicity). The $r = 1$ case is obvious. If all prime divisors of r divide n, then $\Phi_n(x^r) = \Phi_{rn}(x)$ (see [23]), giving the result. Suppose $r = ps$ with p a prime that does not divide n, and

$s \in \mathbb{Z}$. Then

$$\Phi_n(x^r) = \Phi_n(x^s)\Phi_{np}(x^s) = \prod_{\substack{t|s \\ (t,n)=1}} \Phi_{\frac{s}{t}n}(x) \prod_{\substack{u|s \\ (u,np)=1}} \Phi_{\frac{s}{u}np}(x) =$$

$$\prod_{\substack{p|d|r \\ (d,n)=1}} \Phi_{\frac{r}{d}n}(x) \prod_{\substack{u|r \\ (u,np)=1}} \Phi_{\frac{r}{u}n}(x) = \prod_{\substack{d|r \\ (d,n)=1}} \Phi_{\frac{r}{d}n}(x)$$

where the first equality is stated in [23] and is easy to show, the second is by induction, and for the third let $d = pt$. □

6. The cryptographic exponent and MOV security

Suppose A is an abelian variety over $\mathbb{F}_q$, and $p = \mathrm{char}(\mathbb{F}_q)$. Theorems 6.3 and 6.1 below show that the cryptographic exponent $c_{A,q}$ captures the MOV security of A. In other words, if $A(\mathbb{F}_q)$ has a subgroup C of sufficiently large prime order, then $\mathbb{F}_{q^{c_{A,q}}}$ is the smallest extension F of $\mathbb{F}_p$ such that C can be embedded in the multiplicative group $F^\times$ of F.

If $A(\mathbb{F}_q)$ has a point of sufficiently large prime order ℓ, then Theorem 6.1 shows that $c_{A,q}$ is the smallest positive half-integer k such that $q^k - 1$ is an integer divisible by ℓ, while Theorem 6.3 shows that $c_{A,q}$ is in fact the smallest positive rational number k such that $q^k - 1$ is an integer divisible by ℓ. Thus the cryptographic exponent $c_{A,q}$ is a finer invariant than the embedding degree (which is the smallest positive integer k such that $q^k - 1$ is divisible by ℓ). For examples that show that the embedding degree can be very far from a good measure of cryptographic security in the case of ordinary (i.e., non-supersingular) elliptic curves, see §4 of [25].

Theorem 6.1 (Theorem 8 of [38])**.** *Suppose A is an elementary supersingular abelian variety over $\mathbb{F}_q$, ℓ is a prime number, ℓ divides $|A(\mathbb{F}_q)|$, and $\ell \nmid 2c_{A,q}$. Then*

$$c_{A,q}\mathbb{N} = \{k \in \frac{1}{2}\mathbb{N} : q^k - 1 \textit{ is an integer divisible by } \ell\}.$$

Proof. By Theorem 4.6, ℓ divides $\Phi_{2c_{A,q}}(\sqrt{q})$ if q is a square, and ℓ divides $\Phi_{c_{A,q}}(q)$ if q is not a square. By Lemma 5.1, $c_{A,q}$ is the smallest positive half-integer k such that $q^k - 1$ is an integer divisible by ℓ. □

Remark 6.2. Suppose A is a g-dimensional elementary supersingular abelian variety over $\mathbb{F}_q$. Lemma 4.7(iv) shows that if $\ell > 2g + 1$, then $\ell \nmid 2c_{A,q}$. Thus Theorem 6.1's constraint that $\ell \nmid 2c_{A,q}$ only rules out some (small) primes $\ell \leq 2g + 1$, and for cryptography we are only interested in large primes ℓ.

Retain the notation f_A and G_A from Theorem 2.7(iii).

Theorem 6.3. *Suppose A is an elementary supersingular abelian variety of dimension g over $\mathbb{F}_q$, $q = p^n$, ℓ is a prime divisor of $|A(\mathbb{F}_q)|$, $\ell \neq p$, and s is the multiplicative order of p mod ℓ. If q is a square, assume $\ell > (1+p)^{ng/(2f_A)}$. If q is not a square, assume $\ell > (1+\sqrt{p})^{2ng/(3f_A)}$ and $\ell > 7$. Then $p^s = q^{c_{A,q}}$, so $\mathbb{F}_{q^{c_{A,q}}}$ is the smallest extension of $\mathbb{F}_p$ whose multiplicative group has a subgroup of order ℓ.*

Proof. Write c for $c_{A,q}$. The goal is to prove that nc is the order of p modulo ℓ. By Lemma 5.1, it suffices to show that ℓ divides $\Phi_{nc}(p)$ and $\ell \nmid nc$.

First, suppose n is even (i.e., q is a square). We first show that $\ell \nmid nc$. Since $\varphi(2c) = \deg(G_A) = 2g/f_A$, we have

$$\ell > (1+p)^{ng/(2f_A)} = (1+p)^{n\varphi(2c)/4} \geq 3^{n\varphi(2c)/4}. \tag{6.1}$$

Thus $\ell > 3^{n/4} \geq n/2$. By our conditions, $\ell > 2$. Since n is even, it follows that $\ell \nmid n$. If $\ell \mid 2c$, then since $\ell > 2$ and $n \geq 2$, (6.1) implies $\ell > 3^{\varphi(2c)/2} \geq 3^{(\ell-1)/2} \geq \ell$, a contradiction, so $\ell \nmid nc$.

Continue to assume that n is even. By Theorem 4.6, ℓ divides $\Phi_{2c}(p^{n/2})$. By Lemma 5.2, $\Phi_{2c}(p^{n/2}) = \prod_{\substack{d \mid \frac{n}{2} \\ (d,2c)=1}} \Phi_{\frac{nc}{d}}(p)$, so ℓ divides $\Phi_{\frac{nc}{d}}(p)$ for some divisor d of $n/2$ that is relatively prime to $2c$. By our hypotheses, Lemma 4.7(i,ii), and the fact that $\varphi(ab) \leq \varphi(a)b$ for all $a, b \in \mathbb{N}$, we have

$$(1+p)^{ng/(2f_A)} < \ell \leq |\Phi_{\frac{nc}{d}}(p)| \leq (1+p)^{\varphi(cn/d)} \leq (1+p)^{\varphi(2c)n/(2d)} = (1+p)^{ng/(df_A)}.$$

Thus $d = 1$, i.e., ℓ divides $\Phi_{nc}(p)$ as desired.

Now suppose that n is odd (i.e., q is not a square). We first show that $\ell \nmid nc$. We have

$$\ell > (1+\sqrt{p})^{2ng/(3f_A)} = (1+\sqrt{p})^{n\deg(G_A)/3} \geq (1+\sqrt{p})^{n\varphi(c)/3} \geq (1.34)^{n\varphi(c)} \tag{6.2}$$

by Lemma 4.7. If $\ell \mid n$, then (6.2) implies $\ell > (1.34)^n \geq (1.34)^\ell > \ell$, the last inequality holding for all $\ell \geq 7$. This contradiction shows that $\ell \nmid n$. If $\ell \mid c$, then (6.2) implies $\ell > (1.34)^{\varphi(c)} \geq (1.34)^{\ell-1} > \ell$, the last inequality holding for all $\ell \geq 10$. This contradiction shows that $\ell \nmid c$.

Let ω be a q-Weil number for A, and let $H = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. By Theorem 2.8(i), ℓ divides

$$G_A(1) = \prod_{\sigma \in H}(1-\omega^\sigma) = \prod_{\sigma \in H} \prod_{\nu^n = \omega^\sigma}(1-\nu).$$

Then there exist $\sigma \in H$ and $\nu \in \mathbb{C}$ such that $\nu^n = \omega^\sigma$ and ℓ divides $\prod_{\tau \in G}(1-\nu^\tau) \in \mathbb{Z}$, where $G := \mathrm{Gal}(\mathbb{Q}(\nu)/\mathbb{Q})$. Replacing ω by ω^σ if necessary, we may assume $\sigma = 1$. Write $\omega = \sqrt{q}\zeta_m$, with ζ_m a primitive m-th root of unity. Then for some d we can write $\nu = \sqrt{p}\zeta_d$ with a primitive d-th root of unity ζ_d such that $\zeta_d^n = \zeta_m$. Then m divides d (since $\zeta_m^d = \zeta_d^{nd} = 1$), which divides nm (since $(\zeta_d)^{nm} = \zeta_m^m = 1$). Let $t = d/m \in \mathbb{Z}$. Then t divides n. Since n is odd, so is t. Since ζ_d^t is a primitive m-th root of unity, there is a $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\zeta_d^t = \zeta_m^\delta$. Thus,

$$\nu^t = \sqrt{p}^t \zeta_d^t = \sqrt{p}^t \zeta_m^\delta = \pm\omega^\delta / p^{(n-t)/2} \in \mathbb{Q}(\omega),$$

so $[\mathbb{Q}(\nu) : \mathbb{Q}(\omega)] \leq t$. Since $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(G_A) = 2g/f_A$, we have

$$(1+\sqrt{p})^{2ng/(3f_A)} < \ell \leq |\prod_{\tau \in G}(1-\nu^\tau)| \leq (1+\sqrt{p})^{[\mathbb{Q}(\nu):\mathbb{Q}]} \leq (1+\sqrt{p})^{2tg/f_A}.$$

Thus $t > n/3$. Since n is odd and divisible by t, we must have $t = n$, i.e., $d = mn$. Thus, ℓ divides

$$|\prod_{\tau \in G}(1-\nu^\tau)| = |\prod_{\tau \in G}(1-(\sqrt{p}\zeta_{mn})^\tau)| = |\prod_{\tau \in G}(\sqrt{p}-\zeta_{mn})^\tau|,$$

which divides

$$\prod_{\tau \in G}(p-\zeta_{mn}^2)^\tau = \prod_{\gamma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{mn}^2)/\mathbb{Q})} (p-(\zeta_{mn}^2)^\gamma)^{[\mathbb{Q}(\nu):\mathbb{Q}(\zeta_{mn}^2)]} = \Phi_{nc}(p)^{[\mathbb{Q}(\nu):\mathbb{Q}(\zeta_{mn}^2)]},$$

since ζ_{mn}^2 is a primitive nc-th root of unity. Thus ℓ divides $\Phi_{nc}(p)$, as desired. □

Definition 6.4. *Suppose V is a connected commutative algebraic group over a finite field K. Let $C(V,K)$ denote the smallest extension F of K such that every subgroup of $V(K)$ of prime order embeds in $F^\times$.*

In other words, $C(V,K)$ is the smallest extension F of K such that any attack on the discrete logarithm problem in $F^\times$ gives an attack on the discrete logarithm problem in all subgroups of prime order in $V(K)$.

Corollary 6.5. *Suppose A is an elementary supersingular abelian variety over $\mathbb{F}_q$, and $|A(\mathbb{F}_q)|$ has a prime divisor that does not divide $2c_{A,q}$. If $c_{A,q} \in \mathbb{Z}$, then $C(A,\mathbb{F}_q) = \mathbb{F}_{q^{c_{A,q}}}$. If $c_{A,q} \notin \mathbb{Z}$, then $C(A,\mathbb{F}_q) = \mathbb{F}_q \cdot \mathbb{F}_{q^{c_{A,q}}}$, a degree 2 extension of $\mathbb{F}_{q^{c_{A,q}}}$. In particular, if q is prime then $C(A,\mathbb{F}_q) = \mathbb{F}_{q^{c_{A,q}}}$.*

Proof. Let M denote the compositum of $\mathbb{F}_q$ and $\mathbb{F}_{q^{c_{A,q}}}$. Then $M = \mathbb{F}_{q^{c_{A,q}}}$ if and only if $c_{A,q} \in \mathbb{Z}$. By Theorem 4.6, $C(A,\mathbb{F}_q) \subseteq M$. Under our hypotheses, by Theorem 6.1 we have $\mathbb{F}_{q^{c_{A,q}}} \subseteq C(A,\mathbb{F}_q)$. Since $\mathbb{F}_q \subseteq C(A,\mathbb{F}_q)$, we have $C(A,\mathbb{F}_q) = M$. □

The following example shows that the conclusions of Theorems 6.1 and 6.3 are false if the conditions on ℓ are dropped (with $\ell = 2$).

Example 6.6. *(See §4 of* [25] *for related examples for ordinary elliptic curves.) Suppose $p = 2^t - 1 > 3$ is a Mersenne prime. Let E be any supersingular elliptic curve over $\mathbb{F}_p$. Since $p > 3$ we have $F_{E,p}(x) = x^2 + p = (x + \sqrt{-p})(x - \sqrt{-p})$, $c_{E,p} = 2$, $|E(\mathbb{F}_p)| = p + 1 = 2^t$, $F_{E,p^2}(x) = (x+p)^2$, $c_{E,p^2} = 1$, and $|E(\mathbb{F}_{p^2})| = (p+1)^2 = 2^{2t}$. Thus every subgroup of $E(\mathbb{F}_p)$ and of $E(\mathbb{F}_{p^2})$ of prime order has order 2, so embeds in $\mathbb{F}_p^\times$.*

Remark 6.7. Example 6.6 shows that $\mathbb{F}_{q^{c_{A,q}}}$ can be larger than the smallest extension F of $\mathbb{F}_p$ such that every subgroup of $A(\mathbb{F}_q)$ of prime order embeds in $F^\times$, since $F = \mathbb{F}_p$ but $\mathbb{F}_{p^{c_{E,p}}} = \mathbb{F}_{p^2} = \mathbb{F}_{(p^2)^{c_{E,p^2}}}$ in Example 6.6.

7. The possible cryptographic exponents

Next we determine exactly which security parameters can occur, for simple supersingular abelian varieties. Since cryptographic security is based on cyclic subgroups, for purposes of cryptography it suffices to consider simple abelian varieties. Let

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

Note that W_n is finite, and we have $W_1 = \{1,2\}$, $W_n = \emptyset$ if n is odd and $n > 1$,

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

$$W_8 = \{15,16,20,24,30\}, \quad W_{10} = \{11,22\}, \quad W_{12} = \{13,21,26,28,36,42\}.$$

Let k' denote the largest odd divisor of a natural number k. Throughout this section, p is prime and $q = p^n$. Define

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

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

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

so $K_1(2) = \{2, 4\}$, $K_1(3) = \{2, 6\}$, and $K_1(p) = \{2\}$ if $p > 3$.

The next result can be shown to follow from Proposition 3.3 of [54]. Recall that f_A was defined in Theorem 2.7(iii), and by Theorem 2.8(ii) is 1 or 2 if A is simple.

Proposition 7.1 ([54]). *Suppose A is a simple supersingular abelian variety of dimension g over $\mathbb{F}_q$.*

(i) *If q is a square, then $f_A = 2$ if and only if $2c_{A,q} \in X_p$.*

(ii) *If q is not a square, then $f_A = 2$ if and only if $c_{A,q} = 1$ and $g = 2$.*

Theorem 7.2 (Theorem 11 of [38]). *Suppose $g, n \in \mathbb{N}$, n is even, and p is prime. Then $c = \frac{m}{2}$ occurs as the cryptographic exponent of a simple supersingular abelian variety of dimension g over $\mathbb{F}_{p^n}$ 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 under Honda-Tate theory (see Theorem 2.7) to a simple supersingular abelian variety A over $\mathbb{F}_{p^n}$ of dimension $d = f_A \deg(G_A)/2 = f_A\varphi(m)/2$, with $c_{A,p^n} = m/2$. By Proposition 7.1(i), $d = g$ if and only if $m \in (W_g \cap X_p) \cup (W_{2g} - X_p)$. □

Theorem 7.3 (Theorem 12 of [38]). *Suppose $g, n \in \mathbb{N}$, n is odd, and p is prime. Then an integer c occurs as the cryptographic exponent of a simple supersingular abelian variety of dimension g over $\mathbb{F}_{p^n}$ if and only if $c \in K_g(p)$.*

Proof. Let $q = p^n$. If $\omega = \sqrt{q}\zeta$ is a supersingular q-Weil number, then it corresponds under Honda-Tate theory to a simple supersingular abelian variety A over $\mathbb{F}_q$ of dimension

$$d = f_A[\mathbb{Q}(\omega) : \mathbb{Q}]/2 = f_A[\mathbb{Q}(\omega) : \mathbb{Q}(\omega^2)]\varphi(c_{A,q})/2, \tag{7.1}$$

by Lemma 4.7(i,iii). Let $c = c_{A,q}$. It follows from Lemma 2.6 of [54] that $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^2)$ if and only if $c \in V_p$. It now follows from Proposition 7.1(ii) and (7.1) that $d = \varphi(c)/2$ if $c \in V_p$, and that $d = \varphi(c)$ if $c \notin V_p$ and either $g \neq 2$ or $c \neq 1$. So if $c \neq 1$, then $d = g$ if and only if $c \in (W_{2g} \cap V_p) \cup (W_g - V_p)$. If $c = 1$ and $d = 1$ then $F_A(x) = x^2 - q$, so $|A(\mathbb{F}_q)| = 1 - q < 0$, a contradiction. Thus $c = 1$ (i.e., $\omega = \pm\sqrt{q}$) if and only if $d = 2$. □

For any given g and q, it is easy to work out from Theorems 7.2 and 7.3 exactly which values can occur as cryptographic exponents $c_{A,q}$ for g-dimensional simple supersingular abelian varieties A over $\mathbb{F}_q$, and to compute the values in Table 1.

Remark 7.4. The case $g = 1$ recovers well-known results on elliptic curves. Suppose A is an elliptic curve over $\mathbb{F}_q$. If q is not a square then $c_{A,q} = 2$ if $p > 3$, if $p = 3$ then exactly 2 and 6 occur, and if $p = 2$ then exactly 2 and 4 occur. If q is a square then $c_{A,q} = m/2$ with $m \in \{1, 2, 3, 4, 6\}$, where $m = 1$ and 2 occur for all (square) q, and for $m \in \{3, 4, 6\}$, $m/2$ occurs if and only if $p \not\equiv 1 \pmod{m}$.

Corollaries 7.5–7.9 below give the results when n is even and $2 \leq g \leq 6$, while Corollary 7.10 gives the results when n is odd and $2 \leq g \leq 6$.

Corollary 7.5 (Corollary 13 of [38]). *If n is even and p is prime, then the only possible cryptographic exponents c_{A,p^n} for simple supersingular abelian surfaces A over*

$\mathbb{F}_{p^n}$ 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,p^n} 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,p^n} if and only if $p \not\equiv 1 \pmod{m}$.

Corollary 7.6. *If n is even and p is prime, then the only possible cryptographic exponents c_{A,p^n} for simple 3-dimensional supersingular abelian varieties A over $\mathbb{F}_{p^n}$ are the numbers of the form $\frac{m}{2}$ with $m \in \{7,9,14,18\}$. For $m \in \{7,14\}$, $\frac{m}{2}$ occurs as a c_{A,p^n} if and only if $p \not\equiv 1,2,4 \pmod{7}$, and for $m \in \{9,18\}$, $\frac{m}{2}$ occurs as a c_{A,p^n} if and only if $p \not\equiv 1 \pmod{3}$.*

Corollary 7.7 (Corollary 13 of [38])**.** *If n is even and p is prime, then the only possible cryptographic exponents c_{A,p^n} for simple 4-dimensional supersingular abelian varieties A over $\mathbb{F}_{p^n}$ are the numbers of the form $\frac{m}{2}$ with*

$$m \in \{5,8,10,12,15,16,20,24,30\}.$$

For $m \in \{5,8,10,12\}$, $\frac{m}{2}$ occurs as a c_{A,p^n} if and only if $p \equiv 1 \pmod{m}$, and for $m \in \{15,16,20,24,30\}$, $\frac{m}{2}$ occurs as a c_{A,p^n} if and only if $p \not\equiv 1 \pmod{m}$.

Corollary 7.8. *If n is even and p is prime, then the only possible cryptographic exponents c_{A,p^n} for simple 5-dimensional supersingular abelian varieties A over $\mathbb{F}_{p^n}$ are 5.5 and 11. For $m \in \{11,22\}$, $\frac{m}{2}$ occurs if and only if $p \not\equiv 1,3,4,5,9 \pmod{11}$.*

Corollary 7.9. *If n is even and p is prime, then the only possible cryptographic exponents c_{A,p^n} for simple 6-dimensional supersingular abelian varieties A over $\mathbb{F}_{p^n}$ are the numbers of the form $\frac{m}{2}$ with $m \in \{7,9,13,14,18,21,26,28,36,42\}$. For $m \in \{7,14\}$, $\frac{m}{2}$ occurs as a c_{A,p^n} if and only if $p \equiv 1,2,4 \pmod{7}$. For $m \in \{9,18\}$, $\frac{m}{2}$ occurs if and only if $p \equiv 1 \pmod{3}$. For $m \in \{13,26\}$, $\frac{m}{2}$ occurs if and only if $p \not\equiv 1,3,9 \pmod{13}$. For $m \in \{21,42\}$, $\frac{m}{2}$ occurs if and only if $p \not\equiv 1,4,16 \pmod{21}$. The value 14 occurs as a c_{A,p^n} if and only if $p \not\equiv 1,9,25 \pmod{28}$, and 18 occurs if and only if $p \not\equiv 1,13,25 \pmod{36}$.*

The following result was given in Corollary 14 of [38] when $2 \le g \le 5$.

Corollary 7.10. *If n is odd and p is prime, then the exact sets of cryptographic exponents c_{A,p^n} that occur for simple supersingular abelian varieties A of dimension g over $\mathbb{F}_{p^n}$ with $2 \le g \le 6$ are given below.*

(i) *Suppose $g = 2$.*
- (a) $c_{A,p^n} \in \{1,3,4,6\}$ *if $p \ge 7$;*
- (b) $c_{A,p^n} \in \{1,3,4,5,6\}$ *if $p = 5$;*
- (c) $c_{A,p^n} \in \{1,3,4\}$ *if $p = 3$;*
- (d) $c_{A,p^n} \in \{1,3,6,12\}$ *if $p = 2$.*

(ii) *Suppose $g = 3$.*
- (a) *There does not exist such an A if $p \neq 3,7$;*
- (b) $c_{A,p^n} = 14$ *if $p = 7$;*
- (c) $c_{A,p^n} = 18$ *if $p = 3$.*

(iii) *Suppose $g = 4$.*
- (a) $c_{A,p^n} \in \{5,8,10,12\}$ *if $p \ge 7$;*
- (b) $c_{A,p^n} \in \{8,10,12,15\}$ *if $p = 5$;*
- (c) $c_{A,p^n} \in \{5,8,10,12,30\}$ *if $p = 3$;*
- (d) $c_{A,p^n} \in \{5,8,10,20\}$ *if $p = 2$.*

(iv) *Suppose $g = 5$.*
- (a) *There does not exist such an A if $p \neq 11$;*
- (b) $c_{A,p^n} = 22$ *if $p = 11$.*

(v) *Suppose* $g = 6$.

(a) $c_{A,p^n} \in \{7, 9, 14, 18\}$ *if* $p = 5$ *or* $p = 11$ *or* $p \geq 17$*;*

(b) $c_{A,p^n} \in \{7, 9, 13, 14, 18\}$ *if* $p = 13$*;*

(c) $c_{A,p^n} \in \{7, 9, 18, 42\}$ *if* $p = 7$*;*

(d) $c_{A,p^n} \in \{7, 9, 14, 42\}$ *if* $p = 3$*;*

(e) $c_{A,p^n} \in \{7, 9, 14, 18, 28, 36\}$ *if* $p = 2$.

Corollary 7.11 (Corollary 15 of [38]). *Suppose* $n, g \in \mathbb{N}$*,* n *and* g *are odd,* $g > 1$*, and* p *is a prime.*

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

(ii) *If* $p \equiv 3 \pmod 4$*, and there exists a simple supersingular abelian variety of dimension* g *over* $\mathbb{F}_{p^n}$*, 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 $\mathbb{F}_{p^n}$. Since $g > 1$ is odd, we conclude from Theorem 7.3 that $\varphi(c_{A,p^n}) = 2g \equiv 2 \pmod 4$ and $p \mid c_{A,p^n}$. This is only possible if $c_{A,p^n} = p^b$ or $2p^b$, and $p \equiv 3 \pmod 4$. □

Our results show that when the dimension g is 6 then 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 4, the highest security parameter is $30/4 = 7.5$, and this is attained if and only if $p = 3$ and q is not a square. This surpasses the elliptic curve case, where the highest security parameter is 6. In fact, Corollaries 7.7 and 7.10(iii) show that dimension 4 surpasses dimension 1 over every finite field.

Over every finite field of non-square order and characteristic $\neq 3$, supersingular abelian surfaces surpass supersingular elliptic curves.

In dimensions 2 and 3 the highest security parameter is 6, which ties the elliptic curve case. The supersingular abelian surfaces with security parameter 6 are in characteristic 2, while supersingular elliptic curves with security parameter 6 occur only in characteristic 3; there may be efficiency advantages in using abelian surfaces over binary fields, rather than elliptic curves over ternary fields.

8. Primitive subgroups

In this section, L/K is a cyclic extension of degree r and V is a connected commutative algebraic group over K. In this paper we are interested in the case where V is an abelian variety (usually an elliptic curve) over a finite field. In [39, 41] we consider the case where V is the multiplicative group $\mathbb{G}_m$.

The **Weil restriction of scalars** $\mathrm{Res}_{L/K}V$ is a commutative algebraic group over K of dimension $r \dim(V)$ such that

$$(\mathrm{Res}_{L/K}V)(K) \cong V(L). \tag{8.1}$$

See for example §1.3 of [52] for the definition and properties of the Weil restriction of scalars. For now, write V's group operation multiplicatively.

Definition 8.1. *Define the* **primitive subgroup** $V_{L/K}$ *of* $\mathrm{Res}_{L/K}V$ *to be*

$$V_{L/K} := \ker\Big[\mathrm{Res}_{L/K}V \xrightarrow{\oplus \mathrm{N}_{L/F}} \bigoplus_{K \subseteq F \subsetneq L} \mathrm{Res}_{F/K}V\Big],$$

where $\mathrm{N}_{L/F} : \mathrm{Res}_{L/K}V \to \mathrm{Res}_{F/K}V$ *is the natural map that induces the usual norm maps*

$$\mathrm{N}_{L/F} : V(L) \to V(F), \qquad x \mapsto \prod_{\sigma\in\mathrm{Gal}(L/F)} \sigma(x).$$

Notation 8.2. When $K = \mathbb{F}_q$, write V_r (or $V_{r,q}$ if necessary) for $V_{\mathbb{F}_{q^r}/\mathbb{F}_q}$.

This is the meaning of the notation E_r and $\mathcal{E}_r$, including E_3 and E_5, that we use below.

The variety $V_{L/K}$ is the variety V_L of [32] and $\mathrm{N}_{L/F}$ is the map $R_{L/F,V}$ of Remark 5.11 of [32]. The primitive subgroup $V_{L/K}$ is a commutative algebraic group over K of dimension $\varphi(r)\dim V$, and $V_{L/K}(K)$ consists of all elements of $V(L)$ whose norm down to $V(F)$ is the identity, for every intermediate field $k \subseteq F \subsetneq L$ (see Theorems 5.5 and 5.8 of [32]). Note that $V_{K/K} = V$. There is an isogeny defined over K (see [13] or Theorem 5.2 of [32]):

$$\mathrm{Res}_{L/K}V \quad \sim \bigoplus_{K\subseteq F\subseteq L} V_{F/K} = V \times \cdots \times V_{L/K}. \tag{8.2}$$

By (8.2) and (8.1), studying $V(L)$ can be reduced to studying $V_{F/K}(K)$ for all intermediate fields F.

Now suppose $\mathcal{E}$ is an abelian variety over K with identity $O_{\mathcal{E}}$, and write the group law additively as usual. Then the norm maps above are called trace maps. We have $\mathrm{Tr}_{L/K}(Q) = \sum_{\sigma\in\mathrm{Gal}(L/K)} \sigma(Q)$, and

$$\mathcal{E}_{L/K}(K) \cong \{Q \in \mathcal{E}(L) : \mathrm{Tr}_{L/F}(Q) = O_{\mathcal{E}} \quad \text{for every } k \subseteq F \subsetneq L\}. \tag{8.3}$$

If r is prime, then

$$\mathcal{E}_{L/K}(K) \cong \{Q \in \mathcal{E}(L) : \mathrm{Tr}_{L/K}(Q) = O_{\mathcal{E}}\} \tag{8.4}$$

and is the trace zero subgroup of $\mathcal{E}(L)$ (see also §3.2 of [18] and [30]). When E is an elliptic curve, E_r was studied in [37, 53].

9. Boosting the security parameter

In this section we use primitive subgroups to boost the security parameter of supersingular elliptic curves or, more generally, supersingular abelian varieties, by a factor of $r/\varphi(r)$. It follows from Theorem 9.2 that if $\mathcal{E}$ is an elementary supersingular abelian variety over $\mathbb{F}_q$, $\gcd(r, 4qc_{\mathcal{E},q}) = 1$, and the primitive subgroup $\mathcal{E}_r(\mathbb{F}_q) \subseteq \mathcal{E}(\mathbb{F}_{q^r})$ has a point of prime order $\ell \nmid 2c_{\mathcal{E},q}$, then $\mathcal{E}_r(\mathbb{F}_q)$ is as cryptographically secure as $\mathcal{E}(\mathbb{F}_{q^r})$ against the known subexponential attacks on the discrete logarithm problem in $(\mathbb{F}_q \cdot \mathbb{F}_{q^{rc_{\mathcal{E},q}}})^\times$.

Recall the notation f_A and G_A from Theorem 2.7(iii) (so $f_A = 1$ exactly when the characteristic polynomial of Frobenius is irreducible). Theorem 9.1 and Corollary 9.4 below are variations on Theorems 24 and 17 of [38], respectively.

Theorem 9.1 (Theorem 5.9 of [32])**.** *Suppose $r \in \mathbb{N}$, $\mathcal{Z}$ is the set of primitive r-th roots of unity, $\mathcal{E}$ is an abelian variety over $\mathbb{F}_q$, and $F_{\mathcal{E}}(x) = \prod_{i=1}^{2g}(x - \eta_i)$ with $\eta_i \in \bar{\mathbb{Q}}$. Then $\mathcal{E}_r$ is an abelian variety over $\mathbb{F}_q$, and $F_{\mathcal{E}_r}(x) = \prod_{\zeta\in\mathcal{Z}}\prod_{i=1}^{2g}(x - \eta_i\zeta)$.*

Theorem 9.2. *Suppose $\mathcal{E}$ is an elementary supersingular abelian variety over $\mathbb{F}_q$. Fix $r \in \mathbb{N}$ such that $\gcd(r, 2qc_{\mathcal{E},q}) = 1$. Then:*

(i) *$\mathcal{E}_r$ is an elementary supersingular abelian variety over $\mathbb{F}_q$ of dimension $\varphi(r)\dim(\mathcal{E})$;*

(ii) *writing $G_{\mathcal{E}}(x) = \prod_{i=1}^{s}(x - \eta_i)$, letting $\mathcal{Z}$ denote the set of primitive r-th roots of unity, and letting $H_r(x) := \prod_{\zeta \in \mathcal{Z}} \prod_{i=1}^{s}(x - \eta_i\zeta)$, then $G_{\mathcal{E}_r}(x) = H_r(x)$ and $F_{\mathcal{E}_r}(x) = H_r(x)^{f_{\mathcal{E}}}$;*

(iii) $c_{\mathcal{E}_r,q} = rc_{\mathcal{E},q}$*;*

(iv) $\alpha(\mathcal{E}_r, q) = \frac{r}{\varphi(r)}\alpha(\mathcal{E}, q)$*;*

(v) *if $f_{\mathcal{E}} = 1$, then $\mathcal{E}_r$ is simple over $\mathbb{F}_q$;*

(vi) *If $r \neq 2$, and $\mathcal{E}_r(\mathbb{F}_q)$ has a point of prime order $\ell \nmid 2c_{\mathcal{E},q}$, then $C(\mathcal{E}_r, \mathbb{F}_q) = C(\mathcal{E}, \mathbb{F}_{q^r})$.*

Proof. By Theorem 5.5 of [32], $\mathcal{E}_r$ is isomorphic over $\mathbb{F}_{q^r}$ to $\mathcal{E}^{\varphi(r)}$, so is a supersingular abelian variety of dimension $\varphi(r)\dim(\mathcal{E})$. We have $F_{\mathcal{E}}(x) = G_{\mathcal{E}}(x)^{f_{\mathcal{E}}}$. By Theorem 9.1, $F_{\mathcal{E}_r}(x) = H_r(x)^{f_{\mathcal{E}}}$. The splitting field K_G of $G_{\mathcal{E}}$ over $\mathbb{Q}$ is unramified outside $2qc_{\mathcal{E},q}$, while $\mathbb{Q}(\zeta_r)$ is unramified outside r. Since $\gcd(r, 2qc_{\mathcal{E},q}) = 1$, it follows that K_G and $\mathbb{Q}(\zeta_r)$ are disjoint over $\mathbb{Q}$. Since $\mathrm{Gal}(K_G/\mathbb{Q})$ acts transitively on the roots of the irreducible polynomial $G_{\mathcal{E}}$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$ acts transitively on $\mathcal{Z}$, it follows that $\mathrm{Gal}(K_G(\zeta_r)/\mathbb{Q})$ acts transitively on the roots of H_r. Thus $H_r(x)$ is irreducible over $\mathbb{Q}$, so $G_{\mathcal{E}_r}(x) = H_r(x)$, giving (ii). By Theorem 2.7(iii), $\mathcal{E}_r$ is elementary over $\mathbb{F}_q$, and we have (i). Definitions 4.1 and 4.5 give (iii,iv). If $f_{\mathcal{E}} = 1$, then $F_{\mathcal{E}_r}$ is irreducible over $\mathbb{Q}$, so $\mathcal{E}_r$ is simple over $\mathbb{F}_q$, giving (v).

By Lemma 4.4 we have $c_{\mathcal{E},q} = c_{\mathcal{E},q^r}$, so by (iii) we have $c_{\mathcal{E}_r,q} = rc_{\mathcal{E},q} = rc_{\mathcal{E},q^r}$. By Corollary 6.5, if $\mathcal{E}_r(\mathbb{F}_q)$ has a point of prime order $\ell \nmid 2c_{\mathcal{E},q}$, then $C(\mathcal{E}, \mathbb{F}_{q^r})$ is $\mathbb{F}_{q^{rc_{\mathcal{E},q}}} = \mathbb{F}_{q^{c_{\mathcal{E}_r,q}}}$ if $c_{\mathcal{E},q^r}$ $(= c_{\mathcal{E},q}) \in \mathbb{Z}$ and is $\mathbb{F}_{q^{2c_{\mathcal{E}_r,q}}}$ otherwise, while $C(\mathcal{E}_r, \mathbb{F}_q)$ is $\mathbb{F}_{q^{c_{\mathcal{E}_r,q}}}$ if $c_{\mathcal{E}_r,q} \in \mathbb{Z}$ and is $\mathbb{F}_{q^{2c_{\mathcal{E}_r,q}}}$ otherwise. If $r \neq 2$, then $c_{\mathcal{E},q} \in \mathbb{Z}$ if and only if $c_{\mathcal{E}_r,q} \in \mathbb{Z}$ by (iii). Now (vi) follows. □

Remark 9.3. If E is a supersingular elliptic curve over $\mathbb{F}_q$, then $f_E \neq 1$ if and only if $f_E = 2$, q is a square, and $G_E(x) = x + \sqrt{q}$ or $x - \sqrt{q}$, in which case $c_{E,q} = 1/2$ or 1, so the embedding degree is 1.

Corollary 9.4. *Suppose E is a supersingular elliptic curve over $\mathbb{F}_q$. Fix a prime number r that does not divide $2pc_{E,q}$, where $p = \mathrm{char}(\mathbb{F}_q)$. Then:*

(i) *E_r is an elementary supersingular abelian variety over $\mathbb{F}_q$ of dimension $r - 1$, and $E_r(\mathbb{F}_q)$ is the trace zero subgroup of $E(\mathbb{F}_{q^r})$;*

(ii) $\mathrm{Res}_{\mathbb{F}_{q^r}/\mathbb{F}_q}E$ *is isogenous over $\mathbb{F}_q$ to $E \times E_r$;*

(iii) $c_{E_r,q} = rc_{E,q}$*;*

(iv) $\alpha(E_r, q) = \frac{r}{r-1}\alpha(E, q)$*;*

(v) *E_r is simple over $\mathbb{F}_q$, except when all the following hold:*
   (a) *q is a square,*
   (b) $G_E(x) = x \pm \sqrt{q}$*,*
   (c) *p has even order in $(\mathbb{Z}/r\mathbb{Z})^{\times}$.*

   When (a), (b), and (c) hold, then $c_{E,q} = \frac{1}{2}$ or 1, and E_r is isogenous over $\mathbb{F}_q$ to A^2 where A is a simple abelian variety over $\mathbb{F}_q$ and $\alpha(A, q) = \frac{2c_{E,q}r}{r-1} \in \{\frac{r}{r-1}, \frac{2r}{r-1}\}$.

Proof. Parts (i–iv) follow from Theorem 9.2, (8.2), and (8.4). For (v), by Theorem 9.2(v) it suffices to consider the case $f_E \neq 1$ (and $r > 2$). By Remark 9.3 and Theorem 9.1, $f_E = 2$, q is a square, and $G_{E_r}(x) = \prod(x + \zeta_r^j\sqrt{q})$ or $\prod(x - \zeta_r^j\sqrt{q})$, products with j running over $(\mathbb{Z}/r\mathbb{Z})^{\times}$. By Theorem 2.7, there is a simple supersingular abelian variety A such that $G_{E_r}(x) = G_A(x)$. By Proposition 3.3 of [54] and our assumptions, $f_A = 2$ if and only if p has odd order in $(\mathbb{Z}/r\mathbb{Z})^{\times}$ (and $f_A = 1$

otherwise). If $f_A = 1$, then $F_{E_r} = G_{E_r}^2 = F_{A^2}$, so E_r is isogenous over $\mathbb{F}_q$ to A^2 by Theorem 2.6. If $f_A = 2$, then $F_{E_r} = F_A$, so by Theorem 2.6, E_r is simple over $\mathbb{F}_q$. □

10. A method of compression and decompression

We present a method for compressing and decompressing points in trace zero subgroups of elliptic curves (which was given in [38], with additional details in [46, 40]). Note that the methods of this section hold for general elliptic curves, without the restriction that the curves be supersingular. Our compression/decompression algorithm is practical when $r = 3$ or 5. A compression/decompression algorithm was given in §3.3 of [37] in the case where $r = 3$ and $q = p$ is a prime congruent to 4 or 7 $\pmod 9$ (an English translation was given on p. 18 of [53]); we thank a referee for pointing this out to us.

10.1. **The general method; r odd.** Suppose

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{10.1}$$

is an elliptic curve over a finite field $\mathbb{F}_q$ and r is an odd positive integer. Let

$$A_0 = \{Q \in E(\mathbb{F}_{q^r}) : \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(Q) = O_E\},$$

the trace zero subgroup of $E(\mathbb{F}_{q^r})$. When r is prime, then A_0 is the primitive subgroup E_r defined in Definition 8.1.

Write $\mathbb{F}_{q^r} = \mathbb{F}_q[z]/f(z)\mathbb{F}_q[z]$ with $f(z) \in \mathbb{F}_q[z]$ irreducible and of degree r.

Compression Algorithm: The input is a point $P = (s, t) \in A_0 - O$. The output is an element of $\mathbb{F}_q^{r-1}$ that is a compression of P.

(i) Write $s = \sum_{i=0}^{r-1} s_i z^i$ with the $s_i \in \mathbb{F}_q$, i.e., write s with respect to the basis $\{1, z, \ldots, z^{r-1}\}$ for $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$.

(ii) Output $(s_1, \ldots, s_{r-1}) \in \mathbb{F}_q^{r-1}$ i.e., drop t and the first coordinate s_0 of s.

Decompression Algorithm: The input is $(s_1, \ldots, s_{r-1}) \in \mathbb{F}_q^{r-1}$. The output is a point $P = (s, t) \in E(\mathbb{F}_{q^r})$ such that $s = \sum_{i=0}^{r-1} s_i z^i$ for some $s_0 \in \mathbb{F}_q$.

(i) Compute the (monic) characteristic polynomial $Q(X)$ of the linear transformation on $\mathbb{F}_{q^r}$ given by multiplication by $\sum_{i=1}^{r-1} s_i z^i$.

(ii) With the $Q(X)$ computed in (i), set

$$\begin{aligned} Q(X - S) = {}& \big(X^{(r-3)/2} + \sum_{i=0}^{(r-5)/2} \beta_i X^i\big)^2 (X^3 + a_2X^2 + a_4X + a_6) \\ & + \big(X^{(r-3)/2} + \sum_{i=0}^{(r-5)/2} \beta_i X^i\big)\big(\sum_{i=0}^{(r-1)/2} \alpha_i X^i\big)(a_1X + a_3) - \big(\sum_{i=0}^{(r-1)/2} \alpha_i X^i\big)^2, \end{aligned} \tag{10.2}$$

with r unknowns $S, \alpha_0, \ldots, \alpha_{(r-1)/2}, \beta_0, \ldots, \beta_{(r-5)/2}$. Then equate coefficients of like powers of X in (10.2) to obtain r equations in the r unknowns, and solve that system of equations. The finite set of solutions for S includes s_0. We thus obtain a finite list of candidates for s.

(iii) Use (10.1) to solve for t (discarding any candidate s_0's that do not produce a $t \in \mathbb{F}_q$).

The compression algorithm is clearly efficient, since it just consists of dropping t and one coordinate of s. We found a way to make decompression practical when $r = 3$ or 5, the two cases most relevant for cryptographic applications. We demonstrate this in §§10.3–10.5 below.

To be sure of recovering P, rather than a different point in $E(\mathbb{F}_{q^r})$, the compressor can augment the compressed point $(s_1, \ldots, s_{r-1})$ by some extra bits that allow the decompressor to determine which solution of the system of equations to choose to obtain s_0 (and which of two possibilities to choose for t). However, this makes compression less efficient, since the compressor must determine all the solutions of the system.

10.2. **Explanation of the method.** We now explain where equation (10.2) comes from. Let X and Y denote the coordinate functions on the elliptic curve E. Since $\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(P) = O_E$, there is a function $\mathcal{F}(X,Y)$ on E with simple zeros at the points $\sigma^i(P)$ for $0 \le i \le r-1$, a pole of order r at O_E, and no other zeros or poles. Writing $P = (s,t)$, then the function $g(X) := Q(X - s_0) = \prod_{i=0}^{r-1}(X - \sigma^i(s))$, where σ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, can be viewed as a function on E with zeros at $\pm\sigma^i(P)$ for $0 \le i \le r-1$, a pole of order $2r$ at O_E, and no other zeros or poles. Thus

$$g(X) = \gamma \mathcal{F}(X,Y)\tilde{\mathcal{F}}(X,Y), \tag{10.3}$$

where $\tilde{\mathcal{F}}$ is $\mathcal{F}$ composed with multiplication by -1 on E, and $\gamma \in \mathbb{F}_q^\times$. We can write

$$\mathcal{F}(X,Y) = h_1(X) + h_2(X)Y$$

with $h_1(X), h_2(X) \in \mathbb{F}_q[X]$. We have $-(x,y) = (x, -y - a_1x - a_3)$ in E, so

$$\tilde{\mathcal{F}}(X,Y) = h_1(X) - h_2(X)(Y + a_1X + a_3)$$

and

$$\begin{aligned}(10.4)\quad \mathcal{F}(X,Y)\tilde{\mathcal{F}}(X,Y) &= \\ h_1(X)^2 - h_1(X)h_2(X)(a_1X + a_3) &- h_2(X)^2(X^3 + a_2X^2 + a_4X + a_6).\end{aligned}$$

Since X has a double pole at O_E and Y has a triple pole at O_E, it follows that $\deg(h_2) = (r-3)/2$ and $\deg(h_1) \le (r-1)/2$. (Note that this is all valid when $r = 2$, with $h_2(X) = 0$ and $h_1(X) = X - s$; see §10.5 when r is twice an odd number.) Write

$$h_1(X) = \sum_{i=0}^{(r-1)/2} \alpha_i X^i, \quad h_2(X) = X^{(r-3)/2} + \sum_{i=0}^{(r-5)/2} \beta_i X^i \tag{10.5}$$

with the α_i's and β_i's in $\mathbb{F}_q$. Now combine (10.3), (10.4), and (10.5) (and note that γ must be -1), to obtain (10.2).

10.3. **The case** $r = 3$**.** Suppose $r = 3$ and the characteristic of $\mathbb{F}_q$ is not 3. We give an efficient decompression algorithm. Under our assumptions, we can take $a_2 = 0$ in (10.1), and can take the irreducible polynomial defining the degree 3 extension $\mathbb{F}_{q^3}$ to be of the form $f(z) = z^3 + r_1z + r_0$ with $r_i \in \mathbb{F}_q$. Then the characteristic polynomial of multiplication by $s_1z + s_2z^2$ is

$$Q(X) = X^3 + 2s_2r_1X^2 + (3s_1s_2r_0 + s_1^2r_1 + s_2^2r_1^2)X + s_1^3r_0 - s_2^3r_0^2 + s_1s_2^2r_0r_1.$$

The difference of the two sides of (10.2) is now

$$
\begin{aligned}
(10.6)\quad & (3S - \alpha_1^2 + a_1\alpha_1 - 2s_2r_1)X^2 \\
&\quad + (\alpha_0(a_1 - 2\alpha_1) + a_3\alpha_1 + 3S^2 - 3s_1s_2r_0 - s_1^2r_1 + 4Ss_2r_1 - s_2^2r_1^2 + a_4)X \\
&\quad\quad + a_6 + S^3 + a_3\alpha_0 - \alpha_0^2 - s_1^3r_0 + 3Ss_1s_2r_0 \\
&\quad\quad\quad + s_2^3r_0^2 + Ss_1^2r_1 - 2S^2s_2r_1 - s_1s_2^2r_0r_1 + Ss_2^2r_1^2.
\end{aligned}
$$

Setting the coefficient of the quadratic term of (10.6) equal to 0 and solving for S gives

$$S = (\alpha_1^2 - a_1\alpha_1 + 2s_2r_1)/3.$$

Substituting into (10.6), setting the coefficient of the linear term equal to 0, and solving for α_0 gives

$$\alpha_0 = (3(a_4 + a_3\alpha_1 - 3s_1s_2r_0 - s_1^2r_1) - a_1^2\alpha_1^2 + 2a_1\alpha_1^3 - \alpha_1^4 + s_2^2r_1^2)/(3(2\alpha_1 - a_1)).$$

Substituting into (10.6) and setting the constant term equal to 0 gives a degree 8 polynomial in $\mathbb{F}_q[\alpha_1]$, which can be rewritten as $m(\alpha_1^2 - a_1\alpha_1)$ with

$$
\begin{aligned}
m(w) = {} & w^4 + a_1^2w^3 + 3(3(a_1a_3 + 2a_4 + 6s_1s_2r_0 + 2s_1^2r_1) - 2s_2^2r_1^2)w^2 \\
& + (27(a_3^2 + a_1^2s_1s_2r_0 + 4(a_6 - s_1^3r_0 + s_2^3r_0^2 + s_1s_2^2r_0r_1)) \\
& \quad + 3r_1(3a_1^2s_1^2 + 24s_1^2s_2r_1 - a_1^2s_2^2r_1) + 8s_2^3r_1^3)w \\
& + 27(a_1^2a_6 - a_1a_3a_4 - a_4^2 - a_1^2s_1^3r_0 + a_1^2s_2^3r_0^2 + a_1a_3s_1^2r_1 + a_1^2s_1s_2^2r_0r_1 - s_1^4r_1^2 \\
& + 2a_4s_1^2r_1 + 3a_1a_3s_1s_2r_0 + 6a_4s_1s_2r_0 - 9s_1^2s_2^2r_0^2 - 6s_1^3s_2r_0r_1 + 2s_1s_2^3r_0r_1^2) \\
& \quad + 18(a_1^2s_1^2s_2r_1^2 - a_4s_2^2r_1^2 + s_1^2s_2^2r_1^3) + 2a_1^2s_2^3r_1^3 - 9a_1a_3s_2^2r_1^2 - 3s_2^4r_1^4.
\end{aligned}
$$

Compute the roots of the polynomial $m(w)$. Let $s_0 = S = (R + 2s_2r_1)/3$, where R is a root of $m(w)$.

The compressor can transmit three extra bits so that the decompressor can determine the decompressed point with no ambiguity (two to determine which root of the degree 4 polynomial m to choose, and one to determine t).

10.3.1. *$r = 3$, characteristic 2.* When $r = 3$ and $q = 2^n$ with n not divisible by 3, we may take $r_0 = r_1 = 1$. If further $a_1 = 0$ in (10.1), then decompression becomes easier if the compression algorithm drops s_1 or s_2, rather than s_0. In that case, setting the coefficient of the quadratic term of (10.6) equal to 0 yields the equation $s_0 = \alpha_1^2$. Solving for α_1 amounts to taking a square root. Using the linear term of (10.6) one obtains

$$s_1^2 + s_1s_2 + s_2^2 + s_0^2 + a_3\alpha_1 + a_4 = 0,$$

a quadratic polynomial in s_1 (or s_2). So the decompression algorithm reduces to taking one square root in $\mathbb{F}_{2^n}$ and solving one quadratic polynomial over $\mathbb{F}_{2^n}$. Taking square roots in a field of characteristic 2 is just a single exponentiation, and solving a quadratic equation is not much harder.

10.3.2. *$r = 3$, characteristic ≥ 5.* When the characteristic of $\mathbb{F}_q$ is at least 5, we may take a model for E with $a_1 = a_2 = a_3 = 0$. Then $S = (R + 2s_2r_1)/3$, where R

satisfies

$$\begin{aligned}&R^4 + R^2(18a_4 + 54s_1s_2r_0 + 18s_1^2r_1 - 6s_2^2r_1^2)\\&\qquad + R(108(a_6 - s_1^3r_0 + s_2^3r_0^2 + s_1s_2^2r_0r_1) + 8(9s_1^2s_2r_1^2 + s_2^3r_1^3))\\&\quad + 27(2s_1s_2^3r_0r_1^2 - a_4^2 + 6a_4s_1s_2r_0 - 9s_1^2s_2^2r_0^2 + 2a_4s_1^2r_1 - 6s_1^3s_2r_0r_1 - s_1^4r_1^2)\\&\qquad\qquad + 18s_2^2(s_1^2r_1^3 - a_4r_1^2) - 3s_2^4r_1^4 = 0.\end{aligned}$$

If $q \equiv 1 \pmod 3$, we can take $r_1 = 0$, and then R is a root of

$$R^4+(18a_4+54s_1s_2r_0)R^2+108(a_6-s_1^3r_0+s_2^3r_0^2)R+27(6a_4s_1s_2r_0-9s_1^2s_2^2r_0^2-a_4^2).$$

When $a_1 = a_2 = a_3 = 0$, an equation for E_3 in $\mathbb{A}^3$ over $\mathbb{F}_q(\mu)$ where μ is a primitive cube root of unity was given in [17], (4.16) of [37], §3.2 of [18], and §2.4.1 of [12], namely

$$(3x_0^2 + 3\mu x_1x_2 + a_4)^2 = 12x_0(x_0^3 + \mu x_1^3 + \mu^2x_2^3 + a_4x_0 + a_6).$$

Naumann [37, 53] gave a compression/decompression algorithm in the case where $r = 3$ and $q = p$ is an odd prime congruent to 4 or 7 $\pmod 9$.

10.4. $r = 5$**, characteristic** 3**.** Let $q = 3^n$ with $\gcd(n, 30) = 1$. We will make the decompression algorithm efficient for the elliptic curve $y^2 = x^3 - x - 1$ over $\mathbb{F}_q$. (A similar computation can be done for $y^2 = x^3 - x + 1$. Both these curves have security parameter 6, which is maximal among all supersingular elliptic curves over all finite fields.)

Write $\mathbb{F}_{q^5} = \mathbb{F}_q[z]/f(z)\mathbb{F}_q[z]$ with $f(z) = z^5 - z + 1$. Define $b_0, \cdots, b_4 \in \mathbb{F}_q[S]$ by $Q(X - S) = X^5 + \sum_{i=0}^4 b_iX^i$ where

$$Q(X) = X^5 - s_4X^4 + (s_2^2 - s_1s_3 - s_2s_3 - s_1s_4)X^3 + \cdots$$

is the characteristic polynomial of multiplication by $\sum_{i=1}^4 s_iz^i$ on $\mathbb{F}_{q^5}$. Write

$$X^5 + \sum_{i=0}^4 b_iX^i = (X + \beta_0)^2(X^3 - X - 1) - (\alpha_2X^2 + \alpha_1X + \alpha_0)^2.$$

Taking the difference of the two sides gives

$$\begin{aligned}&(\alpha_2^2 + \beta_0 + b_4)X^4 + (1 - \alpha_1\alpha_2 - \beta_0^2 + b_3)X^3\\&\qquad + (\alpha_1^2 - \alpha_0\alpha_2 - \beta_0 + b_2 + 1)X^2 + (\beta_0^2 - \beta_0 - \alpha_0\alpha_1 + b_1)X + \alpha_0^2 + \beta_0^2 + b_0.\end{aligned}$$

Setting the coefficient of the degree four term equal to 0 and solving for β_0 gives

$$\beta_0 = -\alpha_2^2 - b_4.$$

Setting the coefficient of the cubic term equal to 0 and solving for α_1 gives

$$\alpha_1 = (1 - \alpha_2^4 + \alpha_2^2b_4 - b_4^2 + b_3)/\alpha_2.$$

Setting the coefficient of the quadratic term equal to 0 and solving for α_0 gives

$$\alpha_0 = \frac{\alpha_2^8 + \alpha_2^6b_4 + b_4^4 + b_4^2(1 + b_3) + (1 + b_3)^2 + \alpha_2^4(b_3 - 1) + \alpha_2^2(1 + b_4^3 - b_4b_3 + b_2)}{\alpha_2^3}.$$

Setting the constant (respectively, coefficient of the linear) term equal to 0 gives polynomials in α_2^2, so replace α_2^2 with a new variable, w. The resulting equations are, respectively, $p_1(w) = 0$ and $p_2(w) = 0$ where

$$\begin{aligned}
p_1(w) = {} & w^8 - b_4 w^7 + (1 + b_4^2 - b_3)w^6 + (b_4 - b_4^3 - b_2)w^5 + (b_4 - b_4^2 + b_4^4 - b_3 - b_4 b_2)w^4 \\
& + (1 - b_4 + b_4^2 - b_4^5 - b_3 + b_4^3 b_3 + b_2 - b_3 b_2 + b_0)w^3 \\
& + (-1 + b_4^2 - b_4^3 + b_4^4 + b_4^6 + b_3 + b_4 b_3 - b_3^2 - b_3^3 - b_2 - b_4^3 b_2 + b_4 b_3 b_2 + b_2^2)w^2 \\
& + (-1 - b_4^2 - b_4^3 - b_4^4 - b_4^5 - b_4^7 + b_3 + b_4 b_3 - b_4^2 b_3 - b_4^3 b_3 - b_3^2 \\
& - b_4 b_3^2 + b_4 b_3^3 - b_2 - b_4^2 b_2 - b_4^4 b_2 + b_3 b_2 - b_4^2 b_3 b_2 - b_3^2 b_2)w \\
& + 1 - b_4^2 - b_4^6 + b_4^8 + b_3 - b_4^6 b_3 + b_3^3 - b_4^2 b_3^3 + b_3^4, \\
p_2(w) = {} & w^6 - w^4 + (-1 - b_4 - b_4^3 + b_2)w^3 + (-1 + b_4^2 - b_3 - b_4 b_2 + b_1)w^2 \\
& + (-1 - b_4 + b_4^2 + b_4^3 - b_3 - b_4 b_3 - b_2 + b_4^2 b_2 - b_3 b_2)w - 1 + b_4^6 - b_3^3.
\end{aligned}$$

Taking the resultant of p_1 and p_2 eliminates the variable w, and gives a (degree 27) polynomial $h(S) \in \mathbb{F}_q[S]$ that has s_0 as a root. The polynomial $h(S)$ is of the form $H(S^3 - S)$ for a certain degree 9 polynomial $H(S) \in \mathbb{F}_q[S]$ (this follows from the fact that $(x, y) \mapsto (x + 1, y)$ is an automorphism of $y^2 = x^3 - x - 1$, of order 3), and this simplifies finding the roots of h. Transmitting 6 extra bits allows one to recover s_0 and t exactly, with no ambiguity; 5 bits determine which root to choose (of at most 27), and one bit determines the sign of the y-coordinate t.

Remark 10.1. One could express p_1 and p_2 as polynomials in w and the b_i's (or s_i's), and compute the resultant with the b_i's (or s_i's) viewed as variables. The computation of the resultant would need to be done only once, but the resultant polynomial computed this way is so large that evaluating it each time on particular b_i's or s_i's takes longer than computing the resultant anew each time with particular values for the b_i's or s_i's.

10.4.1. *An explicit example.* Consider the case $E : y^2 = x^3 - x - 1$, $q = 3^{19}$, and $r = 5$. Then $\mathbb{F}_q = \mathbb{F}_3[\eta]/(\eta^{19} - \eta^2 + 1)$, $\mathbb{F}_{3^5} = \mathbb{F}_3[z]/(z^5 - z + 1)$, and $\mathbb{F}_{q^5} = \mathbb{F}_3[z, \eta]/(z^5 - z + 1, \eta^{19} - \eta^2 + 1)$.

Suppose that the compressor's output is $(s_1, s_2, s_3, s_4) \in \mathbb{F}_q^4$, where

$$\begin{aligned}
s_1 &= \quad \eta^{18} + \eta^{17} - \eta^{16} - \eta^{13} - \eta^{10} + \eta^9 + \eta^7 + \eta^6 + \eta^5 + \eta^4 + \eta^2 + \eta - 1, \\
s_2 &= \quad \eta^{17} + \eta^{16} - \eta^{13} - \eta^{12} - \eta^{11} - \eta^8 + \eta^7 - \eta^5 + \eta^4 + \eta^2, \\
s_3 &= -\eta^{17} + \eta^{16} - \eta^{15} + \eta^{14} + \eta^{13} + \eta^{12} - \eta^{10} + \eta^7 - \eta^4 + \eta - 1, \\
s_4 &= -\eta^{18} - \eta^{16} - \eta^{14} - \eta^{13} + \eta^{12} + \eta^{11} - \eta^{10} - \\
&\qquad \eta^9 + \eta^8 + \eta^7 + \eta^6 + \eta^5 + \eta^4 - \eta^3 + \eta^2 + \eta + 1.
\end{aligned}$$

Applying the algorithm above, one computes that the resultant of $p_1(w)$ and $p_2(w)$ is $h(S) = H(S^3 - S)$ where $H(t)$ is the product:

$$\begin{aligned}
&(\eta^{18} + \eta^{15} - \eta^{13} + \eta^{12} + \eta^{11} - \eta^{10} - \eta^{9} - \eta^{8} + \eta^{6} + \eta^{5} + \eta^{4} - \eta + 1)*\\
&(t - \eta^{17} - \eta^{14} + \eta^{13} - \eta^{12} - \eta^{11} + \eta^{10} + \eta^{9} - \eta^{7} - \eta^{6} + \eta^{5} - \eta^{4} - \eta^{3} - \eta^{2})*\\
&(t + \eta^{18} + \eta^{17} + \eta^{16} + \eta^{15} + \eta^{13} - \eta^{12} + \eta^{11} + \eta^{10} - \eta^{9} + \eta^{7} + \eta^{5} - \eta^{4} - \eta^{3} + \eta + 1)*\\
&(t^2 + (2\eta^{18} + \eta^{17} - \eta^{16} - \eta^{15} - \eta^{14} + \eta^{13} - \eta^{12} + \eta^{11} + \eta^{10} - \eta^{9} - \eta^{8} - \eta^{6} - \eta^{5} - \eta^{4})t\\
&\quad + \eta^{18} + \eta^{17} - \eta^{16} + \eta^{15} + \eta^{13} - \eta^{11} + \eta^{10} + \eta^{9} + \eta^{7} + \eta^{5} - \eta^{2} + 1)*\\
&(t^5 + (\eta^{17} - \eta^{15} - \eta^{14} - \eta^{12} - \eta^{11} + \eta^{9} - \eta^{7} + \eta^{6} - \eta^{5} + \eta^{4} - \eta^{3} - \eta^{2} + 1)t^4\\
&\quad + (\eta^{18} + \eta^{17} + \eta^{16} + \eta^{15} - \eta^{1}4 + \eta^{8} - \eta^{7} - \eta^{3} + \eta^{2} + \eta + 1)t^3\\
&\quad + (2\eta^{18} - \eta^{16} - \eta^{15} + \eta^{12} - \eta^{10} + \eta^{9} - \eta^{8} + \eta^{6} + \eta^{5} - \eta^{4} + \eta - 1)t^2\\
&\quad + (2\eta^{16} - \eta^{15} - \eta^{13} + \eta^{11} + \eta^{10} - \eta^{9} + \eta^{8} - \eta^{6} - \eta^{5} - \eta^{4} + \eta^{3} + \eta^{2} - \eta + 1)t\\
&\quad - \eta^{17} + \eta^{16} + \eta^{15} - \eta^{14} + \eta^{13} + \eta^{11} + \eta^{10} + \eta^{9} + \eta^{8} + \eta^{7} - \eta^{6} + \eta^{3} - \eta^{2} - \eta).
\end{aligned}$$

Let ρ_1 and ρ_2 be the two roots of $H(t)$ in $\mathbb{F}_q$ (corresponding to the two linear factors above, in the same order). Then $S^3 - S - \rho_1$ is irreducible in $\mathbb{F}_q[S]$, but $S^3 - S - \rho_2 = (S - \delta)(S - \delta + 1)(S - \delta - 1)$ where

$$\delta = \eta^{18} + \eta^{17} + \eta^{15} - \eta^{14} + \eta^{12} + \eta^{11} + \eta^{10} - \eta^{8} + \eta^{7} - \eta^{6} - \eta^{5} - \eta^{4}.$$

All three of δ, $\delta + 1$, and $\delta - 1$ give s_0's such that $\sum_{i=0}^{4} s_i z^i$ is the x-coordinate of a point in the trace zero subgroup of $E(\mathbb{F}_{3^{95}})$.

Remark 10.2. On a Macintosh desktop computer with a Dual 2.5 GHz PowerPC G5 processor running OS 10.4.7, using the computational algebraic number theory software package KASH3 [29] to compute the resultant and find its roots, using $y^2 = x^3 - x - 1$ decompression takes about 300 ms when $q = 3^{19}$ and takes about 700 ms when $q = 3^{43}$ (these values of q are good parameters in the sense that they are in a cryptographically useful range and the order of the trace zero subgroup is divisible by a large prime). This could be sped up by writing a dedicated program.

10.5. **The case $r = 2m$ with m odd.** Suppose E is an elliptic curve over a field K, and F is a quadratic extension of K. Let E' denote the quadratic twist of E corresponding to F/K. Then $E_{F/K}$ is isomorphic to E' over K (see Example 1.5(ii) of [32]), and $\mathrm{Res}_{F/K}E$ is isogenous over K to $E \times E'$ by (8.2). Note that in this ($r = 2$) case $\sigma(P) = -P$; since the x-coordinates of points in the trace zero subgroup $E_{F/K}(K) \subset E(F)$ lie in K, they are already compressed.

More generally, suppose M/K is a cyclic extension of odd degree m, and let $L = FM$. Then L/K is a cyclic extension of (even) degree $r = 2m$. By Proposition 5.10 of [32], $E_{L/K} \cong (E_{F/K})_{M/K} \cong (E')_{M/K}$ over K. Thus to study the primitive subgroup $E_{L/K}$ we are reduced to studying the primitive subgroup $(E')_{M/K}$.

11. Shortening cryptographic transmissions

We explain how to use the results of this paper to shorten transmission sizes in pairing-based cryptography. (See also [38] and §4 of [40].) We illustrate this concretely in the case of short signatures.

11.1. **Shortening transmissions using abelian varieties.** Pairing-based cryptography can be performed using abelian varieties and a Weil or Tate pairing on the ℓ-torsion, with ℓ not the characteristic of the field, if the abelian variety has a polarization whose degree is prime to ℓ. The pairings can be efficiently computed for supersingular elliptic curves and for Jacobians of supersingular hyperelliptic curves (and Jacobians of non-supersingular curves of low embedding degree). Our "optimal" abelian varieties in §12 give good supersingular abelian varieties to use.

11.2. **Shortening transmissions using primitive subgroups.** Theorem 9.4 shows that MOV security can be boosted by a factor of $r/\varphi(r)$ by going from a supersingular elliptic curve E over $\mathbb{F}_q$ to a primitive subgroup E_r over $\mathbb{F}_q$. One could view E_r as an abelian variety of dimension $\varphi(r)$ and do pairing-based cryptography for that abelian variety (if one can compute the pairings). A better way, just using elliptic curve arithmetic and pairings, is to view $E_r(\mathbb{F}_q)$ as a subgroup of $E(\mathbb{F}_{q^r})$, use the arithmetic in $E(\mathbb{F}_{q^r})$, and use our (de)compression algorithm in §10 to shorten cryptographic transmissions for pairing-based cryptography by a factor of 4/5 (when $r = 5$) or 2/3 (when $r = 3$), while preserving MOV security.

11.3. **RS compression of BLS signatures.** We first recall the Boneh-Lynn-Shacham (BLS) signature scheme [6]. Let $E : y^2 = f(x)$ be a supersingular elliptic curve over $\mathbb{F}_q$, and let $P \in E(\mathbb{F}_q)$ be a point of large prime order ℓ. Let c denote the cryptographic exponent $c_{E,q}$ defined in Definition 4.5. Let $e\colon \langle P\rangle \times \langle P\rangle \to \mathbb{F}_{q^c}^\times$ be a pairing that satisfies $e(P,P) \neq 1$ and $e(aP, bP) = e(P,P)^{ab}$ for every $a, b \in \mathbb{Z}$. One can use a modified Weil or Tate pairing for e. The public information is q, E, P, ℓ, e, and a cryptographic hash function $H\colon \{0,1\}^* \to \langle P\rangle$. Alice's private key is a randomly chosen integer a in the range $1 \le a \le \ell$, and her public key is $P_A = aP$. To sign a message $M \in \{0,1\}^*$, Alice computes $P_M = H(M)$ and $aP_M = (s,t) \in \langle P\rangle$. Alice's signature is $s \in \mathbb{F}_q$ (and an optional additional bit to recover the sign of t). To verify the signature, Bob computes $t = \sqrt{f(s)} \in \mathbb{F}_q$, sets $Q = (s,t)$, and checks that $e(P,Q) = e(P_A, P_M)$ (and also checks $e(P,Q) = e(P_A,P_M)^{-1}$, if the additional bit was not sent). In [7], Boneh, Lynn, and Shacham suggest using MNT elliptic curves [34] in place of supersingular elliptic curves. MNT curves are ordinary elliptic curves of embedding degree 3, 4, or 6.

In the Rubin-Silverberg (RS) modification of the BLS signature scheme, the signer compresses the signature using the algorithm in §10, and the verifier decompresses the signature before verifying. Take q and supersingular E as above, except that if q is a square take E so that $\sqrt{q}$ is not a q-Weil number for E (it suffices to take E with embedding degree > 1). Let $p = \mathrm{char}(\mathbb{F}_q)$, let r be a prime that does not divide $2pc_{E,q}$, and let P be a point of large prime order ℓ in the trace zero subgroup of $E(\mathbb{F}_{q^r})$ (in practice, this will mean taking $P \in E(\mathbb{F}_{q^r})$ of sufficiently large prime order). Take a pairing e and a hash function H as above, where now $c := c_{E,q} = c_{E,q^r}$. Alice's private and public keys are as in the BLS scheme. To sign M, as before, Alice computes $P_M = H(M)$ and aP_M. Alice's signature is the compression of aP_M given by the algorithm in §10. To verify the signature, Bob uses the decompression algorithm of §10 to produce the finite set of possible decompressions $\{Q_i\} \subset E(\mathbb{F}_{q^r})$. Bob verifies that $e(P, Q_i) = e(P_A, P_M)$ for some i (if additional bits are sent, Bob need only check this for one i, but the signer then needs to perform extra work to compute the additional bits).

The RS modification produces signatures that are $\frac{r-1}{r}$ as large as the corresponding BLS signatures. By Corollary 9.4, any attack on the RS modification of the BLS signature scheme corresponding to $P \in E_r(\mathbb{F}_q) \subset E(\mathbb{F}_{q^r})$ gives an attack on the security of the BLS signature scheme corresponding to P. In both cases, the security relies on the difficulty of the Elliptic Curve Diffie-Hellman Problem in the subgroup generated by the point P. Compared with BLS, RS signing is no more work than BLS signing, and RS verification requires an additional reconstruction step to recover s; for applications with a powerful verifier, this is not a problem.

11.4. **New composite order bilinear groups.** Recently, composite order bilinear groups have been used to solve important problems including partial homomorphic encryption [5], non-interactive zero-knowledge proofs [24], searching encrypted data [9], efficient group signatures [10], and fully collusion-resistant traitor tracing [8]. Supersingular elliptic curves have been the only secure instantiations of composite order bilinear groups (§2.1 of [5]), namely, Boneh et al. fix an RSA modulus n, take the smallest positive integer m such that $mn-1$ is a prime $\ell \equiv 2 \pmod 3$, and use the n-torsion points on $E : y^2 = x^3 + 1$, a supersingular elliptic curve over $\mathbb{F}_\ell$ with $\ell + 1 = mn$ points and with $c_{E,\ell} = \alpha(E, \ell) = 2$.

The following algorithm gives a new method for constructing composite order bilinear groups. It makes use of the abelian varieties E_3 and E_5, for which §10 gives efficient (de)compression algorithms, and for which one can rely on elliptic curve arithmetic without needing knowledge of higher-dimensional varieties.

Let p and q be primes $\equiv 1 \pmod 6$ and let $n = pq$. Take an integer that has order 6 modulo p and an integer that has order 6 modulo q, and use the Chinese Remainder Theorem to obtain an integer $z \equiv 2 \pmod 3$ that has order 6 modulo both p and q. Take the integer m of smallest absolute value such that $z + 3nm$ is a prime ℓ (by Dirichlet's Theorem, there are infinitely many primes of the form $z + 3nt$). Then $E : y^2 = x^3 + 1$ is a supersingular elliptic curve over $\mathbb{F}_\ell$ with $\ell + 1$ points and $F_E(x) = x^2 + \ell$. By Theorem 9.1, $F_{E_3}(x) = x^4 - \ell x^2 + \ell^2 = \ell^2 \Phi_6(\frac{x^2}{\ell})$. Thus $c_{E_3,\ell} = 6$, $\alpha(E_3, \ell) = 3$, and $|E_3(\mathbb{F}_\ell)| = \ell^2 - \ell + 1 = \Phi_6(\ell)$, which is divisible by n since ℓ has order 6 modulo n. Similarly, if p and q are primes $\equiv 1 \pmod{10}$, $n = pq$, and ℓ is a prime $\equiv 2 \pmod 3$ that has order 10 modulo p and q, then $|E_5(\mathbb{F}_\ell)|$ is divisible by n, $c_{E_5,\ell} = 10$, and $\alpha(E_5, \ell) = 2.5$. In this way, E_3 and E_5 give new composite order bilinear groups, whose orders are RSA moduli n. However, for fixed RSA security, while the MOV security per bit improves on the construction in [5] by a factor of $\frac{3}{2}$ (resp., $\frac{5}{4}$), one needs twice (resp., four times) as many bits, so RSA security per bit is worse. Thus, the construction in [5] seems to be the best available option.

12. Supersingular abelian varieties to use in pairing-based cryptography

12.1. **Optimality.** We consider a supersingular abelian variety over a finite field to be "optimal" if it has the highest security among abelian varieties of that dimension over the same field.

Definition 12.1 (Definition 16 of [38]). *An* **optimal** *supersingular abelian variety over $\mathbb{F}_q$ is a simple supersingular abelian variety A over $\mathbb{F}_q$ such that $c_{A,q} \geq c_{B,q}$ for every simple supersingular abelian variety B over $\mathbb{F}_q$ of the same dimension as A.*

Optimal supersingular elliptic curves are well-known. For example, over $\mathbb{F}_{p^n}$ with n odd, the elliptic curves $y^2 = x^3 + ax$ are supersingular and optimal (with $c_{E,p} = 2$) if $3 < p \equiv 3 \pmod 4$ and $0 \neq a \in \mathbb{F}_p$, the curves $y^2 = x^3 + b$ are supersingular and optimal (with $c_{E,p} = 2$) if $2 < p \equiv 2 \pmod 3$ and $0 \neq b \in \mathbb{F}_p$, the curves $y^2 + y = x^3 + x + 1$ and $y^2 + y = x^3 + x$ are supersingular and optimal (with $c_{E,q} = 4$) if $p = 2$, and $y^2 = x^3 - x \pm 1$ are supersingular and optimal (with $c_{E,q} = 6$) if $p = 3$ and $\gcd(n, 6) = 1$.

Thanks to Table 1, over $\mathbb{F}_{p^n}$ with n odd, to obtain higher MOV security per bit than for supersingular elliptic curves one can use supersingular abelian surfaces when $p = 2$ or $p > 7$, and supersingular abelian four-folds when $p = 3$ or 5 (in fact for all p, but surfaces do at least as well when $p \neq 3, 5$). We construct optimal examples below (as we did in §5.2 and §5.1 of [38]).

When $p = 7$, one could use the supersingular abelian three-fold that is the Jacobian J of the curve $y^2 = x^8 + x^4 + 5x^3 + 6x^2 + x + 2$ over $\mathbb{F}_{7^n}$ (when $\gcd(n, 14) = 1$), which was shown in [20] to have embedding degree 14, and thus $\alpha(J, 7^n) = \frac{14}{3}$. By Table 1 this is optimal and improves MOV security by a factor of $2\frac{1}{3}$ over supersingular elliptic curves in characteristic 7.

When q is a square, to obtain higher MOV security one could use abelian four-folds. One can either use the $g = 4$ part of Example 12.3 below, or take the abelian four-fold E_5 for an elliptic curve E with $c_{E,q} = 3$ (by Corollary 9.4, if $p \neq 5$ then $c_{E_5,q} = 15$ and $\alpha(E_5, q) = \frac{15}{4} = 3.75$).

12.2. **Optimal supersingular surfaces.** When $p > 3$, start with an optimal supersingular elliptic curve E over $\mathbb{F}_p$ (so $c_{E,p} = 2$). By Corollary 9.2, the abelian surface E_3 over $\mathbb{F}_{p^n}$ has $\alpha(E_3, p^n) = 3$ for all odd n, and thus by Table 1 is optimal.

When $\gcd(n, 6) = 1$, the Jacobian of the curve $y^2 + y = x^5 + x^3$ over $\mathbb{F}_{2^n}$ was given in Galbraith's paper [20] and has $c_{A,q} = 12$ and $\alpha(A, q) = 6$, so is an optimal supersingular abelian surface over $\mathbb{F}_{2^n}$.

When n is odd and $q = 2^n$ there are exactly 2 isogeny classes of elliptic curves E over $\mathbb{F}_q$ with $c_{E,q} = \alpha(E, q) = 4$, namely those of $C^+ : y^2 + y = x^3 + x + 1$ and $C^- : y^2 + y = x^3 + x$. Applying Corollary 9.4 with these curves and $r = 3$ produces two abelian surfaces $C_3^\pm$ over $\mathbb{F}_{2^n}$, with $\alpha(C_3^\pm, q) = 6$, $c_{C_3^\pm,q} = 12$, Weil number $\pm\sqrt{2^n}e^{2\pi i/24}$, and

$$F_{C_3^\pm}(x) = x^4 \mp 2^{\frac{n+1}{2}}x^3 + 2^n x^2 \mp 2^{\frac{3n+1}{2}}x + 2^{2n}.$$

By Corollary 9.4(ii) (or directly from the definition), $c_{C_3^\pm,q} = 12$ and $\alpha(C_3^\pm, q) = 6$. Using the characteristic polynomials to compute $|C_3^\pm(\mathbb{F}_{2^n})|$, sample values of prime n for which $|C_3^+(\mathbb{F}_{3^n})|$ is of a size suitable for cryptographic applications and has a large prime factor are $n = 109$, 113, and 127, for which the largest prime divisor ℓ of $|C_3^+(\mathbb{F}_{3^n})|$ has $\lceil \log_2(\ell) \rceil = 189$, 173, and 207, respectively. For C_3^- take $n = 103$, 113, and 139, for which $\lceil \log_2(\ell) \rceil = 193$, 193, and 201, respectively. In each case, when used in the RS modification of BLS signatures as in §11.3, the signature length is $2n$, $\lceil \log_2(\ell) \rceil$ measures the discrete log security, and $12n = \log_2(q^{c_{A,q}})$ measures the MOV security.

12.3. **Optimal supersingular four-folds.** Suppose that $\gcd(n, 6) = 1$, let $q = 3^n$, and let $E^\pm$ be $y^2 = x^3 - x \pm 1$. These two curves give the two isogeny classes of elliptic curves over $\mathbb{F}_q$ with $c_{E,q} = 6$. Let $\left(\frac{3}{n}\right)$ denote the Jacobi symbol, which is $+1$ if $n \equiv \pm 1 \pmod{12}$, and is -1 if $n \equiv \pm 5 \pmod{12}$. Then

$$F_{E^\pm,q}(x) = x^2 \pm (\tfrac{3}{n})3^{\frac{n+1}{2}}x + 3^n, \quad |E^\pm(\mathbb{F}_q)| = 3^n + 1 \pm (\tfrac{3}{n})3^{\frac{n+1}{2}},$$

$$F_{E_5^\pm,q}(x) = \frac{x^{10} \mp (\frac{3}{n})3^{\frac{5n+1}{2}}x^5 + 3^{5n}}{x^2 \pm (\frac{3}{n})3^{\frac{n+1}{2}}x + 3^n}, \quad |E_5^\pm(\mathbb{F}_q)| = \frac{3^{5n} + 1 \mp (\frac{3}{n})3^{\frac{5n+1}{2}}}{3^n + 1 \pm (\frac{3}{n})3^{\frac{n+1}{2}}}.$$

Either directly, or applying Corollary 9.4(iii) to $E^\pm$ over $\mathbb{F}_q$ with $r = 5$, gives $c_{E_5^\pm,q} = 30$ and $\alpha(E_5^\pm, q) = \frac{5}{4}\alpha(E^\pm, q) = 7.5$. Sample values of prime n for which $|E_5^+(\mathbb{F}_q)|$ is of a size suitable for cryptographic applications and has a large prime factor are $n = 43$, 47, 73, and 79; if ℓ is the largest prime divisor of $|E_5^+(\mathbb{F}_q)|$, then $\lceil \log_2(\ell) \rceil = 166$, 260, 458, and 485, respectively. For E_5^- take $n = 41$, 43, 59, 61, and 113, for which $\lceil \log_2(\ell) \rceil = 157$, 265, 223, 344, and 697, respectively. In each case, when used in the RS modification of BLS signatures as in §11.3, the signature length is $4\log_2(q)$, $\lceil \log_2(\ell) \rceil$ measures the discrete log security, and $\log_2(q^{c_{A,q}}) = \log_2(3^{30n})$ measures the MOV security.

When $q = 2^n$ with n odd, Corollary 9.2 with the elliptic curves $C^\pm$ of §12.2 and $r = 5$ implies that $\alpha(C_5^\pm, q) = 5$, so the abelian four-folds $C_5^\pm$ are optimal over $\mathbb{F}_q$.

By [16], the Jacobians J of $y^2 = x^5 - x \pm 1$ are supersingular abelian surfaces over $\mathbb{F}_5$ with $c_{J,5} = 5$. When $q = 5^n$ with $\gcd(n, 10) = 1$, Theorem 9.4 with $r = 3$ implies that $c_{J_3,q} = 15$ and $\alpha(J_3, q) = 15/4 = 3.75$, so the abelian four-folds J_3 are optimal over $\mathbb{F}_q$.

12.4. **Optimal Jacobians when q is a square.** In the next result we take superelliptic curves C_1 (in fact, Fermat quotients) over $\mathbb{F}_q$ defined by polynomials of degree n, whose Jacobian varieties A_1 have cryptographic exponent 1 over $\mathbb{F}_{q^2}$, and twist them by characters of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_{q^2})$ of order n to produce curves over $\mathbb{F}_{q^2}$ whose Jacobian varieties are simple $\varphi(n)/2$-dimensional abelian varieties of cryptographic exponent n. They have the advantage of occurring in arbitrarily large characteristic. We obtain optimal Jacobian varieties over finite fields of square size.

See [15] for supersingular Jacobians J of curves of genus $\frac{p-1}{2}$ with $c_{J,p^2} = \frac{p}{2}$.

Theorem 12.2 (Theorem 20 of [38])**.** *Suppose that $a, b, n \in \mathbb{N}$ have no common divisor greater than* 1*, n is odd, and*

$$n + 2 - (\gcd(n, a) + \gcd(n, b) + \gcd(n, a + b)) = \varphi(n).$$

Let q be a prime power congruent to $-1 \pmod{n}$*. For $\gamma \in \mathbb{F}_{q^2}^\times$, let C_γ be the curve*

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

over $\mathbb{F}_{q^2}$ and write A_γ for its Jacobian variety. Then:

(i) $\dim(A_\gamma) = \frac{\varphi(n)}{2}$,

(ii) *A_γ is supersingular,*

(iii) $c_{A_1,q^2} = 1$,

(iv) *if in addition γ generates $\mathbb{F}_{q^2}^\times$ modulo n-th powers, then A_γ is simple, $c_{A_\gamma,q^2} = n$, $A_\gamma(\mathbb{F}_{q^2})$ is cyclic, and $|A_\gamma(\mathbb{F}_{q^2})| = \Phi_{2n}(q)$.*

Proof. The dimension g of A_γ is the genus of C_γ. From the formula for the genus of $C_{\pm 1}$ given on p. 55 of [11] and the fact that the genus of C_γ is independent of γ, it follows that $g = \varphi(n)/2$. Let $F = \mathbb{F}_{q^2}$.

Since $q \equiv -1 \pmod{n}$, Theorem 20.15 of [45] shows that the Frobenius endomorphism of A_1 over F is multiplication by $-q$. In particular, the characteristic polynomial of Frobenius of A_1 over F is $(x+q)^{2g}$. By Theorem 2.5(v), A_1 is supersingular. By Theorem 2.7(iii), A_1 is elementary over F. By definition, $c_{A_1,q^2} = 1$. Since every A_γ is isomorphic to A_1 over the algebraic closure $\bar{F}$, every A_γ is supersingular.

The endomorphism ring $\mathrm{End}_{\bar{F}}(A_\gamma)$ contains the group of n-th roots of unity $\boldsymbol{\mu}_n$ in $\bar{F}$, 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 $\zeta \in \boldsymbol{\mu}_n \subset \mathrm{End}_{\bar{F}}(A_\gamma)$. 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 $[\phi_\gamma] = [\lambda' \circ \phi_1 \circ \lambda^{-1}] = [\lambda^{-1}] \circ [\phi_1] \circ [\lambda'] = [\lambda^{-1}] \circ (-q) \circ [\lambda'] = -q \circ [\lambda' \circ \lambda^{-1}] = -q \circ [\zeta]$.

Suppose 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 of $-[\zeta]$ on A_γ is divisible by $\Phi_{2n}(x)$ and has the same degree $2g = \varphi(n) = \varphi(2n)$, so they are equal. Thus $F_{A_\gamma,q^2}(x) = \prod_\xi (x - \xi q)$, product over primitive $2n$-th roots of unity ξ, which is $q^{\varphi(2n)}\Phi_{2n}(x/q)$. Since $\Phi_{2n}(x)$ is irreducible, so is $F_{A_\gamma,q^2}(x)$. Therefore A_γ is simple and $c_{A_\gamma,q^2} = n$. By Theorem 2.8(i), $A_\gamma(F)$ is cyclic and $|A_\gamma(F)| = q^{\varphi(2n)}\Phi_{2n}(1/q) = \Phi_{2n}(q)$. □

Example 12.3 (Example 21 of [38]). *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* $\alpha + \beta \ne \ell$. *Let* q *be a prime power congruent to* $-1 \pmod{n}$, $F = \mathbb{F}_{q^2}$, *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 variety. Then by Theorem 12.2,* A *is simple and supersingular,* $\mathrm{genus}(C) = \dim(A) = g$, $c_{A,q^2} = n$, $A(F)$ *is cyclic of order* $\Phi_{2n}(q)$, *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 by Theorem 7.2. Optimal examples over* F *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.*

13. Security

For pairing-based cryptography, the security comes from both the abelian variety discrete log security and the MOV security. Theorem 6.3 shows that the MOV security comes from $\mathbb{F}_{q^{c_{A,q}}}$. Allowing $c_{A,q}$ to take half-integer values when q is a square means that $c_{A,q}$ correctly captures the MOV security of supersingular abelian varieties, unlike the embedding degree, which is $2c_{A,q}$ when $c_{A,q} \notin \mathbb{Z}$ (and is $c_{A,q}$ otherwise). Joux and Lercier [28] recently examined the security of the discrete log problem in $\mathbb{F}_{q^n}^\times$ for "moderate" q. They point out that their variant of the function field sieve should be taken into account when computing MOV security for abelian varieties in low characteristic, such as when $\mathrm{char}(\mathbb{F}_q) = 3$ and $c_{A,q} = 30$ or 6, and when $\mathrm{char}(\mathbb{F}_q) = 2$ and $c_{A,q} = 12$, especially when $q = 2^n$ with n composite.

Gaudry (Theorem 1 of [21]) has a probabilistic attack on the discrete log problem in $A(\mathbb{F}_q)$, for A a g-dimensional abelian variety, with runtime $O(q^{2-2/g})$ up to logarithmic factors, with the constant depending (badly) on g. His method is based on index calculus. Viewing the trace zero subgroup E_5 as a 4-dimensional abelian variety over $\mathbb{F}_q$, Gaudry's attack on $E_5(\mathbb{F}_q)$ runs in time $O(q^{3/2})$ up to log factors, with a large constant. Asymptotically, this is better than Pollard Rho's $O(\sqrt{q^g}) = O(q^2)$ (though the crossover point with Pollard Rho has not been determined). Applied to the trace zero subgroup E_3, viewed as an abelian surface over $\mathbb{F}_q$, Gaudry's attack is $O(q)$ up to log factors, which is no better than Pollard Rho.

By (8.1) and (8.2), solving the discrete log problem in the primitive subgroup $E_r(\mathbb{F}_q)$ essentially solves the discrete log problem in $E(\mathbb{F}_{q^r})$.

A referee has alerted us to a new preprint of Diem and Scholten [14] that gives an attack on the discrete logarithm problem for trace zero subgroups of non-supersingular Jacobians of hyperelliptic curves of genus 2, that can be viewed as a variant of the Weil descent attack [22]. Further work is needed to determine whether this has implications for primitive subgroups associated to supersingular elliptic curves or abelian varieties.

14. Conclusion

We define the cryptographic exponent and security parameter for elementary supersingular abelian varieties over finite fields and relate them to the cryptographic security and the embedding degree. We determine exactly what values can occur. We give a compression algorithm that compresses points on the trace zero subgroup of $E(\mathbb{F}_{q^r})$ by a factor of $r/(r-1)$ for which we can make decompression efficient when $r = 3$ or 5. We construct optimal supersingular abelian varieties to use in pairing-based cryptography. We use our results on primitive subgroups, our compression algorithm, and our constructions to shorten pairing-based cryptography transmissions and keys, in the supersingular case. We give a generalization to abelian varieties of an elliptic curve result of Balasubramanian and Koblitz.

References

[1] R. Balasubramanian, N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptology **11** (1998), 141–145.

[2] P. S. L. M. Barreto, *Pairing-based crypto lounge*, `http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html`.

[3] P. S. L. M. Barreto, S. D. Galbraith, C. Ó hÉigeartaigh, M. Scott, *Efficient pairing computation on supersingular abelian varieties*, Des. Codes Cryptogr. **42** (2007), 239–271.

[4] D. Boneh, M. Franklin, *Identity based encryption from the Weil pairing*, in Advances in Cryptology — Crypto 2001, Lect. Notes in Comp. Sci. **2139**, Springer, Berlin, 2001, 213–229; journal version in SIAM J. Comput. **32** (2003), 586–615.

[5] D. Boneh, E-J. Goh, and K. Nissim, *Evaluating 2-DNF formulas on ciphertexts*, in Proceedings of TCC 2005, Lect. Notes in Comp. Sci. **3378**, Springer, Berlin, 2005, 325–341.

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

[7] D. Boneh, B. Lynn, H. Shacham, *Short signatures from the Weil pairing*, J. Cryptology **17** (2004), 297–319.

[8] D. Boneh, A. Sahai, B. Waters, *Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys*, in Advances in Cryptology — Eurocrypt 2006, Lect. Notes in Comp. Sci. **2442**, Springer, Berlin, 2006, 573–592.

[9] D. Boneh, B. Waters, *Conjunctive, subset, and range queries on encrypted data*, in Theory of Cryptography, Proceedings of the 4th Theory of Cryptography Conference, TCC 2007, Lect. Notes in Comp. Sci. **4392**, Springer, Berlin, 2007, 535–554.

[10] X. Boyen, B. Waters, *Compact Group Signatures Without Random Oracles*, in Advances in Cryptology — Eurocrypt 2006, Lect. Notes in Comp. Sci. **2442**, Springer, Berlin, 2006, 427–444.

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

[12] C. Diem, *A Study on Theoretical and Practical Aspects of Weil-Restrictions of Varieties*, Dissertation, 2001, `http://www.math.uni-leipzig.de/~diem/dissertation_diem.dvi`.

[13] C. Diem, N. Naumann, *On the structure of Weil restrictions of abelian varieties*, J. Ramanujan Math. Soc. **18** (2003), 153–174.

[14] C. Diem, J. Scholten, *An attack on a trace-zero cryptosystem*, preprint.

[15] I. Duursma, *Class numbers for some hyperelliptic curves*, in Arithmetic, geometry and coding theory (Luminy, 1993), de Gruyter, Berlin, 1996, 45–52.

[16] I. Duursma, K. Sakurai, *Efficient algorithms for the Jacobian variety of hyperelliptic curves $y^2 = x^p - x + 1$ over a finite field of odd characteristic p*, in Coding theory, cryptography and related areas (Guanajuato, 1998), Springer, Berlin, 2000, 73–89.

[17] G. Frey, *How to disguise an elliptic curve (Weil descent)*, lecture at ECC '98, `http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/frey.ps`.

[18] G. Frey, *Applications of arithmetical geometry to cryptographic constructions*, in Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, 128–161.

[19] 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.

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

[21] P. Gaudry, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, to appear in J. Symbolic Comput.

[22] P. Gaudry, F. Hess, N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), 19–46.

[23] S. W. Golomb, *Cyclotomic polynomials and factorization theorems*, Amer. Math. Monthly **85** (1978), 734–737.

[24] J. Groth, R. Ostrovsky, A. Sahai, *Perfect Non-interactive Zero Knowledge for NP*, in Advances in Cryptology — Eurocrypt 2006, Lect. Notes in Comp. Sci. **2442**, Springer, Berlin, 2006, 339–358.

[25] L. Hitt, *On the minimal embedding field*, in Pairing-Based Cryptography—Pairing 2007, Lect. Notes in Comp. Sci. **4575**, Springer, Berlin, 2007, 294–301.

[26] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.

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

[28] A. Joux, R. Lercier, *The Function Field Sieve in the Medium Prime Case*, Advances in Cryptology — Eurocrypt 2006, Lect. Notes in Comp. Sci. **4004**, Springer, Berlin, 2006, 254–270.

[29] KASH, `http://www.math.tu-berlin.de/~kant/kash_main.html`.

[30] T. Lange, *Trace zero subvarieties of genus 2 curves for cryptosystems*, J. Ramanujan Math. Soc. **19** (2004), 15–33.

[31] A. K. Lenstra and E. R. Verheul, *The XTR public key system*, in Advances in Cryptology — CRYPTO 2000, Lect. Notes in Comp. Sci. **1880**, Springer, Berlin, 2000, 1–19.

[32] B. Mazur, K. Rubin, A. Silverberg, *Twisting commutative algebraic groups*, Journal of Algebra **314** (2007), 419–438.

[33] 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.

[34] A. Miyaji, M. Nakabayashi, S. Takano, *New Explicit Conditions of Elliptic Curve Traces for FR-Reduction*, IEICE Transactions on Fundamentals E84-A(5) (2001), 1234–1243.

[35] W. B. Müller, W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar. **16** (1981), 71–76.

[36] D. Mumford, Abelian varieties, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Oxford University Press, London, 1970.

[37] N. Naumann, *Weil-Restriktion abelscher Varietäten*, Diplomarbeit, Universität Essen, 1999, unpublished.

[38] K. Rubin, A. Silverberg, *Supersingular abelian varieties in cryptology*, in Advances in Cryptology — CRYPTO 2002, Lect. Notes in Comp. Sci. **2442**, Springer, Berlin, 2002, 336–353.

[39] K. Rubin, A. Silverberg, *Torus-based cryptography*, in Advances in Cryptology — CRYPTO 2003, Lect. Notes in Comp. Sci. **2729**, Springer, Berlin, 2003, 349–365.

[40] K. Rubin, A. Silverberg, *Using primitive subgroups to do more with fewer bits*, in Proceedings of ANTS-VI, Lect. Notes in Comp. Sci. **3076**, Springer, Berlin, 2004, 18–41.

[41] K. Rubin, A. Silverberg, *Compression in finite fields and torus-based cryptography*, SIAM Journal on Computing **37** (2008), 1401–1428.

[42] 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.

[43] E. F. Schaefer, *A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field*, in Computational aspects of algebraic curves, Lecture Notes Ser. Comput., 13, World Sci. Publ., Hackensack, NJ, 2005, 1–12, `http://math.scu.edu/~eschaefe/0317.pdf`.

[44] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Reprint of the 1971 original, Publications of the Mathematical Society of Japan **11**, Princeton University Press, Princeton, NJ, 1994.

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

[46] A. Silverberg, *Compression for Trace Zero Subgroups of Elliptic Curves*, in the Proceedings of the Daewoo Workshop on Cryptography, in Trends in Mathematics **8** (2005), 93–100.

[47] P. J. Smith, M. J. J. Lennon, *LUC: A New Public Key System*, in Proceedings of the IFIP TC11 Ninth International Conference on Information Security IFIP/Sec '93, North-Holland, Amsterdam, 1993, 103–117.

[48] P. Smith, C. Skinner, *A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms*, in Advances in Cryptology — Asiacrypt 1994, Lect. Notes in Comp. Sci. **917**, Springer, Berlin, 1995, 357–364.

[49] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[50] 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.

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

[52] A. Weil, Adeles and algebraic groups, Progress in Math. **23**, Birkhäuser, Boston, 1982.

[53] A. Weimerskirch, *The Application of the Mordell-Weil Group to Cryptographic Systems*, MS thesis, Worcester Polytechnic Institute, 2001, `http://weimerskirch.org/papers/Weimerskirch_MordellWeilMSThesis.pdf`.

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

[55] H. J. Zhu, *Supersingular abelian varieties over finite fields*, J. Number Theory **86** (2001), 61–77.

Mathematics Department, University of California, Irvine, CA 92697, USA
E-mail address: krubin@uci.edu
E-mail address: asilverb@uci.edu