A note on how to (pre-)compute a ladder

Improving the performance of X25519 and X448

Thomaz Oliveira[1], Julio López[2], and Francisco Rodríguez-Henríquez[1]

[1] Computer Science Department, Cinvestav-IPN
thomaz.figueiredo@gmail.com, francisco@cs.cinvestav.mx
[2] Institute of Computing, University of Campinas
jlopez@ic.unicamp.br

Abstract. In the RFC 7748 memorandum, the Internet Research Task Force specified a Montgomery-ladder scalar multiplication function based on two recently proposed prime elliptic curves. The purpose of this function is to support the Diffie-Hellman key exchange algorithm included in the coming version of the Transport Layer Security cryptographic protocol. In this paper, we describe a ladder variant that permits to accelerate the fixed-point multiplication function when applied on the Diffie-Hellman key pair generation step. Our function combines a right-to-left version of the Montgomery ladder with the pre-computation of multiples of the base point and, by requiring very modest memory resources and a small implementation effort, it obtains significant performance improvements on desktop architectures. Moreover, our proposal fully complies with the RFC 7748 specification. To our knowledge, this is the first proposal of a Montgomery ladder procedure for prime elliptic curves that admits the extensive use of pre-computation.

1 Introduction

Since the last decades, Elliptic Curve Cryptography (ECC) has been largely used for achieving highly secure and highly efficient cryptographic communication implementations. In particular, ECC has become the prime choice for realizing key exchange and digital signature-verification protocols. However, reports released in 2013 suggested that the National Security Agency (NSA) secretly introduced backdoors to internationally-used encryption standards [29]. Immediately thereafter, new revelations [28] indicated that the same agency had tampered the elliptic curve-based pseudorandom number generator standard Dual_EC_DRBG, which was consequently removed from the SP 800-90A specification by NIST [23,24].

These events prompted in 2014 that the Transport Layer Security (TLS) working group of the Internet Engineering Task Force requested from the Crypto Forum Research Group (CFRG), recommendations of new elliptic curves to be integrated into the next version of the TLS protocol [30]. The requirements for the selection of such curves were based on [4,27], which advocate for a number of designs practices and elliptic curve properties, including rigidity in the curve-generation process and simplicity in the implementation of cryptographic algorithms. After a long and lengthy discussion, two prime elliptic curves, known as Curve25519 and Curve448, were chosen for the 128-bit and 224-bit security levels, respectively (see §3 for more details). The RFC 7748 [19] memorandum describes the implementation details related to this choice, including the curve parameters and the Montgomery ladder-based scalar multiplication algorithms, also referred to as X25519 and X448 functions.

The Montgomery ladder procedure along with the Montgomery curves were introduced in [21]. Since then, the Montgomery ladder has been carefully studied by many authors, as discussed for example, in the survey by Costello and Smith in [9]. We know now how to use the Montgomery ladder for computing the point multiplication kP, where P is usually selected as a point that belongs to a prime order r subgroup of an elliptic curve, and k is an integer in the $[1, r-1]$ interval. Nevertheless, arguably the most important application of the Montgomery ladder lies in the Diffie-Hellman shared-secret computation as described in [19].

The classical Montgomery ladder as it was presented in [21], is a left-to-right scalar multiplication procedure that does not admit in a natural way efficient pre-computation mechanisms. In an effort to obtain this feature, and in the context of binary elliptic curves, the authors of [25] introduced a right-to-left Montgomery ladder that was amenable for pre-computing multiples of a fixed base point P in an off-line fashion. However the procedure presented in [25] crucially depended on the computation of point halving operations, a primitive that can be performed efficiently in binary elliptic curves but that in general, we do not know how to compute for prime elliptic curves. Hence, it appeared that the finding of the right-to-left ladder procedure of [25] was circumscribed to binary elliptic curves, and it was not obvious how to extend it to their prime elliptic curve counterparts.

Our contributions In this note, we present an alternative way to compute the key exchange protocol presented in [19]. In short, we propose different X25519 and X448 functions which can take advantage of the fixed-point scenario provided by the Diffie-Hellman key generation phase. This algorithm achieves an estimated performance increase of more than 30% at the price of a small amount of extra memory resources. In addition, it does not intervene with the original RFC specification and it is straightforward to implement, preserving the simplicity feature of the original design.

The remainder of this paper is organized as follows. In §2 we briefly describe the Diffie-Hellman protocol. In §3 we give more details on the CFRG selected elliptic curves. The Montgomery ladder-based scalar multiplication functions X25519 and X448 are analyzed in §4. Our proposal is discussed in §5 and our concluding remarks and future work are presented in §6.

2 The Diffie-Hellman protocol

The Diffie-Hellman key exchange protocol, introduced by Diffie and Hellman in [10], is a method that allows to establish a shared secret between two parties over an insecure channel. Originally proposed for multiplicative groups of integers modulo p, with p a prime number, the scheme was later adapted to additively-written groups of points on elliptic curves by Koblitz and Miller in [15,20]. Commonly known as elliptic curve Diffie-Hellman protocol (ECDH), this variant is concisely described in Algorithm 1.

Algorithm 1 The elliptic curve Diffie-Hellman protocol

Public parameters: Prime p, curve $E/\mathbb{F}_p$, point $P = (x, y) \in E(\mathbb{F}_p)$ of order r

Phase 1: Key pair generation

	Alice		**Bob**
1:	Select the private key $d_A \xleftarrow{\$} [1, r-1]$	1:	Select the private key $d_B \xleftarrow{\$} [1, r-1]$
2:	Compute the public key $Q_A \leftarrow d_A P$	2:	Compute the public key $Q_B \leftarrow d_B P$

Phase 2: Shared secret computation

	Alice		**Bob**
3:	Send Q_A to Bob	3:	Send Q_B to Alice
4:	Compute $R \leftarrow d_A Q_B$	4:	Compute $R \leftarrow d_B Q_A$

Final phase: The shared secret is the point R x-coordinate

As shown in Algorithm 1, the ECDH protocol is divided into two phases; in the first phase, both parties generate their private and public key pair. The private key d_A (d_B) is an integer chosen uniformly at random from the interval $[1, r-1]$ while the public key Q_A (Q_B) is the resulting point of the scalar multiplication of d_A (d_B) by the base-point P. In the majority of the proposed elliptic curve-based standards and specifications (e.g. [11,6,22], including [19]), the point P is fixed and its coordinates are explicitly given in the documentation. At the implementation level, this setting is usually called fixed- or known-point scenario.

After computing their respective public/private key pair, each party sends her public key to the other. Next, they perform the point multiplication of the received public key by their own private key. The group properties of $E(\mathbb{F}_p)$ guarantee that,

$$R = d_A Q_B = d_A(d_B P) = d_B(d_A P) = d_B Q_A = R.$$

As a result, the parties have access to a common piece of information, represented by the x-coordinate of R, which is only disclosed to themselves. [3] Since the public key Q_B (Q_A) is not known a priori by Alice (Bob), the scalar multiplication in the second phase is said to be performed in a variable- or unknown-point scenario.

[3] Here, we are considering an ideal but unrealistic scenario. In practice, an inappropriate choice of the elliptic curve parameters, the prime p, the order r, the implementation of the scalar multiplication algorithm, among many other aspects, could disqualify this statement.

3 The curves

The [19] memorandum specifies two Montgomery elliptic curves of the form

$$E_A/\mathbb{F}_p : v^2 = u^3 + Au^2 + u.$$

The standard specification for the 128 bits of security level uses the prime $p = 2^{255} - 19$, and the curve parameter is given by $A = 486662$. This curve is commonly known as Curve25519 and was proposed in 2005 by Bernstein [1]. The point group order is given as $\#E_{486662}(\mathbb{F}_{2^{255}-19}) = h \cdot r \approx 2^{255}$, with $h = 8$ and

$$r = 2^{252} + 27742317777372353535851937790883648493.$$

The order-r base-point $P = (u, v)$ is specified as

$$\begin{aligned} u_P =& \texttt{0x9} \\ v_P =& \texttt{0x20AE19A1B8A086B4E01EDD2C7748D14C} \\ & \texttt{923D4D7E6D7C61B229E9C5A27ECED3D9}. \end{aligned}$$

The recommendation for the 224-bit security level is to use $p = 2^{448} - 2^{224} - 1$ and $A = 156326$. This curve was originally proposed by Hamburg in the Edwards form as Ed448-Goldilocks [14], but it is referred in [19] as Curve448. The group order $\#E_{156326}(\mathbb{F}_{2^{448}-2^{224}-1}) = h \cdot r \approx 2^{448}$, with $h = 4$ and

$$\begin{aligned} r =& 2^{446} - 13818066809895115352007386748515 \\ & 426880336692474882178609894547503885. \end{aligned}$$

For this curve, the base-point P is given by

$$\begin{aligned} u_P =& \texttt{0x5} \\ v_P =& \texttt{0x7D235D1295F5B1F66C98AB6E58326FCECBAE5D34F55545D060F75DC2} \\ & \texttt{8DF3F6EDB8027E2346430D211312C4B150677AF76FD7223D457B5B1A}. \end{aligned}$$

4 The scalar multiplication operation

Let $E_A/\mathbb{F}_p$ be an elliptic curve and P an order-r point in $E_A(\mathbb{F}_p)$. Then, for any n-bit scalar $k = (k_{n-1}, \ldots, k_2, k_1, k_0)_2 \in [1, r-1]$, the scalar multiplication operation is given by

$$Q = kP = k_{n-1}2^{n-1}P + \cdots + k_2 2^2 P + k_1 2P + k_0 P.$$

As presented in §2, the scalar multiplication function is used throughout the two first ECDH phases; first, to generate the public keys Q_A and Q_B and later, in the second phase, to compute the common point R.

4.1 Left-to-right Montgomery ladder

Initially proposed to improve the performance of integer factorization algorithms, the Montgomery ladder [21] is now largely used in the design of constant-time scalar multiplication implementations. [4] This is because its ladder step structure, assures that the same arithmetic operations are executed independently of the scalar bits k_i values. A high-level description of this procedure is presented in Algorithm 2.

Algorithm 2 Left-to-right Montgomery ladder

Input: $P = (u_P, v_P) \in E_A(\mathbb{F}_p)$, $k = (k_{n-1} = 1, k_{n-2}, \ldots, k_1, k_0)_2$
Output: $u_{Q=kP}$

$R_0 \leftarrow \mathcal{O}$; $R_1 \leftarrow u_P$;
for $i = n - 1$ **downto** 0 **do**
  if $k_i = 1$ **then**
    $R_0 \leftarrow R_0 + R_1$; $R_1 \leftarrow 2R_1$
  else
    $R_1 \leftarrow R_0 + R_1$; $R_0 \leftarrow 2R_0$
  end if
end for
return $u_Q \leftarrow R_0$

If the difference between the points R_1 and R_0 is known, it is possible to derive efficient formulas for computing $R_0 + R_1$ that refer only to the u-coordinates of the operands, a formula that sometimes is named as differential addition [9]. [5] That is the main rationale for Algorithm 2; throughout its execution, the Montgomery ladder maintains the invariant $R_1 - R_0 = P$ by computing at each iteration

$$(R_0, R_1) \leftarrow \begin{cases} (2R_0, 2R_0 + P), & \text{if } k_i = 0 \\ (2R_0 + P, 2R_0 + 2P), & \text{if } k_i = 1. \end{cases}$$

Furthermore, in order to avoid expensive field inversions within the point arithmetic functions, one can accelerate the scalar multiplication by using projective coordinates, using the transformation $(u = U/Z)$.

A low-level description of the left-to-right ladder on prime elliptic curves in Montgomery form is given in Algorithm 3. [6] When computed with the parameters listed in §3, this algorithm is called X25519 (with $n = 255$) or X448 (with $n = 448$) [19]. The $\oplus$ notation stands for the exclusive-or logical operator, while

[4] See [9], for a comprehensive historical recount of this classical algorithm and its variants.

[5] It is also possible to express the u-coordinate of the resulting point $R_i = 2R_i$, for $i = 0, 1$, using only the u-coordinate of the operand P, an operation known as differential doubling [9].

[6] The description is closely related to [19, §5].

the symbols $+, -, \times, ^2$ and $^{-1}$ represent the field $\mathbb{F}_p$ arithmetic operations of addition, subtraction, multiplication, squaring and inversion, respectively.

Algorithm 3 Low-level left-to-right Montgomery ladder

Input: $P = (u_P, v_P) \in E_A/\mathbb{F}_p$, $k = (k_{n-1} = 1, k_{n-2}, \ldots, k_1, k_0)_2$, $a_{24} = (A+2)/4$
Output: $u_{Q=kP}$

Initialization: $U_{R_0} \leftarrow 1$, $Z_{R_0} \leftarrow 0$, $U_{R_1} \leftarrow u_P$, $Z_{R_1} \leftarrow 1$, $s \leftarrow 0$
for $i \leftarrow n-1$ **downto** 0 **do**
  `# timing-attack countermeasure`
  $s \leftarrow s \oplus k_i$
  $U_{R_0}, U_{R_1} \leftarrow$ cswap(s, U_{R_0}, U_{R_1})
  $Z_{R_0}, Z_{R_1} \leftarrow$ cswap(s, Z_{R_0}, Z_{R_1})
  $s \leftarrow k_i$
  `# common operations`
  $A \leftarrow U_{R_0} + Z_{R_0}$; $B \leftarrow U_{R_0} - Z_{R_0}$
  `# addition`
  $C \leftarrow U_{R_1} + Z_{R_1}$; $D \leftarrow U_{R_1} - Z_{R_1}$
  $C \leftarrow C \times B$, $D \leftarrow D \times A$
  $U_{R_1} \leftarrow D + C$; $U_{R_1} \leftarrow U_{R_1}^2$
  $Z_{R_1} \leftarrow D - C$; $Z_{R_1} \leftarrow Z_{R_1}^2$; $Z_{R_1} \leftarrow u_P \times Z_{R_1}$
  `# doubling`
  $A \leftarrow A^2$; $B \leftarrow B^2$
  $U_{R_0} \leftarrow A \times B$
  $A \leftarrow A - B$
  $Z_{R_0} \leftarrow a_{24} \times A$; $Z_{R_0} \leftarrow Z_{R_0} + B$; $Z_{R_0} \leftarrow Z_{R_0} \times A$
end for
$U_{R_0}, U_{R_1} \leftarrow$ cswap(s, U_{R_0}, U_{R_1})
$Z_{R_0}, Z_{R_1} \leftarrow$ cswap(s, Z_{R_0}, Z_{R_1})
$Z_{R_0} \leftarrow Z_{R_0}^{-1}$
$u_{R_0} \leftarrow U_{R_0} \times Z_{R_0}$
return $u_Q \leftarrow u_{R_0}$

At each iteration i of Algorithm 3, the conditional swap function (cswap) exchanges the values of the R_0 and R_1 coordinates when the bits k_{i-1} and k_i are different. This function is a countermeasure for potential cache-based attacks [16,17], which could reveal the scalar digits (the private key in Alg. 1) by determining the access order of the points R_0 and R_1. The *cswap* function consists only of simple logic operations, so its cost will be disregarded in our estimations. For more details on the implementation of this function see [19,25].

Cost estimations Let $\mathbf{m}$, $\mathbf{m_{a24}}$, $\mathbf{m_{uP}}$, $\mathbf{s}$, $\mathbf{i}$ and $\mathbf{a}$ represent the cost of a general multiplication, multiplication by the constant $(A+2)/4$, multiplication by the u-coordinate of the base-point P, squaring, inversion and addition/subtraction over the field $\mathbb{F}_p$, respectively. Then, the computing cost of the left-to-right

Montgomery ladder is,

$$n \cdot (4\mathbf{m} + 1\mathbf{m_{a24}} + 1\mathbf{m_{uP}} + 4\mathbf{s} + 8\mathbf{a}) + 1\mathbf{m} + 1\mathbf{i}.$$

More specifically, at the 128 bits of security level, the X25519 function costs,

$$1021\mathbf{m} + 255\mathbf{m_{a24}} + 255\mathbf{m_{uP}} + 1020\mathbf{s} + 2040\mathbf{a} + 1\mathbf{i},$$

where each operation is performed in the prime field $\mathbb{F}_{2^{255}-19}$. At the 224-bit security level case, the cost for computing the function X448 is,

$$1793\mathbf{m} + 448\mathbf{m_{a24}} + 448\mathbf{m_{uP}} + 1792\mathbf{s} + 3584\mathbf{a} + 1\mathbf{i},$$

with the arithmetic operations being carried out in the prime field $\mathbb{F}_{2^{448}-2^{224}-1}$.

5 How to (pre-)compute a ladder

Our proposal for improving the performance of the X25519 and X448 functions focuses in the first phase of the Diffie-Hellman protocol (see Alg. 1). There, the scalar multiplication is performed in the fixed-point setting. More specifically, the point operand is always the base-point described in the [19] document (see §3 for more details).

One possible solution for taking advantage of this scenario was published in [2]. In short, the authors pre-compute the points $P_{ij} = i16^j P$, for $1 \le i \le 8$ and $0 \le j \le 63$ and represent the Curve25519 in Edwards form to process the scalar multiplication through a windowed variant of the traditional double-and-add method. In addition to the significant amount of required memory space, the main drawback of this approach is that complex cache-attack countermeasures need to be applied during the retrieval of the pre-computed points P_{ij}, which go against the principle of implementation simplicity promoted in [4,27].

Thus, instead of designing a timing-protected double-and-add algorithm, we suggest using a slightly modified version of the right-to-left Montgomery ladder presented in [25] as explained in the following subsection.

5.1 Right-to-left Montgomery ladder with pre-computation

The operating principle of Algorithm 4 is to compute $Q = kP$ using the Montgomery differential arithmetic formulas for the point doubling and point addition operations. This is achieved by recording and storing the difference $R_0 - R_1$ in the point R_2 through the whole execution of the procedure. Indeed, in the case that the bit $k_i = 1$, then R_0 is added to the accumulator R_1 (Step 6) and the difference R_2 does not change, since the operation $2R_0 = R_0 + R_0$ is performed in Step 10. On the other hand, if $k_i = 0$, nothing is added to the accumulator R_1, so it is necessary to increase the difference R_2 by R_0 (Step 8) in order to account for the unconditional doubling performed in Step 10. Notice that at each iteration, the accumulator R_1 is updated in the same fashion as it would

Algorithm 4 Right-to-left Montgomery ladder

Input: $P = (u_P, v_P) \in E_A(\mathbb{F}_p)$, $k = (k_{n-1} = 1, k_{n-2}, \ldots, k_1, k_0)_2$
Output: $u_{Q=hkP}$

Pre-computation: Calculate and store u_{P_i}, where $P_i = 2^i P$, for $0 \le i \le n$
Initialization: Select an order-h point $S \in E_A(\mathbb{F}_p)$
$R_0 \leftarrow P$, $R_1 \leftarrow S$, $R_2 \leftarrow P - S$
for $i \leftarrow 0$ **to** $n - 1$ **do**
  if $k_i = 1$ **then**
    $R_1 \leftarrow R_0 + R_1$
  else
    $R_2 \leftarrow R_0 + R_2$
  end if
  $R_0 \leftarrow u_{P_{i+1}}$
end for
return $u_Q = hR_1$

be done in a traditional right-to-left double-and-add algorithm. It follows that at the end of the main loop, $R_1 = kP + S$.

The reason why the accumulator R_1 must be initialized with a point $S \notin \langle P \rangle$ is because the Montgomery differential formulas are not complete. Hence, one must prevent the cases where $R_0 = R_1$ or $R_0 = R_2$. One can get rid of S by performing a scalar multiplication by the cofactor h, thus obtaining,

$$hR_1 = h \cdot (kP + S) = hkP + hS = hkP.$$

Notice that for Montgomery curves, the cofactor h is as little as four. So this last correction does not represent a computational burden. Furthermore, in § 5.2 we show a trick specially tailored for the X25519 and X448 functions, which eliminates the point S at almost no cost, and that allows us to return the correct $R_1 = kP$ result. Nevertheless, we stress that the points S and $P - S$ can be clearly specified beforehand and therefore, this matter should not bring any complications for the programmer.

Remark 1. Given that the difference between R_0 and R_1 is volatile, the point addition formula requires an extra field multiplication as compared with the formulas for the classical ladder of Algorithm 2. This is basically because R_2 is now represented in projective coordinates, which means that its Z-coordinate value will be in general different than one. For that reason, it is not practical to use this ladder variant for variable-point scenarios. Nonetheless, if the point P is known a priori, this overhead can be compensated by pre-computing the u-coordinates of the multiples $2^i P$ in affine coordinates which, at the price of memory storage, saves the calculation of $n - 1$ point doublings in the main loop and two field multiplications in the point addition formula.

Remark 2. In order to save a few extra field additions/subtractions, the computation of the point addition $R_3 \leftarrow R_0 + R_1$, with $R_2 = R_0 - R_1$, can be done in accordance with the first version of the formulas presented by Peter Montgomery in [21] as,

$$U_{R_3} \leftarrow Z_{R_2}(U_{R_0}U_{R_1} - Z_{R_1}), \qquad Z_{R_3} \leftarrow U_{R_2}(U_{R_1} - Z_{R_1}U_{R_0}).$$

In our case, $Z_{R_0} = 1$.

Remark 3. Notice that no side-channel countermeasures are required to retrieve the coordinates u_{P_i} from memory, since they are public and do not have any direct correlation to the sensitive information contained in the scalar k.

5.2 Implementing the pre-computable ladder

Before presenting a low-level description of the known-point scalar multiplication using Algorithm 4, we must examine the point S selection and how to better process the bits of the scalar k.

Strategies When selecting the private key k (Alg. 1, Step 1), presumably to facilitate the programming effort, the X25519 specification [19] recommends to generate 32 bytes at random as $k = K_0 + K_1 2^8 + \ldots + K_{31} 2^{248}$ with byte-words $K_i \xleftarrow{\$} [0, 255]$, and to perform the following operations:

$$K_0 \leftarrow K_0 \wedge 248, \qquad K_{31} \leftarrow K_{31} \wedge 127, \qquad K_{31} \leftarrow K_{31} \vee 64,$$

where the symbols $\wedge$ and $\vee$ represent the logical conjunction and disjunction operators. For the X448 function, 56 randomly-chosen bytes are required, which are further processed as

$$K_0 \leftarrow K_0 \wedge 252, \qquad K_{55} \leftarrow K_{55} \vee 128.$$

Those procedures are equivalent to compute, respectively,

$$k'' \xleftarrow{\$} [0, 2^{251} - 1], \qquad k' \leftarrow k'' + 2^{251}, \qquad k \leftarrow 8 \cdot k'$$

and,

$$k'' \xleftarrow{\$} [0, 2^{445} - 1], \qquad k' \leftarrow k'' + 2^{445}, \qquad k \leftarrow 4 \cdot k'.$$

Consequently, we decided to process only the bits of k' in the main loop of our function. At the end of the algorithm, as we eliminate the point S from the accumulator by multiplying it by h, we will have the correct resulting point $Q = h \cdot (k'P + S) = kP$. In order to obtain a non-invasive procedure with respect to the RFC specification, we simply start processing the scalar from the $(\log_2 h + 1)$-th bit of k.

Point S selection In the Curve25519 setting, we could select an order-8 point S. However, because of its elegant u-coordinate, we decided to choose the order-4 point:

$$u_S = \texttt{0x1},$$
$$v_S = \texttt{0x141B0B6806563D503DE05885280B59109CA5EE38D}$$
$$\texttt{7B56C9C165DB7106377BBD8}.$$

The point $P - S$ is given by:

$$u_{P-S} = \texttt{0x215132111D8354CB52385F46DCA2B71D440F6A51E}$$
$$\texttt{B4D1207816B1E0137D48290},$$
$$v_{P-S} = \texttt{0x5199331F1F5630BBFA49B1B1B02B207B493D0A63B}$$
$$\texttt{B4F8F01C011242F9C6E9E7C}.$$

For the Curve448, the order-4 point S is given by:

$$u_S = \texttt{0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE}$$
$$\texttt{FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE},$$
$$v_S = \texttt{0x45B2C5F7D649EED077ED1AE45F44D54143E34F714B71AA96C945AF01}$$
$$\texttt{2D1829750734CDE9FADDBDA4C066F7ED54419CA52C85DE1E8AAE4E6C}.$$

And the (u, v) coordinates of $P - S$ are:

$$u_{P-S} = \texttt{0xF0FAB725013244423ACF03881AFFEB7BDACDD1031C81B9672954459D}$$
$$\texttt{84C1F823F1BD65643ACE1B5123AC33FF1C69BAF8ACB1197DC99D2720},$$
$$v_{P-S} = \texttt{0x45CD0137F88682464AE12E4E2CFCEA7E9360F6FE1E04AE1C5065F397}$$
$$\texttt{533F2282EE2643E610A0CC8E9B07D43D47C9658D05E22F0F077395DD}.$$

Algorithm Next, in Algorithm 5, we present the low-level details of our approach. Again, the term n represents the bit length of $\#E_A(\mathbb{F}_p) = h \cdot r$ and $q = \log_2 h$. [7] The pre-computation phase (Step 1) consists of computing the multiples $2^i P$ and store their u-coordinates. These $n - q$ coordinates are computed a priori from the base-point P and their values are listed in Appendix A for both, Curve25519 and Curve448. Assuming that the architecture is byte-addressable, the memory space required for Curve25519 is approximately $(255 - 3) \cdot 32B \approx 8KB$, while in the Curve448 setting, we need $(448 - 2) \cdot 56B \approx 25KB$.

The conditional swap function is identical to the one used in Algorithm 3. However, in this case the inputs are the coordinates of the accumulator R_1 and the difference point R_2. Moreover, the s variable that controls the swap is set to one, since the Montgomery point additions, in terms of memory location, are

[7] For the sake of simplicity, in the remaining of this paper it will be assumed that h is a small power of two.

Algorithm 5 Low-level right-to-left Montgomery ladder

Input: $P = (u_P, v_P), S = (u_S, v_S), P - S = (u_{P-S}, v_{P-S}) \in E_A/\mathbb{F}_p$, $a_{24} = (A+2)/4$
$k = (k_{n-1} = 1, k_{n-2}, \ldots, k_1, k_0)_2$

Output: $u_{Q=kP}$

1: **Pre-computation** u_{P_i}-coordinates of $P_i = 2^i P$, for $0 \leq i \leq n-q-1$
2: **Initialization:** $U_{R_1} \leftarrow u_S$, $Z_{R_1} \leftarrow 1$, $U_{R_2} \leftarrow u_{P-S}$, $Z_{R_2} \leftarrow 1$, $s \leftarrow 1$
3: **for** $i \leftarrow 0$ **to** $n-q-1$ **do**
4: `# timing-attack countermeasure`
5: $s \leftarrow s \oplus k_{i+q}$
6: $U_{R_1}, U_{R_2} \leftarrow \text{cswap}(s, U_{R_1}, U_{R_2})$
7: $Z_{R_1}, Z_{R_2} \leftarrow \text{cswap}(s, Z_{R_1}, Z_{R_2})$
8: $s \leftarrow k_{i+q}$
9: `# addition`
10: $A \leftarrow U_{R_1} \times u_{P_i}$; $B \leftarrow Z_{R_1} \times u_{P_i}$
11: $A \leftarrow A - Z_{R_1}$; $A \leftarrow A^2$
12: $B \leftarrow X_{R_1} - B$; $B \leftarrow B^2$
13: $U_{R_1} \leftarrow Z_{R_2} \times A$
14: $Z_{R_1} \leftarrow U_{R_2} \times B$
15: **end for**
16: **for** $i \leftarrow 0$ **to** $q-1$ **do**
17: `# doubling`
18: $A \leftarrow U_{R_1} + Z_{R_1}$; $A \leftarrow A^2$
19: $B \leftarrow U_{R_1} - Z_{R_1}$; $B \leftarrow B^2$
20: $U_{R_1} \leftarrow A \times B$
21: $A \leftarrow A - B$
22: $Z_{R_1} \leftarrow a_{24} \times A; Z_{R_1} \leftarrow Z_{R_1} + B; \mathbb{Z}_{R_1} \leftarrow Z_{R_1} \times A$
23: **end for**
24: $Z_{R_1} \leftarrow Z_{R_1}^{-1}$
25: $u_{R_1} \leftarrow U_{R_1} \times Z_{R_1}$
26: **return** $u_Q \leftarrow u_{R_1}$

always performed as $R_1 \leftarrow R_1 + 2^i P$ throughout the algorithm. Also, given that the most significant bit k_{n-1} is always equal to one, it is unnecessary to include another couple of *cswap* functions after the main loop. At the end of the function (Steps 16-23), we must perform q consecutive point doublings to process the least significant bits of k and to eliminate the point S from the accumulator R_1.

Cost estimations The cost of the Algorithm 5 can be estimated as

$$(n-q) \cdot (4\mathbf{m} + 2\mathbf{s} + 2\mathbf{a}) + q \cdot (2\mathbf{m} + 1\mathbf{m_{a24}} + 2\mathbf{s} + 4\mathbf{a}) + 1\mathbf{m} + 1\mathbf{i}.$$

If the Curve25519 is used, then $n = 255$ and $q = 3$. As a result, the fixed-point scalar multiplication would cost

$$1015\mathbf{m} + 3\mathbf{m_{a24}} + 510\mathbf{s} + 516\mathbf{a} + 1\mathbf{i},$$

where the arithmetic operations are over $\mathbb{F}_{2^{255}-19}$. In the Curve448 context, $n = 448$ and $q = 2$. As a consequence, we have the following cost in terms of

$\mathbb{F}_{2^{448}-2^{224}-1}$-operations:

$$1789\mathbf{m} + 2\mathbf{m_{a24}} + 896\mathbf{s} + 900\mathbf{a} + 1\mathbf{i}.$$

These results show that, while our approach does not save much in terms of general field multiplications, it completely eliminates the multiplication by u_P [8] and drastically reduces the number of multiplications by the constant $(A+2)/4$. In addition, it saves half of the field squarings and about three quarters of additions/subtractions.

For the programmer, the only extra effort is to organize the pre-computed points in the memory and load them during the main loop execution, since the remaining field and logic operations are very similar to ones presented in Algorithm 3. In the next subsection, we present a comparative based on the arithmetic of state-of-the-art software implementations.

5.3 Comparison

In this part, we present a more concrete analysis of the performance efficiency of Algorithm 5. For this purpose, we measured the field arithmetic cost of different state-of-the-art constant-time software implementations of the Diffie-Hellman protocol on Curve25519 and Curve448. After that, we computed the ratios of $\mathbf{m_{a24}}$, $\mathbf{m_{uP}}$, $\mathbf{s}$ and $\mathbf{i}$ to $\mathbf{m}$, which are considered the most representative field arithmetic operations for scalar multiplication implementations. As a result, we were able to show the practical savings of our proposal in terms of general field multiplications $\mathbf{m}$.

Regarding the X25519 implementations, we selected the code from Bernstein et al. [2], which represents the $\mathbb{F}_{2^{255}-19}$ elements in radix-2^{51}, the AVX2 approach from Faz-Hernández and López [12] and the curve25519-donna library from Langley [18]. [9] For the X448 function, we considered the original implementation of Hamburg in [14]. The source code of [2,14] were downloaded from the eBACS [3] web page, the [12] implementation was shared by its authors via personal communication and the curve25519-donna library was retrieved from its GitHub repository [18].

Every field arithmetic code was compiled with the clang/LLVM compiler version 3.9 with optimization flags `-O3 -march=haswell -fomit-frame-pointer` and further benchmarked in an Intel Core i7-4700MQ 2.40GHz machine (Haswell architecture) with the Hyper Threading and Turbo Boost technologies disabled. The ratios are presented in Table 1.

[8] In fact, given that the difference of the point operands $P_i - R_1$ is variable, the $\mathbf{m_{uP}}$ operations were changed into two general multiplications and were included in the $\mathbf{m}$ operation count.

[9] The benchmarking reports in [3] shows that the library of Chou [7] currently holds the speed record on computing the scalar multiplication over Curve25519. However, the author decided to embed the field arithmetic functions into the ladder step, in a single assembly code. Isolating the field operations would be impractical and could alter the author's original intentions.

Table 1. Ratios of selected arithmetic operations to the general field multiplication in state-of-the-art software implementations

Implementation	Ratios to **m**				
	$\mathbf{m_{a24}}$	$\mathbf{m_{uP}}$	**s**	**i**	**a**
Bernstein et al. [2]	0.23†	0.23†	0.76	203.29	< 0.1
Faz-Hernández and López [12]	0.28	0.41	0.96	84.33	< 0.1
Langley [18]	0.60	1.00‡	0.82	192.55	< 0.1
Hamburg [14]	0.24	1.00‡	0.75	405.00	< 0.1

† Estimated

‡ The general field multiplication (**m**) is used to implement this operation

The cost of the $\mathbf{m_{a24}}$ operation in the Bernstein et al. implementation was estimated as follows. After analyzing the assembly code, we concluded that $\mathbf{m_{a24}}$ takes 10 `movq`, 5 `mov`, 5 `shr`, 5 `add`, 4 `addq`, 5 `mulq` and 1 `imulq` machine instructions. Next, we added its latencies [13] and, to calculate a lower bound of our speed improvements, we applied an aggressive throughput of 0.25. Finally, given that the $\mathbf{m_{uP}}$ is similar to the $\mathbf{m_{a24}}$ operation, we also assumed a similar cost. In Table 2, we present the performance improvements of our proposal in terms of the general field multiplication.

Table 2. A comparative between Montgomery-ladder approaches in the fixed-point scenario

Implementation	**Estimated costs** †		**Diff.**
	Mont. ladder left-to-right (Alg. 3)	Mont. ladder right-to-left (Alg. 5)	
Bernstein et al. [2]	2116.89**m**	1606.68**m**	-24.10%
Faz-Hernández and López [12]	2260.48**m**	1589.77**m**	-29.67%
Langley [18]	2457.95**m**	1627.55**m**	-33.78%
Hamburg [14]	4097.52**m**	2866.48**m**	-30.04%

† Because of its negligible cost, the field addition/subtraction operation was not included

The above comparison suggests that at least a 24.10 to 33.78% of speed-up can be reached in the first phase of the ECDH protocol by using Algorithm 5. When considering the complete Diffie-Hellman scheme, the improvement ranges from 12.05 to 17.68%. In practice, these estimated savings can be further improved if we take into consideration compiler optimizations and the machine throughput. In addition, while the field addition/subtraction cost is imperceptible if measured separately, it constitutes a significant part in the whole protocol execution timings.

6 Conclusion

In this note, we presented an alternative way to compute the elliptic curve Diffie-Hellman protocol with Montgomery ladders. Particularly, we focused on the key-generation phase, which can be characterized as a fixed-point scenario. For this phase, we assumed that the relevant multiples of the base-point can be pre-computed off-line, which helps to boost the computation of the scalar multiplication via a right-to-left variant of the Montgomery ladder. As a result we achieved, in the Curve25519 setting, estimated performance improvements that range from 24 to 34% of speedup, at the price of just $8KB$ of memory space. Our proposal carefully minimizes coding modifications with respect to the specifications given in the RFC 7748 memorandum.

Currently, we do not have a high-speed software implementation of our approach. However, we provide in Appendix B, a Magma [5] script of our X25519 alternative function, which shows that the generated public keys are in accordance with the test vectors listed in [19, §6.1]. In the near future, we intend to work on software implementations targeting different architectures to evaluate the real optimization speed-ups that can be accomplished by our approach.

We also would like to explore the potential savings that our ladder approach can bring for digital signature protocols and other elliptic-curve based protocols. Finally, building on the work of [26], we would like to explore a Montgomery ladder variant, which can be applied to prime elliptic curves equipped with efficient endomorphisms such as the Four$\mathbb{Q}$ elliptic curve [8]. For that kind of elliptic curves, the ladder variant presented in [26], allows for an important saving in the number of required point doubling operations when working in the fixed-point scenario.

Acknowledgments

We would like to thank Daniel Cervantes for his useful comments and Armando Faz-Hernández for sharing with us insightful comments about the point multiplication software library reported in [12].

References

1. D. J. Bernstein. Curve25519: New Diffie-Hellman Speed Records. In *Proceedings of PKC 2006*, volume 3958 of *LNCS*, pages 207–228. Springer Berlin Heidelberg, 2006.
2. D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang. High-speed high-security signatures. *Journal of Cryptographic Engineering*, 2(2):77–89, 2012.
3. D. J. Bernstein and T. Lange. eBACS: ECRYPT Benchmarking of Cryptographic Systems. `https://bench.cr.yp.to`. Accessed in Mar 2017.
4. D. J. Bernstein and T. Lange. SafeCurves: choosing safe curves for elliptic-curve cryptography. `http://safecurves.cr.yp.to`. Accessed in Mar 2017.

5. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
6. Certicom Research. SEC 2: Recommended Elliptic Curve Domain Parameters, 2010. Version 2.0. Standards for Efficient Cryptography. `http://www.secg.org/sec2-v2.pdf`.
7. T. Chou. Sandy2x: New Curve25519 Speed Records. In *Proceedings of SAC 2015*, pages 145–160. Springer International Publishing, 2016.
8. C. Costello and P. Longa. Four$\mathbb{Q}$: Four-Dimensional Decompositions on a $\mathbb{Q}$-curve over the Mersenne Prime. In *Proceedings of ASIACRYPT 2015*, volume 9452 of *LNCS*, pages 214–235. Springer, 2015.
9. C. Costello and B. Smith. Montgomery curves and their arithmetic: The case of large characteristic fields. Cryptology ePrint Archive, Report 2017/212, 2017.
10. W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
11. ECC Brainpool. Standard Curves and Curve Generation, 2005. Version 1.0. `http://www.ecc-brainpool.org/download/Domain-parameters.pdf`.
12. A. Faz-Hernández and J. López. Fast Implementation of Curve25519 Using AVX2. In *Proceedings of LATINCRYPT 2015*, pages 329–345. Springer International Publishing, 2015.
13. A. Fog. Instruction tables: Lists of instruction latencies, throughputs and micro-operation breakdowns for Intel, AMD and VIA CPUs. `http://www.agner.org/optimize/`, 2016.
14. M. Hamburg. Ed448-Goldilocks, a new elliptic curve. Cryptology ePrint Archive, Report 2015/625, 2015. `http://eprint.iacr.org/2015/625`.
15. N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of computation*, 48:203–209, 1987.
16. P. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *Proceedings of CRYPTO 99*, volume 1666 of *LNCS*, pages 388–397. Springer Berlin Heidelberg, 1999.
17. P. C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems. In *Proceedings of CRYPTO 96*, volume 1109 of *LNCS*, pages 104–113. Springer Berlin Heidelberg, 1996.
18. A. Langley. curve25519-donna. `https://github.com/agl/curve25519-donna`. Accessed in Mar 2017.
19. A. Langley, M. Hamburg, and S. Turner. Elliptic Curves for Security, 2016. Request for Comments. `https://tools.ietf.org/html/rfc7748`.
20. V. S. Miller. Use of elliptic curves in cryptography. In *Proceedings of CRYPTO 85*, volume 218 of *LNCS*, pages 417–426. Springer Berlin Heidelberg, 1986.
21. P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48:243–264, 1987.
22. National Institute of Standards and Technology. FIPS PUB 186-4: Digital Signature Standard (DSS). Federal Information Processing Standards, 2013. `http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf`.
23. National Institute of Standards and Technology. NIST Removes Cryptography Algorithm from Random Number Generator Recommendations, 2014. `https://www.nist.gov/news-events/news/2014/04/nist-removes-cryptography-algorithm-random-number-generator-recommendations`.
24. National Institute of Standards and Technology. Special Publication 800-90A Rev.1: Recommendation for Random Number Generation Using Deter-

ministic Random Bit Generators, 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf.
25. T. Oliveira, D. F. Aranha, J. López, and F. Rodríguez-Henríquez. Fast Point Multiplication Algorithms for Binary Elliptic Curves with and without Precomputation. In *Proceedings of SAC 2014*, volume 8781 of *LNCS*, pages 324–344. Springer Berlin Heidelberg, 2014.
26. T. Oliveira, J. López, and F. Rodríguez-Henríquez. The Montgomery ladder on binary elliptic curves. Submitted to Journal of Cryptographic Engineering, 2017.
27. K. Patterson. Formal request from TLS WG to CFRG for new elliptic curves. Crypto Forum Research Group archives, 2015. https://mailarchive.ietf.org/arch/msg/cfrg/Hvihr_yQhVB_Qdl-mtwTdVbHGiU.
28. N. Perlroth. Government Announces Steps to Restore Confidence on Encryption Standards. *New York Times*, 2013. https://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/.
29. N. Perlroth, J. Larson, and S. Shane. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *New York Times*, 2013. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.
30. E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3, 2017. Internet-Draft. https://tools.ietf.org/html/draft-ietf-tls-tls13-19.

A Pre-comupted points

Tables 3 and 4 list the pre-computed u-coordinates of the multiples 2^iP for the functions X25519 and X448, respectively.

A.1 X25519

Table 3. Pre-computed u-coordinates of the multiple points $2^i P \in E_{486662}(\mathbb{F}_{2^{255}-19})$, for $0 \leq i \leq 251$

i	$u_{2^i P}$-coordinate
0	0x9
1	0x20D342D51873F1B7D9750C687D1571148F3F5CED1E350B5C5CAE469CDD684EFB
2	0x79CE98B7E0689D7DE7D1D074A15B315FFE1805DFCD5D2A230FEE85E4550013EF
3	0x275FA6D7AAD65C2DD83B884DC8B65CA17A78EDCAAD74A91EF1716FED48C99968
4	0x32B9DE1FE60CD384092C29D3743DAFF60EECD85AB67F137E9A756061D03D1F56
5	0x225702830BDB66F2179D9B857B1796CDB0E1A9ECA08F211A1173EFED732B584F
6	0x383EC61DBB0A08C73164CEEF8414550BB4EE26621848FD63479B4ADB55092DA8
7	0x2750F78D9193A117A7B368314FD7C0E1DF4A5CCB10020DC5D836793D9525ECB9
8	0x4300017536976A742EC8747F7505CD6BC80E610D669ACAB1A1EED36F680D98E8
9	0x77E26C20F461B757AB588C22B7C01423B1EB4F94F64C2F3E3E19B08A2F34AD91
10	0x6CF7675455043271CD82EBFEB999E7F1FB9E1A65E2534B15F28F1F17911BC25A
11	0x70E9A9F4DC26E6A684D27C6B95F9663852F685F59A4BCD86048275C88FADC08E
12	0x164CA945E90BF20C9C4382723929B893FEDE061E4C23B57C18270048BD5AF144
13	0x713F86C3ECD70086F45513BC35CE26884F2E53DECE130D4DC95EE68DF5338A30
14	0x6D86CBEA7630F1AF147937E160CD88247871FAFB98A1E5D970A7513152C01CD1
15	0x48FE50F21D91AA1C462ABF6518F263DFBA7F1BB3E1DC4FD8C6615A4A92C66AA8
16	0x78D56B996581973DBC3B124C1B9C8796DBDB8ECC61673F3C2E6EF372157B5FBB
17	0x726CA3EA9D9D544BED383A009627BD621B50F0A60E584435CC2A16E4CCDB3E6
18	0x6DCE203294D89D1903C23FC563A8F1B3869A30C2E2285F7D04ED75D54384FA1A
19	0x44E368C03660D9B3B6370952A9A16C2184A36AE78073FE2265B51242E03E459E
20	0x138EED350AFA8E181BACD1C9839B74D9691240251E82FAE8D6441AD5BD1BE747
21	0x3CB7754217FE24F74B201ECB65F47B27AB9939CB27D1783621761D723C35AC8C
22	0x631024BE83846BA1127BCE1B470CC5418AF3F3C01101E581C0D5B52ACBA552AE
23	0xA731BC34FDEFC26CA95055D36F94D37EB8BF476184EE8C235252027E3B43E22
24	0x33E342AF57F94619983D7D942C47B14BE611374D4064CB444CC2CDE638B46DE8
25	0x152B0BA37A3B4B0F439C7C8DF54C5B72245B9D13462A89239BF204B45964C76A
26	0x5EBF100C71D364B3C03A684D680239026BAF2E807B32F96C25CA4B28C07E950E
27	0x4CD087E96ABAD6C575145FEDA4E0EE5A44F4250A5862415956C9DE701AD2B6FE
28	0x6893CEDBCF053A23B7D5676BF577DBC309D25C8525A0F2F5036B67F0967FA084
29	0x47A9764A579C54A66E97C5B5DAC2B4E851B65398083FAFCFCC67B0AB49E72BA4
30	0x5B7BD9A03F1B6296F302B25FD458CF8F987159031CFA933018B0818C9FE60E09
31	0x2D964FA3C55CDBDB379EB67A71AE3FCA74B39F689000CBDB658A1E33BFE14C52
32	0x6A8E0BFAB511D23D72DDC7E8B0D4E3561183208D3D7886C269A92CA1DE7DC30
33	0x44BA5F7122A7037DC549254F7BB94806ACA31F8245D65C6FC97CAA704ABB685C
34	0x3049227132DB5D63288D3966ABC13AFDA5F448FFEF1516FD31826F3FFE604382
35	0x504C367CBFEF1D7E37E0C7ED6C274DF5F1BC87CFE94CB52504925D5391D1C039
36	0xC473E7D3FF03058666B4BF5975C6F05B4DF9E855FC9B5AB416DC59CF0984F84

Table 3. Continued from previous page

i	$u_{2^i P}$-coordinate
37	0x733C0497DB75FA40D84F22E98C6D7661D282910E70C855344547BBEC3097E663
38	0x68BBAB49A5F7F20AE525C2832DE2658F882747069B24A72F3BDAECCB18E7C90
39	0x7253CDC84A5842EA56479796FBF9574AEE87D8171421E67350CDCFC1F6C030C8
40	0x316DD22533B8C9EF101F1C691228B46210BFD6EB8B9EA8F3411F13EC850643A5
41	0x69FF58BEAF8E4D9EE8431972C74CB76D3440DE7ECD2B8CD81F68299A9375BBC3
42	0x1E8CA67880D693D2F198C5D1E65707B9967708F6C60B88FA3D56EAF415BC702E
43	0x716047EE80EAF383585FBCEEC6BABC4B292D6034A9CDE7AF8AD8C9A1DAA261A1
44	0x19F7B46135A1D4637F1731091FC8195B214CA5F89057CAEA4520C23D8185FCCF
45	0x7DCD1A2404E2EF0D53B61FF9FC7AD742260583F5573932EB107CCD8271C03A7
46	0x351840915043ADCD04EA20BA677DA28CF905E25AD57D2FEB325EEF65C492DA7
47	0x3AE2723F54724401A5CC05498BA8B8347B2638F23630C68FC58669B2C93C6562
48	0x6DAD68316E7B98AF3CC8A62697340B5F6CCD1C4BB5353FA1905223BEF8A2B40E
49	0x3672A790EB6683B89587A244667100C7EFF5269AD66A344FE6B13798432C1308
50	0x4FA7427358C550806481662855407FB2D41B3E6F9BC0C923D6DA166587502DD3
51	0x2700C58D2E148DE161D88319276E8C79E77E2FAE91135D271DCE26514785BF3B
52	0x65570803693BBB3DAEF94487CCAB79F0F4747CF68C0348755AD706F8E60CED92
53	0x1496E2ED1DD388D91786AE9208654D2B48AD5E478890C6B47B1E0CFB3C343F38
54	0x473A0A71500924A1E75CE4A05F1F8390550EF64046734FD66C4ABDCE1AA04D98
55	0x28ACBEEE1CAD574CE4F84E469F8AAF63E0116EADB45CF05F5DCBC01DD25B486B
56	0x74FBDEC3F21F1468E1CF08BE13F2133537DC2C1B4F888D59E1080A830239691D
57	0x5CA32C1CB7936CF0FB18514B57922BD544344B8EC1C97B3B6C98B5BDAE8D5BD9
58	0x3294569BCFA09314603F65E3D8AA139AD65403839781E76205DA0202DC252634
59	0x15B35861C03829E2737C2A24EC93640BC8616AF266773BDE4AA736887DD941DD
60	0x733350C17ACEBBBAFC697EA8B5F03B354BF7AE172F54E86E883B59D150D1B370
61	0x68EB9D1BEF9ACD199F5D7C52C2FA75F882828B21518B2288AC989DCA123A5F59
62	0x4E93BB962572AEC0302B5867BBE1842DDA4C48F44D7C5274F768DDA753B4A03B
63	0x2AA29215FD79CA46A578DC25F516D03DDA7E58F8BE9D2CE426114BF5EB14DFE4
64	0x70E6554F481DD6856EB8F924D9D7A99F3B4204AC2C531FE1FD86D0D8D78881C
65	0x83F00E1C86D82A2F7846563BDA5927E950F028E35E48C857611E86540EE929D
66	0x46D5FE296C841ADDBC6918510DB9AE915BBB081634967BA8BFF03A0E899029DD
67	0x549334D92260AF1021C71E1F9B278F2A6E0A4B2CEF3334AC499625D1A1925271
68	0x44C5C8ED8DED7AAD4CDC942074A4EAC5B0968BD2709C70E2FF23972C9AD37990
69	0x6E4D3B92C30171AE119250BEF16CC777A36C203694F58B9BC79EE0782AF5E5E0
70	0x58F8F796339F667EE943D148CB35930AC7FC8FDC59D15B1AE9AD73FE46C7DA6D
71	0x571F6D8AE6D6E1C7F6DC2F529813F38245258DB6BDB92051C664612028B89B49
72	0x69F56B8AA94E013DC9563B0833CA80FC637309A37E2F1B4D8CD25C8CADF00A3D
73	0x5F7D48AFAC2E89DC400B9E75FD8C4B3FB70F69CEFEDD49A06906CB906615A56A
74	0x8305E3B24781177AD8BF3D1257C8A9EB6227409B5DC3B518D68576065C6AA9D
75	0x7BB70A72B7B9DC6227AC8101D054E7DEA2CD07CFDDC4D7990C8E91736DF74E6B
76	0x3D3710779DD891EDE81407D2E7F83BF7B023A046A55892C68DCBE5800F8D7539
77	0x344961169E9D6D96ECCA6E05BDBD6D9B51955E7E902812D0BEAEC747EC6CB182
78	0x7AC0039090B1D5DD02BA00AFBBE4797DC3875C06B769635D93D14171740F3276
79	0x62AD527A779F0CAEEA8B8EEE68C1A1EC0DC395EE1DE73ADFE3E84B6AF6CBB10A
80	0x29F5446637DF7928C01F72B5EEEC05F72410A04C74953AE70E885191C0EF7BB
81	0x1848DDDDF05261863D205150E174BD119C65DEFC7367E9A0ADBCE95EFAA896F
82	0x60E7A5961CEA64FFD14916BF3420D14908A2B525DBF2209E9ECAAB07A0301DA1

Table 3. Continued from previous page

i	$u_{2^i P}$-coordinate
83	0x195C3B6D9E2E22790BD78B071A3AB2597D4B3AEC7F766094FFC75142F43013CB
84	0x71DDAAECA14FED726BC7D262765A99C3493DFE91D793A257378188B3D41505E
85	0x212BDDF24D81FCB2E5C85DBB6F277181E27B438835CE18B673E9FB6E0401A72E
86	0x25E445FDAF7170DFC2AB011D1954EDA15116AB2349D41FCF28E421D4CEACA69B
87	0x28E66E4250896D3D768ECFBD723EC0AB35C480F4736C73D834D77B4ED57F1C62
88	0x75DB973256578F67CA23E1E3324CE3F3AB87D627BBE1CE2A71ECA744319244A1
89	0x1E0357163AD7146BB565BFEE3F397893E6F9DA97601E0628EC0B8F228CAD4C23
90	0x430F23EE2039D9F6C6D7043E791038F9DFE3856292A0F2799FD49E7AB85D08D8
91	0x31BA059A821A8B8287995D4A13CAF97D590D599530508FF7529F5B8B70EF9277
92	0x50F90FFEE58350F8DF9D5E8012DA5DCF1A4F785BEEA4D15DD2376C923AE08469
93	0x1B8C5EF8E0A65CADFE08468694F27987ADD268D3E1EB677CD20D47B051627E1E
94	0xF3467CB7D5370A00EF175DBF1D428148E5E40626592228E24288E5AB2A2FFB4
95	0x160D64680BB982074BFFC5D98F9124C44A4A5A383F7FB8135A9150D34E3B0EC2
96	0x13B92ED74D3B0F2EFCAEC64D09ED5C008258817FDD4AAB389DD4CE4324F9A5A4
97	0x6B23C6EE9D8015819CA8D328AB7A93DDEE926B707D4832F9C4795771924D9DD9
98	0x7E6765C93F067ABBF04292137C10E3034161C26760EF6B70EE2DDA1DC8727A5
99	0x662DF48860D0CE671CA1C913540ED91FF207177B15B976F13C4434D4DED0490A
100	0x5ACDDCCE87C39B1BB65DC2630F63CD08E7DF7DCCD04C90022C4AE26DD44D6263
101	0xB22A9A2625954BB25C3093DE918B2E595E664441C5740477121703698666F4B
102	0x644371F381B323E75D1FC05294D17F159222860C64B783928FDB54782A034629
103	0x4BFE9C79CF6DBBB95DCDF037B5A90CF677B1D10A6492A033DEACE0B18ED38E62
104	0x7F7CCEAFF56198C5DE3F9FE24AFF630C68F978EE968E9CCC451B2F3CD8053B74
105	0x6A4BD29824984678B1A4FB0441A439D2C9DF96E4BB50C722D0F68E6C37D16BA6
106	0x6590CA8B831BA9520BFE910FF17AB22E7B9AEF3994C23F592299F46AA58C166E
107	0x623E17243B220968030F56AFB8CF02BF4E76752C23ECA105BD16AD890B73DBCD
108	0x2C47072CF350AF0FF90D65C512EE3907E3AF9F5D4147A0B9DBB734BD102E9D7
109	0x5451B13D931278A338CAF5C0EE29AE5F7C914CC596A59EA08307B28D41F2A89A
110	0x1B5A4F8C173B166D6C4E4E7FB14BC2E6F3995A04E30873592FF93A0B841BF6E1
111	0x62E856A09537053B1C7EF7D5BF376EEC35BD3A8F90A8CE8ED5C385AE313DFE35
112	0x2EBFDB18BDB8DD91BF0A020FE7C42C361B4FCD5ED7668B630FB917DB86E6E575
113	0x4A2DE0E53D3B412783687503088FED26B83FCDD1972428F8616F756694C4E90E
114	0x27A906AEAB314F04ED93156A16A620F0960B48ADE62CCF2BD190499056DB6AE0
115	0xCA73DC8B94A18256BAA560B15CAB0ACBAE4A5E9710551305F5D14A1B60223C0
116	0x45C236C92B3044E0FA3713A30CD4DBDA423B5C8782627090FF9BBB8C5DFD15C1
117	0x2A1769136407486E3CBE52CAFA7C7DC25F4549650DBD6299EAC366F9412A16E5
118	0x598DFBDB846E3312A73C6912B2A2663C27B5BCCB6D0715535261B484DF8AB611
119	0x1AB956BA87F5E55966E64DA2E003BE055A20D4BDCD8BFB100A982D945F3D5C6C
120	0x37286AF7BA6212A37AEA47752A1BFD7B0536650473C8D08B95E64C547CDDA10F
121	0x4F32FC2A0740D7691527C39DDF5EF656B5F43DD6D895ED4EBDB81B87E51DCD6B
122	0x2C56EA619E0D1AE4D10CBD4308F47238E6B3C9C78A0EB465CA97CAF8B929258E
123	0x491C778285C0B45E48DA390C69B12664FA560951F228E8A4736B976D011F1403
124	0x3CDE5CE1E90D9F8418252846522B4B52B0FA0ACF710060E2CE30EE4340BB5FD3
125	0x5E57AE7A8EB25524DEE1CADE4D8B6B5396026403C2F3AFF12740358841E56BE8
126	0x579B93607B02480F496E9AA27F1022578D7A6A539B243364786A83BAC9E1D963
127	0x5A69D580A68DE6C5C19D7537F6E6BA70F87F19049E585C88FA7A5FF5E151E820
128	0x70FD1D5462B583565DF9329E57D3B79E6985D03660782ABC3ABCAAE366B2332B

Table 3. Continued from previous page

i	$u_{2^i P}$-coordinate
129	0x525A5EFED50035D2A5A4B21BE3532F500EF90DFF97BBA0AD2883FE77BD3DFD09
130	0x68AB42D23D8F27EA737DD47DD3EC50E36696D237172C4F1D286A12A7D9C74A4D
131	0x3BA354A2CA7729C3A0874BB358CCDE7500A44A12EC48E1AAFF5682DEB8831C96
132	0x2BAA671B84BDDFD96965F100BCB925EED01DA63F02C2B66310A8CBF646FE1A8C
133	0x4D201364E5624CE5DB0232AC9DC38D19C9B8D211D5E6C798D8708AAA31CD614C
134	0x372F82A7AAD6DF229EE9CD9AC350414237E9D71FE2EA4F436E3A814E3DA80401
135	0x7F6BD7C1286F03EDE18C930F5BF875A9C21A1E14B0ECFED22C42F284FCEF9748
136	0x36342E8AD5339DAC025D6EDC0795AED5655CFDCD12E79A7DE779CF391B3B623F
137	0x715EB92F5DCF10345FFB345A0AD82F59B9FDFE73C725A6B8643EEA462C553347
138	0x394A302EA134DECD6B07BBB025B3EE5D950759E770E392A4D87FC25684DC4407
139	0x2217FB4CDEDE4E5CB6E273AFE2E0FB6B2DB3ACE247386772D25B50EBA9A2D515
140	0x56B930843E0CB5E23D3AEF4A2041DC79E4B98CF9376D4C0A5CEB8DC8CB599224
141	0x5C5A9CC436B503A4EFC634EBDFD7C6A71A7D9500DB7D56E995E9A72F9DD0FE04
142	0x49C3BA5A2D3C0BE8B878D1F84211575CEC07D1A1FBFF1BD149F904ECA8A9B2E3
143	0x6B12C7861943435D6E194D042A5A7589413E64849E44417C926D95AFBF657AD1
144	0x142B11226EF9CC5966F6720519ADCCDB5B062220310427BCDB26392BF78F77BF
145	0x5BD03323B2A2BAEF83B81580154E6FF9EF8DEC83C87947A22F6D3667B03BA3C8
146	0x14C450FBEA005EB43153501C91230EE42D8568D6383163F30539D6557E5BEA2E
147	0x4ED564301273CD1F7EF8C39B04CB3E5876F91C785B9A2BCDEE708E5CD06FC53E
148	0x2BE916B7164A4B19703F7D608FFA80199207CF7D9FF710791247DC100D93771A
149	0x36BD9D9861466826AE131394372A942A84680A9E79EA77A27088B52BA6B9EF9B
150	0x3EC7A5A5B31619584819E66C4CADBA290301D43294AE4B762C891624DF5CF45C
151	0x6481DD352481A014E2A9B502DB48EBA061A6FF473BE4A56939039BC2CF4B6E73
152	0x796638D270A0825223450142E702B0E0EA6DDC07A7A35A540DD97B8221832534
153	0x65D393AF41555A6450E887E9AFAE955E9CDFE155E6EC1BCC560799DE6E16B197
154	0x613B8CEA69FCE2AD1B5E7BD06C87983EB6C52A17FDE88368964BE9751B465747
155	0x367973BC038D55461F0CC661924708EF35E37BB5C3A38F3B12AFC7F5725169D
156	0x75B6C92B6342F84FB23E03AE8128321D19CC01AE12F56CB09B80A2069A186CA0
157	0x71F9B0B5478403619B02C9A7C38244AF405EF350D6C4CE9B090862E4A014C2C
158	0x6BEAA132A09DE68D9CE4B0187041BB8E0F9F3CB65DBA881B6B5504DE09541CF6
159	0x703A75B7C9249A7E073E943DAFC6B5996E392CCE8AD8D66F5669649A259238F1
160	0x35D26E6AE1A6650E611EFB5C5CBB75D05B3B3D78282E516111020A46F19C94AC
161	0x352900C6FAA0156092C97B24E0D645F28F23758D2EB54795ED7653DD1E7FD6E0
162	0x51D889005929191BE55A696EEA7E0D93B71E5345B18731D732A362A8B5ADA52
163	0x505E66D2BEAD6AE7BF0EF4892F562C6E12000453A7C6E41374103AAFF9B7CBEC
164	0x447F2E69F1EB36F0008916966ED73DDC771F30FE3D1C3D6186A4FED2F8679550
165	0x255CD523F4B17C67C4BAE23EDC0D674D3F9A80580BBB743B1E1E6A4CB14B0713
166	0x2D747E15F4055F4911CB348AF010AEF706BB012646F99ED3528BA9B9AA2A5D73
167	0x7B3DBF91100843A30FB774AD961FE4287F8D82E3FD809ECF315D64653B583C51
168	0x6FA7C62E590B873216C011B7967BFF65030E2040B157A77EA495E65E6EB21F65
169	0xF014EA0BDCEA322CA338D47FD884C931F83ADCB2A74C2EB80849C07ADC4FA7
170	0x6DFEB772916E108278A6EFA2BB29B04CF5FCB08CC55BA9A2295ED7F225DD1755
171	0x6DCBC872880BC42DF817489FB51871E34CD91F519EA0CA353AF856F9DCC2E843
172	0x5D9B20DDA0D20FABEBB06CFE1F755C5CE60C29BE89F19E60074B1F92F942FE8F
173	0x2DCF700A3253EAB2B12312052A244F3F8A93C71FE788BDADE209DE1415CCE1EC
174	0x58F60489D84710C363F9BB3A385F0583ED08A4445073049E766F42A2FE5F0743

Table 3. Continued from previous page

i	$u_{2^i P}$-coordinate
175	0x82692A7C212CCFFCD51C6F07D5EA21DFF604D8BA1148ADF8C9572DF224B574E
176	0x2EE967C725A420622519AA76B0B913E753143C17CB20C878ACD9B53E5BB0A852
177	0x2AF6F7D4F6840C3BA3584DFCC8EC2FE034AB2D7E3C0A22843A3FA758FEA4636D
178	0xEFB35541E2560C2BB04A95433E0516799DD7A954984673C4C821515513268F7
179	0x30B589A80FA838DE99C987BF21D569D64EE4DBCEF02E004186E09CCE59610094
180	0x22C06901E4BDF7CCC6E74636F712818084ADB05B31D379A6E88EEE6A42651A20
181	0x2B2306CA05364E0418739A0D43100F2040C1D5D788D3B4E9B3E6D6BD371680D4
182	0x2E7F7A37713EE262F58FF83BC9059BD014BD597B8C16350D677D4AC29CDF47BB
183	0x3F7D39DAE1CEC5098962D5C51F410E00F232D0C0D57D2706EEE133C28EEF19EB
184	0x10CDA8D446A8B6570156AA0D23B9E478152E955741D035729366E1CDC491529C
185	0x4966CBA6D476A3E734FB18C61704C99A8669B85EAF98D248E1B31C73769BDE52
186	0x60136C684955816A41813BD6A05285C1B19C78DF98013393F703E6177CAE6E40
187	0x42E556E57CA51D0201DE6E1234E92E5680096F2332F14D61FA86FCB2F831B0A6
188	0x42AAA36AD8450FAB09DD71C167275DA27627D817082B5B1FFA871F47BC6B5E0
189	0x748B31C293A89D1C110B81A9CB0ECBE5D56806CF24C2031F5B76C486FF4F46D6
190	0xC4CBAE53928C3C9E8B5CFDF3740A0508BE0023E5D911659F3D1E45DB394CA13
191	0x788F17CFAA61E768010FC06CC7231678BB80C3E648306F9897C53E109657F63A
192	0x6DE6FEECF4C1AD5E869A04E78947E929F9F88DDB3899E6635476BCD40C09D276
193	0x1511CA5D2922E1B1CE3F140D4EB38C7AF56721EB850A410570BEB2ECC3C85D8B
194	0x131FC458DBB36CC4900532F0E272AC4C9F12C7817ECEA39ABEF64C018B1C7E8E
195	0x1B38F2BA0AD806EC5445149245D21CF83F5F0B1601721653EE81E37188DB75C3
196	0x27453BC79F3643F2F2204C98D018E44F5B3ED5853EFF07107297DD7CF2CB409E
197	0x1ADA4EE255E6DA71FD4B6809331E2488630051C5B5E58EC653F5EA5C93E9C5B5
198	0x6E28AB8F57745090DB251DB879D5B4C4068304F0C2BE0DF70FBBDECA86CAC989
199	0x71DB9639138EE4946F27BA6CC39641C67AF28EFB35541FA0266A29E4C1976CC5
200	0x7B9CE360D97A891C83AE371E388287383C3D3412BED1FC188EFB62185F8E49C3
201	0xD47330E9D4E794679A98B63D73210626EE9126696F8568206A53A081727CE3D
202	0xC6C250AE08D09A607F6E9B748A0181BAC545D434F9ACD36482C95A362FB87AC
203	0x7386722EE45A17423C8C07DC09BB54C14B4E064A3A0E0C81C27EBB8897D41318
204	0x7447BD25F4AC1EB4A7B8C9FC9D4F673A09128828D9E471403BBD5106ADF4C912
205	0x9D4D51D5734B25001B3E681368A4B03EA57C6E3601C7CDF74C7B6D70193C70
206	0x24F62040006F2A2B148F7AA52E937B936026051F41AD5A5642AEFE56A71B1ECF
207	0x3A6F6EF529A382A83F53CF6F9B65CE7CD5E2041A7D3002EC1B4815D294839879
208	0x5953C61E2F7A29DCD34D08B478BAEFC6EAFF3115CFCCF7722129AE6DA00CFE17
209	0x2C837DE6B54F8B610D62DEC13FD6F4094599D9D381A6070220216AE9C1D38746
210	0x318240EA6DCD3731E3C2893DA9F93520C26BECD0B8AB8587D87BCF6A0249361C
211	0x4B9E8E183318CAD2616209EE3B5A03BDA28069DA3EF2C3BEEE8A2A775A39EC3E
212	0x4BCE80E44158A5A0D3702369FEEDB00541E7610380913732536471AFDAD1D18A
213	0x765FE8508356BBDA6DA4A0F853A68E3A379B4825C35B221D89E43E8501CF3CBA
214	0x2B1556BA2980AFBEC1F2D9AD9516917006F4C5CD05EA2E4DAEB0FC25C22F6D94
215	0x36DD012E9ECC7E0C9551CD91F07933E6F0DFAC193BD25FFF2691001B3C4DE20F
216	0x23A02E337DE2E7C005799EAC0C8EF429F0E3415F9F5EB0AF2CE102811BE2BE10
217	0x50391D4A210BFA9E5A2EAF026F5FD6DBD622859C6C8A53E1F46873CAB8093C8
218	0x416431229499B3246A48DFFB23155F873A2E8F76D1C3F3183CD71F813D3D6F02
219	0x1A0A8596A83BFF201FF2BD14D41B15BC03D303DB1FFDDC6D6FD6786DDD15C794
220	0x50DF5C1C0999EBE8C03B6C858CDEC59CEC00F11804625BA59031F52F72C89E4

Table 3. Continued from previous page

i	$u_{2^i P}$-coordinate
221	0x43F731D58FE787059FFDF09DB6428A61BDD7007E9E9C535A40A7FE4E8AA47E7D
222	0x59A6D2ADAE7287D64035C6EEE99E2859547567EE14819C8181126B43BC0A7995
223	0x73719E19A0EFD3992667BC0E42379388037025BAA9975C740D92CB13AB0FBA65
224	0x5E2E862EEEE04CC21D4B085D181F2D587EF930688A243CBAA3749B5A959181BE
225	0x1A993D815401388AD7B216C4D40673829D98188B1ADEF65AF88D92D0461B388B
226	0x467641745F4426683CFDA1BC299E86DC1215AA72BE74FAD8232A7A52CFFCCD5A
227	0x2520ECE9C57A6F40574D358157EF14BBC3C60E3F458E92E654276074E17DE093
228	0x7DC3D8CB834EF7C288CFE692E54ABF5A32275FC68E0C6E5F95C8A0A0871E9183
229	0x3D5C4222B189380249ADBA1C6969957B6916A85519B73061671D100BC8D3D4F5
230	0x4051DA835E0B2119125105A0F7119B47046CDC817703F02B3B6B895DDC4241B6
231	0x38EFD6821FD02058E3FEF8A3A22D85C3EB9D75BC4D7457BDF71B376B7FF3ADAE
232	0x79884898F64FD547FC9BF28F9E2499FEFAF9E86CCF66EFAFABB54936AB404981
233	0x366367C76E23C45139C949861B2A9C82C6BD73B9734B32B602CC0B175D8A351C
234	0x5AFC265B0F6C2801F4E99F6F1DC8726526A8C19C1B5E7F3ADB76B3CB579B8605
235	0x59A90505480FC54A29FB8518489159B6F4E8BC0BD654EB46C6F0ED1C15D3C2C6
236	0x379207A7B966A2B493CB818CE3E1CDEFC6B9725382EA8A72C6ADE14FEA844958
237	0x9E5560B011B3E4AB0FBCB5F1F8A25D872CD2F397104966BF24B1FF9B4DF27E9
238	0x4ECBCB9625763E4F77345430F50DD6388602219724874828F941E8E560970371
239	0x7BA68F2E3021927934816D246B23E4341C28AC8010FED67E3C7265FDD8BF4A52
240	0x61F18371AF81CDB83262F11D0C0854E40DFB40B304B9846C6255F1196F658B3F
241	0x6565325F4DB3EF97295FDBA4ABCE964BC2B23AB67974DED8B725B508706E5F05
242	0x6780A79D2645172082031255F99C51BFE1DF9D2013B1C9DE91151BFE14C860C1
243	0x5379115BF6F99A683DD9E240DF246F3F260B4AE5136073F6B70F049590441C7C
244	0x52347196589D468EA3D7346390BAB23923940707940C80B7DB20D7B282E66B1C
245	0x74D4DEA0C05C0E59FD5A191BFB2B5AF2BD89222D20F0C4CE4B724B49787A185D
246	0x7C038C0380EB684DB2377E325AAA04E45F28399381F41C81046FEF1EBBEE0346
247	0x2DC6089AA6276D989FC3138AD61AF9C9011E53DE14DB91030E931FEE002D435C
248	0x32B86DD7910C43D7EA99645DEBA2B20A44FB152B34977EE22DBE50770D036208
249	0x7E3CC0CC2E3C74958DB26F4B242C0D1D38CC2A010FEBB9AEF12C6E2C5B766AC6
250	0x7BD9C0463CF0B99DFB9DE223ABA5CEA5D921F396C24A1F21F9E3553F6AEDEE49
251	0x4C2F559BB05F85CB5CE4EE4903EFDAA639A30A3A2DC2989B8FB4AFA27C013F5

A.2 X448

Table 4. Pre-computed u-coordinates of the multiple points $2^i P \in E_{156326}(\mathbb{F}_{2^{448}-2^{224}-1})$, for $0 \leq i \leq 445$

i	$u_{2^i P}$-coordinate
0	0x5
1	0x6391322257CAE3D49AEF4665D8BD5CCCAC9ABEFB511E83D75F3C766616266FC1 BF3747F1DA00ED7125E8F0255A1208087D32A4BC1C743CB6
2	0x93B44A7B78726BA8D0B048BD7144074F8BDAD24EF9D0A6C8264F6C00B135FFCE A11545E80D18364ACC8EBFBCC45358E0DA5FD5E5146E2B1
3	0x7E151299F7AC54588F064F2F4DB920FFB5E4561B2B45211160384C399C7ED4D2 9D1F86E05F523AA35714A3277A6F9F6E6E24CE92DDB3839
4	0x596178E0BEBD4493010E83DAB7CAAF7251A322D68CA9082C72E47166A1155D84 6B4FAF43B502602077F98F144FD98C0D5D6B65A89B58216B
5	0xA85E243C02C0B34AAFFB854A8B4E901932EB5169113B2D2A5ED251F110021E41 845B332128417046BA8BA65A0DD748B39F3F7A9ECD64F7C3
6	0xB6DBE35A6846BE08AF63F2E18405E08BF47DD56FA3D36D4C548D40C05372DD37 C0ADC1C08F9B33CE0C3433988D5E137B34B8802226FA40B0
7	0xB65E6EE82DE58631584772AF7E552892D363A9AB6F09A0A552A00415D2350FE6 3AF34F41B78FCA1904E47948B204B7771B632E9537B736AC
8	0x735C7F30E6872E5E4215C0147C8A112D697F668C9BD0F92F5F1E4E6BADC128A0 B654E697CD4BAE2144D54E726B54C1FA63A09B00DD3C17F
9	0x627E19A6F2A3E6C3B201C5A9B2C6974A3479DD49C6A6B955EF751F947331D8A7 62FA7740C2DB7BCB89CDBC033EEB2C84616E3AD50267D9CF
10	0x87484072435797043A4C335772FD801177B6533F5CFC730F2965F6EE2FED6242 CFBE340E421DEF4DE28583BD092031CB0DE4BAABF8B520E
11	0x3A6CBE48A04BA8E84067084C48D55A2084AC497FC359EADE348363F9123A5676 2D788741B761D4DDB639D350B1C437F091F88A031F39FD09
12	0x434D0BF4C12B3E83654403B6183155682DCF25E943FE0540F5222B5DF73891C3 337E8246A7B0E8C2FB8C96B22B351E7B7B7BFE0F318CF6A0
13	0xFF1D0C4EEAD0EAFFB5917DAAAF02C72DED11E8CC6E425B679F4B7CDBD03D8B16 D037ECD5E1799B3F4D80AEBF488FA92B36888C9FBB3382BA
14	0x241BE78EEE28132DB40F371D415B754F22090D0FA6B8A064A9FB6065FC2AB92F 7935E6F6D0A351F5AFDFF545D7CCF632E04C1E495BDEDA61
15	0x8D5D1A018ED79DEA75D91F065F87AAD6E088F4A3A55C8F9400A5C837D10D461A 75C5D49016545427757 8720A23E7E5D5EA9D9ED944CDAC70
16	0xE7E11D7331583245839DF12B84051B8076414C6AE0A8737D82A054C01B0686D6 6DD8BE89D3FE6DE82D6BB2A86317FB9D6C99FA60DD7BF7C7
17	0xE68631D48A2CFD1FDAEEC90149D10E9D33EB84C549C7D68BA3C570B8C56BF786 1298EE450230BB01BB7783388B6A70C89B06E966E5D10F7F
18	0xB8FF74512FCAF81C9A17CA80380CE7DD7CB57FA34F37B6F25F0F937EAF36E2C5 C38F66E9B780CD027700969E549DD750C7353E647661D4E4
19	0xA3736944489C9D193EEE44FA6384E56FC36976D1DEAE83CAA9D101CE8235E520 788119192566F5C8E830A9724AD435D51551D7CD1DBFC091
20	0xE8A1719D8A51D40641C32F8589BB029473792E67B76F87DAABE2068A15F1BE1E 3946DBB03D753ED3C87081FBFCCCB98CD1D08E87D9C1799E

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
21	0x96A934C1721F5FD19A0BD3244EA214B4044973D23266970FC92CDD0F6D609B16 A4197217BFE66797C67D2621651341DA41F49707488E0EAF
22	0xF31CEFFF9CC06FB22D4DFA50A5C0E60D9EDCD5180A3F036BECC2CD48605A2D99 B726627C3EDFD0F13DE09853BD947D164648312207A5CC80
23	0x62C6BCA7BFDC3E35F11D0E13638237199DBDFB18B9022C435820A3776FF69301 C3081380EE0E20BD285217C0B4F76D8C0F41847A916A2B91
24	0x2606BC4916DA2A90D9A32239BB9F2AE131E7D879C1D036760CDFF0C810C133E1 3A1774FDFBF66A140C217484CD3E3F642F3430CDADD1D972
25	0xBCAAE8384A40D318418971822C1657B40CACEDDCB20900DA8BB2467BAA17372C 26E643064491C6AA4DA22A84CA38E27230B40BA2A2340D68
26	0x24A204E07FDF3E8ECDA873ACD953E4F2B6C481D377E3DD2099A993B4B735AB32 FE1644D9CE159BFDC05982C592F91ECA034596F122B95264
27	0x396F5BC43ED55FE5595E6CEC23EA4740769BD6075D89104194845B8E5F28B4C7 EB510A1075B541602F8E98EEA6261406BE7477A6D89BBD34
28	0xA0867B78A564FB117718C6BF99DE73CB8AB8EB78FED4CE21D5EBB169A1667DE0 7A84C0CDFE45ABC9062C4E060C08A02C46C1BE4ADA749EBA
29	0x4CF3831ADA4671A07BD1B75EE1CA3329B6B179A8FB092DBB07C47CDC0B30DC6E EF1774F7C31298E2243E8F5D2405C4DFD039C22EF63B9387
30	0x662EE4C5915236B0A6ADA449C90EEC7634DAE43068F8C7CDB045835D977C038A A860B965271CB4462A7FFCDEAFD049C2C83A0E96189B67A
31	0x21253F52BE158C9EE7648518E318039431B656FD4E5E3769336886E77518052B 0B70F9745A4346D58AD659DC653FE07F27E0DC44AE3B124E
32	0x1DE70592C3B7687940D92BC25F0983877E367245B05CE09B877C23798CFE9D02 8A53BCC32EF838070BE5053F19D49233CA0724ED0B06687D
33	0x3E142E5957C29BB9A6A6EEA8FCD7514F618AF1CCA120D80481CDF547E7DA28AA 438BE0B7BFEB2A820FCFFBA125A863621278B722F95C8590
34	0x81DCAB6CD28C1D010788DEF9A29C6061AB00517D68679F731A221CD3587A02A3 E5D30E63775A725FA4EB35846C67625AC74FB7A37D88C29B
35	0x7B8C9E632C04495AEFE25576E12199825F2BC3D692992F1476093BF6D176E2E0 BA88B11E8E29ABA93ACD870757FE672A1A4E487A395DA940
36	0x9CBCB3769256022EA109E1169F277E6C94F003588D28AB783C30221FCEE0EEAB 7438976C67E10A5EBE9E5F02EC588EBAB279EE7B13B88426
37	0x9EC3F913FF0CBC67C3FA10E4A387C0B09DEA2C848A621202126E50A115ECC1A4 0BAA08566A580A7CD928DBFCAB89B25B95C9F49986D099FC
38	0xA5B29A5EB6F91C50772F5022E1CE25AA915ED227A176BF517399D8DA524FE22C B04426C44A9D6E0FB3DD7CDFCF071456941EBA9EAA6D0227
39	0xC8CBF41B9107CAA431BA5118A2B8C39C9FAE46D947E9C919EAC59CA0A1348839 E8C7E3DA7D606C8E76A35655F4108D96695EC18722EDE602
40	0x8CA114DBF53EB43CDD34DD43F0DBBE4E16C5F479AE8DF64B06E399EFE43C93EA 9A54F5491E25766E6A5E2CE0249C64EF615722C90D776092
41	0x4F69F11616828CA54D201E049421B761D62E05EF5A05A2F21D9D10C96C11D515 46DA774102D21F0EAD6774A758E6B6FC6D267C99E5AA69FB
42	0x72E4E052CB23C86CD870242FA0653524D5C195329DC8D7C8B38AD7C5110E2B83 EF2AA0361EE9449E3F00A425C8F563DDB8788529E7F40FCA
43	0x962A815852A5D167C0EF4828843189DAD49D96CEA0D29D118C4C03C238EEACB8 AC2BDD28EDD064CF6C830778F3121EC017674F079C229D06

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
44	0xD69833E7EAA8CBCA33C38ACB705DB2407C8B4B7E325ADD352886D844174290D0 E1BA353446B2E24863918AED7AB8C4D7C0E9F3698637FF79
45	0x780F527495869F4DD72CDB5475F3816AA0C0DBD575D5455AB8D15AC4A49CBDF9 84AEC02FC4B9F6A36A0956C9882D36B036FA91FD2E4F1170
46	0x2132C906ABF28D5A751EB545D8F16BF9F97A11BE1CD019C506CD2EC2A29E9769 02A189232E4EE9B469531FB2B9E0DED0C9E643D6DA83C482
47	0xA3EAFC3ADE29C7DEA0719FDD7CBE6AE19E91C0D9517AC78F628B425DA9662C77 723B1195B11BEBEA1B3D8F6364D4CFA8F4369B4D4BD78933
48	0x2F6A415A26D06E0A5989A89D5F8B793B4D77DFB2E07B62D8AC6C76A4D9F749D0 49E70B5575EC69FA040ADC19A758BA2323AADE8BD7B87CC0
49	0x84313A5D69CD78B806B2A5665A065ABB99B1BA58F6FBF7642714DFF899835CCF 18FA6181D2559CFCC6020DABACA13075597B1285AEF9FAE
50	0xFD8DA20F1347C014DE2D33531EC7830AEFFCC3C8ED029F05077367A77FF39770 8F51383685A337023FC98B74E9D6AEB8E4DDFA4125C0965
51	0xF4AC7CA9E597348AE6E51FF3987B69B8F1883032EB7FDB15DAEC1E3C49E8FE8C E1F0FED0A98F71193987C4D6359675B0FAB7C32668B2D38D
52	0xC486C795636FF91A454E2347CFF4F1D954236EF24E383335A2EA72060F2D96F8 3DC8C4BB8C78FECB711891A5196AA13E1D005DB2AAE5FC4E
53	0xA38406E5CEF4A3F732D35D55CA7985DE949A6D31C641557B89C66D1CD0BA0289 17CE5E183AE5686C2BC6A03A2A76B19CAED66207340D6F98
54	0x40FF76441D9867FDF5CDB3F4EACF355E7863F13308C8011B0089D1ECEF545806 98A3C5D8F503904147C4BD153DE1C4054E61BF8C8E9F9BD4
55	0x1A0BD315E45321E4C23E1CA6076829FF91B537F3A47B43BFE518232FB6BA493B DDAD1A9286D8E5B6FFED63B4CC450E68CB86B2953751FE6A
56	0x3CAF41ED767B247CBB69FC5DB7D37751EDD9F046A93B00F6FC6D4F2914A24346 EA0A657CDA31591FAD0B2F319F8CCD4C2FD13EA399F21ACD
57	0xA880693271A90FD4934E76BC1CC107EB8E7229931DFFD5093A09B6A146A2DB90 73CEE9D638919AF08D073FE6CABDD17122CEE01F86EB4B89
58	0x5A69E122AF53AA611ACA5C9719F29485E96CA09F0CEE7A76E3CE52FDC39391E6 5F0166E8B3FD4AD0216319304D98D8B9D7BDE862AA0C8595
59	0xAEB68CAD00BBA107BFEAEC239C88B4ECF121A247A52F7E97CE59E0AB6E401448 7C88C0A99F4595F6C1A955FF66191BA63EE71B5812B1015E
60	0x1F25518BAE82AC7B10C9B7A8652297929F4679ECCA81E42DCA33A8ACD21BAB65 4ED3FB4AEA08BE8D0F06F172BE2F485E9EA94A5D4D25096A
61	0xA7C0512954574EF24A94F9DC8AE4017113BDDD88EBBEFC7792BA8178DEFBB81E 6E7BD5C273C68603CF980FAB40B563127D5CAE9FB566D4D7
62	0x27EA0D19868EA59AE943DF97C1C9B1C24C1B86F1EA1A82D15163CB441312FC46 FC570B68F63E8118CD82559C927D59DEDD1687E48A27D618
63	0xB7E2374A6F01A73FFF301966CE4A188E86F19F340D3029C35EB08F96A5E5B4C0 0DF92D957A2E90F95D19C56ED4630E3631F831ED0C2C78A2
64	0x731A354E301224607F0C9B15CDCC86A7B033DDB6225B6DEAA7953440D014F083 1D7F42AAEDF9A50F7941A67612CD9B5C9A583241F15F95CE
65	0x939F2AAEB74C1D3669AFBD848A8E54759CA69DEDF48B7B360A3679D5727A5978 E97E08A4924D92D929809EC22E1DAFE22FB7AD30CFA9168B
66	0x9436350DEB1E5AD9C4425356310BFED40581573238B3BA6595CFC250D9226DC4 4D33FDE32FD48B3AC2910D7A3347067106BE938691D8B372

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
67	0x6F7412AEC59BEA9E2DE33D00C738052CB320764989507A98447B9B952BF5BA59 A6C4C2EBBC5B5B060CDB9975F998EDF43C51B6B0B7AC5DCD
68	0x22BB9DC08EF7685C4E4205C4ED666393AC983E0AA99C723BE76AF935E06F4BC8 C3D26C88201DA0CF608CB01EAFFAF4616DA9994935D29AB
69	0xDED341B81E8DD0B57A5CBAAA91600F740C4B6FD30946BECBBF4BFC68BB558A59 1A1732998191ED6EA40E897706CACBDF8B735845125DCA03
70	0x55C1791A7CE0E8F4846A0D8DBC67C96DC05501457E1C322FC3D3CB2C9D8E35BD D714F60C7C89BACCA7DF9EE3761D211CB78AAB5207B053D2
71	0xF15C23E411B6A0681161C0D19366FF109177D3F23CCD0DC77074EE9AF9A60CA0 E9D5FFB1F7415AC234586D0FF66D60DA945BA0A930D5D792
72	0xEE0AB65A7F7110C5A8F5441F3C89C1663B7FB31B2DAFC040D1B9E307A7B2809B 723F6070CC25C7C0836FF1DB99B2C3692B5537E0381F0B0E
73	0x87D74279D60FC962C3D88D8F1245A38475B34303B18684ABC01E04D5227F1BC9 65CCF72A940BD3EF9FFE9701CD9F847827D2587244040080
74	0x2CE9F6E06EB93A139C5A8AB60E07237A8627BFC2A4075CB4F2BFDF3E2D7EC63A B563650E607A5756393BE8FA8E0C5303962497293538AE09
75	0x863A3B598DB87287B9BA0BF7E35DAC1696C02EA40C503E90469F081687423222 D237FE68BD282F1AB9C1E4148060B7E82B17E9C2D1EF45B9
76	0xC4DC3C183417606E577C5861651E85A94B0A87912AD230BE847DC18547D1BB65 F9AD5DFC52062D54D4F575B353599CC6D6262DC90022539D
77	0x4D953FEE60FF39E71AB28466380DCC8834A5DD2681D77B17B681422DF72F8995 8E4EE0D66DBD710108295B2581EE62943970BF0CD35F3E3C
78	0xA1602DBCE85F2CEF2E8E10EE4EB4FCEE217162A5D4374758DCC06AC0E65EED16 2CB3A00D3B25869150C7CEF9A8DAD42D243F8C338696EC05
79	0x96E98C2E13B25F835FE3EAEA4FA8975A52E1C9B0B4DDFA05A3E111D7128415E9 7F64A6A87F48C2D558C04AD8E2687534E0610EC29670CC7E
80	0xAF2A90B7BF66462B15B84028EA2D35068BA5631A50428F1552AD857A33F2063F CA2013F3B3D72264DF234D5E1126E1197D45E6795CCE3B66
81	0x6F3702AE2D23EF84D424C9C0D94CF745BA1B603872E5B56140F345DEE78B3170 809EE4B49F6311062F57B6C443D8EFE3E5C6B53BF0EB0FBF
82	0x21587887B228DFAEE86D7E5DD22ECCDA368020082E52DDC0BB57CE94E533601A 725EDA78519A358B456E1123838CF1A070276F809BFCF307
83	0xD27040F7345D7A3233F1379B351D972BCC92272A30D653DE382C6E18EB83F609 2BBFD08D73944C34F92E96EDC0CDAFC1E7AB76D70FB59C9A
84	0x6B29BE29CEFE729FC109EB70D61530A05454B73C779F53E99238AA8BD806AA50 13D5DAC955659A80EB3E4825A1FBBEC49AF171A79DAFB662
85	0xE3781499678CE823016BC9EF1CB2171E45BA25C4A1F9998F177538CEEE559C83 20AE3FA9A51044A54A2C59EC43C09AEDAB5445D5A62AF803
86	0x8A390C3F24B133E2E53C3591F7D413D09F54721173B96EA40D52AD7312815784 05F704E092725BB8EEE1B00388315B1D90B97C687490BA2
87	0xF141CBE854D33A16E248047CB19E154D8E069FF4DB14CB53A4CC90DFE565DE4C A4D4025A14CD18C756FBE496D13FB6C37AC56A97055EAC58
88	0x44D112C4EC20CDFD1288470128DD01C2F7129786528BE37CC66848F158FF8BE2 401B62092572732799CB4E82BDC333C112101050066DF986
89	0x1092C5F3DD1AA94A2CFDC359B73774C5F2AD3394235521C4B5F34CB8C2D3424F BEE04078D98066297587EF93F66C0F8AA121DC5B43741D96

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
90	0x1A7B9A970AE366C2B2FBB829690DE6FA127D62C653537E0AA08B99C3C2D5B5D6F6CF5AAE8F4CEBC4E3AE5D39D268100877E00FA57244FEFF
91	0x7DBFF981528A1EE5C38C9E91D1A34AEA490FBEDBCB3F96A86E3457545E88004801A6F0AA51C6C4D6E8E1F6C9C52EA5FA62203325BD12A0EF
92	0x690F9EA95FC53D06B4B628D54A187699C53895E88FE3FC9CF1DEE950D9E14AA651C60A88F96DEDBF78E763B52872076D2C1FC056CAB3C4C0
93	0xBF58E5F3E3E0BAF5A0DA35DAF9922FB4B669046FE691E8AC8B2B34EB1586D932973B3BC5F501A69E387D3436D369A649814EB5AB3C6BC805
94	0x8AF6C5A100B5E6B41CCF75581BE2169DFC3E206214751E131695235A1EAF4C501376E314167AB5A4E34070A1E7191B9CA7DA45FE2E2AC659
95	0x49131139DE641EAC86A997C9787C0D05171E71B2D253E4D46E8A33F14F3134D0E1CE84232D080AF4E0977722FB02C6FCA54385AC153592F6
96	0x9139662125F6D12EF68488CA186CA478602BE2AA4ED6D66DB8D40E0EB36E66A94FCDB6F86B6C8A68D61F8DE789ADD22022F8A860C6BFF592
97	0x618F16D4F410DBC661642CF3AAAEB3DC83DBE583E5370E197F8D77333524D45DC5638877BF1BBC3AA9259636519C6A370E36774D2AAFAFB9
98	0xCF0C0840B008FD37F62537B1D007F7383920DDC93C19929AF77D6AF70421FFED11F384DAE83200F9E2D3C6974930506B9C2BDC8F8E8F2DA7
99	0x80687346BC6C5DED8822BD9C8E831DC48DA440E58F20A89D518B9E374EE17091389CBEB0AF5EBDA8AADAF69EA5426E2009742874C5525516
100	0x5634EF2A4C303A8804C64236417D7FEBDB09E8FAF08C9225C9476E513247262B69D23604A84771F7CF796C6611E8AA53AF7A77863D00577
101	0x193989314F00C42882F96D6B264B5F014015451292FF0725D8956E8D30485706AD6CA0879C12FE200E092400359F04F7021A18FEDB6EB1B7
102	0x68A95AB54763354FEE1472E12E5B6A0687E023F6B1C3C5204E985850FCCA54075FF3814AF27976515AB355D7BD058D01656FA5C25FC08981
103	0x86D04595344AA40DA4990B344ABE9963AE736FC48563ADFC38D390AF25B1F78CB3D6E6A060E87BD69D57CC718F58953FEB0D91CE25892C6F
104	0x839511BDAC85B6C36D9481000D77E8A1333B370A7003C021161E0EBD595F8FC50934CFA81711DF0DE971C804BD7F809B4645868D462CD3CB
105	0xDD66008F17FE78613373F4ADB23B09E1252CB6F0C4F64DCF82E712D80DA27AF4033F864FB6415EDB81DBF81F864C8181D10CCFA38F0E47C2
106	0xB1B7C08D39ECDA5C3DBF9EE40E26D73CC1EE835E3E67AAFA68BF3B7280870B4A48CD11352038ACDA6D209E7FAAF61DB49433E4C1EE7FC235
107	0x1C0BD3A29C5C9D9F61183248EEAF1D9F45715D105BB1FD16431444FFFAF3EE8D3CE945EEA312D2BAC6B9643050B48270D7B0411A98ADFC13
108	0x1879F66628BC28A794E9A152D833F4280CEF1B24A723F3DA50C46DEBC906568EAB09365B8C0A83486C4224E106BB935542A57BFB4F9D74B4
109	0xC0EF5C085A8361FA872BCC5FEA8974740321580C3066900E920DC7B1DA198EC6202299D8C115B2AC17301911FC333342C014A2ADF879103F
110	0xEFFE63BF4A805E996ED6DB284BC943FE3AFC02AE0F5B7DEB22C548C389B58C8CE3C3AAC65B7E2567593F39E05C3022BC09ECE98A92FBBA30
111	0x4AC20A05FD250BE8BAA09B7E85AFC881FABD1ACC04B5B0B6B25422865B305EB305E8F4519830FC1813237F6710BDE43136DB4C1AB4721BA8
112	0x9FEA66646F5A0F94A54D0B384B947307CE3C6806D2D762510EBAB89185CEB5F00CF0EDC46008C7A1BEB6E4F5ADEA419D349BCA18B1BE5334

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
113	0x5D428E8191297D4DBD9FBAFE9CEBEBFB80EDEE22ECD3F2804F363C8F6089C43E 06C87D40CA83A74DDCF4B289524A6661A7C61D12E5A84687
114	0x6A0C37147D546FB92D5BFB4AEC2B595FC3A9C1FD6D1718A55E771FD70EC074E7 07B5109E30EFA153DCD9B0A354A9344336B06952180C38E5
115	0xA99E014ABA66E67FF48FC10D14005552F4BDCF4A3ADEE2C8EF9AE120C017EA6B B243BCDA224652F097BAC6D8BF1D3BB4137CD13B5A1C5D6B
116	0xFEB173F569DB0C8C8A2B502D74B8740F3CAC38F539C6838002C5897D18D9A009 1B0E368B7FFE97D2E176598198063ABEEBF84BADE94C3D33
117	0x638E9DA9F188963331738A47C64AB1F327DD82D3767C29D9ECD9DF4DAACCD878 DE33CB6CA7DCAF47B8191C98A7847DD3167804B1A9C58A3D
118	0xD38E1623A1A216677EAD6A6F33CFDE30FBC18717B2A0F519E7A68F5A3A551F39 244316B9827615AD81321655AA8724B0B2E22956069AB1D7
119	0x781C024797FE2BD8C9FAACD19A67ED0DD4F716361A4A71DFB56446D459B2E7A5 6E072F9043F047AC5A4D599A91B05307443372FE924C47AC
120	0xF05C422E24694C0D9E8A8B3DA5D6A6CF85710438F333CD99764B82CE79DEB5F7 718126F604D064E0DEAF3E2E4A85A5972C74D4EC8C0F725A
121	0x36A3FC4530D45DCF5FD6BBE8677D511F15EAA0A130B9FA56DDB886229B6A5B31 6D0DCD03A46314ECFE5421526E0FC8147FC904CD77FE55F4
122	0xAE9D4CD2CEEEC47818969116314CC8751DB6F51367EFD5B6DB45DF3995FDDB44 EC35013F7617FEEB816EC874032FB999B4C0F3517E41B04C
123	0x63B9B0AC841FD6A1B66AACFD188D2FA3C8B5098A671EC38B4372F087CC2003E5 1C81DC531D3F2702232F600F6D290F0448CCA1C27735E4F1
124	0xAA313F898FEE7FD763E6A46C91E7D5ECEF59A67788095D3750EB98EE9B9E1312 43315AB06BEE6DAC053CA601DE3A2553E142EDBA95C6C0C0
125	0x331ECE0A0F5B8F2BFA42559CF12D9EE5470DF57AB9284D8860858D082C98EF97 1F82DBD2EB776AB708C540518C69E7FF920FCEEC37565BFA
126	0x38646D65F6CA0720C44159B0FFDB7CB36A7DF933C9D4E6E1E86DBC086FCE9FBD E5BEDD6B08631875D6C0E612BBF4245CB744DD78F97912A8
127	0xAC58119E8E4E3C68388E982AF067F36331EAF98A860B2ABDA97923FCB12D6ECB 569FD95C176E26D23BBD95C7AEBC4A0052413918FF28F95A
128	0xBF7CFBDDB0005EB95299C9DE4FE8CAF27B02B60D93EA9FE990121BC4AD4E3995 61413902CE430070C8495C0D1A818C277D9D312B327881FB
129	0x6FDA89F6840BACBE41730A270763A303678CAB3915221262A6A5448916FB3A4D D49BAEBED11323A92A61E07D02465C7BFDDB28890A14AA49
130	0x5E29B1EE3ACD6C848A15359A9B05C1FBF71198FE59A889E1A2393C621227B608 893C421929DFD2BCACCDA3AAFA89B2DCE849BDFD513B8C4C
131	0x30FFEF3D63A7957C42F172572982D1848A40269CD1BCB17AF64648256D8978C4 72951CC3066EE45ED35592307C40E38E5486D42E28B9995E
132	0x43488DC83B76304D105BFE90A4346FE99CD2870B0DB7A5D19138FC07F9156146 54983C3F47DC987F66B5FFF13120F85A3B28EA25DFE4FBDB
133	0xBAC61DA098ACC34F095AFBE6EDE2968F44B73C9AA927E183D74A139681A5D2DA 19461E507F89E84C426B96B6F82583A02F9BBF62E047CFD9
134	0xADD72A15EE1AB555413F863042AA87DD065B4976C59C0B3B43D97B29D5232279 E1EBB8509819B476DC6B798EDE947DB8FCD5E7739AF342E3
135	0xA55FDC68DAE4D6C096B16B748D8AE04E7BCFCDA7B8DE744106212ED848F5F3D2 20D7DDFE9CBA6ACA135CF4EE35E5585B850D83AF594B8C89

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
136	0x477F11B7C436D98FE6D45F1A00AD32FC11A80F8AF1320F939AD50DB42334594A DC3A78011AE403939FD8DF0768065B2ED8495ACA82C04F96
137	0x669CE5446B90D6E820DE36EB77E8BA9DF53EB3A30A6C0C562AA821C862D86162 F19FA542DAA2E83EBC0570FDE69B1CA931340CA3774AC9B5
138	0xD4131B8D1A2E3FCAF372DB20446930F0F379FDF185950616DEA2AB296580E803 ECE552134E95151A313205CC251E46587971E9373EA00F31
139	0x20D79469A5F843D0119ADB66A5545BA93E66DFB54B2396100544D3BB08A30AF9 BF97723F8D017EE796808A0B718FB6FEEBA7715F51AD054F
140	0x947D2F3B47750A5C0F68B96282D7798CA964F16BB565DC0984AD7F4D6ECD3D9E 6CD3B6CB7B5D652676FE16A595B774CF490B3D6E6C7405EC
141	0x55759EA51024200777E532AE7610AEB575A933ADDCEB733EDC778BE4B488B506 BAA39CB95343165099246BA2203CF48FDF492A1CC0824BE2
142	0x53B68097EED99431E065140FA2057035DA85A8C1754AAB56E60E4058910AF94C 70DB460C277FA2790148C221BE3D165ACC6E3CCDF64FAE7A
143	0x444EAB1669426D5BE7E7735CDACC5C7989BF0B37FDE7EEA2109C3F70336088D9 0866D1AA454223574991E39ACD94CCFA86D6A61B5F1BB417
144	0x235E24B279A893957BB760AF5CFA3FD45D0F6DA46D97632CA2CBEFBC996878CE 17F9B1E7274EF3244ED6D07BD3913230F2544E89D7584044
145	0x461BF20C315841BF83400BAF2EC841AFF0DB9A9DC6088C53AF58E6BEBC60E5E2 41D521A29F8D863C746D198F853F930BBEE869E19345F1DF
146	0xA1AD4AC0722EAB782139D00165B16333C5FAA08B2B6F8662CBF423BF75F3CFD4 9745390F7C28E85DE31B44210676ED3CBA55060C843D4A12
147	0x36652928DD5384522370105D41CCCBC8ADE537AB54439148C144CEAEC7BCD271 7B867589FBC9B804321B238ADFAD146FE62956C92FB4D82D
148	0x210649A4E49B0FB9A25E87829DE04C8ECB7251342BA2A1AB32860D02F00003D2 3A87B9307FDAA3BE92F90ECB710D409A461068E549660720
149	0x8E9956422C28B7C365B60B2DEBDEF904EF8D7ADC12C32EC6C3D11EC5F7577048 A25EE96722A315CC77947BF84317BDE43FD7ECC2E9034038
150	0x965EF6975A1BBB1C96E4CC13BE34662C15E1BD0E65808BFA4CB0086FA0278607 FF04A9C68EF59304657F334A8505EF32D13AA0384930A9F6
151	0x5A74EB33C8938D138A9C16A24B0821F5BB50D40A9EEB2B029ED983D19700E9C3 4EAA22887C890FC96BB6D90EF65E000524C4EECC3075B0E9
152	0x45E4539135909C6A95448719A64CA63E2A62E0745D9236CC952B7A1F4709FD78 C78BB6D6FE512B75A22B531B64037F2596945731E17A5D27
153	0x6D7B5EBD7BB43F17B252315C237B85B93FF616A08974CA3E858BFD3B67718635 E893E51E003CD6A5F547BBB53F6D8006314B2D3F6D32BDA4
154	0x6189A5B1CD2DC8676FB67036FB6B570CA2D803D3E1F4D59E7C49890BBF7681E3 E7A3AFECC8FFD38587E9D5120CE8C3F682896B2667839B3F
155	0xA581A48436F9C4972F9C0098D1B08925C52B6537BD54FAEAB25D0AAEAA352235 42953F46E7173C7B4287D98BAA846938B5F0A4FCDEC9E010
156	0xEF1234E1693563A372C98E26F8C9CB92A87C71CD1EDD75ABB62A5BB8A1A9E85A 4C5E65D847E95FC98E44377AA5C55630382FF0DE5676EA13
157	0x1FFF6442DA20F45DC5516114F27A351504D175A709D69E048CAD49DED6D90F09 FD826D3BA26A98EBF0DB14F2882F2D5C61CC9FEED7B75AFE
158	0x53FC17C523903616A6347763DEFA2B275EA81437A8A966502CE3719FC76FB7AC 532A6ABCABAB2CC53ED94C501BDCCBC01618420BD1FA143C

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
159	0xF1838CAC88F07AB2540F51F7CE89BDBEC9EBDB4D22BE78D118A511963058E141 11BF80EE9BB4266501EB4651909C36CF0206408CD536B5BD
160	0x1821CE19CCE0AAFBF0576B98456B0A53D6DE4C2B39C70F804ED5DFB1E9A46BBF 12CE5903BFBAD03B3087B0D068F0CFF104C6EC21477B60B0
161	0x9686DEC66D197494098E1B9A01AB566DFC60E1730CC523E43CA3C2D614CFAA9C F5A8F977F1EAE4D9701A28ED7E206F164E9C5E649A4225CB
162	0xF27B04ABA050B64A370DC8FD7B0D60D82AACDD17C15EF04C8CC34E5A38CA0FA8 0C01EA3DABA25C1E4FDC9F7F500DF3BEF0D9F941F32061F7
163	0xC9D50DA4493438535A28209AD5F295A177B33D6B5522133B5B2F3C1712327E6A 8F138EAB3F1DED1D7F71CC32C74FE125D383391466044F6E
164	0x7DB3FB80C6B64C1C8A3E9C5B72C0FC1F0B3B3516C6CA0508463DB87913D83941 605E65A86CC2DEC518AEDEC52C2AB47977B548CE60C80781
165	0xCA56415C9879DBF01DBA570EBC3FCB40E83C441F24AB1AB9C942D1D127951B8D 508E34F2D846966747FE8DF499384A3BE108EBA9120942E6
166	0x5B52F130C34AE1A5670361C8C0998598F3E80812019CDCE4A5BA3D46B538A6F1 82805017730C4818041FA62D8DE7512EE685FC875E9D8EF3
167	0x6BEC8391F4C715B9CD22A5B8D2F9EFBBC3FD95E3855D9E36EA77FFD20BF738C6 14771731C806E2F933692980D3697E5B371990F3317DB9A8
168	0x89588DB4D6585BB5D07F5A5D893C454FC3655C9FDCCBD31A7EC8B679A3993416 6C355C85F6FF1DDAFC14B603157F2D87D1F5A3E31B307E2D
169	0x387CD1E170D80D70BFA36692DDADD6D81E49079B90458871647C86DEDE185B7D 937707A56ECE12FD7166A74CF2E03B0C057452D075063F5D
170	0x4E8C15561848C26444F913502FE1DAE13F5D752CEF38E19CF171932D29BE9407 6F1561E61166B404E1E0CBB49F92ED6E82B1EF807B8C0DD
171	0x129D415F3DF3E797287E36B3487617296BBE7037D54F04E0CFD5385B7BDE7E07 DF38F0522D074E17084B71791FBD442259E55FE08B5ED9F4
172	0x1F22DB9FF28DFB18341BE482F356F98A12A8AC297BBC22FFB859D321CB13EF0A 5DEAD71CD99A9B810DB71E0723120EDCB3F0A92A5BFA3A8C
173	0x48091ED3D680ACCECE144A25AA2373AEB49332F5BCD809AF3A51D185ADAA9BCB BE554F6E9777E29D1997AC81769EC9E9C698D3B96AD843D1
174	0x20DC5437A026E1A27D46B8CC284528D326C3CE5A06B3136199E4983E0B1C230F 860CE4343E2950E400A5A288C243B06D7050898408E0F616
175	0x332A3FA3501B71C7552EE578F8DE27EF84353217793B0AF89E07016F721C8B9E 636EC6D2F757C85938D8602B1191A2B9762B5F154F911206
176	0x9D50D037AF1A16BD9B87200890A3A072D1193BC1023A931EFE8AA89DECC956F4 95CC68E883A1989ADB7EE2B71DA95AD8A7CFAE5DE8B9EC81
177	0xA1A227D0B981F9EDBC742198D606C05950F0BA7C4A6A8AF34A1F5FF9284CE487 09BC3C9115AEE3D0ABE62D49D71159B1809F8ECB68537B46
178	0x54088DCAE80AEE75C687CD06BEBF026E91C3EEB13981F1D1F5859FB25A5D15BF EF7E793AA0A842C3CD7C4868A54A73106A79385930969CFD
179	0x162B30FF7F5596B6449B8115E0D3B25B54C7E1AB87C2A79E7C1324EE4E87C1B1 CA5B9C716188EF956FB926236CF08B10CF465322CBA4B99B
180	0x73F99DFAC28EC6C5592247E643FD4644A274B4D70BD9E49CAB5E1F10EDA23966 388EF09244FD25653A2621FB26132C36CA2D4265016B2938
181	0x3C3B17C6A3193B5CBFED3E705DEA9346BCECAC91E268F9C8AB35DEF2909FB26A 55F82C6790DC47A4FAC42B8082AEBAA0949F714A3D48AF25

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
182	0x844DAC4C1D98F66BEB8000E16EABAD4AFA51E8AEEFA5E587FEE23BC21A72E44F 8617B751B3C9807393F69482CC3B57833BF77E5DA04C8AAD
183	0x4B2511F292B9866D970A2701B39BB6417B5487771310145C62450E07F5750C94 149094C703453ADE09BD7ED88074D892F91F74E9B11E0BAC
184	0xEC4264544C90BF503450BC9FE9B38E75DEB4CE5823582133A1331917AAE9C8E1 DC184F1D0EEF4A112AB89E6BEB74BA1333AD8A855304A8F0
185	0x162BA597C72B55DDC407509D849804B5148B0E8F15A2E678E78527AD8E2F1EE5 DDF647DCC3A564C38B4C615660430CF078AE20A7A9537FDF
186	0x806761225DFA2F5187B15FF7F607CF80C49D2818D96D00EE19A750082F85B17B 8501A70585B5DC5A7FB4BC34B8F9DBDD25B84E6DF7F387F7
187	0x911CA05A2D9EF317ECE12A696AC170E7713E38991B4E1596F57ABB3EC2D37BF6 85C185A3BA10D9691B6A09170F74069AD983739DFE8F4E4
188	0x1D9F4FBE84C3409C39540FF89EE939CBFE2734AB7934C44F65FB955354514492 E41C92355F27BC6E131E08BC1B27DEAA0EDCD9230014B8A1
189	0x86C1C0E2C81E0B555DDE769AB5E3963B18EC619CCE5E4376BA644085005CD3F6 F71B06871C8C3308163E89643C7E108EC0D72A4EE6D8D23F
190	0xF7E1A38C0F61D31F84CA86AD7DCF0F5E50EB2268C5658D9C549D6067AB207925 44E296548B7970EA8CED1B8D44932DFA9F8F695CB329CF2A
191	0xE71BD2B18AC4052D80CA52FE2AF51E9FB45B23D7629368ADA2F715CE12671EBF 2278CFED3020FF69581A02BF5173AF87A31BE7CEEC7381CA
192	0xB22189FE86026CFCBC64CB2EF2B05AE75AAFA77BBB9DE70797FCEDD4C272D1FB 164490FCDAE604A383D40DFCDE4BF326E49555ABEE043948
193	0x1DEA39FC5C38535136CBFED38C276A5EF2C72A9490C9C9876938247CE442E9FD D26B2C89FC452A3405D2581042B776882DD5CFFA78A93FC8
194	0xEEF61A66C847F636B8640AE6CB0DC46AEE1FF08469170EB1365D7B8D508B2345 973C2D9712EFEAF2C73504432C8AC606EC94750D14C5E4EA
195	0x1F2A57B18AF6E7B78FCD9818857F466CBE33CCBEAAC259601F36ABBADA5F0E36 42257E1D0E37021AE0D5A98475C31EF08F534C2A3901CB7E
196	0xD29D2877E1018329E30366F82C322A12C7BB36257A35510B97CBBFE63804C29B 07E7856707639BB4547E91A029624DC4D4C82E377E9D603D
197	0x7FF0086E15F478CB5A37600041E6FB13F7805B0DA60A4340FDD1F1B2A3060486 89E4BBCE8D07DB00A7BA3ECE4F02BD09E26ECA925A7ADCC0
198	0x166D9FEF098A5A133F2D90950E1F2C807F588ED2CA5CE3FCA0237DC6D649C283 E200D3F3ADAF538D4E26A0C4372E450749978ADB3152E072
199	0x38ACCCC35536FBB950A256AB1D03CE3978ECC511457B28FC86A116FD78BD56B2 252ECC4CB31BF36764A48026BD8A463A0C6E9322C4BAB24E
200	0xB6977FDD1A1E70B36DE44D53897EC800546893FB951C178FA739A0BEDBCEE691 C6CC3BDCA7BA3B812C3000EBD0B4AD7B087C8835511A7666
201	0x1CF83C708AF40942318967BA56671DB87B18F48437F19C095EF0301D9DA8311F 66EBF59F074BEFEA28F239ABB59101248208A3F534648EC9
202	0xF3D2478E69ACF52DA865D2ACE12884EC6D56B479F8C2CB0E6EA804B64F8BF448 ECA48AB5F16E3CD4F6E79C7AF1DF3E3E7E3CF1113ED615D3
203	0xC70BB778BB9B50A9B07FE2BB474C1D8ED43CB3E73BF9A83DC9F22F2993234A0F CB4694B35D33E4E3599D9B61BE917BBE1DC7D0C756616A72
204	0xF2D040991C984C86D5BF08D0331900CCC8AD661E462C1FD325C8B9739A110855 361870545ED051103E4ADF5BA949231F5D23A45F608032E4

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
205	0x93C851E9B7279468A3784FA7F651613786C32844CA668F043C9058A2EB46AA50 6558A581144428AE2089F775487A6AC9065C2AC317EB0392
206	0x564A879AD7F12CD6232D3FB7530D60C3252ADD016853E4F740845155FC4212AF EB91329B1765A649DDEE5713BF0A1AA33B31CE778F710556
207	0x2D9151F71AB2E1E6C97D415189C5A8962533AB1EE19DF2C843359A670BB8B18F 3039567325DF9FCBE6E7D852C9BE0D12122A7283219BAD37
208	0x4A6110D8B7E79695AB1FE6BD8AAC28673B059CEF62E5262A75498B23B22F4BD7 BE36B63B4928988B84F054609EBEA462D95659DB9608FD38
209	0xF9BF8AB0DCC68CB36643EBD516ACA158F8F20A42D3769F7EFD905799DBDDF3A7 D6CB0C4DF15FEA6E952A9A653BA7A1B72B977E8FA4EC779F
210	0xBE6DC736E9F4CD8A145D75E3ED2D1250F180CD8B4FA133D590A974AC7ABD9283 BC9762EFB3C7E4FAC9F0365693D673CB49A8A7FF4BF3FB7A
211	0xA63DE1DC5B2F151F471DB653E23D8EEB8A41613FBDCEAAD57D0E53EB26CF4BA0 A070321533447D4F7970C508ACC48037E7990F4B9E4BA4D2
212	0x33F1F18EE22AD5492061C63289DB380691816AEA799A0AD34339F978FE499A38 6E7BF5F42B4F088F81B211A122207CCBCBBA87C65A6D763D
213	0x66FC117DAE0A60E019CDC17F38B363A8D0C3E9B7CA916BC517F7D30EA0141113 21CF1A8231AC01FAF9B0949E7DC7563FBEA458F9B34399EE
214	0x81F0E0C36612641B78DBCFC21FC0AA9D261D6DCCDACB9AC1035E25430F975166 494A5C9D91809928265FBA5870D1754D4EA6D647320219D8
215	0xAE2D0AC57E916AA6B5DC52F4DAD12A67B8E0342D0D1031DAA7D8BFB80BEBBF79 5B5652BAFB01357D850576B29A8B3943376C98C639016CFA
216	0xAFFBDE4167C868122D809703029F7B690DCEA5A49DB62B6270406751D7349D1E 638BDD098FF3BE510A803A5C2F9BAE627E0857E422802D87
217	0xBF7F5E0D497504481FFDBC6918016FC36A5123D1B45BA667178AA631A993AE20 C52F9A7842DC24537A4A1888BF309F3C6601536513270A5B
218	0x3099B86B6C830F338453217A3E2815B59EC6263AB8C809552EB81D8599C15993 755E3E935DB7B95C8D127461D5A3C6AEA70B4A72728C4236
219	0x85917803634DB8636523B5DD27536326B85DD1A4A8EC405545D55CAAD028EBA2 095902400C8224BEB286FD16ED97D85488BEDCA298A5934F
220	0xDD922F791D1D003DE576A8C02360D13A0DCADBAB1E4059D34A0D8823930AAA6B 6BC39304435DF45150E308C2925A1A49BD434D42A15C5B4D
221	0x55F56E1BFBB897AB2FBE8D724131A4A6870EDEAAC4AE3D9646F19050489CB6A0 17853E4843A002AA4A591FC02AD1A712A77B43C50A64A242
222	0x1643C987EA9D92E99EAB407B45A82D7CBFE54BE5B183A220D69408802289996F 068593DAD0711ED17D01EA70C56C6A2F05E33BB0D3CC9C65
223	0x6E8273FE0DD78AFDB7700C0F2B74FDD20E62AA3FC702E09EF6C024FA65E72812 0BBD0B9FBE8775CEADE712D929BD479E88B79E8A53D41B01
224	0xFDA41163AE413EE81224197D38EFBEC9EC464274BD781B4DB97B4858C1498BBA CE5085EB4F8AF6CE5552FA1F2A0E8A08BCBF50B8F4B8CDA0
225	0xFC8342F4037C4189B2610AEA5801BF62A7D5C0CE5DC021BA567E1290D6BD166D 47C4F306D8801CC153F7C2C3B9C2CC5C02707C70B0CE26E1
226	0xCAD4602CD89D67CE86B5400FC07C656AA709644E2D94284223F904624EED155A 016EC650292045A2E63F22BC917FA0052A3B77415FD027BC
227	0xCA11D31FC5BDC6ED647265D63A5D87B3337DCEC77B1BAA0E2504E44052B96107 7216DB7D384E1449543F6F82CC3D640CE2AF1A0450A20023

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
228	0xB6FB13A30ADD5580397ABA0BBE0752A78D2C106EDD67395DB73B15F267AA1C95 F809719BB761C33FF4CD07B47C17612224E2D3E22D54FC3E
229	0xCC40FB35C5ED015F60C3F719E5B18F26FB0693B4DC39B72CB3CDBDB3AF86FDC4 4A7E4BC768F0AA1ABB81C4A168FC4B7CAAEBC4C6ADBB10C
230	0x648C5F7EC66AA94BC53755E7E27E08A0976A12D269DCB91305C9C3FE61712631 547440AC613E5E94CBD184F078AA1177DBDFF54C442DCDE1
231	0x4D80BB0E7B6261475638F5EFFD71F1F873B30CEC7681B439C12A544D25E3249F 4F95B6EBAB7E2570BE7A0A7A3E55B70F3D49BDB67117C289
232	0x13E1299DE71EF8ED8AE708DF6AFCD11E940E51CC2F2587F462ABF9F85CF726D2 704BCD0B98C1ACB03927DBF42FFA266CA614A468815D0290
233	0x79A4A44BA926DF1F38D671C14E6C586C13EA745A8E3565A034B4BB7C9971C7F1 76E8B8246014B06AE2188097CFAB92969C87851653BB7EC0
234	0xB4688AB67E54B6F765B3D4AA95389A1E335411E16B69CE544D4D2C021591B67C A50F3D593AEDFDCB5D4F04D0E4905EB2BF1B25298CB33EEF
235	0x2B59C7CDFB1C7901540C7D2E2F825D13546CCE9BFE581AE2E665516DBB0B1636 E86278B5B8DFB03B23AA4672D0C1858FCD0289C9034804D3
236	0x801CBBCEDF98A0B265B852161C33E05EEF15AE426E865CD6928CC35F9502D058 88A1682E300919B4479335FAF415D3ED6D2307F674084FD5
237	0x9940736843A1FA7F737D736C85ED147EB8189AD4F6C2DBA175A618667C3885C0 598F7894D39B892A61BA03E782744CCFA734C1BE402EADD4
238	0x5672CAF746A999978C2456660A7198F7D946F37822501FDD361DE33994CE3E69 041327A103E5B8C7979BB342F261EAFAB1A66CE844CB959B
239	0xA636926C69A677A2AE49D303C76C737D784B48D0939ADB303ADBF740A9AD8C38 2D4EC3880C18C8F769EE7DD748257702B5EE7BD5A3AFAA23
240	0xD4060307A0F8D649FE99E4B3D7B624354C2DA4A9AB56EF90E6574C0B888C0EFA A1F714116E714807FFD19D3D17C11633E56CB5B3E3DCB4CE
241	0x9F04338593DE55D238A73364786DD4EC6874318D3EBEF975D291D86FD5FF9461 1D87C1484D5A6687907EBC992824755B592DB8CA5D1F42F0
242	0xB2131A13D30EB790A83D281164685E7A19BD2B979A74BB28C4AA32D7C9D60591 12DEC78F6F8704EF27B110269BD5EA224A6359FE0EF6ED9
243	0xCF3D5ACC4DA27DE2487426D34476B04BDB49B3C73C093A1DCE6E821998BC69D9 16C0C9357434976C238B7B1D617286B423C0A775962B6ED7
244	0x4250E188E42B9D5829603E09B10DFB8FC80D810B67CF70DCF574FF2B4DBA3D01 0B15CEE58F11B6B4BB88035FEA3063C3CB9069C98995AFEA
245	0x2A6195B88A6E686E76BA077019096FA13C5BA8F787A046379EA33C41B884BC80 FE967DBA3B821D09424A680A28052AA38D506C4978BFEA7A
246	0x4CC3EE41E0A7F3CCC3BF51DED69FBD684F2A950C8B84D0CF9498AE08B79F2EE2 24E34BD38A308A11D2B72A468DE0037E605755E2F9E75B2E
247	0x89DCFA4F09D03F969641FEB503B667DBB51ED885427C386A188486BB8A38CCEC ACAC849BB69D27A7C9848D02A965A38B6717F4B9BE855ED1
248	0x95986D2188C62E7C4DCF2C25FAFC9BEE1F149149F44495CB38C9D839A20B4D46 6D1D5B8651BB12A932F9C0080C4165A6CB2D03EDC298B4FF
249	0xD27B983E7222061EBE2A28E091DC78C693A1F35870BA63ADF722BB407B415020 BB7F5A4798E7E316E63C6870D7B71E4F2C84461A18DA70FA
250	0x5DBA5373A03FC27409D989E582B80E5327E495A9F0A540F92EF868AD3FDCAB43 BE49E990B92A68BD82E1E845DC46831C18F4C4119C83E658

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
251	0x82A77D2FE0869CA2A883234FD46EEDCB5B443B72564C71841E0B1CB47AB9927D FE62C77CE7AF6C4CFE2D62B228FE00CE87B4EA7D41C38DAB
252	0x8710D54B504FF6496A38D83A86EBFA771483F67D7C0A27FEDDAD126F6535AD3C 50B1EA8222C402E1CD41EF74EF45E7A4EE949EFE970B55E4
253	0xB353AE20CC1AFEBF10E5EDEC772EC57737D13DACFF538BD48B78C5DBC29927F3 A9F5C1D777F75A07155A1AF6E0738F1445F9CCB133FE799D
254	0x3D465EABD261B837601986C38995B3730D72A3B890E03AB037963893415DD129 BFF95F60AFF4202CC6A2D018B9AB9BCC9FC1A6318E92288A
255	0xC57E59AD22C191113DCD14318112BD766BE2FDFFBC3B662BD2DA1C015024A389 4D42FE8414C365ABBFCB45FE298DFF5CC956109EEF75F47D
256	0xFBCE0EDF82F0A3C14E3400E6811FCAD71DC58C1CC844BCC9BD82385A937E4662 0BCD558E5424C2330A6FE10021A467697B4A6C6965F78FC2
257	0xED0195FEA66B02943F332E02240D1BE354DB1F0B306C520B6024C45B5233549F 0B0A8A99CC2AADD44BF91A8F67A09BB467019EE3922AE951
258	0x7C253219E65F784B955F5E1EE6A2E891260A35F5B5A182757DC320CE13CDEC29 726D0CE60207438125FA737D90D708CA538CBA367B0D607B
259	0x3522F366B4E223ABD3FE7AE09FE1B9FE9628A72007E0C239C17B649FAD427CF9 B2CF949B7F8625C25170E8ABEFCB1A71298F84A601101E99
260	0xB8982059BB668B6CFB58FA2408F93C63396AF3F484B78C83FFD3DAB085F50F03 8CCED552BEFEFC161B506D489B1D54E811FF4E063471B416
261	0x8B39EB05721666F55D245275404F31C7751F552398F698B8DDF22AAA7BF547B6 FC8BCF8113CA6D3003948F2ABE4C5417D3C2837C47AE3DD6
262	0x9E84FF6C9F149A809520CBBA56FB8899942F5B40DE7A864F0E942C37BF9AFC7A EBAB996514D3F348DCD2352DEB29A84D9EEAD92205A1CC19
263	0x1BDB28BFC867CBABC421F8F3DD95107971BC51D5280EDE13E1642338EA0B22E9 3D2F7B7918D87FCBA504755D0E7D1AADC62D6D7751283E62
264	0x78EF6F137BF8735F683E8A2A31F3121D13B487ED833369FB4357D9442A6488E7 49541BD12D6CF032CDDDDCE3DEAB17BDA5249967B8B47ED2
265	0x949FF29AD6947758FB8AE2CD17144C313CF350A72912AD18E2916292BA09A40F CAFFD702B8D22657A951CDCC3F2E8AD304E2DD2A868D9F48
266	0xD74CE5364BF4C7B925FF2656A2D34FC32A2AF0D78FCEE7E68E4BC9147A84FC0E 147B2599CD066C5D041FC6711C6BA61E2839E5CE9CB6955C
267	0x54A2049F7253D0CB80BCD596FFC105B33EFE8C8724F48026B1DB96791A02B7C0 C537BE7CBEE96A1349F77683551DFA5979FD86EAEE5E720A
268	0x981CD51EEF6B2FE7FAB8808009DD3F3F74626EA9A4738F0169548B0CDE3EAE1A A137C21B0FBD05FFBE72E43B73388E5826F54AB8B0CA9139
269	0xB9DCCBFC0CC4AD48BB45227F2BF1DD146294726A3B9F7EF39A6FEF4ED96BB64D 9122FD51C20173084DDD215CA2AAA6A1A1922AA05642C41A
270	0x515835260826AF6B54B0A0F087BDE1CC792ED93C077964068ECB4C16EAF30BDD 2F9A65E4A2920185AE34C39A2A868357C17DBDD462B8A24F
271	0x1F7B4FBA125B516A1D478FBE33AA35FBFBAC1CD7A97FEB497E509AE8C61F86F4 F4EC8D0B834480CF5A20F5BCD0A845DD1B98AAE8785B42B0
272	0xB6B2782F75C89702DC0CC93AED8C3AFCB9792ED05EAF632C0016C7299F552A9E 71DFB2B60172844345F745825729A4CF6831E2225B5ED35B
273	0xB149848CC0895ABBF1C0CF21405384152FD50E7C1B7B92AB1FD1E815B6D6CFE5 A5985E67D3C75C23D0CB29D6190C65CF75C2DB233F19FDA4

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
274	0xA202B6518AD7F70DF5A60884F0A9E899F368A81D9120DB25B96C1A28EFF00B78 45DDCD34AC5C992985A2ABCCCF8C8E46C08F35DB3201AF34
275	0xD95D681EE969406B78438A3A57327E854BC769109DEC30B4E35E622C2593D94B 59D0293577CB5B4B90E06C3610AFF1EE0C537712F676B623
276	0x5D7145EC9A64FEAACC88E577E9D11895157126FC7BA233092F603C018D3EAA0D 6679E0B0A3730E04BF2BCB5659FC401A13E82089BB891255
277	0xACA817FF8E3E9D05350147DA4BD9D7F314726DAE7045A4219E39C6F9E618E179 FE9D22543A62C0267122E763C399674B449E473A7AA6A30
278	0x249CE71BC2D490477E6C5771110C20F7C6700055C0D842A8A1C5B9C706B3584E CA3600D2BFBB9BD2770A2ABEC51644A4B714F59F30AA5A13
279	0x7CECC0B0E62E7A944477EB2F091FB46B59BA98D2D7441C8F8E0A09828E773C9F 1CFE3001419671F4341A1D497ABEF04935CF23918400C6A9
280	0xE4C7A44055E173CE22B6E4F1F50F1A36A863AAFCF76D9417799DED3C5D7C14F0 E308B6093890AA9A10CEE824FC8A0721732B38F294ECA63D
281	0x9C3AF0B1C4CE7FFEDB182B97AFF142FE3CC43E3115535214354323FBAC63D15C 770487FC4D49CD0B67002F518F0A20730DCA0402D6F47294
282	0xF43EABE4E51AC0BAD7F5DEEA47EA67B7FA5C04A578F34A08240CA37E5E60EBA2 FFA3FB2BAC03E135C9E87DCF0DC63F28F12BB23732806E20
283	0xDB472099977E54C7295E62E829DDED3906F8BA51EA5DF2529C1AC75471F94312 A3464B926CF56BC3E48876789F01255D24F71C6FA84CD2E2
284	0x59310DC459BD272B55A84B66A78AAE3935BC0008417BF7AEF83F162DECB66597 F80765AC14AD39F63B16D1C0350FE1D9BB85DC1B8B4CF409
285	0x3B63F919B2DD609646E9B32AD415B1CC6F13696FD84C8E31219457CE70F32C3E 57028A7712E3CFE4CEE52AE44F3FF15B3F7FF9E58F7163F
286	0x3226BCF9A0B01D2A85D4D4C6937D054EC5731AC2AC45184A23024813C396C908 EE709A3CD96F848E4BC2A2797DBACFDE9072CB8785394082
287	0x128E1D000DB8CCDD0A2CDECDCDF247F55049C62A0C0D6FEA70FF57983F24674A 75393ABB26C39F941AD757E35E581DFDDF10F90067727308
288	0x8457F91F767CA91CACD1B59914BE5F38F7C055231DE8E815DD9D373C1FE69CFC 6FA942A0EE5FEF77E7B6D2CBFD9A5EC6BB681B6B8D70E1BD
289	0x1E485B9EDEFBD5DD56BBB5073D13A6D56169E0A9D72BCABE481A82032FF8EF36 39F8E19F60D102643538C317E15940D82105AE543FE07BF4
290	0x33B18ACBE49E8BABF53E3FE7E6D3A8052DC05A3A10606305811DB5E39248D1D7 C67875783921BFDDB03D4B5633BF2BF402E6ED333B97F077
291	0x68472F24C44A8E605F13D3DA03BD7EEAC3AB21D838665523E2999630D7ABD7AA 4699A404C7B1EEE0B598B20CD41A7C332E2EF43C27874B3A
292	0xAC089D26F44DBE0CC7F388AD8B7DB6423FCAD5D041338CA6CDCD9AD7D38C8760 05B0966B21200D8A8BF6C29D4FC2B9DC6613DE56910C80D9
293	0xD338BD5751854723D33E921FAFC4BA59433A300505D31C0EAB9C9DF66A773224 1529BFEC054CA4B3FD072844DEC1B8EDA73A6F0C7A211D15
294	0xE63DAF43A33BCE2C9A5544E658779B84B96EFA7C39195C769DE349CF38138FC6 B2867E6F8AEA27C1D4D1E148153063BABBEDCC512D738368
295	0xE493A6DCB2C134775CDD43CA1C31E22C0C686CA3346108BA0C953BC62C6DA43E A36875D7035DF588C1BDF55D0DDDB728B397E9F788BE5031
296	0xD994EA989A9AE17E496BD6C8E6BFD8D27F3A2337E6FBD830F8BBF24B626F0CD6 7B15E6872EDBC05D6072384B6F9409FBB0CEE8F11AAE762F

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
297	0xC4C29A8094C6FB0DDFA9291EF899D5A2A904F620E99AAB9E3D0A617ECE417B9D 5D85F457BA6132250AED404F5ABCB51EF2459DEFD4EAF769
298	0x2DD3D0F73697620921DD8202FF949CC662142F0F595B996BFAEBB69DB7AD9C42 9DA8207BE0A2321227592456075FC408C391EEE782B7E08D
299	0x4DCF65E3C8877A533E9FB18948B3BC7C4A9F8CB11D5AACF19E6237D2BA1B739F 44376BDF7ADF46E4E664524E8BA4B1B14D9C9183EDE410E9
300	0x1FFF4BAA9E30ED7F78FE42B56020D03995CACCE2B75E129EE2ED0545CC46D723 A97BAEB0339BCC0024B293D8F12C92528892B3F8C3A092E1
301	0x9707D1B02D8169CA2207A54459DF4EF2B051B4E9985090AC9FFC17E8521376AF 1091855B8458AD55F6CE65B3FD34AAA2A19E32FAA9C47B78
302	0x7A0E484547C5A3FF6549F209AC1F3074C51C633FDCD71365914BA4392964FDEB 69CC60329F0C9F3F99C4AA00B214D6558FC725B237C189F0
303	0x34CF7265273CC143EC970D5C7288ACE8FE6AA3DEDDD59B91E40E05A8EBA4A22B 1C9514CFA2477DC5D48CD7114E48E8F083DCD58E5C93C66B
304	0xC4CD0FE9B474BC00115E2A32D9F42F8E06CA31F5E1E7A0B5227037D3C2D163B3 C43458F37843A2C06B4C4BF7F4F26DCA2A5277188B2A9ECB
305	0x893EB9604C88AF5D5933E3EEF435C146877A332A6A4C47316F23614A0BF6AED0 92F7537C6B4685AD1CDE5718A1B7D2B34C3AFE476E6C9727
306	0xE7F520C444B2BB546C6BDA5D5121D475638C83620AF77ACF9F058E917528D7EE 28ECB7038ED7F422150FB88C02840A16CA89A1BD7FF670CC
307	0x9DE0B0A036EC1402418A2FFABA08501DA63FFC02946B4A719DDA8F1A1DDC6894 F2EBF6D523BD22DEE4B5F9BCCC8183920CE6E425AC862266
308	0x1EA61427CE7FD0BEF3251B3A9D680FD4DB3FCAE0B5C0C847268FC494BC3D3643 91854CD6A78A9113EBE193D84279FF10F479B1CE0EA3795C
309	0x4A3E2F410062FD674DC14E2DA52DC72A3FE64F7043BEFEE0D573230227D180AC 419B9E6D7843483CC6C5353F2C4E013755DECB16A4DE3F2C
310	0xB7B453162C78182624763D8EF624313DE20F798DCBA5CFC7FF2E04680986DD13 8C49FA0C763FA0701F26CDD2A3CCAFE7950F75058E5FB6BF
311	0xE9FD2D902F28927E18595C2EA184C656485DE5638D7EB5681F4DF4ECD7894A86 D9EA16E8ADBF52ACCD0D6F79D0CF80F88AA9F810C9C30E3F
312	0x5D56FFA90DA1D1CAF91C5C14B61FA4E040D1B6044954B8DB4348F6783A85110A 1EDBCEF4F87FF2AFCF66E51D5D643B8689D09CA85028466C
313	0xD11913D37DE9AD469347F9028D9274CDF408328659D6275EF7705DDF2DA27FFC 29C3AE2EA4CAB2360EA103229A8E8324EA1FE7FBAC741EAE
314	0xEF64B5A647E98E5A72E9D534E1DFF370155456E555702E691FB00AA58BD1C643 4D452934AE31DA0D2B2406FA4F1225A3FF95F9C365CC3954
315	0x5A9956E7774260F9F127CD4F2F158EBB6746B9E4E65E76B2B3D5CF7952EC840A 3C513B89081A291572B67D67EC5CADB6D8A35F6458256D49
316	0x46EA55E6371FFB356B467F08116BD7015BC5D43F67100BC98D50484BBD9FDDF0 061F0A069591F420E6BF8516262FD2EACDBB402FF0595DCB
317	0x5BE2961A7532C374C45642507663516F3F34BE8089193E6D99D01F4A8B76E5B6 32A8D73EE05A66650AB04E2B7595C76E97E713D6D10B8BE3
318	0x3568D901DC2F29957544CDCDC104A7E4226C827A44833FBF09B866814B645275 8A702B97A7ECC3DF7605665B98AF0E00828EDE26385BB9F3
319	0x8144CF56E32385BFD8FFB713FB063F004DFA7509233AA7B0FEB90A405C54C7C1 52FA31B2521FB212CEDE6690BF8F9661C51BD4B85E17659B

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
320	0xF63657B5AB1BAC31FABF7E5501A4CF4A7451DFF5429BFECFC39D4D4F60B52338 78F7489042452316E9617981D8A1753256A753FA45B52AC1
321	0x5C50C81BCF1B08F6FB01F01548941F7293AFD36833D465AE9A14DFAB8A02B3A0 50A98C5C7B20AE7271D93B4A81B5E6FBA94D01C73DF876BF
322	0x6F00B951E474AA2252BB9AAAF8ADBC265D5DB06C16315E5112BA27548BF67FDD 0B4A99DCED500EC349970D82B1071907C5ACE8C5AF3FDF5E
323	0x54106D89F19CFF87DF826F1DD1A1C0CA361892DDE25FBD0B9D55E3F4EFCC26D0 4362F1F7E59C4750F2A07F9DE5A63F04DD89F10E1539A38F
324	0xA700069EE1FDAD9A0E510A20F21F16275A6076F0E3BC497A900968995F80A88B 26B5DC619CCF67D6579389E3C202DE08CD8BE682C1726366
325	0xAFF38C78048C88E714FD4EE5D5C156B9D127BC3B19BFB26D07BC905E76B1162E 58CA75F56A307D3DC42DB31B9616E06F44415E2D25C7B89B
326	0x271389C14B62743B5A259BEFF83447F0285F953C11AF8486A768ECE8B7EC1CC4 4C402680B040BF8C2A3BBDF3513F052F6C27919D5EB08BE5
327	0xCAD4FF6E25394C5C4081B0039C00618CBD351FCEAA23CC666188E2342F6B1028 EA3568635685300FEF468EFCEBD57238F3D559EF8507C6D3
328	0xC996F44FC666221EECA24B1E6FBC4C537156FC299A11668EB0C9D1F87B83C0D9 A182EE187ECCC1057ABD0C4A46466A5F983C71F25792FCCF
329	0x160C7C4836B93C99E6CBB94E342D8018126B475C27EE9254F507F2474E3BCDDA 37D3B0C63C3CE4AD13B8A7BF02AB9F3FE7ABC09596365B7B
330	0x8C303C9061BF683FD54A8BC429DA485DD9E85A9ECEE6C1F90A1D0A21BC2E85D8 354969103A398037170058A08EE05AEE40CC0A0CA0CD038C
331	0xCCC4989C882C8CE75784C939080AF5560A0FB8A726E3E0D70F2850A65316E9BD 32E246ADE7EB7D46099032A11011F722F650A81E9AD70448
332	0xEF3C881ACE88C76C6B83D039282FDE587474660BCF9C499C67A5496D3537AB5F E36A2425D1E18CDE262BC31B85FF739C5E852FA98AA1BFE0
333	0x87F332F39041F7E23D679D30DED230FC61E9E79E1320F8BF4491991A8875104A 18224F797E7D7873F83603EDE4C83B3E0BAFA1A16F7DC5F5
334	0x128382BF385266E57D4988FB1364C1D7AEFCB162E53BDA721F4B208C2068E6C2 B8E3CE5A15A997159F58707C2D60B16E26EEB9FA5B41EE24
335	0xA3015BCE0AB4874CC480AA9DCBFE4735A24A601FFE90ABCF6B7D93E8E7255DBE A780586E544008FE7ADE886ED1223AA0507DAB7B7A89E0F9
336	0xAE074603BD51583382847C273E34B68994E9AC7C277F621577AD48F29BEF0D22 AF251F93305DBB84A16D93FDA1FB1BB36093907297609B7C
337	0x72CE3690269DBD69516FE5C88AFB173A2D2F8D15428267FCBD613ACAFDFFD4ED 80ED421739F631F35C1EFF538F494D0A8F867AC866044DC7
338	0xB5E821557564766864B06999AAB7373BF1E43DF90B1EAD72F9C7D42619075325 D12A3394E477C6EACE4A78574B3E1246BEBF084B20D750B6
339	0x1D59D95DF90BF7597870BBFF349B0D9CA9C3444D26FB53F806524782078BB56D 914ABB468A65A2C5DC7A9E4D96D0AE888CC06C04FB2E9213
340	0x99489BB4E0E95F19CECF549A32E304A5CEB2F603A856EAD38CD1450BD85767B5 6F09487EABD69BDC85A658BAF32C42D1E3A6AFFF5FFC770F
341	0xC4448BA46083721ED73DD8181D6AC1D3ADBC53C65397426F3576F99D561D4142 92FE1EF922FD62DFF1F5E0EB3F0C558F5F4361960C5DB06F
342	0xE8B70CECB3969092CBC6D48AE9D892E4D70EAE30C5D41A39F48CBCBDA59BA1FB B2C1409205A17751FA2FE17CF6CA7302C01B8E342DF186ED

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
343	0x2B24424CA0539DA62DACC488282F7D6C1A682ECF8F55D9C8A96E7B6B26E87B8F BE24CD381B515CFE9E9FB8F4E8CA3B8A8073C7381B7956BC
344	0xA6A9FF6BEB87B7FA237B1F2236EC725408BB6FC04B0410744C81880B7A5D945D 116BCF4163FEAA7384EFAEB9219CD55C5341358DFE661A54
345	0x9B7E49C8F54543644DBA7CABF7E8AA097A3A9C43F588EA61F8E79C464D109E1D AE4A98F4A378C20ECE3B540FB0FBA141A910FB8268C035D9
346	0xB25C2B174459CE1EED4C97EDC6D423B2AAEE70EBFA0A29D0AD5B9AA3F225F46F B37957FE63289427731BF9E5F7F42E3C46FF132A67849B57
347	0xA08A7328961270BD611B00C021732A19EF302486B1605F4FC64B69C5535D9A77 ACE1E7C6AC6DDA2509A79A0BDE1A0BD544ED94B934742113
348	0x8AD303A308A2B432E7664DB5E2F83015D44E9C512A39BA9FF1B0D1D1D4F3D254 60280EFAB6B52061662A267EB15D081F8881C381159599B0
349	0x1191DD04536EE63239BA636FF06CE07B3410BFD0CB6238D791157CF69CC944B4 D2F7E49613138A3E7E74413DA03A85E6B3D80D8C8014697D
350	0x947D65B60248DB9E9BB522D5951D0FDB510BEE6E72E7E9BC24ED8441BE6B72CE F4299EB80D3AB5E178C268896D777F2D1AE85EA82D6F8739
351	0x32253A73FC6896E09914B8CD865AAA98842377D6D85674DBC4680BDDC624B094 099433182C742D61FA7BC16B3FADD453AEA4520359BF4AD
352	0xB61CF5897D40ED0525FB23140C26C089A36B25440FCFD90528016BD80B5DCB9E F0FEAFB2E04E466F841A5F7689B017DC40A5C605209F6155
353	0x838D9AAD441780CC60A27E20E012E746E428E629048EF57CDCD1FB665F2C1ABF BA9AD017AF8DF5359F2E52BC2E3790A67B55CD96D1D558FC
354	0xA26EF65B1D9DAF5B5E32D20868F5F3EFFDCEE04407DCB478D74E08AE8851A99F 40807CBB05F0CA6D9DDAC937F879974D272C6EE04AEC92D3
355	0xC57668DF3F4641DABF603DAC29D4BC1F741530E84C67DE085E54045CA1D5BD5E 5CB03228E200E8A2D197EA83DA98D8A788364C12AEE545F7
356	0xA9271834B7C08B404A802A34447A10206486DCD83D88D307A934D62527B3558C 023BB443784ECBE7526A3900F3BDA93F53D46CA84F64EF82
357	0xE84E662CA3F2B93082BA36B68C14C6A6381C53A87EDDF782B061D521291DC925 27B0DA73E910F9B159A50E1756B23FD7A7E6AFFFE94CB569
358	0xBC0835B891AB58C1E63C2A1313746C56322EFD0D802B52169A0BA3D9BEAC66FD 3F52B71F9F5F8797283495DC42F44E24A01FB51EC64B59C9
359	0x6E918312C6EB3A65ED8023335B8BB39322849BC592764C2E9070A6CE7BE8A930 0FD0D09D7B9D130E2939B7BBAD5C07ED52B27A8D040B24EB
360	0xF02CAF8FAB05BCAAE3FE62690B978D622027DA5537B2B315C7E641364EE1C6B3 730BA99638256E3398503F7B42CBC059D75D3FC91F5CF1E5
361	0xA98C6C1B195BCC449550BE1C4E848D37DCCC28D1DE6749E3CCCDCFE137F2E0E8 8134B7630FBDE6233E1EB993483658964CA806ADA70240C1
362	0xA9C62927F505F86BCCB5D86321361C09ED028C0439F65B1C02D60B6599554526 5871450CD12E2CC47389CB2AB8123036DF6DBF251AE6F466
363	0xBEDFC3F9D709B915BF1345C4654E5A5C0C32306BEB3DF7F30CA10EB1E47DCE90 C94878D56EA50267773F907D3272ACB256816D9945A89415
364	0xAFB2C32833FD924A91BD8DB1B81EC90424C71AE25EAEBC2498D30EF299469843 6A5195F8AA302ECC9FE9E23E071B3FE30C475D00CEEBC66D
365	0x52396B781B41125651116AD0C2F62B46749CF3F11FF46B4558011E524993E999 92D8641E427602378C3EC150DF4C24E46891C06B5BC1496A

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
366	0xC5EDB425262C57BE2F16472B2881C935BD3BAF1329E8F06E9FE536442F136B06 119482DD5C66F1E0175B7AC2694C2A0B2FC68D9355480910
367	0x700FB65918A02ECC6D3BFCEC2E8B2BE02C00B558EA583C95E83A0530ACCA7298 186C1EDC9E4173A44581C0EC1A3B997F467BBDA8B6ECC624
368	0xEEAFDE25CD2FB59F56C17C506FC7C730A718A589D42169CB4A37111686C92CE6 927AF738C68D85F590EDECF31A53DA1CDBC6D1E27255255F
369	0x298440016396FFCC3B1DDB860EBA1C7EAB467943E09B94E7790145C0FF6EBCEC A01CA402F24D5EFA2845F069E9033F04A28372B5C4F789C6
370	0x689C6D1ACCFF44707EE1EB8312F79EA899573C16AD8393FA683F0EB4D306CFE0 51DFD2C76EEBAB3A1A841B9E19B86B56EED80118F716793
371	0x851CF24C275925B162B99585BBF3C1BD3587E90A091ED0220BCA817B3A5C24FA A7F70017D04C4E88CF05C0DD4BA980FCBA60C36E3A4DFCC6
372	0x9DF7FE26932598A7CD9BE64D537AB13EC73C5E6A5DDF4C6D23E3EB67FBFFBCE5 9D49077CDB67190630E895E8CAAC05EBB9ED98B204F6302D
373	0xDB2108A6958AB3674200B17D178D0E763AE8A49B5E7627182995FCBDE3F7AF93 2DCB32DEAFF6859A9D8A9A1663A366196EDACD3C1B6C0B44
374	0x32BD132A7F8640523677E7901211583B84DB1836A5A40A7205AD655EF2BF755D F4E924E7E3F93AA1C6D1932A7E0AF12DD2A691A03BA381C4
375	0x435E832ABD8B88C278FA14B5180DB0A09A38DA7707C57F4CED8F6B16F7A7AD68 1A8504A40CB19C8316B7E9D6DF8E52B74079591CEE444978
376	0x6566DBD3CD78CC81277CF9FE26B9D9248F80FE85B9BF8091FCBAC8BBA1C73064 CBA7DD0EA5E7BAB3305BF9AFB999EB9224311E7413A20533
377	0xB5C76CA52961AE0CD2DEA1F3144091483F26F6B7CE02A8A9E881050FBB421D92 E2EF41C7886746EA80A1B50029BCB2A92D3461C1F3B3910D
378	0x256412D4C9F251B5711A83BE142E06AD61ED432DB7C416D7DF442BF1B062DAE7 9C91E0F4E98E30AB9F8A60883A1F02371C0FD83A7EA72999
379	0xAA89E5F9F8DF68D15D15248797E9DC42538A67EB000A8637A53C78A585AAF346 3CDA407FE0712771479FCEED790971F0B85633B7BB2B9B72
380	0x2F6FDC882DF3DD3A394672DC11CEEC66F21B1C5E51D6621FA6328C189B918D77 B72EBE386D7E505CEB50C01E399A45C2ADF84B5033ED0942
381	0xE7C134E6CE65B2F78825839CA59E57FB7974730F4C4995B571DDEB938904A46A 6C52165995BA28A305015BB3F18348E8C437BBA5D5897D64
382	0x1421759DC60739D2AFE43CE621D85294F8D27EC55DC100FEA6FD91B4932978F2 5629D31275251CB5C0A2E32D50CAF0EEBD40C78DCF489B80
383	0x1C1E1549432042A2658C64D22B0A60597E2319DC5373B6EE35A78222EAFE5A89 C7A542C5B4EDA7314041FF52A8031DB5239578861FC5B666
384	0x5766D21DDFB2872DCFB4BB638BE363EBB6F4E8502D71A2139C7C7453B64C9E99 1E7A466FEEAA46B8BE9CAB85B638E9A8DBAE70C7655F8DF3
385	0x3F01E2C1B881F99F162A98A35CE37C3A72BD6380379FD5888148B69E23699D11 0A628F9A8A0A327C4444EC00EC0B12D4DE07BCB173FC39C5
386	0x250E341534E453F0663DEA1D623F1FF67BE611B657AC74E806EAD52A0070FA48 321CB00A76A249E3765C93A5D33876C0716F6A76ADB20B31
387	0x879A2E1345E75FE68D9BA37F2AC10ECEF5DF51FB9E01549B9B65F56434262131 40DFAFA637A5E4B1D3CB2F3567CD3089F2DE0F5F2E928273
388	0x221C5CFC6B1419CB20BFB20400000DCF74CAAD432C8C2E0F5BF6CEC31039FCD7 4095D948A5B2CB73DF3D832A793E9395F5B93DC6CDD6BE0D

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
389	0xC817D2BF9526E3350DF74D0DC64320419ECEE86FA6E77BF13C560CB8EE1001F6 6EF0FBC2FDD6C315FEC4FC34AA4EF11B4E9E97840F91C821
390	0x2EF47AB5D42CF80193AD7156382832945B155C2562504090D7BF546AFA5BB769 DCCD73A63B2C08E4974AF5B9D68E20454B36B0E3980FEC47
391	0x557757DBDAECDE484E6878A3FBFA531EDCE19A7265E6DCC13AA5A1DE69C21518 BA6B1A0CA07B48EE60F07C8BD1F4B8D1525C8165739B7787
392	0xCFE46C77E253A76714F5FC71CB6FC3143E04F68CED98D8F5309A85BD42A232AE D3B78FAC9FC6B66AC5EB8D5DB31692F02994358A0F5E961A
393	0x9D9C6D074763AEC129368BEBDF924101842CFDF2CCE5B1BB5604D99813B24F76 065052EA5E89FB7E8ECFA98559244EDFB9B01726790B9875
394	0x8157A75411F1F6ECDD77C8FFD3F3482FB247CA085CAA7F16341E60358A1DA8BB 5472882FAEA133CBA922E1D6645E1B51144E5DA33D8A6CA4
395	0xB6E3DC6618E93DE1A2454C64DB7D38BBE9059CC0F2AA200F971166C3FD707648 8670232F39E2E5B609DFB83165FCF0BCE6AB3FBB69098F08
396	0x80E6702C34FAF34574E43AAAB3CD71D3CEF07F520456BFC0B7D4DA4CF1A43318 2D71ADC6589D673876E7AE6926E525E14FA5C5F655DBC4FE
397	0x57500DB5047A871FD1885918DE8DF7B2574854E8831BB0282AFB929C33236218 5669C46A148369B3B64518E7154EEC9F046D0FC7CC0E8DBC
398	0xB852E77C5C765A60FA1839DB8ADDA7FB1BC107B6486419556C393FC6517EB300 38526EA60E2D13FA724A83A9B8E2B9FD20D2F2FF9EC2B02B
399	0x1032F48F8D9D84B723439812FCA37A64697B91991C7913EAF90F2CBC437C29DA B98775E7AFAD29F379706345F1E52485518D85056250FAF8
400	0x5CA862ED34594EB037D5C9A91CE5694CA395B1C2E05BC95520962121D4E9867C 6C3D1F2D8EFEFA1C060F92F977A9067DA5FBBAC4C54EC88F
401	0x603B1517FFE1455C5AB24E84973C65E5077A5E81B3F1769632EC2BF1989467E7 9252A200B7F9F39009F71C7B4624F74ADAC98100808D21D7
402	0x7ABE78C38D202ABE8D540AA9360FD4C62B8BFA3F045754F8736115670686AD49 DAA0E57FDBE142BD5571DE0C673BB5DCF92048F394DBFD56
403	0xBD1D78F3C67D7121097E8E0DEA744302BA79F1269864604B230E3D07AF474B29 00215D5BE5925BF34CBD5C6730CE9366662D334602E08683
404	0xC1C28B305FE9AE3EE4097C5278C9D29CDC3620A81EA90A73958A9B8D056E7391 224D84C420B88A6024210EACD2A9FAFFEAFEE968FA6B4202
405	0x902D26DDFDBCFB90E8FCF565C0788F624B69244B9ED19077E2C79D2EEE5E98FA 44FA8636A3BDD0FCBE7601D6C7A363710A4DCE3E34754228
406	0x849C775FCE53BB44FF029331EA1631373D2C8B306BED04D42C32AFF3AD8E08C8 B33EB8D2D26F1DEA57B2B15988AA597BB69D75BE7D6B192A
407	0x5BB61B1DA17176EE38808A05596144FF22124A938AC428D935F897AFA6A32B0A F8B50B5184057FB810C460C353AB28573BE8A12C0658FCC1
408	0xD30FD8B8B86A57C21B23033E29AA6E0B825BE2653F41864D64A54A0BBBF5DCA5 0CD80292768E0B1C78D63B72506200CA0C73001912D8952B
409	0x5D530DC0AC429BC056CD19D0C61DC748BD8856AB79024034BE4306B6EEA342BA AA2721A32FEB98FE83980F88377D243E24C1745FCB8B7620
410	0xBD5A75A98572904FB07E17C7B8B2DE390F7EF091FA1FE2F43271A56CC21221AE 8622DA01DE7F3C1DA8F1DE58DB68925BB6855351D202DDC7
411	0xF1C3185F80FEEF6AFC8B216E14B1E96D16F21F07778084AE6AF37F7576A27CBC B21E0D4C4654355E77CC70D589C439EBBB15F3D82E844B8F

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
412	0xD5F9E77152CC4FAB98FBBBBC042A8436A778F0CB480D71917A8CC87AF942AB8F C473BBB2253C5865F0B9761962FA7F6098008485EB9682C7
413	0xA40BBBF879D56E8625B4118ACE2DB3818C8EECCAC52CAEB4D48B30B2417EB4B5 E3F85F77218AF23A3CFA5853AC122196C0A4974F24C3D231
414	0x63BEF8B43633B060F876C710520C6692B98305D579795BB12803B3551AA1764D 95448A47271D5FEC4E63375BBD88BE4706F300533E18F1C7
415	0x25FEC2347FE4BEC2261E51E53E6CC9F7C3821AD16BCDDFC1C1EC3A5E3924C4C1 EAABE5FF75EF3587CD0195EBE2D84A5E12FA6720803E0ED0
416	0x1031E8AC83C914BD56287FA9AACCF5EFC1D4A2EF4711AF9D5CA3D3A9395360B6 8AE4CCA8E077E0975CF51947A6CE28FA7B4869053DC5745A
417	0x99BDD8886A2036E20026C991E79ADCEBE8C01F88D150CCC82B822F0B47B93DBD 9776B453755472D80B88A86D4AF3F6CBBCF96265368EA8B5
418	0x971017F87301954AB96D588FAFE4B349746330553231F505A7DA221D68CC38EB 2C821E83FD9821991668F30E8F6FCC1E9825C3E3271F432D
419	0xA7A69C677CDF91351CD19D5A28450FB1942E55AC0798AFBA1D07A67A1E557EB4 D222852356CA0F64CCD17E43A64A8C2CA9AFC6C21695F379
420	0x15ADC0DE7F380E059EBA6387EA61DE82E2FC991BD2B817BCB1F4358C639522C1 D638E219325C62C66FB462742C9C05D4B39F05566CA9CF90
421	0x2D804DBFE036176D9B6FF35B6184DA7B680CC2302C0EA8D6AEDBFDFAD81B2A03 2362222913CA8F03918047E8133A14D917B25557970923FC
422	0x2FE8EA8E85900A2F37AAA635225202A2D98913EE2CC9F68509E8AADADFC82EFD C29B3FB10825E0EF6FB1B825A35017E5BC4B9D4C68928B6B
423	0x6C328B88D52750298B99C9001A5BAE528E820C213BE5757D8183F5D49DCB3CB6 1E428251BBE10DC1BDF54D6895789888B915A3806B7DDC07
424	0x75F9C47E5E52842FCA90EACCA7B31E15F2A611994D7B7AFC372CEF47E65E9645 943D9C6C8F02AAAA46913EEF81FB2167F03B699FD42B098
425	0x95F569307EB751D6E5BA28518F16DF9CB99D1258A9391EDFC9B77ECC271AA3C9 C3594E9F32A70A6018D65F61115FF46D634D57BC41451813
426	0x4CAB757F3303651A898FFDC129B54A10E418B3D5FA833F15EFEF8142B4366F1C 79C32D83F9124825E4A16A91FC867AC0B49AF875D0249B21
427	0x7FCBFC82CA1FD07EE4EA56CFC4BB85CC6B80A80AEC079564B8F2C0B475A113FB 8F7E39C71995C1B06E952658D79B1C93A6E6A903521EA96B
428	0x999F0F163B5EBB33AA1D10A46B88D10044EC01CE3E3AEDBD78A768C88763D48B E406FB196F4FB2B0528BE24D3354317B0D49EA887391B4CE
429	0x9534275A7ED81507383F1900F6D78375B4DE26C58949C0FCB03C2992C70D1981 A9DC8FED90985E82D7DB8C20073111A16B0C7B1ADA136545
430	0xD7C1161D88C914EB48D11DEEB8B8B5AE9001D609C58364CB5F101E3C0081D6EB A04D758D26A6A8AEAA0233C59219316CFC35156941136655
431	0xFFE86F964A4F2102B42485685519908FB59304A2D0371435E54250F5CC95420A AF6968ECA8EDCCEC633D41907FCE46B00D7945B85AD4C7B6
432	0xDEA28995A63A5B0BE666D03B09CBF2D571BB99BC75669272A934AC9B883FCEB8 8E621FB828A1C011337BC2E27B70C6AAB195A8B817066A8D
433	0xA90ABF865B9C2C77FAB570AA1EF9AE0EDC08B1A3789E121B8D69AF3EB1E3B3C7 42CAD21A48A404E15DE74831AE3F5B81CCA743FFEF5795D
434	0x57BCAC21117E7A1BF3432E3DF924FA1AD6E94D323A46A2CE78EBB1FC4A14A29D 8257290F7BA4829F693526DA99F38EA2A98253551BD5FFE1

Table 4. Continued from previous page

i	$u_{2^i P}$-coordinate
435	0x99467BF6A83F2CC1A49014477DB9927A570C4BC7E26C78F5D6FA7D2DA3CC2989 BD721673B13EA7F49A962AFBAAFC84943EEAB9373CB51BC1
436	0x2091E525DCB1FA187BB2433D27C551970034366DDA55817BE81197E4BF92E974 AB716D3A57C8E78072E54EEDF12FE66245A62075B1D11DF
437	0x6160E08D1053EC0AA4D624F6FE5CAB32BF166829099FD85D098C6ACB25C854F7 E61069BB1DD3AB9A4600F0639F99F004C850BEFEF62DA953
438	0x9190C83B321EF2C4639552871C7993F1F504401779CF13553C719F6319CDF464 CD16182FC4D2D6ABB9796D90FC6DF9E0B8356E39FCC0C6B0
439	0x1BBC8A82A32596DFCC9D04456DC803A6FB175493509445A17592BFDDBC755C04 C58AF03EFC0D287757EACFDDC02B637C25C2E5C3ADA1CA6F
440	0x8AD8AF7C76402EF93B95B8CFE1B5E1B37E8A7423E326A0102B84F618B6B8F28C 42B116AB66A7A70DE5A16C6D2E04D6E7D965BAC2D77E1FE2
441	0xF3E9CAA55BE4F19E68DE103B885E2103C4AB39EB7B8A4D5D3404F6BC10616DF6 BC58F7E81089380EE899E82633AD75D3CA8CB00B793565DF
442	0x567F202FB56E9366341D15B7C9B8D70D480CE0E4E9DA4AA605F83BD7AF3DBCF9 06AE588E219410EE65827817726D27193222BF84A3E95568
443	0x5DC7319BAB560E9EC5C72F81D25203C4547B0E4AFEAB500C800821479AE43A02 1F5DCF214CF38BD4F4223F33B02D1FF6805F2C0F5BA8FF49
444	0xAB2D4FDC41A007BC0DCF9FB3735C2E37912BA6D72D769A7D6A425E73E64CDF4A A74B512A7C4706E97B240BA620D658018683D4B3CC82A9E3
445	0xFF1D656417FD26F5911018CD3E52F5CDA5D5A7547754C58BAE89667DF84D3312 1E1C2DAF0E0E43E7905082D686D666C3C7C7A2C9E877968C

B Magma code

For the sake of illustration, we present an implementation in Magma of the X25519 function based on Algorithm 5.

```
/* X25519: fixed-point scenario */
clear;

/* field */
Fp := GF(2^255 - 19);

/* curve */
E := EllipticCurve([Fp | 0, 486662, 0, 1, 0]);
h := 8;
a24 := 121666;

/* base-point */
P := E![9, 14781619447589544791020593568409986887264606134616475288\
964881837755586237401];

/* point S of order 4 */
S := E![1, 48802004052532134862652268456126542835229456083994414501\
0858506225439688879637];

/* P - S */
D := E![0x215132111D8354CB52385F46DCA2B71D440F6A51EB4D1207816B1E013\
7D48290, 0x5199331F1F5630BBFA49B1B1B02B207B493D0A63BB4F8F01C011242F\
9C6E9E7C];

/* scalar */
k := h*(2^251 + Random(2^251-1));

/* pre-computation of multiples 2^iP */
PI := []; aux := P;
for i:=0 to 251 do
    Append(~PI, aux[1]);
    aux := 2*aux;
end for;

/* X25519 */
function X25519(uP, uS, uPS, PI, k, a24)
    /* init */
    K := IntegerToSequence(k, 2);
    U1 := uS; Z1 := 1;
    U2 := uPS; Z2 := 1;
    s := 1;

    /* main */
    for i:=1 to 252 do
        /* timing-attack countermeasure simulation */
```

```
        s := s + K[i+3];
        if (s mod 2) eq 1 then
            TU := U1; TZ := Z1;
            U1 := U2; Z1 := Z2;
            U2 := TU; Z2 := TZ;
        end if;
        s := K[i+3];

        /* addition */
        A := U1 * PI[i]; B := Z1 * PI[i];
        A := A - Z1; A := A^2;
        B := U1 - B; B := B^2;
        U1 := Z2 * A; Z1 := U2 * B;
    end for;

    for i:=1 to 3 do
        /* doubling */
        A := U1 + Z1; A := A^2;
        B := U1 - Z1; B := B^2;
        U1 := A * B;
        A := A - B;
        Z1 := a24*A; Z1 := Z1 + B; Z1 := Z1 * A;
    end for;

    /* projective to affine */
    Z1 := Z1^-1;
    u1 := U1 * Z1;

    /* end */
    return u1;
end function;

/* Diffie-Hellman: key pair generation phase */

/* Alice (dA) and Bob (dB) private keys according to Sec. 6.2 of RFC7748
   after the preprocessing described in Sec. 5 */
dA_RFC := 0x6A2CB91DA5FB77B12A99C0EB872F4CDF4566B25172C1163C7DA518730A6D0770;
dB_RFC := 0x6BE088FF278B2F1CFDB6182629B13B6FE60E80838B7FE1794B8A4A627E08AB58;

/* Alice (QA) and Bob (QB) public keys according to Sec. 6.2 of RFC7748 */
QA_RFC := 0x6A4E9BAA8EA9A4EBF41A38260D3ABF0D5AF73EB4DC7D8B7454A7308909F02085;
QB_RFC := 0x4F2B886F147EFCAD4D67785BC843833F3735E4ECC2615BD3B4C17D7B7DDB9EDE;

/* alice */
QA := X25519(P[1], S[1], D[1], PI, dA_RFC, a24);
print "chk (QA == QA_RFC)?", QA eq QA_RFC;

/* bob */
QB := X25519(P[1], S[1], D[1], PI, dB_RFC, a24);
print "chk (QB == QB_RFC)?", QB eq QB_RFC;
```