THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 21, Number 1/2020, pp. 77–84

METHODS OF GENERATION OF ELLIPTIC CURVES FOR HYBRID SIDH SCHEME OVER LARGE FIELDS

Michał WROŃSKI, Tomasz KIJKO, Robert DRYŁO

Military University of Technology in Warsaw, Faculty of Cybernetics
Corresponding author: Michał WROŃSKI, E-mail: michal.wronski@wat.edu.pl

Abstract. In this article we consider elliptic curves suitable for hybrid ECDH-SIDH over the field $\mathbb{F}_{p^2}$, which is motivated by saving some hardware resources. Generating elliptic curves $E/\mathbb{F}_p$ for ECDH requires computing the order of the elliptic group $\#E(\mathbb{F}_p)$, which for larger p may be quite time consuming; alternatively one can apply the complex multiplication method (it is showed how to generate elliptic curves natively over $\mathbb{F}_p$, which ensures good balance between security and efficiency). For ordinary elliptic curves $E/\mathbb{F}_p$ of known order $\#E(\mathbb{F}_p)$ we have a formula to compute the order $\#E'\left(\mathbb{F}_{p^2}\right)$, where E' is the quadratic twist of E over $\mathbb{F}_{p^2}$, and check if $E'\left(\mathbb{F}_{p^2}\right)$ is suitable for implementation of ECDH. This ensures incredible high level of classical security (about 751 bits for SIKE-751 field) and very good efficiency using the GLS method based on fast-computable endomorphisms in $E'\left(\mathbb{F}_{p^2}\right)$ to speed scalar multiplication. In this article we also give some examples of elliptic curves suitable for ECDH-SIDH hybrid scheme for fields used in SIKE variants.

Key words: SIDH, ECDH, hybrid scheme, GLS method.

1. INTRODUCTION

As noted in [4] a proposal that is gaining popularity in the PQC (Post-Quantum Cryptography) community is the deployment of hybrid schemes. Hybrid schemes are the schemes where a longstanding classically-secure primitive $\mathcal{P}$ is partnered alongside with the post-quantum primitive $\mathcal{Q}$. In the postquantum cryptography SIDH [5] (the supersingular elliptic curve isogeny key exchange) is a replacement of ECDH (the elliptic curve Diffie-Hellman key exchange) based on the discrete logarithm problem, which can be solved by Shor's polynomial time quantum algorithm [10]. One also considers using both SIDH and ECDH schemes if there would happen that some more efficient classical algorithm breaking SIDH would be found. In SIDH one uses supersingular elliptic curves over $\mathbb{F}_{p^2}$ for prime of the form $p = f l_1^{\alpha_1} l_2^{\alpha_2} \pm 1$ (in practice often $l_1 = 2$, $l_2 = 3$), and works in the $l_1^{\alpha_1}$ and $l_2^{\alpha_2}$ torsion subgroups of $E\left(\mathbb{F}_{p^2}\right)$ (Section 2). If SIDH and ECDH are used simultaneously, to save hardware resources (e.g. to minimize the number of necessary logic cells in FPGA device) it may be convenient to implement both schemes over the same field $\mathbb{F}_{p^2}$.

It is worth to note that implementation of the $\mathbb{F}_q$ arithmetic for fixed q is in hardware much more efficient and requires less logic cells than the implementation of finite field arithmetic, where q, as a parameter, may be changed. Moreover, even implementation of $\mathbb{F}_q$ arithmetic for fixed q requires a lot of logic cells and, if possible, it is recommended to use for ECDH solution using elliptic curve based on the field with the same characteristic as supersingular elliptic curve used in SIDH. However, the exact number of saved logic cells in this way is hard to estimate. This number depends on the size of the field (in general, the bigger field is used, the more logic cells are required in FPGA implementation).

Hybrid SIDH-ECDH scheme naturally requires using two curves: an ordinary $E/\mathbb{F}_p$ or $E/\mathbb{F}_{p^2}$ for ECDH and supersingular $E_1/\mathbb{F}_{p^2}$ for SIDH. In ECDH we will use the group $E(\mathbb{F}_p)$ or $E'(\mathbb{F}_{p^2})$ for ordinary elliptic curve $E/\mathbb{F}_p$, where E' is a quadratic twist of E over $\mathbb{F}_{p^2}$, such that the order $\#E(\mathbb{F}_p)$ or $\#E'\left(\mathbb{F}_{p^2}\right)$ is divisible by large prime r with small cofactor $\#E(\mathbb{F}_p)/r$ or $\#E'\left(\mathbb{F}_{p^2}\right)/r$ (the group order is almost prime). In case of $E'\left(\mathbb{F}_{p^2}\right)$ one can apply the GLS (Gallant-Lambert-Vanstone) method [6] (Section 3) to speed scalar multiplication on E' using an efficient endomorphism on E'. To obtain suitable ordinary curve $E/\mathbb{F}_p$ we need to compute its order $\#E(\mathbb{F}_p)$ and check if $\#E(\mathbb{F}_p)$ or $\#E'\left(\mathbb{F}_{p^2}\right)$ is prime or almost prime (we have $\#E'\left(\mathbb{F}_{p^2}\right)=(p-1)^2+t^2$, where t is the trace of E over $\mathbb{F}_p$). Searching for E by using the Schoof-Elkies-Atkin point counting algorithm for a random elliptic curve may take some time if p is large. An alternative approach is to use the complex multiplication (CM) method to construct an elliptic curve E with sufficiently small CM discriminant d.

2. SIDH ALGORITHM

In this section we recall the SIDH scheme [5]. Let p be a prime number of the form $p=f l_1^{\alpha_1} l_2^{\alpha_2} \mp 1$, where l_1, l_2 are small primes and $f \in \mathbb{N}$. Supersingular elliptic curves over $\mathbb{F}_{p^2}$ used in SIDH satisfy $E\left(\mathbb{F}_{p^2}\right) \cong \left(\mathbb{Z}_{f l_1^{\alpha_1} l_2^{\alpha_2}}\right)^2$. Then $E\left[l_i^{\alpha_i}\right] \subset E\left(\mathbb{F}_{p^2}\right)$ for $i=1,2$.

Suppose that points $P_1, P_2 \in E\left[l_1^{\alpha_1}\right]$ and $Q_1, Q_2 \in E\left[l_2^{\alpha_2}\right]$ generate subgroups $E\left[l_i^{\alpha_i}\right]$ for $i=1,2$ (points P_i and Q_i for $i=1,2$ are publicly known). Alice and Bob exchange a common secret key as follows.

Alice chooses random numbers $0<a_1, a_2<l_1^{\alpha_1}$ and computes $P=a_1P_1+a_2P_2$. Using Vélu's formulas [12], Alice computes as a composition of l_1-isogenies a separable isogeny $\varphi_A: E \to E_A$ with $\ker \varphi_A = \langle P \rangle$. She computes also the images of points $Q_i'=\varphi_A(Q_i)$ for $i=1,2$, and sends $\left(E_A, Q_1', Q_2'\right)$ to Bob.

Similarly, Bob chooses $0<b_1, b_2<l_2^{\alpha_2}$ and computes $Q=b_1Q_1+b_2Q_2$. He computes a separable isogeny $\varphi_B: E \to E_B$ with $\ker \varphi_B = \langle Q \rangle$ and images of points $P_i'=\varphi_B(P_i)$ for $i=1,2$. He sends $\left(E_B, P_1', P_2'\right)$ to Alice.

Receiving $\left(E_B, P_1', P_2'\right)$ Alice computes $P'=a_1P_1'+a_2P_2'=\varphi_B(P)$ and a separable isogeny $\varphi_A': E_B \to E_{BA}$ with $\ker \varphi_A' = \langle P' \rangle$.

Similarly, Bob given $\left(E_A, Q_1', Q_2'\right)$ computes $Q'=b_1Q_1'+b_2Q_2'=\varphi_A(Q)$ and a separable isogeny $\varphi_B': E_A \to E_{AB}$ with $\ker \varphi_B' = \langle Q' \rangle$.

Then elliptic curves E_{BA} and E_{AB} are isomorphic with $E/\langle P, Q \rangle$, hence a common secret element of Alice and Bob is the j-invariant $j(E_{BA})=j(E_{AB})$.

3. GLS METHOD FOR HYBRID SCHEME

In this section we shortly recall the GLS method which can be used to speed up point scalar multiplication on elliptic curves over quadratic fields.

3.1. Description of GLS method

Let $E: y^2=x^3+Ax+B$ be an elliptic curve, and let $E': y^2=x^3+A'x+B'$ be the quadratic twist of E over $\mathbb{F}_{p^2}$, where $A'=u^2A$, $B'=u^3B$ and $u \in \mathbb{F}_{p^2}$ is a non-square in $\mathbb{F}_{p^2}$. The GLS method [6] allows to

speed scalar multiplication on E' using the following efficiently computable endomorphism $\psi = f \circ \Phi_p \circ f^{-1} : E' \to E'$ over $\mathbb{F}_{p^2}$, where Φ_p is the p-th Frobenius endomorphism on E, and $f : E \to E$, $f(x,y) = \left(ux, \sqrt{u}^3 y\right)$, is the isomorphism over $\mathbb{F}_{p^4}$. We have

$$\psi(x,y) = \left(\frac{u}{u^p} x^p, \frac{\sqrt{u^3}}{\sqrt{u^{3p}}} y^p \right). \tag{1}$$

One can show that

$$\psi^2(x,y) + (x,y) = 0 \tag{2}$$

for $(x,y) \in E'\left(\mathbb{F}_{p^2}\right)$. Let $r > 2p$ be a prime, which divides $\#E'\left(\mathbb{F}_{p^2}\right)$. Then there exists $\lambda \in \mathbb{F}_r$ such that $\psi(P) = \lambda P$ for all $P \in E'\left(\mathbb{F}_{p^2}\right)[r]$. Because the equation (2) is satisfied by ψ, one can compute λ as a root of the equation $\lambda^2 + 1 \equiv 0 \pmod{r}$.

A point scalar multiplication kP, where $k \in \{1, \ldots, r-1\}$ and P is a point on an elliptic curve E can be computed using a following decomposition of k:

$$k = k_1 \lambda + k_0 .$$

Then one can write

$$kP = (k_1\lambda + k_0)P = k_1\lambda P + k_0 P = \lambda(k_1 P) + k_0 P \tag{3}$$

where points $k_1 P$ and $k_0 P$ can be computed simultaneously using for example simultaneous multiple point multiplication algorithm [7]. The most convenient situation we have got, when $k_0, k_1 < \sqrt{r}$.

In [1] it was showed that if cofactor $h' = \#E'\left(\mathbb{F}_{p^2}\right)/r$ is equal to 1 (one can show the same for $h' = 4$), then choosing k_0, k_1 as random integers from the interval $\left[0, \sqrt{r}\right)$ ensures good distribution of k. In this case the number of impossible and equivalent keys is negligible, comparing to the number of all possible keys.

4. CONSTRUCTING ELLIPTIC CURVES OVER $\mathbb{F}_p$ AND $\mathbb{F}_{p^2}$ USING THE CM METHOD

In this section we recall the complex multiplication (CM) method to construct an elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ with sufficiently small CM discriminant d. For the theory of the CM method see [8] and for its computational methods and applications see [11, 2].

4.1. CM method

Let E be an elliptic curve over $\mathbb{F}_q$, where q is a power of odd prime p, and let End(E) be the endomorphism ring of E over the algebraic closure $\overline{\mathbb{F}}_p$. The curve E is ordinary if and only if End(E) is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field K. The Frobenius endomorphism $\Phi_q(x,y) = \left(x^q, y^q\right)$ satisfies the characteristic equation $\Phi_q^2 - t_q \Phi_q + q = 0$, where t_q is the trace of E over $\mathbb{F}_q$. An isomorphism $\mathrm{End}(E) \to \mathcal{O}$ takes Φ_q on a root $\pi_q = \dfrac{t_q \pm \sqrt{t_q^2 - 4q}}{2}$ in $\mathcal{O}$ of the characteristic polynomial $x^2 - t_q x + q$. We have $K = \mathbb{Q}\left(\sqrt{-d}\right)$, where $t_q^2 - 4q = -dy^2$ for square-free $d \in \mathbb{N}$ and $y \in \mathbb{N}$. Let $N(\alpha) = \alpha\overline{\alpha}$, $\alpha \in K$, be the norm, where bar is the complex conjugation. We have $N(\pi_q) = q$ and

$\#E(\mathbb{F}_q) = N(\pi_q - 1)$. We also have $\#E\left(\mathbb{F}_{q^2}\right) = N\left(\pi_q^2 - 1\right)$ and $\#E'\left(\mathbb{F}_{q^2}\right) = N\left(\pi_q^2 + 1\right)$, where E' is a quadratic twist of E over $\mathbb{F}_{q^2}$.

Thus if we know the quadratic field $K = \mathbb{Q}\left(\sqrt{-d}\right)$ such that $\mathrm{End}(E)$ is an order in K, then one can compute the number of points on E as follows. The maximal order $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, where

$$\omega = \begin{cases} \sqrt{-d}, & \text{for } d \equiv 1,2 \pmod 4, \\ \dfrac{1+\sqrt{-d}}{2}, & \text{for } d \equiv 3 \pmod 4. \end{cases} \tag{4}$$

The minimal polynomial of ω is equal to

$$f_\omega = (x-\omega)(x-\omega) = \begin{cases} x^2 + d, & d \equiv 1,2 \pmod 4, \\ x^2 - x + \dfrac{1+d}{4}, & d \equiv 3 \pmod 4. \end{cases} \tag{5}$$

Since E is ordinary, p splits in K into a product $p\mathcal{O}_K = P\overline{P}$ of two different prime ideals $P, \overline{P}$, this is equivalent that $-d \bmod p$ is a quadratic residue (the Legendre symbol $\left(\dfrac{-d}{p}\right) = 1$). These ideals have generators $P = (p, \omega - a_1)$ and $\overline{P} = (p, \omega - a_2)$, where $a_1, a_2 \in \mathbb{F}_p$ are roots of $f_\omega \bmod p$. Hence one can also determine generators of P^s, $\overline{P}^s$, where $q = p^s$, and an integral basis of P^s regarded as a 2-dimensional lattice. Using the Gauss reduction algorithm [3, Alg. 1.3.14] one can compute the shortest vector in this lattice, which is a generator $\pm\pi_q$ or $\pm\overline{\pi}_q$ of P^s or $\overline{P}^s$, hence compute the order $\#E(\mathbb{F}_q) = N(\pm\pi_q - 1)$ (here we assume that $d \neq 1,3$ if $d = 1,3$ we have more generators of these prime ideals multiplying π_q or $\overline{\pi}_q$ by units $\pm 1, \pm i$ for $d = 1$ and by $\pm 1, \pm\zeta_3, \pm\zeta_3^2$ for $d = 3$).

Now assume that a prime p splits in $\mathcal{O}_K$ into a product of two prime ideals $p\mathcal{O}_K = P\overline{P}$, and we want to construct an ordinary elliptic curve over $\overline{\mathbb{F}}_p$ with $\mathrm{End}(E)$ isomorphic to $\mathcal{O}_K$. Such a curve is defined over the field $\mathbb{F}_q$, where $q = p^s$ for the smallest s such that P^s is a principal ideal. In particular, E is defined over $\mathbb{F}_p$ if and only if P is principal. There exists the Hilbert class polynomial $H_K(x) \in \mathbb{Z}[x]$ which depends only on K such that $H_K(x) \bmod p$ splits over $\mathbb{F}_q$ into linear factors and roots $j \in \mathbb{F}_q$ of $H_K(x)$ are exactly j-invariants of elliptic curves over $\mathbb{F}_q$ with $\mathrm{End}(E) \cong \mathcal{O}_K$. In practice computation of $H_K(x)$, where $K = \mathbb{Q}\left(\sqrt{-d}\right)$ and $d \in \mathbb{N}$ is square-free, is possible only for sufficiently small d (e.g. $d < 10^{13}$ see [11]), because the degree of $H_K(x)$ is equal to the order of the class group $Cl(\mathcal{O})$, which is about of the size $O\left(\sqrt{d}\right)$.

Given a prime p the following algorithm can be used to determine parameters of an ordinary elliptic curve $E/\mathbb{F}_p$ such that the order $\#E(\mathbb{F}_p)$ or $\#E'\left(\mathbb{F}_{p^2}\right)$ is prime or almost prime for quadratic twist E' of E over $\mathbb{F}_{p^2}$.

Algorithm 4.1. Input: a prime p, a bound B on d, a bound h_0 on cofactor of the order $\#E(\mathbb{F}_p)$ or $\#E'\left(\mathbb{F}_{p^2}\right)$ for quadratic twist E' of E over $\mathbb{F}_{p^2}$.

Output: The algorithm outputs the sets S and S' of parameters of ordinary elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}(E) \cong \mathcal{O}_K$ for $K = \mathbb{Q}\left(\sqrt{-d}\right)$ and $d \leq B$ such that $[d, p, n, h] \in S$ (resp. $[d, p, n', h'] \in S'$) iff there exists an ordinary elliptic curve $E/\mathbb{F}_p$ such that $\#E\left(\mathbb{F}_p\right) = n$ and n/h is prime for some divisor $h \leq h_0$ of n (resp. $\#E'\left(\mathbb{F}_{p^2}\right) = n'$ for quadratic twist E' of E over $\mathbb{F}_{p^2}$ and n'/h' is prime for some divisor $h' \leq h_0$ of n').

Let $S := \varnothing$ and $S' := \varnothing$.
for $d := 1,\ldots,B$ do

if d is square-free and $\left(\frac{-d}{p}\right) = 1$ then

compute prime ideal $P \subset \mathcal{O}_K$ such that $p\mathcal{O}_K = P\overline{P}$.

if P is not principal, then take the next d,

else

compute the generator π of $P = (\pi)$, compute $n = N(\pi - 1)$ and $n' = N\left(\pi^2 + 1\right)$,

if n/h is prime for some divisor $h \le h_0$ of n, then append $[d, p, n, h]$ to S,

if n'/h' is prime for some divisor $h' \le h_0$ of n', then append $[d, p, n', h']$ to S',

end for.
return S and S'.

Given parameters from the sets S and S' in the above algorithm we can check if the embedding degree l with respect to prime $r = n/h$ or $r = n'/h'$ is sufficiently large, where $l = \min\{m > 0 : r \mid q^m - 1\}$. The Weil and Tate pairing can be used to move the DLP from the subgroup of order r in E or E' to the extension field $\mathbb{F}_{p^l}$, where subexponential method exists (MOV attack [9]). In practice we can check that $r \nmid \left(q^m - 1\right)$ for $m \le L$, where L is a sufficiently large bound.

If we use quadratic twist E' then $\psi(P) = \lambda P$ (section 2) and $\lambda^2 + 1 = 0 \pmod r$, hence we can determine $0 \le \lambda < r$ solving the quadratic equation $\lambda^2 = -1 \pmod r$.

Given parameters of an elliptic curve with sufficiently small CM discriminant the following algorithm allows to determine the equation of this curve.

Algorithm 4.2. Input: Parameters from the set S or S' determined by the algorithm 4.1.

Output: An equation of an elliptic curve $E/\mathbb{F}_p$ or $E'/\mathbb{F}_{p^2}$ whose order is computed by the algorithm 4.1, where E' is a quadratic twist of E over $\mathbb{F}_{p^2}$.

1. Compute the Hilbert class polynomial $H_K(x)$.
2. Compute a root $j \in \mathbb{F}_p$ of $H_K(x) \bmod p$.
3. If input parameters are from the set S, then write the equations of elliptic curves $E_1/\mathbb{F}_p$ and $E_2/\mathbb{F}_p$ with the j-invariant j and k non-square in $\mathbb{F}_p$:

$$E_1/\mathbb{F}_p \ : \ y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}, \quad E_2/\mathbb{F}_p \ : \ y^2 = x^3 + \frac{3jk^2}{1728 - j}x + \frac{2jk^3}{1728 - j},$$

If $\#E_1(\mathbb{F}_p) = nh$, the return $E_1/\mathbb{F}_p$. Else return $E_2/\mathbb{F}_p$.

4. If input parameters are from the set S', then return the equation of an elliptic curve $E'/\mathbb{F}_{p^2}$ with the j-invariant j and k non-square in $\mathbb{F}_{p^2}$:

$$E'/\mathbb{F}_{p^2} \ : \ y^2 = x^3 + \frac{3jk^2}{1728 - j}x + \frac{2jk^3}{1728 - j}.$$

4.2. Elliptic curves for SIDH underlying fields

We used algorithms 4.1 and 4.2 to construct elliptic curves in short Weierstrass form over $\mathbb{F}_{p^2}$ for the following chracteristics of basefields: SIKEp434, SIKEp503, SIKEp610, SIKEp751.

We implemented the presented algorithms in Magma Computational Algebra System. As input parameters we bounded the cofactor $h \le 4$ ($h_0 = 4$) and we checked that the embedding degree $l > 10^6$ (we did not computed the exact value of l, since full factorization of large number would be required). The upper bound for the discriminant d was 1,856,563 (it is the highest number for which the class number is equal to 100, where the class number denotes the number of classes of order $\mathcal{O}_K$ for $K = \mathbb{Q}\left(\sqrt{-d}\right)$). In Appendix A we give examples of curves $E/\mathbb{F}_{p^2}$ for each considered SIDH p value.

5. CONCLUSION

In this article we discussed searching for ordinary elliptic curves suitable for using in ECDH protocol in hybrid SIDH-ECDH scheme. From computational efficiency point of view, especially in hardware implementations, such ordinary elliptic curves should be defined over field $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, where SIDH is also defined over $\mathbb{F}_{p^2}$. Because primes used in SIDH are large, searching for cryptographically suitable ordinary elliptic curves for ECDH using the Schoof-Elkies-Atkin point counting algorithm may be inefficient. Therefore, as described in this paper one can search for parameters of these curves and construct them using the CM method. In this paper we considered construction of these curves over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ taking in the second case quadratic twist over $\mathbb{F}_{p^2}$ of ordinary elliptic curve defined over $\mathbb{F}_p$, which allows to use fast computable endomorphisms and apply the GLS method to decrease scalar multiplication for almost half time.

REFERENCES

1. D. ARANHA, P. FOUQUE, B. GÉRARD, J. KAMMERER, M. TIBOUCHI, J. ZAPALOWICZ, *GLV/GLS decomposition, power analysis, and attacks on ECDSA signatures with single-bit nonce bias*, Advances in Cryptology – ASIACRYPT 2014: Proceedings, In: Lecture Notes in Computer Science (Eds: P. Sarkar and T. Iwata), **8873**, pp. 262-281, Springer, Berlin, Heidelberg, 2014, http://dx.doi.org/10.1007/978-3-662-45611-8_14.
2. R. BRÖKER, P. STEVENHAGEN, *Efficient CM-constructions of elliptic curves over finite fields*, Mathematics of Computation, **76**, *260*, pp. 2161-2179, 2007, http://dx.doi.org/10.1090/S0025-5718-07-01980-1.
3. H. COHEN, *A course in computational algebraic number theory*, Graduate texts in Math., **138**, Springer-Verlag, 1993.
4. C. COSTELLO, P. LONGA, M. NAEHRIG, *Efficient algorithms for supersingular isogeny Diffie-Hellman*, IACR Cryptology ePrint Archive, p. 413, 2016, https://eprint.iacr.org/2016/413.pdf.
5. L. DE FEO, D. JAO, J. PLÛT, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Journal of Mathematical Cryptology, **8**, *3*, pp. 209-247, 2014, http://dx.doi.org/10.1007/978-3-642-25405-5_2
6. S. GALBRAITH, X. LIN, M. SCOTT, *Endomorphisms for faster elliptic curve cryptography on a large class of curves*, Advances in Cryptology – EUROCRYPT 2009: Proceedings, In: Lecture Notes in Computer Science (ed. A. Joux), **5479**, pp. 518-535, Springer, Berlin, Heidelberg, 2009, http://dx.doi.org/10.1007/978-3-642-01001-9_30.
7. R. GALLANT, R. LAMBERT AND S. VANSTONE, *Faster point multiplication on elliptic curves with efficient endomorphisms*, Advances in Cryptology – CRYPTO 2001: Proceedings, In: Lecture Notes in Computer Science (ed. J. Kilian), **2139**, pp. 190-200, Springer, Berlin, Heidelberg, 2001, http://dx.doi.org/10.1007/3-540-44647-8_11.
8. S. LANG, *Elliptic functions, second ed.,* Springer-Verlag, 1987.
9. A. MENEZES, T. OKAMOTO, S. VANSTONE, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on information Theory, **39**, *5*, pp. 1639-1646, 1993.
10. P. SHOR, *Algorithms for quantum computation: Discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994, http://dx.doi.org/10.1109/SFCS.1994.365700.
11. A. SUTHERLAND, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Mathematics of Computation, **80**, *273*, pp. 501-538, 2009, http://dx.doi.org/10.1090/S0025-5718-2010-02373-7.
12. J. VÉLU, *Isogénies entre courbes elliptiques*, CR Acad. Sci. Paris, Séries A 273, pp. 305-347, 1971.

APPENDIX A

Propositions of elliptic curves for SIDH base fields

All elliptic curves are given in short Weierstrass form $E/\mathbb{F}_{p^2} : y^2 = x^3 + Ax + B$, where the defining polynomial f of the field $\mathbb{F}_{p^2}$ has the form $f(v) = v^2 + 1$, and $A = a_1 v + a_0$ and $B = b_1 v + b_0$.

A.1. Weierstrass elliptic curve over $\mathbb{F}_{p^2}$ for $\boldsymbol{p = 2^{216}3^{137} - 1}$

a_1 = 135a6c8a512b6ef9b1d6ef49b3e57d19ef656b9662d46797f600fc61b5e35818eddc6e8e\
03b188e049838ed3384d7c5006b5d376ae1d8 (hex)
a_0 = 13e7d1aff0d9369d961d8dc005cb871042416362bc610fb8d2525087bd450fd8f6f914aa\
3cd79fa44605d2bea69d9cdf7dcce58609859 (hex)
b_1 = 1dbd23a585dc3b80fc60f909de813527ffa62752b97a4247035f79377a03b09a6e141f22\
d9bd673212f9f553a4679c1383f9a89c7d947 (hex)
b_0 = 1ed4d92d623001c2a80b905088a4904e5b041cd2e599b085226aecd0752ea226f9f5d356\
360efdc83d8a9cdd4c6853339deb834ebf1a6 (hex)

The elliptic curve $E/\mathbb{F}_{p^2}$ was obtained using algorithms 4.1 and 4.2 with $d = 305827$.

The order $\#E(\mathbb{F}_{p^2}) = r \cdot h$, where r and h are:

r = 4db194809d18b920f2ecf68816ae3d3d0063244f01221708ab42abe1b46445ab96af6359\
a5732ca2221c664b96c55f373d2cdca4125428ff2d55e7f82c48976c63e7f3cd263fa7c2\
ede3afcd0365b852b14f99217ad9bbaba13772a2e8a46824d8a324efb0a6c94cf76b73f55 (hex)
h = 1

A.2. Weierstrass elliptic curve over $\mathbb{F}_{p^2}$ for $\boldsymbol{p = 2^{250}3^{159} - 1}$

a_1 = 33bdb0bece4f26e6080f5e26d3ab2df22638611f0adaf0cf425e702ae2f3dab40da2c163\
5542102e434fc1e51dbb6657896b9f08e4cc5a185cdde773ae4d29 (hex)
a_0 = 247a30c48fb286ac140365223a67c093504053bbd050cbed3d47f3e3b6d380a8a08f5ab1\
d812c223e6dd3cef40281d4b63bfd98e6a1beccfe79170221a9ba (hex)
b_1 = 3b434501f7bb044a2572c5b00ddda63c11dcadb5b8ab74ca82424ece7d496bb039ad6969\
638fd6685ca941d5bb2fb12028cc21fd3d4fc2d7fe9bb1b296ebe4 (hex)
b_0 = 17bc4cf97c3e5dc51c98e37eb1ffcb14a493f3baed8556032266e5a1193128841dcd0dec\
96abf155a68400f36e58d220b9af866d85606af3ecb746ba8ac0da (hex)

The elliptic curve $E/\mathbb{F}_{p^2}$ was obtained using algorithms 4.1 and 4.2 with $d = 1476343$.

The order $\#E(\mathbb{F}_{p^2}) = r \cdot h$, where r and h are:

r = 40ce90246ee1945b40a8279a12deaf3e1172b15017ef7790edceab348626d3e32dd59733\
04fe8ce28dd9fdbc9482f7f24ce5df11f4e90518ead0ca68ccfdca3a446d195d3d1386d9\
99f8c78f35598811e7422c68fc4292b6b901c5ef0f360a30bf6ff8618027f3ef60484cc9\
0020a191ab4d3510d15d135c27b07ae8401 (hex)
h = 4

A.3. Weierstrass elliptic curve over $\mathbb{F}_{p^2}$ for $\boldsymbol{p = 2^{305}3^{192} - 1}$

a_1 = 211fddac8f6d7c6faa281a45e331c29756be54f984c193f498a0eac0411c4aa08dbc7733\
cf0bd61e164ec225b6fcbb7f60f055054ae584a81dbf0d3d1e13cfab90298c6234ed7025\
516a639e1 (hex)
a_0 = 1e8d865f8150e0be2fcef0c9ca37ec3582e9bebddc7c7354fd4b6d9a48044a447163448b\
9a0e04184d493e6985a1994d47449620f8da732344051111dc5cf90f5a92d62b1b883d5c\
5568d48b9 (hex)

b_1 = 16159557293205bd5f4328c84b191a9046a50df676f4c5b3d4ad6d84a9de9b99c7b9186c\
5e233883365073fec4b957446dfcf8ba9846b69afac538479dd21ec9b70079b43243ce90\
43f2c67b6 (hex)
b_0 = 19afcc5b94b64311c1b5e77f778c61b712382ec854b1e8d2f79deffd863e0da9a05bac4f\
c2c63e485bb5c14771593638b757bff2475781ae3e1c3b0ac8c59b13ff15be6e81d2219b\
ffca4ce00 (hex)

The elliptic curve $E/\mathbb{F}_{p^2}$ was obtained using algorithms 4.1 and 4.2 with $d = 115355$.

The order $\#E\left(\mathbb{F}_{p^2}\right) = r \cdot h$, where r and h are:

r = 62be190269d1337b7b4473c93e6441063df9649ba3ea4086448fb5da1152cde50c05e045\
50fc4cce0d97825638b19a7cced4e22754a3f20928d249c196dab8cd7fe09ba529b9fe11\
677fdb801b42192ca7412e04198e69faf1913dc358fb2e3dc063c02b51abe78582d1ac44\
52444ec3f26842827c131ffabc4ca68d4d282659b7594194db3fe690071ee74938716f51\
c47e7d8356f5ee195 (hex)
h = 1

A.4. Weierstrass elliptic curve over $\mathbb{F}_{p^2}$ for $\boldsymbol{p = 2^{372}3^{239} - 1}$

a_1 = 16b5791f312f1dc72d064566291cec764f77adcb677f4120b1ace65d050416cde1c0824f\
7ac70e4b9d02386e5de6477fb9da9506785e0d98d34ddf489cc5fef6b88562a9833eaba6\
6e8f3b9677cd3cc53af0342ef862f534b476c8d04bf1 (hex)
a_0 = 239398f492a5be2a4658eae37656fededac8f0049e927417f30aa0e7173c80821e8b9feb\
302c4e5ba2fc44dad27c711e13230039711aa8d72f32c738d6d7670465534ab9aec0cb9a\
8dfebd30880e13d07f74cac11c516134a32208c401e1 (hex)
b_1 = 46206d8c94eb69ef977670be4941ad475b8d78dbdfb83f1f31102d6c797eadbd209b147d\
64f50f0419edd14ad344b700a79bbb511fa8be15d1cbd9a329ecec878a0bebd997c46953\
93c67126cb6299be8829966c6acc55b52390f2512443 (hex)
b_0 = 2b25b124bcb7ae4fe32fa60e213f8c7dcc4b2df35395aca791ce7c21ccda19d6f4cefc71\
71ea19c2f5420d885503f67e4c325a11b8fde9728aea3d2550de466e7323cee012cc38aa\
5b6d88d9c7c951d6184ebfe2375caf27e9553a30c20b (hex)

The elliptic curve $E/\mathbb{F}_{p^2}$ was obtained using algorithms 4.1 and 4.2 with $d = 268819$.

The order $\#E\left(\mathbb{F}_{p^2}\right) = r \cdot h$, where r and h are:

r = 30e91d466df5429960d2536b6ae0d99aa4835fed951f1d323fb4c115170a25e037e40347\
e3ab06e7a12f5ff7b20ad617c8df437cfa421554fe2e49ca85bab790796cf84d4d74319a\
6c9bca37551ae9f5f5f6aff3b7f731b89b2da43f258ab5a0f8a1e44b2bbb21ae571c1526\
ed56ef3c2dd334e843953705a91b59951db2efa00698c3f307bf98478a3111057db32555\
59039c66c1685eb26d51ebe0ceb5b9f9a9a98036296a93cdd36e6ae17e2e6f8523d4a164\
62103af52eac5f35 (hex)
h = 1

Received June 28, 2019