Efficient Elliptic Curve Diffie-Hellman Computation at the 256-bit Security Level

Kaushik Nath and Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute
203, B. T. Road
Kolkata - 700108
India
{kaushikn_r,palash}@isical.ac.in

Abstract

In this paper we introduce new Montgomery and Edwards form elliptic curve targeted at the 256-bit security level. To this end, we work with three primes, namely $p_1 := 2^{506} - 45$, $p_2 = 2^{510} - 75$ and $p_3 := 2^{521} - 1$. While p_3 has been considered earlier in the literature, p_1 and p_2 are new. We define a pair of birationally equivalent Montgomery and Edwards form curves over all the three primes. Efficient 64-bit assembly implementations targeted at Skylake and later generation Intel processors have been made for the shared secret computation phase of the Diffie-Hellman key agreement protocol for the new Montgomery curves. Curve448 of the Transport Layer Security, Version 1.3 is a Montgomery curve which provides security at the 224-bit security level. Compared to the best publicly available 64-bit implementation of Curve448, the new Montgomery curve over p_1 leads to a 3%-4% slowdown and the new Montgomery curve over p_2 leads to a 4.5%-5% slowdown; on the other hand, 29 and 30.5 extra bits of security respectively are gained. For designers aiming for the 256-bit security level, the new curves over p_1 and p_2 provide an acceptable trade-off between security and efficiency.

Keywords: Elliptic curve cryptography, Elliptic curve Diffie-Hellman key agreement, Montgomery form, Edwards form, 256-bit security.

1 Introduction

One of the most extensively used modern cryptographic primitives is the Diffie-Hellman (DH) [12] key agreement protocol. Koblitz [16] and Miller [19] have independently shown that the DH protocol can be instantiated using cyclic groups arising from the theory of elliptic curves. Among the various models of elliptic curves, the Montgomery form [20] provide the most efficient model for implementing DH key agreement. The famous and widely deployed Curve25519 [6] is a Montgomery form curve. As part of the Transport Layer Security (TLS) protocol, Version 1.3 [24], RFC 7748 [18] specifies two elliptic curves, namely Curve25519 and Curve448, for DH key agreement. Curve25519 provides security at the 128-bit security level and Curve448 provides security at the 224-bit security level.

Various cryptographic primitives targeted at the 256-bit security level have been proposed in the literature. For example, both SHA-2 and SHA-3 have variants for the 256-bit security level [1]. In the context of public key cryptography, there are proposals for cryptographic pairings targeted at the 256-bit security level [17, 3]. A general purpose elliptic curve called E-521 has been proposed in [2] for the 256-bit security level.

In view of the above discussion, design and implementation of ECDH key agreement protocol at the 256-bit security level is a relevant research problem. TLS, Version 1.3, however, does not include a 256-bit secure solution. A possible reason for this omission is the apprehension that the computation of key agreement at the 256-bit security level will be significantly slower than that at the 224-bit security level. While, there will indeed be a slowdown, to the best of our knowledge, the magnitude of this slowdown is presently unknown. Consequently, it is not clear whether such a slowdown is an acceptable trade-off for achieving higher security.

We consider the following four primes: $2^{506} - 45$, $2^{510} - 75$, $2^{521} - 1$ and $2^{448} - 2^{224} - 1$. For convenience of notation, we will denote $2^{506} - 45$ as p506-45, $2^{510} - 75$ as p510-75, $2^{521} - 1$ as p510-1, and $2^{448} - 2^{224} - 1$

as $p448\text{-}224\text{-}1$. Fix a prime p. Given $A \in \mathbb{F}_p \setminus \{-2, 2\}$ and $B \in \mathbb{F}_p \setminus \{0\}$, the Montgomery curve $E_{M,A,B}$ over $\mathbb{F}_p$ is given by the equation $E_{M,A,B} : By^2 = x^3 + Ax^2 + x$. Given $a, d \in \mathbb{F}_p \setminus \{0\}$ and $a \neq d$, the twisted Edwards curve $E_{E,a,d}$ is given by the equation $E_{E,a,d} : au^2 + v^2 = 1 + du^2v^2$. For convenience of notation, a Montgomery curve $E_{M,A,1}$ will be denoted as $M[A]$; an Edwards curve $E_{E,1,d}$ will be denoted as $E[d]$; and a twisted Edwards curve $E_{E,-1,d}$ will be denoted as $\widetilde{E}[d]$. If we wish to emphasize the underlying prime p, then we will write $M[p, A]$, $E[p, d]$ and $\widetilde{E}[p, d]$ instead of $M[A]$, $E[d]$ and $\widetilde{E}[d]$ respectively.

Our Contributions

In this work, we propose new curves at 256-bit security level and perform efficient 64-bit implementation of ECDH key agreement. A summary of the new curves is given in Table 1. Also, for comparison, we include the two curves $M[156326]$ and $E[39082/39081]$ at the 224-bit security level which are part of TLS, Version 1.3. The curve $M[156326]$ has been named Curve448 in [18].

The prime $p521\text{-}1$ has been considered earlier in [2] which introduced the curve $E[p521\text{-}1, -376014]$ (and named it E-521) as part of a suite of general purpose high security elliptic curves. Using the isogenies given in [10], it can be shown that E-521 is 4-isogenous to $M[1504058]$ shown in Table 1. To the best of our knowledge, neither of the curves $M[1504058]$ or $E[376015/376014]$ appear earlier in the literature. Also, to the best of our knowledge, the primes $p506\text{-}45$ and $p510\text{-}75$ have not been considered earlier in the literature and so the question of proposing curves over the corresponding fields do not arise.

From Table 1, we observe that $M[p506\text{-}45, 996558]$, $M[p510\text{-}75, 952902]$ and $M[p521\text{-}1, 1504058]$ provide 29, 30.5 and 36.5 bits more security compared to $M[p\text{-}448\text{-}224\text{-}1, 156326]$ (i.e., Curve448).

Prime	Security	Mont	Base Pt (Mont)	Ed	Base Pt (Ed)
$p448\text{-}224\text{-}1$	223	$M[156326]$	$(5, \cdot)$	$E[39082/39081]$	$(\cdot, -3/2)$
$p506\text{-}45$	252	$M[996558]$	$(3, \cdot)$	$E[249140/249139]$	$(\cdot, 2)$
$p510\text{-}75$	253.5	$M[952902]$	$(4, \cdot)$	$\widetilde{E}[-238225/238226]$	$(\cdot, 3/5)$
$p521\text{-}1$	259.5	$M[1504058]$	$(8, \cdot)$	$E[376015/376014]$	$(\cdot, 9/7)$

Table 1: Montgomery and Edwards curves at the 256-bit security level proposed in this work along with Curve448 of TLS, Version 1.3. In the table, $M[156326]$ is Curve448.

To assess the performance of the new curves, we have carried out a 64-bit assembly implementation of the DH shared secret computation over the new Montgomery curves. Field elements are represented using a number of 64-bit words or limbs. Our target processors were the Skylake and later generation Intel processors. So, we chose the packed or saturated limb representation of field elements. Further details of field representation are provided in Section 4.

Timing measurements were taken on the Skylake and the Kaby Lake processors. For comparison, we have considered the best previously reported [23] 64-bit implementation of the shared secret computation phase of the DH protocol over Curve448 on the Skylake and Kaby Lake processors. Detailed cycle counts are reported later. Below we summarize the main findings. The following statements refer to the DH shared secret computations over the mentioned curves.

1. $M[p506\text{-}45, 996558]$ is about 1.3%-1.4% faster than $M[p510\text{-}75, 952902]$.

2. $M[p506\text{-}45, 996558]$ is about 19% faster than $M[p521\text{-}1, 1504058]$.

3. $M[p506\text{-}45, 996558]$ is about 3%-4% slower than Curve448.

4. $M[p510\text{-}75, 952902]$ is about 4.5%-5% slower than Curve448.

5. $M[p521\text{-}1, 1504058]$ is about 21%-22% slower than Curve448.

While $M[p521\text{-}1, 1504058]$ provides 36.5 bits of extra security compared to Curve448, the slowdown is also quite significant. On the other hand, $M[p506\text{-}45, 996558]$ and $M[p510\text{-}75, 952902]$ provide 29 and 30.5 bits of extra security compared to Curve448 and the slowdowns for these curves are much less marked. So, if security around the 256-bit security level is desired, either of the curves $M[p506\text{-}45, 996558]$ or $M[p510\text{-}75, 952902]$ seem to provide a reasonable trade-off between speed and security.

The curve $E[p506\text{-}45, 249140/249139]$ which is birationally equivalent to $M[p506\text{-}45, 996558]$ can be used for the key generation phase. The small base point on $E[p506\text{-}45, 249140/249139]$ is helpful for fixed base scalar multiplication. Also, curve $E[p506\text{-}45, 249140/249139]$ can be used to implement a signature scheme following the approach used for EdDSA [8]. Similarly, if the curve $M[p510\text{-}75, 952902]$ is used for shared secret computation of the DH protocol, then the curve $\widetilde{E}[p510\text{-}75, -238225/238226]$ which is birationally equivalent to $M[p510\text{-}75, 952902]$ can be used for key generation and also for instantiation of a signature scheme following [8].

We have made the source codes of our implementations publicly available at the following link.

http://github.com/kn-cs/mont256-dh.

2 Montgomery and (Twisted) Edwards Form Elliptic Curves

Let p be a prime and $\mathbb{F}_p$ be the finite field of p elements. Following TLS, Version 1.3, we consider elliptic curves over $\mathbb{F}_p$, where p is a large prime. Montgomery curve $E_{M,A,B}$ and twisted Edwards curve $E_{E,a,d}$ have already been defined. In our applications, we will have $B = 1$ and a to be either 1 or -1. If $a = 1$, then the corresponding curve is simply called an Edwards form curve (instead of twisted Edwards form curve). If a is a square and d is not a square in $\mathbb{F}_p$, then the addition formula in $E_{E,a,d}$ is complete [7]. In this case, $E_{E,a,d}$ is called a complete twisted Edwards curve. Further, if $a = -1$, then particularly efficient addition formulas are known [15].

If $p \equiv 1 \bmod 4$, -1 is a square modulo p. In this case, if d is a non-square, the addition formula over $E_{E,-1,d}$ is both complete and the fastest. On the other hand, if $p \equiv 3 \bmod 4$, -1 is a non-square modulo p and so the addition formula over $E_{E,-1,d}$ is not guaranteed to be complete. In this case, one considers the Edwards curve $E_{E,1,d}$ with d a non-square so that the addition formula is complete. It is not, however, the fastest. If the base point on $E_{E,1,d}$ is small, then the difference in the number of operations between the addition formulas on $E_{E,-1,d}$ and $E_{E,1,d}$ is small. More concretely, if the base point on $E_{E,1,d}$ is $(\cdot, 2)$, then this difference is just two left shifts. See [22] for details.

For $p \equiv 3 \bmod 4$, addition formula over $E_{E,-1,d}$ is not guaranteed to be complete making constant time implementation of scalar multiplication problematic. On the other hand, for the verification phase of a signature scheme based on the EdDSA template [8], constant time implementation is not an issue. For this application, one may move from $E_{E,1,d}$ to $E_{E,-1,d'}$, for some d' (see below) using a birational equivalence and perform the main computation of signature verification over $E_{E,-1,d'}$.

We refer to [20, 9, 11] for background theory and further details about Montgomery form curves. For (twisted) Edwards curves, we refer to [13, 5, 7].

2.1 Montgomery-Edwards Connection

RFC7748 [18] of TLS, Version 1.3 specifies both Montgomery and Edwards form curves for a given security level. In the present state of knowledge, the shared secret computation of the DH key agreement is performed best on a Montgomery form curve. On the other hand, the key generation phase as well as the computations required for an elliptic curve signature scheme based on the template in [8] are performed best on an Edwards form curve.

Edwards and Montgomery curves can be connected by either birational equivalences or by isogenies. For example, for the 128-bit security level, Curve25519 and Ed25519 are birationally equivalent. Similarly, at the 224-bit security level, Curve448 (i.e., $M[p448\text{-}224\text{-}1, 156326]$) and $E[p448\text{-}224\text{-}1, 39082/39081]$ are birationally equivalent. Additionally, Curve448 is 4-isogenous to $E[p448\text{-}224\text{-}1, -39081]$ [18]. The curve $E[p448\text{-}224\text{-}1, -39081]$ was proposed in [14] where it was named Ed448-Goldilocks and it has been called Edwards448 in [18].

We provide below some explicit birational equivalences between Montgomery and Edwards form curves. These can be obtained by composing the elementary birational equivalences provided in [5, 7]. The verification of these birational equivalences, on the other hand, can be done by direct substitution.

Case $p \equiv 3 \bmod 4$: Let $E_{M,A,B} : By^2 = x^3 + Ax^2 + x$ be a Montgomery curve and $E_{E,1,d} : u^2 + v^2 = 1 + du^2v^2$ be an Edwards curve over $\mathbb{F}_p$. Note that -1 is not a square in $\mathbb{F}_p$.

1. If $(A + 2)/B$ is a square in $\mathbb{F}_p$, then the map

$$(x, y) \quad \mapsto \quad (u, v) = (\delta x/y, (x - 1)/(x + 1)), \tag{1}$$

where $\delta^2 = (A + 2)/B$, is a birational equivalence from $E_{M,A,B}$ to $E_{E,1,d}$ with exceptional points $y = 0$ and $x = -1$. Conversely, the map

$$(u, v) \quad \mapsto \quad (x, y) = ((1 + v)/(1 - v), \delta(1 + v)/(u(1 - v))), \tag{2}$$

is a birational equivalence from $E_{E,1,d}$ to $E_{M,A,B}$ with exceptional points $u = 0$ and $v = 1$. The relation between A and d is $(A + 2)/4 = 1/(1 - d)$.

2. If $(A - 2)/B$ is a square in $\mathbb{F}_p$, then the map

$$(x, y) \quad \mapsto \quad (u, v) = (\delta x/y, (x + 1)/(x - 1)), \tag{3}$$

where $\delta^2 = (A - 2)/B$, is a birational equivalence from $E_{M,A,B}$ to $E_{E,1,d}$ with exceptional points $y = 0$ and $x = 1$. Conversely, the map

$$(u, v) \mapsto (x, y) = ((v + 1)/(v - 1), \delta(v + 1)/(u(v - 1))), \tag{4}$$

is a birational equivalence from $E_{E,1,d}$ to $E_{M,A,B}$ with exceptional points $u = 0$ and $v = 1$. The relation between A and d is $(A - 2)/4 = 1/(d - 1)$.

Suppose that d is not a square so that the addition formula over $E_{E,1,d}$ is complete. Since both d and -1 are not squares, $-d$ is a square. So, the map

$$(u, v) \quad \mapsto \quad (\hat{u}, \hat{v}) = (\gamma u, 1/v), \tag{5}$$

where $-\gamma^2 = d$, is a birational equivalence with exceptional points $v = 0$ from the Edwards curve $E_{E,1,d} : u^2 + v^2 = 1 + du^2v^2$ to the twisted Edwards curve $E_{E,-1,-1/d} : -\hat{u}^2 + \hat{v}^2 = 1 + (-1/d)\hat{u}^2\hat{v}^2$.

Case $p \equiv 1 \bmod 4$: Let $E_{M,A,B} : y^2 = x^3 + Ax^2 + x$ be a Montgomery curve and $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ be an Edwards curve over $\mathbb{F}_p$. Note that -1 is a square in $\mathbb{F}_p$.

1. If $(A + 2)/B$ is a square in $\mathbb{F}_p$, then the map

$$(x, y) \quad \mapsto \quad (u, v) = (\delta x/y, (x - 1)/(x + 1)), \tag{6}$$

where $-\delta^2 = (A+2)/B$, is a birational equivalence from $E_{M,A,B}$ to $E_{E,-1,d}$ with exceptional points $y = 0$ and $x = -1$. Conversely, the map

$$(u, v) \quad \mapsto \quad (x, y) = ((1 + v)/(1 - v), \delta(1 + v)/(u(1 - v))), \tag{7}$$

is a birational equivalence from $E_{E,-1,d}$ to $E_{M,A,B}$ with exceptional points $u = 0$ and $v = 1$. The relation between A and d is $(A + 2)/4 = 1/(1 + d)$.

2. If $(A - 2)/B$ is a square in $\mathbb{F}_p$, then the map

$$(x, y) \quad \mapsto \quad (u, v) = (\delta x/y, (x + 1)/(x - 1)), \tag{8}$$

where $-\delta^2 = (A-2)/B$, is a birational equivalence from $E_{M,A,B}$ to $E_{E,-1,d}$ with exceptional points $y = 0$ and $x = 1$. Conversely, the map

$$(u, v) \quad \mapsto \quad (x, y) = ((v + 1)/(v - 1), \delta(v + 1)/(u(v - 1))), \tag{9}$$

is a birational equivalence from $E_{E,-1,d}$ to $E_{M,A,B}$ with exceptional points $u = 0$ and $v = 1$. The relation between A and d is $(A - 2)/4 = -1/(d + 1)$.

2.2 Security Properties

Let n and n_T be the orders of $E(\mathbb{F}_p)$ and its quadratic twist respectively. Let ℓ and h (resp. ℓ_T and h_T) be such that $n = h \cdot \ell$ (resp. $n_T = h_T \cdot \ell_T$). Suppose that ℓ and ℓ_T are primes. Cryptography is done over an ℓ-order subgroup of $E(\mathbb{F}_p)$. The parameters h and h_T are called the co-factors of the curve and its twist respectively.

The embedding degrees k and k_T of the curve and its twist are defined as follows. The parameter k (resp. k_T) is the smallest positive integer such that $\ell | (p^k - 1)$ (resp. $\ell_T | (p^{k_T} - 1)$).

The complex multiplication field discriminant D of E is defined in the following manner. Let $t = p+1-n$. By Hasse's theorem, $|t| \leq 2\sqrt{p}$ and in the cases that we considered $|t| < 2\sqrt{p}$ so that t^2-4p is a negative integer; let s^2 be the largest square dividing $t^2 - 4p$; define $D = (t^2 - 4p)/s^2$ if $t^2 - 4p \bmod 4 = 1$ and $D = 4(t^2 - 4p)/s^2$ otherwise.

SafeCurves [4] suggests that all of the parameters ℓ, ℓ_T, k, k_T and D should be large to ensure security against various known attacks. Considering twist security, the security level of a curve in terms of bits is defined to be $\frac{1}{2} \min(\log_2 \ell, \log_2 \ell_T)$.

3 Curves for the 256-bit Security Level

Since our target is 256-bit security, we need a κ-bit prime where κ is about 512. Further, we chose to work over (pseudo-)Mersenne primes $2^m - \delta$ with δ small, so that we can leverage the efficient algorithms for arithmetic modulo such primes.

The prime $p521$-1 is a Mersenne prime and has been suggested earlier for defining elliptic curves [2]. This prime provides a few bits more security than our target 256-bit security level. So, we considered some pseudo-Mersenne primes which are less than 2^{512}. For efficiency reasons, we wished to have δ small. Due to this reason, we chose not to work with the prime $2^{511} - 187$ suggested in [2]. We found two other pseudo-Mersenne primes less than 2^{512} which may be considered for 256-bit security. These are $p506$-45 and $p510$-75.

Curves over $\mathbb{F}_{2^{506}-45}$: Let $p = 2^{506} - 45$. We ran a search program to find Montgomery curves $M[p, A]$ satisfying the security criteria given in Section 2.2. The minimum positive value of A for which $(h, h_T) = (4, 4)$ and the other parameters mentioned in Section 2.2 are large is $A = 996558$. This gives the curve $M[p506\text{-}45, 996558]$. The curve $E[p506\text{-}45, 249140/249139]$ is birationally equivalent to $M[p506\text{-}45, 996558]$ using the birational equivalences given by (3) and (4). The quantity 249140/249139 is a non-square modulo p506-45 and so the addition formula over E[p506-45,249140/249139] is complete. The parameters for $M[p506\text{-}45, 996558]$ are as follows.

$$\begin{aligned}
n &= 20949699890535307968084414059696634574186509094675614652693064755 8152\backslash \\
&\quad 562969918759152506342735396235844228848989060057559719826245562055728\backslash \\
&\quad 669755385685788, \\
\ell &= 5237424972633826992021103514924158643546627273668903663173266188 95381\backslash \\
&\quad 407424796897881265856838490589610572122472650143899299565613905139321\backslash \\
&\quad 67438846421447, \\
\log_2 \ell &= 504, \\
h &= 4, \\
k &= (\ell - 1)/17, \\
n_T &= 20949699890535307968084414059696634574186509094675614652693064755 81525\backslash \\
&\quad 629698795838725522290823194962710846465792676315294599825923112745821 5\backslash \\
&\quad 6296145754252, \\
\ell_T &= 52374249726338269920211035149241586435466272736689036631732661889 53814\backslash \\
&\quad 074246989596813805727057987406777116164481690788236499564807781864553 9\backslash \\
&\quad 074036438563, \\
\log_2 \ell_T &= 504, \\
h_T &= 4, \\
k_T &= (\ell_T - 1), \\
D &= -454312355750617562644920221395107582312080441825232116394954947347 79\backslash \\
&\quad 419592882800858550177100850366751591345062685609028019017410186908272 5\backslash \\
&\quad 988805571050252, \\
\lceil \log_2(-D) \rceil &= 508.
\end{aligned}$$

The point $(3, \cdot)$ is a point of order ℓ on the Montgomery curve $M[p506\text{-}45, 996558]$; the corresponding point on the Edwards curve $E[p506\text{-}45, 249140/249139]$ is $(\cdot, 2)$. The set of scalars is defined to be $4(2^{503} + \{0, 1, \ldots, 2^{503} - 1\})$. Given a 64-byte scalar a, assuming the least significant byte ordering, the clamping function $\mathsf{clamp}(a)$ is defined as follows: clear bits 0 and 1 of the first byte; set bit number 1 of the last byte and clear bits numbered 2 to 7 of the last byte.

Remarks: Let $\alpha = (A + 2)/4 = 249140$. The curves $M[p506\text{-}45, 4\alpha - 2]$ and $E[p506\text{-}45, 1 - \alpha]$ can be shown to be 4-isogenous using the isogenies given in [10]. Further, using the fact that $-\alpha$ is a square in $\mathbb{F}_p$, the curves $M[p506\text{-}45, 2 - 4/\alpha]$ and $E[p506\text{-}45, 1 - \alpha]$ are birationally equivalent using the birational equivalences given by (3) and (4).

Curves over $\mathbb{F}_{2^{510}-75}$: Let $p = 2^{510} - 75$. We ran a search program to find Montgomery curves $M[p, A]$ satisfying the security criteria given in Section 2.2. The minimum positive value of A for which an optimal value of (h, h_T) is obtained is $A = 793638$. In this case, neither $(A + 2)$ nor $(A - 2)$ are squares in $\mathbb{F}_p$. So, the birational equivalences in Section 2.1 for connecting Montgomery and Edwards curves cannot be applied. One may consider a quadratic twist of $E_{M,A,1}$. Since 2 is not a square, $E_{M,A,2}$ is a quadratic twist of $E_{M,A,1}$. Then $E_{M,A,2}$ can be connected to $E_{E,-1,d}$ using either of the birational equivalences given by (6), (7) or, (8), (9). The form of d in these two cases are $(A-2)/(A+2)$ and $(A+2)/(A-2)$ respectively. Since both $(A+2)$ and $(A-2)$ are not squares, both $(A-2)/(A+2)$ and $(A+2)/(A-2)$ are squares. Consequently, the completeness of the addition formula over $E_{E,-1,d}$ is not ensured. Since $p \equiv 1 \bmod 4$, it is desirable to use birational equivalences to connect a Montgomery curve to a twisted Edwards form curve having a complete addition formula. For $A = 793638$, this does not seem to be possible using the birational equivalences in Section 2.1.

The next value of A for which an optimal value of (h, h_T) is obtained is $A = 952902$. In this case, we obtain the curves $M[p510\text{-}75, 952902]$ and $\widetilde{E}[p510\text{-}75, -238225/238226]$ which are birationally equivalent using the birational equivalences given by (6) and (7). The quantity $-238225/238226$ is a non-square modulo $p510\text{-}75$ and so the addition formula over $E[p510\text{-}75, -238225/238226]$ is complete. The parameters for $M[p510\text{-}75, 952902]$ are as follows.

$$\begin{aligned}
n &= 335195198248564927489350624955146153186984145514809834443089036093044\backslash \\
& 100751840662869613465178025950119140505107956858789953330856566350769\backslash \\
& 9101693245950696, \\
\ell &= 418993997810706159361688281193932691483730181893512293053861295116305\backslash \\
& 125939800828587016831472532437648925631384946073487441663570707938462\backslash \\
& 387711655743837, \\
\log_2 \ell &= 507, \\
h &= 8, \\
k &= \ell - 1, \\
n_T &= 335195198248564927489350624955146153186984145514809834443089036093044\backslash \\
& 100751836685970480249730319221265361087801367443752734363284030977727\backslash \\
& 4115131257091204, \\
\ell_T &= 837987995621412318723376562387865382967460363787024586107722590232610\backslash \\
& 251879591714926200624325798053163402719503418609381835908210077444318\backslash \\
& 528782814272801, \\
\log_2 \ell_T &= 508, \\
h_T &= 4, \\
k_T &= \ell_T - 1, \\
D &= -325310369051208815436075592806876377044871206601624247034270696834445\backslash \\
& 974097335403637319053453446802029316328771464346619663200532150290780 1\backslash \\
& 0832342319114820, \\
\lceil \log_2(-D) \rceil &= 510.
\end{aligned}$$

The point $(4, \cdot)$ is of order ℓ on the Montgomery curve $M[p510\text{-}75, 952902]$; the corresponding point on the twisted Edwards curve $\widetilde{E}[p510\text{-}75, -238225/238226]$ is $(\cdot, 3/5)$. The set of scalars is set to be $8(2^{510} + \{0, 1, \ldots, 2^{510} - 1\})$. Given a 64-byte scalar a, assuming the least significant byte ordering, the clamping function $\mathsf{clamp}(a)$ is defined as follows: clear bits 0, 1 and 2 of the first byte; set bit number 5 of the last byte and clear bits numbered 6 and 7 of the last byte.

Remark: Let $\alpha = (A+2)/4 = 238226$, which is a square. The curves $M[p510\text{-}75, 4\alpha - 2]$ and $\widetilde{E}[p510\text{-}75, \alpha - 1]$ can be shown to be 4-isogenous using the isogenies given in [10]. Further, $M[p510\text{-}75, 4/\alpha - 2]$ and $\widetilde{E}[p510\text{-}75, \alpha - 1]$ are birationally equivalent using the birational equivalences given by (6) and (7). $M[p510\text{-}75, 2 - 4/\alpha]$ and $\widetilde{E}[p510\text{-}75, \alpha - 1]$ are birationally equivalent using the birational equivalences given by (8) and (9).

Curves over $\mathbb{F}_{2^{521}-1}$: The curve E-521 [2] is same as the curve $E[p521\text{-}1, -376014]$. Using the isogenies given in [10], the curve $E[p521\text{-}1, -376014]$ is 4-isogenous to $M[p521\text{-}1, 1504058]$. This gave us $M[p521\text{-}1, 1504058]$. Since the birational equivalences in Section 2.1 are simpler than the isogenies in [10], we obtained the Edwards form curve $E[p521\text{-}1, 376015/376014]$ which is birationally equivalent to $M[p521\text{-}1, 1504058]$. The birational equivalences are given by (3) and (4). The quantity 376015/376014 is a non-square modulo $p521\text{-}1$ and so the addition formula over $E[p521\text{-}1, 376015/376014]$ is complete.

The parameters for $M[p521\text{-}1, 1504058]$ are as follows.

$$\begin{array}{rcl}
n & = & 686479766013060971498190079908139321726943530014330540939446345918554\backslash \\
 & & 318339765470190350660665463139854677463626093657041727713179481016927\backslash \\
 & & 1973685174680434092, \\
\ell & = & 171619941503265242874547519977034830431735882503582635234861586479638\backslash \\
 & & 579584941367547587665166365784963669365906523414260431928294870254231\backslash \\
 & & 7993421293670108523, \\
\log_2 \ell & = & 519, \\
h & = & 4, \\
k & = & \ell - 1, \\
n_T & = & 686479766013060971498190079908139321726943530014330540939446345918554\backslash \\
 & & 318339765740234161267466827771140781798652202514565696684420462311835\backslash \\
 & & 3174371407549680212, \\
\ell_T & = & 171619941503265242874547519977034830431735882503582635234861586479638\backslash \\
 & & 579584941435058540316866706942785195449663050628641424171105115577958\backslash \\
 & & 8293592851887420053, \\
\log_2 \ell_T & = & 519, \\
h_T & = & 4, \\
k_T & = & \ell_T - 1, \\
D & = & -256360991493463887298108185526313986556096537835271988322251560295127\backslash \\
 & & 393498401498104027631835788522464000067572831290069462218128904642355 0\backslash \\
 & & 69855506040176465004, \\
\lceil \log_2(-D) \rceil & = & 523.
\end{array}$$

The point $(8, \cdot)$ is a point of order ℓ on the Montgomery curve $M[p521\text{-}1, 1504058]$; the corresponding point on the Edwards curve $E[p521\text{-}1, 376015/376014]$ is $(\cdot, 9/7)$.

The set of scalars for $E_{M,1504058,1}$ is set to be $4(2^{518} + \{0, 1, \ldots, 2^{518} - 1\})$. Given a 65-byte scalar a, assuming the least significant byte ordering, the clamping function $\mathsf{clamp}(a)$ is defined as follows: clear bits 0 and 1 of the first byte; set bit number 0 of the last byte and clear bits numbered 1 to 7 of the last byte.

Remark: Let $\alpha = (A + 2)/4 = 376015$. The curves $M[p521\text{-}1, 2 - 4/\alpha]$ and $E[p521\text{-}1, 1 - \alpha]$ are birationally equivalent using the birational equivalences given by (3) and (4).

4 Implementation

Let $m = \lceil \log_2 p \rceil$. Elements of $\mathbb{F}_p$ are m-bit strings which are represented using κ 64-bit words. Each such word is termed as a limb by convention. We have used packed or saturated limb representation of the field elements, according to which, m is written as $m = \eta(\kappa - 1) + \nu$ with $1 \leq \nu \leq \eta$, where $\eta = 64$. So, the first $\kappa - 1$ limbs of a field element are 64 bits long and the last limb has length between 1 and 64 bits.

Prime	m	κ	η	ν	$64\kappa - m$
$p448\text{-}224\text{-}1$	448	7	64	64	0
$p506\text{-}45$	506	8	64	58	6
$p510\text{-}75$	510	8	64	62	2
$p521\text{-}1$	521	9	64	9	55

Table 2: Saturated limb representations of primes related to this work.

The four primes that we have worked with are specified in Table 2 along with their representations. For the two primes $p506\text{-}45$ and $p521\text{-}1$, the value of $64\kappa - m \geq 3$ (which means, there are three or more "free" bits in the last limb), for the prime $p510\text{-}75$, $64\kappa - m = 2$ (which means, there are two "free" bits in the last limb) and for the prime $p448\text{-}224\text{-}1$, $64\kappa = m$ (which means, there are no "free" bits in the last limb). There are consequences of these features to the Montgomery ladder computation which are mentioned below.

In [22], it was shown that the condition $64\kappa - m \geq 3$ allows dropping the reductions after additions/subtractions in the Montgomery ladder computation. The condition $64\kappa - m \geq 3$ holds for the primes p506-45 and p521-1 and consequently, the reductions after additions/subtractions in the ladder computation can be omitted. For the prime p510-75, $64\kappa - m = 2$. Following the analysis in [22], the reductions after the additions in the ladder computation can be omitted, but, the reductions after the subtractions need to be performed to avoid leading to an overfull situation.

The Skylake and later processors provide the instruction triplet known as `mulx/adcx/adox`. These instructions allow the use of two independent carry chains for efficiently multiplying/squaring two large integers having 64-bit saturated limb representation. A general algorithmic description for multiplication/squaring of 64κ-bit numbers, $\kappa \geq 4$ can be found in [21]. We have used these algorithms for the implementation of integer multiplication/squaring. For reducing an element after an integer multiplication/squaring, we have been used the algorithm reduceSLPMP from [21].

4.1 Timings

We have carried out the timing experiments on a single core of Skylake and Kaby Lake processors. The turbo-boost and hyper-threading features were turned off while measuring the cpu-cycles. An initial cache warming was done with 25000 iterations and then the median of 100000 iterations was recorded. The time stamp counter TSC was read from the CPU to RAX and RDX registers by RDTSC instruction.

Platform specifications: The specifications of the hardware and software tools used in our software implementations are given below.

Skylake: Intel®Core™ i7-6500U 2-core CPU @ 2.50GHz. The OS was 64-bit Ubuntu 14.04 LTS and the source code was compiled using GCC version 7.3.0.

Kaby Lake: Intel®Core™ i7-7700U 4-core CPU @ 3.60GHz. The OS was 64-bit Ubuntu 18.04 LTS and the source code was compiled using GCC version 7.3.0.

Curve	Field	Security	Skylake	Kaby Lake	Ref
Curve448	$\mathbb{F}_{2^{448}-2^{224}-1}$	223	536362	521934	[23]
$M[p506\text{-}45, 996558]$	$\mathbb{F}_{2^{506}-45}$	252	558757	538971	This work
$M[p510\text{-}75, 952902]$	$\mathbb{F}_{2^{510}-75}$	253.5	566088	546849	This work
$M[p521\text{-}1, 1504058]$	$\mathbb{F}_{2^{521}-1}$	259.5	689588	666044	This work

Table 3: CPU-cycle counts on Skylake and Kaby Lake processors for shared secret computation on the Montgomery form curves.

Timings in the form of cpu-cycles are provided in Table 3 for Skylake and Kaby Lake processors. For comparison we have considered the timings of the most efficient (to the best of our knowledge) publicly available 64-bit implementation of Curve448, which is the software implementation along with the work [23]. We downloaded the mentioned software for Curve448 and measured the cpu-cycles on the same platforms on which we have measured the cpu-cycles of our implementations. This has been done to keep the comparisons consistent.

5 Conclusion

In this paper, we have proposed new Montgomery and Edwards form elliptic curves targeted at the 256-security level. Efficient 64-bit assembly implementations of Diffie-Hellman shared secret computation on these curves have been made. Timings have been obtained on the Skylake and Kaby Lake processors of Intel. Compared to Curve448, two of the new curves provide 29 and 30.5 bits of additional security with slowdowns of 3%-4% and 4.5%-5% respectively. Consequently, at the 256-bit security level, these two curves provide acceptable security/efficiency trade-off compared to Curve448 which provides security at the 224-bit security level.

References

[1] FIPS PUB 180-4. Secure Hash Standards. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf, 2015.

[2] Diego F. Aranha, Paulo S. L. M. Barreto, C. C. F. Pereira Geovandro, and Jefferson E. Ricardini. A note on high-security general-purpose elliptic curves. *IACR Cryptology ePrint Archive*, 2013:647, 2013.

[3] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *J. Cryptology*, 32(4):1298–1336, 2019.

[4] D. J. Bernstein and T. Lange. Safecurves: choosing safe curves for elliptic-curve cryptography. http://safecurves.cr.yp.to/index.html, Accessed on November 23, 2019.

[5] D. J. Bernstein and Lange T. Faster addition and doubling on elliptic curves. In *Advances in Cryptology - ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer, 2007.

[6] Daniel J. Bernstein. Curve25519: New Diffie-Hellman Speed Records. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings*, volume 3958 of *Lecture Notes in Computer Science*, pages 207–228. Springer, 2006.

[7] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In Serge Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer, 2008.

[8] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *J. Cryptographic Engineering*, 2(2):77–89, 2012.

[9] Daniel J. Bernstein and Tanja Lange. Montgomery curves and the Montgomery ladder. In Joppe W. Bos and Arjen K. Lenstra, editors, *Topics in Computational Number Theory inspired by Peter L. Montgomery*, pages 82–115. Cambridge University Press, 2017.

[10] Craig Costello and Michael Naehrig. Isogenies between (twisted) Edwards and Montgomery curves. https://cryptosith.org/papers/isogenies_tEd2Mont.pdf, 2015. Accessed on September 16, 2019.

[11] Craig Costello and Benjamin Smith. Montgomery curves and their arithmetic - the case of large characteristic fields. *J. Cryptographic Engineering*, 8(3):227–240, 2018.

[12] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions of Information Theory*, 22(6):644–654, 1976.

[13] Harold M. Edwards. A Normal Form for Elliptic Curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007.

[14] Mike Hamburg. Ed448-goldilocks, a new elliptic curve. *IACR Cryptology ePrint Archive*, 2015/625, 2015. https://eprint.iacr.org/2015/625.

[15] Hüseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In Josef Pieprzyk, editor, *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, volume 5350 of *Lecture Notes in Computer Science*, pages 326–343. Springer, 2008.

[16] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[17] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. In Nigel P. Smart, editor, *Cryptography and Coding, 10th IMA International Conference, Cirencester, UK, December 19-21, 2005, Proceedings*, volume 3796 of *Lecture Notes in Computer Science*, pages 13–36. Springer, 2005.

[18] Adam Langley and Mike Hamburg. Elliptic curves for security. Internet Research Task Force (IRTF), Request for Comments: 7748, https://tools.ietf.org/html/rfc7748, 2016. Accessed on September 16, 2019.

[19] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO'85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, pages 417–426. Springer Berlin Heidelberg, 1985.

[20] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.

[21] Kaushik Nath and Palash Sarkar. Efficient Arithmetic in (Pseudo-)Mersenne Prime Order Fields. *IACR Cryptology ePrint Archive*, 2018/985, 2018. https://eprint.iacr.org/2018/985.

[22] Kaushik Nath and Palash Sarkar. “Nice” Curves. Cryptology ePrint Archive, Report 2019/1259, 2019. https://eprint.iacr.org/2019/1259.

[23] Thomaz Oliveira, Julio López Hernandez, Hüseyin Hisil, Armando Faz-Hernández, and Francisco Rodríguez-Henríquez. How to (pre-)compute a ladder - improving the performance of X25519 and X448. In Carlisle Adams and Jan Camenisch, editors, *Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers*, volume 10719 of *Lecture Notes in Computer Science*, pages 172–191. Springer, 2017.

[24] Version 1.3 TLS Protocol. RFC 8446. https://datatracker.ietf.org/doc/rfc8446/?include_text=1, 2018. Accessed on September 16, 2019.