Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications

Katsuyuki Okeya[1,⋆], Hiroyuki Kurumatani[1,⋆], and Kouichi Sakurai[2]

[1] Hitachi, Ltd., Software Division,
Kaneichi Bldg. 549-6, Shinano-cho, Totsuka-ku, Yokohama, 244-0801, Japan
{okeya_k, kurumahi}@soft.hitachi.co.jp
[2] Kyushu University,
Department of Computer Science and Communication Engineering
6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract. We show that the elliptic curve cryptosystems based on the Montgomery-form $E^M : BY^2 = X^3+AX^2+X$ are immune to the timing-attacks by using our technique of randomized projective coordinates, while Montgomery originally introduced this type of curves for speeding up the Pollard and Elliptic Curve Methods of integer factorization [Math. Comp. Vol.48, No.177, (1987) pp.243-264].
However, it should be noted that not all the elliptic curves have the Montgomery-form, because the order of any elliptic curve with the Montgomery-form is divisible by "4". Whereas recent ECC-standards [NIST,SEC-1] recommend that the cofactor of elliptic curve should be no greater than 4 for cryptographic applications.
Therefore, we present an efficient algorithm for generating Montgomery-form elliptic curve whose cofactor is exactly "4". Finally, we give the exact consition on the elliptic curves whether they can be represented as a Montgomery-form or not. We consider divisibility by "8" for Montgomery-form elliptic curves.
We implement the proposed algorithm and give some numerical examples obtained by this.

Keywords: Elliptic Curve Cryptography, Montgomery-form, Efficient Implementation, Timing-attacks

1 Introduction

We consider the exact condition on the elliptic curves whether they can be represented a Montgomery-form or not, and present an efficient algorithm for generating Montgomery-form elliptic curves whose cofactor is exactly "4". We also implement the algorithm and give some numerical examples obtained by this.

⋆ Okeya and Kurumatani are supported by Information-technology Promotion Agency, Japan (IPA).

H. Imai, Y. Zheng (Eds.): PKC 2000, LNCS 1751, pp. 238–257, 2000.

1.1 Elliptic Curves with the Montgomery-Form

Montgomery introduced the non-standard form $E^M : BY^2 = X^3 + AX^2 + X$ of elliptic curves in [Mon87], while the most standard form of elliptic curves is $E : y^2 = x^3 + ax + b$, which is called the Weierstrass-form.

1.2 A New Application: Preventing Timing-Attacks

We observe that the elliptic curve cryptosystems based on the Montgomery-form $E^M : BY^2 = X^3 + AX^2 + X$ are immune against timing-attacks [Koc, Koc96].

Kocher [Koc, Koc96] presented the timing-attacks: Attackers carefully measure the amount of time required to perform the private key operations, so that they might be able to decide fixed Diffie-Hellman exponents. This attack could be applicable to the elliptic curve cryptosystems including ECDSA ([ANSI]).

Time required to perform the conventional scalar multiplication algorithm based on the Weierstrass-form depends on the bit-patterns (and on the ratio between the number of zeros and the number of ones) of the secret value.

Whereas we show that the scalar multiplication on the Montgomery-form elliptic curve does *not* depend on the bit-patterns (nor on the ratio between the number of zeros and the number of ones) of the secret value. It has exactly seven multiplications and four square-multiplications on $\mathbf{F}_p$ per bit. This is due to the specific algorithm for computing scalar multiplication nP from P, which repeatedly calculates either $(2mP, (2m+1)P)$ or $((2m+1)P, (2m+2)P)$ from $(mP, (m+1)P)$ in the Montgomery-form elliptic curves.

The computation via by choosing a representive in the projective coordinates randomly is also useful for making it more difficult to measure the amount of time required. We compute the scalar d multiplications on the affine coordinates (x, y) via a corresponding projective coordinates (kx, ky, k), where k is randomly choosed.

Thus, Montgomery-form elliptic curves are shown to be useful for public-key cryptosystems from the point of view of not only efficient implementation but also protection against timing-attacks.

1.3 Montgomery-Form has Cofactor 4

However, the class of Montgomery-form is restricted in the elliptic curves. We should note that the order of elliptic curve with the Montgomery-form is always divisible by "4"as remarked in [Mon87]. Therefore, not all elliptic curves have a Montgomery-form.

Whereas recent ECC-standards [NIST99, SEC-1] recommend that the cofactor of elliptic curves be within "4" for cryptographic use. Thus, we shall design Montgomery-form elliptic curves with cofactor exactly "4" for ECC-standards [NIST99, SEC-1].

1.4 Our Criteria and Generating Algorithm

We consider transformability of elliptic curves from a Weierstrass-form to a Montgomery-form, and give exact condition on the elliptic curves whether they can be represented as a Montgomery-form or not. For checking whether its cofactor is exactly "4", we further consider divisibility by powers of 2 for the curve orders of the Montgomery-form elliptic curves. In particular, the discussion of divisibility by 8 is the most significant.

Using our criteria, we present an efficient algorithm for generating Weierstrass-form elliptic curves with Montgomery-form and with which cofactor is equal exactly to 4. Our algorithm handles not only the original curve itself but also its twist so that it can find the good curve more efficiently. We also implement our algorithm by using Schoof's order-counting algorithm, then experimentally confirm the validity of our algorithm. In fact, our algorithm has produced many curves with cryptographic properties desireble for practical applications.

We should note that in this paper we mainly discuss on the elliptic curves over prime fields. However, the similar argument can be applicable to any elliptic curves over any finite fields including Optimal Extension Fields (OEF) [BP98, KMKH99].

2 Preliminaries

In this section, we define technical terms for the following sections. Let $p(\geq 5)$ be a prime and $\mathbf{F}_p$ be the finite field of order p. For $A, B \in \mathbf{F}_p$, an elliptic curve defined by

$$E^M : BY^2 = X^3 + AX^2 + X$$

is called a Montgomery-form elliptic curve or a Montgomery-type elliptic curve. For numbers $a, b \in \mathbf{F}_p$, an elliptic curve defined by

$$E : y^2 = x^3 + ax + b$$

is called a Weierstrass-form elliptic curve or a Weierstrass-type elliptic curve. The set of ($\mathbf{F}_p$-rational) points of E or E^M forms a group with the point at infinity $\mathcal{O}$ as the identity element. Refer to the next section for additional-operation formulae on the Montgomery-form elliptic curves. The number of points of E (resp. E^M) is called curve orders and denoted by $\#E$ (resp. $\#E^M$). For a point P on an elliptic curve, (point) order is the least positive integer n such that $nP = \mathcal{O}$. For example, the point $(0, 0)$ on any Montgomery-form elliptic curve is of order 2. Cofactor is the quotient of the curve order divided by the base point order.

Let $r \in \mathbf{F}_p$ be quadratic non-residue. For a Weierstrass-form elliptic curve $E : y^2 = x^3 + ax + b$,

$$E_r : y^2 = x^3 + ar^2x + br^3$$

is called a twist of E and for a Montgomery-form elliptic curve $E^M : BY^2 = X^3 + AX^2 + X$,

$$E_r^M : \frac{B}{r}Y^2 = X^3 + AX^2 + X$$

is called a twist of E^M. It is clear that $\#E+\#E_r = 2(p+1)$ and $\#E^M+\#E_r^M = 2(p+1)$.

We define a Weierstrass-form elliptic curve E as transformable to the Montgomery-form, if there exists a Montgomery-form elliptic curve defined over $\mathbf{F}_p$ $E^M : BY^2 = X^3 + AX^2 + X$ such that E and E^M are isomorphic over $\mathbf{F}_p$. Namely, there exists $s, t, \alpha, \beta \in \mathbf{F}_p, s, t \neq 0$ such that the function mapping $(x, y) \in E(\mathbf{F}_p)$ to $(s(x-\alpha), t(y-\beta))$ is a group isomorphism of $E(\mathbf{F}_p)$ and $E^M(\mathbf{F}_p)$. $\#E = \#E^M$ if E is transformable to E^M.

3 Cryptographic Advantages of Montgomery-Form Elliptic Curves

3.1 A Comparison between the Montgomery-Form and the Weierstrass-Form about the Operations

The operations on the Montgomery-form elliptic curve $E^M : BY^2 = X^3+AX^2+X$ for affine coordinates are as follows. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ be points on E^M. Then, the point $P_3 = (x_3, y_3) = P_1 + P_2$ is the following:

addition formulae $(P_1 \neq \pm P_2)$

$$\Lambda = (y_2 - y_1)/(x_2 - x_1)$$
$$x_3 = B\Lambda^2 - A - x_1 - x_2$$
$$y_3 = \Lambda(x_1 - x_3) - y_1$$

doubling formulae $(P_1 = P_2)$

$$\Lambda = (3{x_1}^2 + 2Ax_1 + 1)/(2By_1)$$
$$x_3 = B\Lambda^2 - A - 2x_1$$
$$y_3 = \Lambda(x_1 - x_3) - y_1$$

Next, we set $(x, y) = (X/Z, Y/Z)$ for a point (x, y) on E^M, and give operations on projective coordinates. The n-times point of a point $P = (X, Y, Z)$ is denoted by $nP = (X_n, Y_n, Z_n)$. According to [Mon87], $(m+n)P = mP + nP$ without Y is as follows.

addition formulae $(m \neq n)$

$$X_{m+n} = Z_{m-n}[(X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)]^2$$
$$Z_{m+n} = X_{m-n}[(X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)]^2$$

doubling formulae $(m = n)$

$$4X_nZ_n = (X_n + Z_n)^2 - (X_n - Z_n)^2$$
$$X_{2n} = (X_n + Z_n)^2(X_n - Z_n)^2$$
$$Z_{2n} = (4X_nZ_n)((X_n - Z_n)^2 + ((A+2)/4)(4X_nZ_n))$$

The addition formulae require four multiplications and two squarings on $\mathbf{F}_p$ and the doubling formulae require three multiplications and two squarings on $\mathbf{F}_p$.

The scalar multiplication nP requires us repeatedly to calculate either $(2mP, (2m+1)P)$ or $((2m+1)P, (2m+2)P)$ from $(mP, (m+1)P)$ depending on each bit of binary digit of n. Put k the bit length of n. Then the repeating time is $(k-2)$. Without loss of generality, we can assume $Z_1 = 1$. So, addition

formulae require three multiplications. It needs to compute $2P$ at first, the computation time of nP is $(3M + 2S)(2k - 3)$, where M is the computation time of the multiplications and S is the computation time of the squarings on the finite field.

On the scalar multiplications on Weierstrass-form elliptic curves, Jacobian coordinates using window method is the fastest ([CMO98]). Assume that the size of definition field is 160 bits and that $1S = 0.8M$. The scalar multiplications on Weierstrass-form require $10M$ per bit on average. The scalar multiplications on Montgomery-form require $9.2M$ per bit. Thus, the Montgomery-form elliptic curves are faster than the Weierstrass-form elliptic curves by about 10 percent.

Remark 1. There are more detailed comparisons between the computation times of the Montgomery-form and those of the Weierstrass-form in [TK99, Izu99a, Izu99b, OSK99].

3.2 The Montgomery-Form Elliptic Curves against Timing-Attacks

A timing-attack is a way of guessing a private key information from its calculating time of operation on cryptosystems like the RSA and DSS([Koc, Koc96]), and is adaptable to elliptic curve cryptosystems. In the case of elliptic curve cryptosystem, it is a way of guessing a private key d from the calculating time of the scalar multiplication dP of a base point P by d. It is effective that the calculating time is far from the average time.

The number of additions and that of doublings in the scalar multiplications on the Montgomery-form elliptic curves depend just on the bit-lengths but do *not* depend on the bit-patterns (nor on the ratio between the number of zeros and the number of ones): in the previous section, we see that the specific algorithm for computing the scalar multiplications dP on the Montgomery-form elliptic curves using projective coordinates repeatedly calculate either $(2mP, (2m+1)P)$ or $((2m+1)P, (2m+2)P)$ from $(mP, (m+1)P)$ depending on a certain bit. Of course, the point $2mP$ is mP doubled, the point $(2m + 1)P$ is mP added by $(m + 1)P$, and the point $(2m + 2)P$ is $(m + 1)P$ doubled. Thus, the scalar multiplication requires *one addition on the elliptic curve* and *one doubling on the elliptic curve* per bit. The number of additions and that of doublings, which are just one respectively, do *not* depend on whether the certain bit is 0 or 1.

However, on the Weierstrass-form elliptic curve, the number of additions and that of doublings in the scalar multiplications *depend* on the bit-patterns (and on the ratio between the number of zeros and the number of ones): for computing the scalar multiplications dP, it needs to calculate repeatedly either $2mP$ or $(2m + 1)P$ from mP (when using window method, it is more complicated but the following result is almost same). Since $2mP = 2(mP)$ and $(2m + 1)P = P + 2(mP)$, the scalar multiplication requires one doubling on the elliptic curve, or one doubling and one addition on the elliptic curve depending on whether the certain bit is 0 or 1. The computation time in the case that the certain bit is 0 is shorter than that in the case that it is 1 by one addition on the elliptic curve. Assume that the scalar value d has many zeros as compared with

ones. In that case the number of additions and that of doublings in the scalar multiplication are small, and its computation time is far from the average time. Hence, timing-attacks are effective for such values.

Elliptic curves defined over finite fields with characteristic 2 using scalar multiplications like the Montgomery-form also immune to timing-attacks. Refer to [AMV93] for the scalar multiplications with characteristic 2 like the Montgomery-form. We need to pay attention that the assumptions in [AMV93] for deriving scalar multiplications are not in general. That is, we may not assume that the z-coordinate of any $(2m+1)P$ is equal to 1. (See Appendix A for the detailed descriptions.)

3.3 Further Improvement: Randomized Projective Coordinates

In the previous section, we saw that the Montgomery-form elliptic curves have the advantage of immunity to timing-attacks. In this section, we propose further improvement for preventing timing-attacks — *randomized projective coordinates*.

The number of additions and that of doublings in the scalar multiplications on the Montgomery-form elliptic curves are constant, but the computation times of the additions and those of the doublings on the elliptic curves are *not* constant. This is because the additions on the elliptic curves require four multiplications and two squarings on the finite field which is the definition field of the elliptic curves, and the doublings on the elliptic curves require three multiplications and two squarings on the finite field, and the multiplication/squaring on the finite field has discrepancies among its computation times although the number required of multiplications and that of squarings on the finite field for the addition/doubling on the elliptic curve are constant. For values which extremely small compared with the characteristic p of finite fields, the computation times of multiplication/squaring are short. Consequently, computation times of addition/doubling are short for points having such values. And the computation time of the scalar multiplication is short comparatively if there are such points in the calculating of the scalar multiplication. Therefore, the computation time of the scalar multiplication on the elliptic curve depends on *the operations on the finite field*. The same values have the same time required for computation, and it is easy for us to guess which values have the time required for computation far short/long from the average. The fact mentioned above gives an information for timing-attacks.

We present *randomized projective coordinates* for avoiding the situation above:

INPUT A scalar value d and a base point $P = (x, y)$.
OUTPUT The scalar multiplication dP.

1. Generate a random number k.
2. Calculate $P = (kx, ky, k)$ expressed by projective coordinates.
3. Calculate dP using the scalar multiplication algorithm with projective coordinates on the Montgomery-form elliptic curve.
4. Output dP.

Since $(kx, ky, k) = (x, y, 1)$ in projective coordinates, the computation result is coincide with the result using $(x, y, 1)$, which is usual choice. The computation times using random numbers for the same value are different. Some of them may be short, but they are not always short. This fact prevents timing-attacks.

Remark 2. Using only randomized projective coordinates is not good enough for preventing timing-attacks. (See [Cor99] for preventing Differential Power Analysis (DPA) by using randomized projective coordinates. It prevents leaking any specific bit of a point in projective coordinates.) On the computation of the scalar multiplication dP of a point P by a private key d on the Weierstrass-form, the number of additions and that of doublings are *proper* to the private key d (and the number of additions and that of doublings in the scalar multiplication using window-methods are also proper to d). That is, the number of additions and that of doublings for another private key d' are different from those of d, in general. Therefore, an adversary repeatedly obtains computation times for the same point, and he can estimate the number of additions and that of doublings on the elliptic curve for the private key by statistical treatment for the distribution of the computation times.

On the other hand, in the case of the Montgomery-form, the number of additions and that of doublings on the elliptic curve are constant for the same bit length private keys. Thus, if we could assume that the computation time of additions and that of doublings on the elliptic curve are constant for any point, the computation time of the scalar multiplications are constant. However, a close situation appears by using randomized projective coodinates.

4 Transformability from Weierstrass-Form to Montgomery-Form

In this section, we study transformabilities from the Weierstrass-form to the Montgomery-form. Any Montgomery-form elliptic curve has the point $(0, 0)$ of order 2. It is easy to find that there exists a Weierstrass-form elliptic curve without the Montgomery-form, since some Weierstrass-form elliptic curves have no points of order 2. The Weierstrass-form elliptic curves with the Montgomery-form should have the point of order 2 which is mapped to $(0, 0)$ on the Montgomery-form elliptic curves. In fact, they are transformable to the Montgomery-form if they have such a point. The next proposition ensures that.

Proposition 1. *A Weierstrass-form elliptic curve $E : y^2 = x^3 + ax + b$ is transformable to the Montgomery-form if and only if it satisfies two conditions as follows:*

1. *The equation $x^3 + ax + b = 0$ has at least one root in $\mathbf{F}_p$*
2. *The number $3\alpha^2 + a$ is quadratic residue in $\mathbf{F}_p$, where α is a root of the equation $x^3 + ax + b = 0$ in $\mathbf{F}_p$.*

Proof. Assume that E satisfies such conditions. Let s be one of the square roots of $(3\alpha^2+a)^{-1}$ in $\mathbf{F}_p$, and set $B=s, A=3\alpha s$. Then, the function mapping point (x,y) on E to $(s(x-\alpha), sy)$ gives an isomorphism E to E^M, where E^M is the Montgomery-form elliptic curve defined by $BY^2=X^3+AX^2+X$.

Conversely, assume that the Weierstrass-form elliptic curve E is transformable to a Montgomery-form elliptic curve $E^M : BY^2=X^3+AX^2+X$. Then, the Weierstrass-form elliptic curve should have points of order 2 in $\mathbf{F}_p$. Thus, the condition 1 is satisfied.

The isomorphism from the Weierstrass-form elliptic curve to the Montgomery-form elliptic curve is given that (x,y) maps to $(s(x-\alpha'), t(y-\beta'))$ for some $s,t,\alpha',\beta' \in \mathbf{F}_p, s,t \neq 0$. Since the point $(\alpha,0)$ of order 2 on the Weierstrass-form elliptic curve corresponds to the point $(0,0)$ on the Montgomery-form elliptic curve, we get $\alpha'=\alpha, \beta'=0$. So, the isomorphism maps to $(s(x-\alpha), ty)$. This point is on the Montgomery-form elliptic curve. We obtain

$$Bt^2y^2 = s^3(x-\alpha)^3 + As^2(x-\alpha)^2 + s(x-\alpha). \tag{1}$$

For simplicity, set $f(x)=x^3+ax+b$. Since the point (x,y) is on the Weierstrass-form elliptic curve, substitute $y^2=f(x)$ at the formula (1), we find $Bt^2=s^3$ by comparing x^3-terms. We obtain

$$s^2f(x) = s^2(x-\alpha)^3 + As(x-\alpha)^2 + (x-\alpha), \tag{2}$$

by substituting $Bt^2=s^3$ and dividing by s at the formula (1).

$$s^2f'(\alpha) = 1 \tag{3}$$

is derived from the formula (2) with derivation by x and substitution of α for x. Thus, $f'(\alpha)$ should be quadratic residue in $\mathbf{F}_p$, and the condition 2 is satisfied. □

Remark 3. Any Montgomery-form elliptic curve is transformable to the Weierstrass-form elliptic curve. For the Montgomery-form elliptic curve $E^M : BY^2=X^3+AX^2+X$, we set $s=B, \alpha=A/3B, a=1/s^2-3\alpha^2, b=-\alpha^3-a\alpha$. Then, the Weierstrass-form elliptic curve $E : y^2=x^3+ax+b$ is transformable to E^M.

Remark 4. There are other claims which decide whether the Weierstrass-form elliptic curves are transformable to the Montgomery-form elliptic curves or not ([Izu99a, Izu99b]). The above proposition is easy to handle in random elliptic curves generation.

Example 1. $p=5, y^2=x^3+2x$.
Since the equation $x^3+2x=0$ has one root $\alpha=0$ in $\mathbf{F}_5$, Condition 1 of Proposition 1 is satisfied. However, the number $3\alpha^2+a(=2)$ is quadratic non-residue. Thus, this curve is not transformable to the Montgomery-form.

Example 2. $p = 7, y^2 = x^3 + 3x + 6$.
Since the equation $x^3 + 3x + 6 = 0$ has one root $\alpha = 3$ in $\mathbf{F}_7$, Condition 1 is satisfied, and the number $3\alpha^2 + a(= 2)$ is quadratic residue. Thus, this curve is transformable to the Montgomery-form. $s = 2$ is one of square roots of $1/2$ in $\mathbf{F}_7$. We obtain the numbers $B = s = 2, A = 3\alpha s = 4$. Hence, the Montgomery-form elliptic curve is the equation $2Y^2 = X^3 + 4X^2 + X$, and the point (x, y) on the Weierstrass-form elliptic curve $y^2 = x^3 + 3x + 6$ corresponds to the point $(2(x - 3), 2y)$ on the Montgomery-form elliptic curve $2Y^2 = X^3 + 4X^2 + X$.

Proposition 2. *Let r be quadratic non-residue in $\mathbf{F}_p$, and $E_r : y^2 = x^3 + ar^2x + br^3$ be the twist of $E : y^2 = x^3 + ax + b$. Then, E is transformable to the Montgomery-form if and only if E_r is transformable to the Montgomery-form.*

Proof. Assume that E is transformable to the Montgomery-form. According to Proposition 1, There exists $\alpha \in \mathbf{F}_p$ such that $f(\alpha) = 0$ and that $f'(\alpha)$ is quadratic residue, where $f(x) = x^3 + ax + b$. Set $f_r(x) = x^3 + ar^2x + br^3$. $f_r(r\alpha) = r^3 f(\alpha) = 0$, and $f_r'(r\alpha) = r^2 f'(\alpha)$, so it is quadratic residue. According to Proposition 1, E_r is also transformable to a Montgomery-form.

Conversely, assume that E_r is transformable to the Montgomery-form. Since r^{-1} is quadratic non-residue in $\mathbf{F}_p$, the elliptic curve E is the twist of E_r. As above, E is transformable to the Montgomery-form. □

Example 3. The integer 3 is quadratic non-residue in $\mathbf{F}_7$. The elliptic curve $y^2 = x^3 + 6x + 1$ is the twist of the elliptic curve $y^2 = x^3 + 3x + 6$. the number $\alpha = 2$ is the root of the equation $x^3 + 6x + 1 = 0$ and the number $3\alpha^2 + 6 = 4$ is quadratic residue. Thus, the curve is transformable to the Montgomery-form. On the other hand, we know that the elliptic curve $y^2 = x^3 + 3x + 6$ is transformable to the Montgomery-form by Example 2. Proposition 2 shows us the twist $y^2 = x^3 + 6x + 1$ is also transformable to the Montgomery-form.

According to Proposition 2, the transformabilities of a given Weierstrass-form elliptic curve and of its twist coincide with each other. When we generate elliptic curves randomly, we need to decide curve orders for judging the securities of the curves. Ordinarily, we do that for an elliptic curve candidate and its twist at the same time, since the relation $\#E + \#E_r = 2(p + 1)$ gives us that one curve order drives from the other curve order. When we generate the Weierstrass-form elliptic curves with the Montgomery-form, we can deal with a candidate and its twist together because of the coincidence of their transformabilities.

Let Δ be the discriminant of the polynomial $f(x) = x^3 + ax + b$, namely, $\Delta = -16(4a^3 + 27b^2)$. The definition of discriminant gives the following:

- The equation $f(x) = 0$ has three roots in $\mathbf{F}_p \Rightarrow (\Delta/p) = 1$
- The equation $f(x) = 0$ has one root in $\mathbf{F}_p \Rightarrow (\Delta/p) = -1$

Here $(\cdot/\cdot)$ denotes the quadratic residue symbol. Let α, β and γ be roots of the equation $f(x) = 0$ in the algebraic closure of $\mathbf{F}_p$ or a suitable extension field of $\mathbf{F}_p$. It is easy to find the equation $\Delta = -16(3\alpha^2 + a)(3\beta^2 + a)(3\gamma^2 + a)$ by calculation. Using relations above, we easily find many conditions for

transformability such as the following: When $p \equiv 1 \pmod 4$, if the equation $f(x) = 0$ has three roots, the Weierstrass-form elliptic curve defined by the equation $y^2 = f(x)$ is transformable to the Montgomery-form.

5 Divisibilities by Powers of 2 for Curve Orders of the Montgomery-Form

Montgomery mentioned the divisibilities by "4" for curve orders of Montgomery-form in his paper ([Mon87]). According to this paper, the curve orders with the Montgomery-form are always divisible by 4. Whereas recent ECC-standards ([NIST99,SEC-1]) recommend that the cofactor of elliptic curve be within "4" for cryptographic use. For generating Montgomery-form elliptic curves with cofactor 4, we need to study the divisibilities by integers for curve orders, especially by "8".

The next proposition and corollary discribe the divisibilities by 4 for curve orders.

Proposition 3. *Let* $E^M : BY^2 = X^3 + AX^2 + X$ *be the Montgomery-form elliptic curve. Then,* E^M *has :*

1. three points of order 2	*if* $A^2 - 4$ *is quadratic residue*
2. exactly one point of order 2*, which is* $(0, 0)$	*if* $A^2 - 4$ *is quadratic non-residue*
3. the points $(1, \pm\gamma)$ *of order* 4	*if* $(A + 2)/B$ *is quadratic residue*
4. the points $(-1, \pm\gamma')$ *of order* 4	*if* $(A - 2)/B$ *is quadratic residue,*

where γ *is one of the quadratic roots of* $(A+2)/B$ *and* γ' *is one of the quadratic roots of* $(A - 2)/B$*.*

Proof. The elliptic curve E^M always has the point $(0, 0)$ of order 2. The equation $X^2 + AX + 1 = 0$ has two roots in $\mathbf{F}_p$ if the discriminant of the equation $A^2 - 4$ is quadratic residue. Hence, E^M has two other points of order 2 (1.). The equation $X^2 + AX + 1 = 0$ has no roots in $\mathbf{F}_p$ if the discriminat $A^2 - 4$ is quadratic non-residue (2.). If $(A + 2)/B$ is quadratic residue, the double points of the points $(1, \pm\gamma)$ are both $(0, 0)$. Thus, they are points of order 4 (3.). The case that $(A - 2)/B$ is quadratic residue is similar (4.). □

Corollary 1. *The curve orders of the Montgomery-form are always divisible by* 4 *([Mon87]). Thus, any Montgomery-form elliptic curve has the cofactor which is greater than or equal to* 4*.*

Proof. First, we assume that the discriminant $A^2 - 4$ is quadratic residue. Then, the curve has three points of order 2 and the curve order is divisible by 4. Next, we assume that the discriminant $A^2 - 4$ is quadratic non-residue. Then either $(A + 2)/B$ or $(A - 2)/B$ is quadratic residue. Thus, the curve has a point of order 4 and the curve order is divisible by 4. □

Remark 5. The book "Elliptic Curves in Cryptography", which was recently published ([BSS99]), has many numerical examples of elliptic curves. The following ellptic curve is in the Example 11 at p.185, a Weierstrass-form elliptic

curve with cofactor 4.

$p =$ 000045e1 8f0df0d6 ed244807 b126feeb c1eab4de c8263bdd 6dc120d1
e36b6cb5 d7114f5d 883276d0 e29dad93 bcb542dd ed75343f

$a =$ 00000005

$b =$ 00002655 4794e358 360936a7 3a77d75b e7d64d49 13a8f5d1 7354a69b
3423929a 57f98a1d b34c1563 beb79dff 0d40b990 5062b347

The equation $x^3 + ax + b = 0$ has three roots in $\mathbf{F}_p$. Thus, Condition 1 of Proposition 1 is satisfied. Let α, β and γ be three roots. That is,

$\alpha =$ 0000195b 9279f672 f0a52665 f24df394 812aa7e3 da3e8816 1603b4b2
7de839f5 0d1b79ad ac86d1c2 99b2501e 18663a2b af699cad

$\beta =$ 00003c74 de1cde6b 718e6bb6 622f43f9 5ec725f6 b2f47967 cd03535c
5b1db420 15d739d7 10bef858 585767b0 502b0d90 e97372db

$\gamma =$ 000035f2 ad850ccf 7814fdf3 0dd0c649 a3e39be3 0319763c f87b3994
edd0eb56 8b2feb36 531f2386 d331a359 10d93dff 420d58f6.

The number $3\alpha^2 + a$
$=$ 0000310f 1870d004 25388cb9 418695a8 ff533216 056c5463 cad7fff7
ebac7eae 8e620c5e b5027d67 2bae606e e3aa6419 74131b4b

is quadratic non-residue in $\mathbf{F}_p$, the root α does not satisfy Condition 2. the number $3\beta^2 + a$ and the number $3\gamma^2 + a$ are also quadratic non-residue. Hence, no roots satisfy Condition 2. Therefore, this Weierstrass-form elliptic curve is not transformable to the Montgomery-form elliptic curve, although it has cofactor 4.

That is, not all the Weierstrass-form elliptic curves, of which curve orders are divisible by 4, are transformable to the Montgomery-form elliptic curves.

Concerning the divisibilities by 8 for the curve orders, we obtain the following:

Theorem 1.

$p \equiv 1 \bmod 4 \quad ((-1/p) = 1)$

$A+2$	$A-2$	B	$8 \mid \#E^M$
QNR	*QR*	*QR*	*D*
QNR	*QR*	*QNR*	*ND*
QR	*QNR*	*QR*	*D*
QR	*QNR*	*QNR*	*ND*
QR	*QR*	*QR*	*D*
QR	*QR*	*QNR*	*ND*
QNR	*QNR*	*QR*	*ND*
QNR	*QNR*	*QNR*	*D*

QR:quadratic residue
QNR:quadratic non-residue

$p \equiv 3 \bmod 4 \quad ((-1/p) = -1)$

$A+2$	$A-2$	B	$8 \mid \#E^M$
QNR	*QR*	*QR*	*ND*
QNR	*QR*	*QNR*	*ND*
QR	*QNR*	*QR*	*D*
QR	*QNR*	*QNR*	*D*
QR	*QR*	*QR*	*D*
QR	*QR*	*QNR*	*D*
QNR	*QNR*	*QR*	*D*
QNR	*QNR*	*QNR*	*D*

D:divisible by 8
ND:non-divisible by 8

Proof. In the case that $A^2 - 4$ is quadratic non-residue, it is a consequence of Theorem 2 below because there is just one point of order 2 on the curve. In the case that $A^2 - 4$ is quadratic residue, it is a consequence of Proposition 3 and Proposition 4 below. That is, the curve order of either the given Montgomery-form elliptic curve or its twist is divisible by 8 since either of them has a point of order 4 from Proposition 3, and we obtain the other divisibility from Proposition 4. □

Assume that any probability of quadratic residue in Theorem 1 is exactly $1/2$ and that properties of $A+2$ and $A-2$ for quadratic residue are independent. Then probabilities that the curve orders of the Montgomery-form are divisible by 8 are as follows.

$$\begin{array}{ll} 1/2 & \text{if } p \equiv 1 \pmod 4 \\ 3/4 & \text{if } p \equiv 3 \pmod 4 \end{array}$$

Thus, We can discard certain ratio of the Montgomery-form elliptic curves at the first stage of random elliptic curves generation.

The next theorem concerns the existence or non-existence of the points of order 8.

Theorem 2. *Let A^2-4 be quadratic non-residue.*

$p \equiv 1 \bmod 4 \quad ((-1/p)=1)$

$A+2$	$A-2$	B	u	order 8
QNR	QR	QR	-1	E
QNR	QR	QNR	1	NE
QR	QNR	QR	1	E
QR	QNR	QNR	-1	NE

$p \equiv 3 \bmod 4 \quad ((-1/p)=-1)$

$A+2$	$A-2$	B	u	order 8
QNR	QR	QR	-1	NE
QNR	QR	QNR	1	NE
QR	QNR	QR	1	E
QR	QNR	QNR	-1	E

QR:quadratic residue *E:exist*
QNR:quadratic non-residue *NE:not exist*
,where u is the x-coordinate of points with order 4 of which double points are both $(0,0)$.

Proof. By Proposition 3, in any case that A^2-4 is quadratic non-residue, the curve has exactly two points of order 4 of which x-coordinate is either 1 or -1 and of which double point is the point $(0,0)$.. According to the lemma we show below, all we have to do to determine whether points of order 8 exist or not is to check that both $A+2$ and $1/B$ are quadratic residue if the x-coordinate u is equal to 1, and both $-(A-2)$ and $-1/B$ are quadratic residue if the x-coordinate u is equal to -1. □

Proposition 4. *Let r be quadratic non-residue.*
$8|\#E^M \Leftrightarrow 8 \not| \#E_r^M$ *if* $p \equiv 1 \pmod 4$
$8|\#E^M \Leftrightarrow 8|\#E_r^M$ *if* $p \equiv 3 \pmod 4$

Proof. It is clear from the equation $\#E^M + \#E_r^M = 2(p+1)$ and Corollary 1. □

To complete the proof of Theorem 2, we show the next lemma.

Lemma 1. *Let $E^M : BY^2 = X^3 + AX^2 + X$ be a Montgomery-form elliptic curve. Then, both u^2+Au+1 and u/B are quadratic residue if a point (u,v) on E^M is the double point of some point on E^M. Conversely, in the case that A^2-4 is quadratic non-residue, a point (u,v) on E^M is the double point of some point on E^M if both u^2+Au+1 and u/B are quadratic residue.*

Proof. Assume that the point (u, v) is the double point of some $\mathbf{F}_p$-rational point (x, y) on E^M. The formula of the tangent line at the point (x, y) is

$$Y = \frac{3x^2 + 2Ax + 1}{2By}(X - x) + y. \tag{4}$$

Since the tangent line (4) intersects the curve at the point $(u, -v)$, by substituting the point $(u, -v)$ for the pair of variables (X, Y) followed by multiplying $2By$ and squaring the both sides, we find the equation

$$4Bv^2By^2 = ((3x^2 + 2Ax + 1)(u - x) + 2By^2)^2. \tag{5}$$

Since the points (x, y) and $(u, -v)$ are on the curve, they satisfy the equations $By^2 = x^3 + Ax^2 + x$ and $Bv^2 = u^3 + Au^2 + u$. By using these equations, we find the equation

$$(3x^2 + 2Ax + 1)^2 - 4(x^3 + Ax^2 + x)(u + A + 2x) = 0. \tag{6}$$

Since $x \neq 0$, we divide the equation (6) by x^2, and regard it as an equation with respect to $\left(x + \frac{1}{x}\right)$. We find the equation

$$\left(x + \frac{1}{x}\right)^2 - 4u\left(x + \frac{1}{x}\right) - 4(Au + 1) = 0. \tag{7}$$

$x + \frac{1}{x} \in \mathbf{F}_p$ requires that the discriminant $4(u^2 + Au + 1)$ of the equation (7) should be quadratic residue. Thus, the number

$$u^2 + Au + 1 \tag{8}$$

should be quadratic residue. Let w be one of the square roots of $u^2 + Au + 1$. Then, the solutions of the equation (7) are $x + \frac{1}{x} = 2(u \pm w)$. $x \in \mathbf{F}_p$ requires that the discriminant of this equation with respect to the variable x

$$(u \pm w)^2 - 1 \tag{9}$$

should be quadratic residue. Thus, either $(u+w)^2-1$ or $(u-w)^2-1$ is quadratic residue, and the solutions of these equations are

$$x = (u + w) \pm \sqrt{(u + w)^2 - 1} \tag{10}$$

or

$$x = (u - w) \pm \sqrt{(u - w)^2 - 1}, \tag{11}$$

respectively. For simplicity, we set $\delta = u \pm w$. Then, we find the equation

$$By^2 = (2\delta + A)\left(\delta \pm \sqrt{\delta^2 - 1}\right)^2. \tag{12}$$

Thus, $y \in \mathbf{F}_p$ requires that the number

$$(2\delta + A)/B \tag{13}$$

should be quadratic residue. Hence, $(2(u+w)+A)/B$ is quadratic residue if $(u+w)^2-1$ is quadratic residue, and $(2(u-w)+A)/B$ is quadratic residue if $(u-w)^2-1$ is quadratic residue. ¿From the equation

$$(u \pm w)^2 - 1 = u(2(u \pm w) + A), \tag{14}$$

we find the equation

$$((u \pm w)^2 - 1)\frac{2(u \pm w) + A}{B} = \frac{u}{B}(2(u \pm w) + A)^2. \tag{15}$$

Therefore, u/B is quadratic residue because the left-hand side of the equation (15) is quadratic residue.

Conversely, in the case that A^2-4 is quadratic residue, assume that both u^2+Au+1 and u/B are quadratic residue. Let w be one of the roots of u^2+Au+1. Let (x,y) be the point defined by (10),(11) or (12) depending on the conditions that both $(u+w)^2-1$ and $(2(u+w)+A)/B$ are quadratic residue, or both $(u-w)^2-1$ and $(2(u-w)+A)/B$ are quadratic residue. Then its double point is (u,v). On the other hand, we have the following three equations.

$$((u+w)^2-1)((u-w)^2-1) = u^2(A^2-4) \tag{16}$$

$$(2(u+w)+A)(2(u-w)+A) = A^2-4 \tag{17}$$

$$((u+w)^2-1)(2(u+w)+A)/B = \frac{u}{B}(2(u+w)+A)^2 \tag{18}$$

These three equations (16), (17) and (18) lead that either both $(u+w)^2-1$ and $(2(u+w)+A)/B$, or both $(u-w)^2-1$ and $(2(u-w)+A)/B$ are quadratic residue. □

6 Algorithms to Generate Elliptic Curves with Cofactor 4

In this section, we present an efficient algorithm for generating the Weierstrass-form elliptic curves with whose is equal to 4 and which have the Montgomery-form.

INPUT A prime $p(\geq 5)$.
OUTPUT A Weierstrass-form elliptic curve with the Montgomery-form and with cofactor 4.

1. Find r such that $(r/p) = -1$.
2. Generate a and b, and put $E : y^2 = x^3 + ax + b$.
3. Check the transformability to the Montgomery-form for E as follows.
   3.1 Check the equation $x^3 + ax + b = 0$ has a root in $\mathbf{F}_p$. Go to 2 if it has no roots.
   3.2 Check Condition 2 of Proposition 1 for any root of $x^3 + ax + b = 0$. Go to 2 if no roots satisfy the condition.

4. Check the divisibility by 8 for $\#E$ and $\#E_r$ by using Theorem 1. Go to 2 if they are divisible by 8.
5. Compute $\#E$ and check $\#E = 4l$ or $\#E_r = 4l$ for some prime l. Go to 2 if neither E nor E_r passes.
6. Check other security tests, and output the parameters of the curve if it passes all tests.

At Step 4, we can find the divisibility by 8 for the curve order by checking that just one of $A \pm 2$ and B is quadratic residue or not because we already know that $A^2 - 4$ is quadratic residue or not at Step 3.1.

In the case that $p \equiv 1 \pmod 4$, if the equation has just one root at Step 3.1, we can find the transformability and the divisibility by checking $(3\alpha^2 + a)^{(p-1)/4} \equiv \pm 1 \pmod p$. If it is not equal to 1 or -1, the curve is not transformable. If it is equal to 1, the curve is transformable and $8 \not| \#E_r$, and if it is equal to -1, the curve is transformable and $8 \not| \#E$. In this case, we can remove both one computation time of square root and one computation time of quadratic residue.

In the case that $p \equiv 3 \pmod 4$, we can discard the curve at Step 3.1 when the equation $x^3 + ax + b = 0$ has three roots in $\mathbf{F}_p$, because its curve order and its twist curve order are divisible by 8, if it is transformable to the Montgomery-form.

At Step 6, we use security tests like a MOV reduction ([MOV93]) to check whether the curve is suitable for cryptographic use ([FR94, MOV93, SA98, Sem98, Sma]).

We have implemented this algorithm, and have generated many Weierstrass-form elliptic curves with the Montgomery-form and with cofactor 4. The following curves are some of them. (See Appendix B for more numerical examples)

1. $\lceil \log_2 p \rceil = 160$
   p = f4a8058b eddbd6f3 9f656c5c 8c9f3244 9c4ae98b
   a = 771e67ee 7c7318f7 c1b73997 f9f1794f 2b80633c
   b = 60083263 13ba95ec 80bd966f 3d2752dd 18c58c18
   $\#E$ = f4a8058b eddbd6f3 9f65d54c 4791a3bd ffcb6f44
   = 3d2a0162 fb76f5bc e7d97553 11e468ef 7ff2dbd1 · 4
   A = 082f1bf4 912e93a6 7f283a64 e67eab15 15e34443
   B = 8c26318c c1803eab 069aaff9 882edbc9 0447d09d
   α = af6c44a9 93c02ad0 84ac19df 90a38a0a 6ec8bca8
2. $\lceil \log_2 p \rceil = 192$
   p = 9ee8eff3 b36d910c aec3c1ca 0e636af7 c16db444 5dee43a1
   a = 2e5453d8 bb581d59 5b937f50 980f5344 c698d336 3983491d
   b = 6f8bca6f 36dba7b7 d5d5e9a2 44c0bd43 a0a8075d 8c3eb548
   $\#E$ = 9ee8eff3 b36d910c aec3c1ca f535369c cc9c3692 c3245abc
   = 27ba3bfc ecdb6443 2bb0f072 bd4d4da7 33270da4 b0c916af · 4
   A = 20f6fa01 d844b599 b4f2e523 ea9bd066 f8211bef c2eb9af0
   B = 56fa585e 5b366ebf f680e2e5 cd2c5104 8e325147 30fd2354
   α = 783f4ef4 1c25c7b9 a52711ab 4c8a7f37 a372dbe0 3bec7feb

The Montgomery-form elliptic curves are not anomalous, since their curve orders are always divisible by 4 and are in the range $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.

We have already checked that discrete logarithm problems on the curves we have generated do not reduce to those on the extension fields of $\mathbf{F}_p$ up to degree 512.

Remark 6. Since any Montgomery-form elliptic curve is transformable to the Weierstrass-form elliptic curve, the security of the Montgomery-form elliptic curve is identical to that of the Weierstrass-form elliptic curve. If there exists an efficient attack for the Montgomery-form, it is also efficient for the Weierstrass-form, and vice versa.

Since the best possible cofactor of the Montgomery-form elliptic curves is 4 and that of the Weierstrass-form elliptic curves is 1, the bit length of the base point orders of the Montgomery-form is shorter by two bits than that of Weierstrass-form on the same definition field.

Therefore, the security of the Montgomery-form for any attack except timing-attacks is slightly weaker (but no hindrances in cryptographic use) than or equal to that of the Weierstrass-form.

7 Extension Fields of $\mathbf{F}_p$

Using OEF(Optimal Extension Field) is a fast computation methods of the operations on the elliptic curves ([BP98, KMKH99]). Montgomery-form elliptic curves can be defined over the extension fields of $\mathbf{F}_p$ as well as $\mathbf{F}_p$. Thus, Montgomery-form elliptic curves defined over OEF are attractive for speeding up the operations. In this section, we describe the results for elliptic curves defined over the extension fields of $\mathbf{F}_p$

Let $\mathbf{F}_{p^m}$ be the extension field of degree m.

Proposition 5. *A Weierstrass-form elliptic curve* $E/\mathbf{F}_{p^m} : y^2 = x^3 + ax + b$ *defined over* $\mathbf{F}_{p^m}$ *is transformable to the Montgomery-form elliptic curve* $E^M/\mathbf{F}_{p^m} : BY^2 = X^3 + AX^2 + X$ *defined over* $\mathbf{F}_{p^m}$ *if and only if it satisfies two conditions as follows:*

1. *The equation* $x^3 + ax + b = 0$ *has at least one root in* $\mathbf{F}_{p^m}$
2. *The number* $3\alpha^2 + a$ *has quadratic roots in* $\mathbf{F}_{p^m}$*, where* α *is a root of* $x^3 + ax + b = 0$ *in* $\mathbf{F}_{p^m}$*.*

Proposition 6. *Let* $r \in \mathbf{F}_{p^m}$ *have no roots in* $\mathbf{F}_{p^m}$*, and let* $E_r/\mathbf{F}_{p^m} : y^2 = x^3 + ar^2x + br^3$ *be twist of* $E/\mathbf{F}_{p^m} : y^2 = x^3 + ax + b$*. Then, E is transformable to the Montgomery-form if and only if* E_r *is transformable to the Montgomery-form.*

Proposition 7. *Let* $E^M/\mathbf{F}_{p^m} : BY^2 = X^3 + AX^2 + X$ *be Montgomery-form elliptic curve. Both of* $u^2 + Au + 1$ *and* u/B *have quadratic roots in* $\mathbf{F}_{p^m}$ *if* (u, v) *on* E^M *is the double point of some point on* E^M*. Conversely, in the case that* $A^2 - 4$ *has no quadratic roots in* $\mathbf{F}_{p^m}$*,* (u, v) *on* E^M *is the double point of some point on* E^M *if both of* $u^2 + Au + 1$ *and* u/B *have quadratic roots in* $\mathbf{F}_{p^m}$*.*

Proof (of propositions). Substitute "have square roots in $\mathbf{F}_{p^m}$" and "have no square roots in $\mathbf{F}_{p^m}$" for "quadratic residue" and "quadratic non-residue", respectively, in the proof of each proposition or lemma. □

Therefore, we can obtain similar methods in $\mathbf{F}_{p^m}$ by the propositions above.

8 Conclusion

In this paper, we show that the Montgomery-form elliptic curves are immune to the timing-attacks, and that the exact condition on the Weierstrass-form with/without the Montgomery-form. We also present an efficient algorithm for generating Weierstrass-form elliptic curves with Montgomery-form whose cofactor is exactly equal to 4. And this algorithm handles not only the original curve itself but also its twist so that it can find the good curve more efficiently. We also implement the algorithm and give some numerical examples obtained by this. In this paper, we should note that we mainly discuss elliptic curves over prime fields. However, the similar argument can be applied to any elliptic curves over any finite fields.

9 Acknowledgments

The authors would like to thank the anonymous referees for their helpful comments.

References

[AMV93] Agnew,G.B., Mullin,R.C., Vanstone,S.A., *An Implementation of Elliptic Curve Cryptosystems Over $F_{2^{155}}$*, IEEE Journal on Selected Areas in Communications, vol.11,No.5, (1993), 804-813. 243, 255

[ANSI] ANSI X9.62, Public Key Cryptography for the Financial Services Industry, *The Elliptic Curve Digital Signature Algorithm(ECDSA)*, (1999). 239

[BP98] Bailey,D.V., Paar,C.,*Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms*, Advances in Cryptology-CRYPTO'98,LNCS1462,(1998),472-485. 240, 253

[BSS99] Blake,I.F.,Seroussi,G.,Smart,N.P., *Elliptic Curves in Cryptography*, Cambridge University Press,(1999). 247

[CMO98] Cohen,H., Miyaji,A., Ono,T., *Efficient Elliptic Curve Exponentiation Using Mixed Coordinates*, Advances in Cryptology - ASIACRYPT '98, LNCS1514, (1998), 51-65. 242

[Cor99] Coron,J.S., *Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems*, Pre-Proceedings of Workshop on Cryptographic Hardware and Embedded Systems(CHES), (1999), 292-302. 244

[FR94] Frey,G., Rück,H.G., *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. 62, (1994), 865-874. 252

[Izu99a] Izu,T., *Elliptic Curve Exponentiation for Cryptosystem*, SCIS'99,W4-1.1 (1999), 275-280. 242, 245

[Izu99b] Izu,T., *Elliptic Curve Exponentiation without y-coordinate*, Technical Report of IEICE. ISEC98-86 (1999), 93-98. 242, 245
[KMKH99] Kobayashi,T., Morita,H., Kobayashi,K., Hoshino,F., *Fast Elliptic Curve Algorithm Combining Frobenius Map and Table Reference to Adapt to Higher Characteristic*, Advances in Cryptology - EUROCRYPT'99,LNCS1592,(1999),176-189. 240, 253
[Kob87] Koblitz,N., *Elliptic curve cryptosystems*, Math. Comp.48, (1987), 203-209.
[Koc] Kocher,C., *Cryptanalysis of Diffie-Hellman,RSA,DSS, and Other Systems Using Timing Attacks*, Available at http://www.cryptography.com/ 239, 242
[Koc96] Kocher,C., *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, Advances in Cryptology - CRYPTO '96, LNCS1109, (1996), 104-113. 239, 242
[Mil86] Miller,V.S., *Use of elliptic curves in cryptography*, Advances in Cryptology - CRYPTO '85, LNCS218,(1986), 417-426.
[MOV93] Menezes,A., Okamoto,T., Vanstone,A., *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transaction on Information Theory, Vol.IT-39, No.5, (1993),1639-1646. 252
[MOC98] Miyaji,A., Ono,T., Cohen,H., *Efficient elliptic curve exponentiation(II)*, SCIS'98,7.1.D,(1998)
[Mon87] Montgomery,P.L., *Speeding the Pollard and Elliptic Curve Methods of Factorizations*, Math. Comp. 48, (1987), 243-264. 239, 241, 247
[NIST99] National Institute for Standards and Technology, *Recommended Elliptic Curves for Federal Government Use*, (1999), Available at http://csrc.nist.gov/encryption/ 239, 247
[SA98] Satoh,T., Araki,K., *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Commentarii Mathematici Universitatis Sancti Pauli, (1998), 88-92. 252
[OSK99] Ohgishi,K., Sakai,R., Kasahara,M., *Elliptic Curve Signature Scheme with No y Coordinate*, SCIS'99,W4-1.3 (1999), 285-287. 242
[SEC-1] Standards for Efficient Cryptography, *Elliptic Curve Cryptography Ver.0.5*, (1999),Available at http://www.secg.org/drafts.htm 239, 247
[Sem98] Semaev,I., *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp. 67, (1998), 353-356. 252
[Sma] Smart,N.P., *The Discrete Logarithm Problem on Elliptic Curves of Trace One*, to appear in Journal of Cryptology. 252
[TK99] Takeuchi,K., Koyama,K., *Fast Computation of Elliptic Curve Cryptosystems*, SCIS'99,W4-1.2 (1999), 281-284 . 242

A Montgomery Scalar Multiplications on the Elliptic Curves Defined over the Finite Fields of Characteristic 2

The following is extracted from [AMV93].

Let E be an elliptic curve over $\mathbf{F}_{2^m}$ having equation

$$y^2 + xy = x^2 + ax^2 + b$$

where $a, b \in \mathbf{F}_{2^m}, b \neq 0$. Let $P = (x_1, y_1, z_1)$ and $Q = (x_2, y_2, z_2)$ be two distinct and nonzero points on E with $P \neq -Q$. If $P + Q = (x_3, y_3, z_3)$, then

$$x_3 = AD \quad and \quad z_3 = A^3 z_1 z_2$$

where $A = x_2z_1 + x_1z_2$, $B = y_2z_1 + y_1z_2$, $C = A + B$ and $D = A^2(A + az_1z_2) + z_1z_2BC$. Since $-Q = (x_2, x_2+y_2, z_2)$ and if $P-Q = (x_4, y_4, z_4)$, then

$$x_4 = A'D' \quad and \quad z_4 = (A')^3z_1z_2$$

where $A' = A$, $B' = x_2z_1+B$, $C' = C+x_2z_1$ and $D' = D+z_1z_2[Bx_2z_1+x_2z_1C+(x_2z_1)^2]$. Therefore,

$$x_4 = A[D + z_1z_2[Bx_2z_1 + x_2z_1C + (x_2z_1)^2]] \quad and \quad z_4 = A^3z_1z_2.$$

Thus, $x_3 = x_4 + z_1^2z_2^2x_1x_2A$ and $z_3 = z_4$.

It follows that to compute x_3 for $P + Q$, we need the x-coordinate of P, Q and $P - Q$. Now to compute kP, we compute $2P$ and then repeatedly compute $(2mP, (2m + 1)P)$ or $((2m + 1)P, (2m + 2)P)$ from $(mP, (m + 1)P)$, depending on whether the corresponding bit in the binary representation of k is a 0 or a 1. Since the difference in each pair is P, if we take the z-coordinate of P to be 1, then the z-coordinate of $(2m+1)P$ will always be 1. Hence, we can assume that either $z_1 = 1$ or $z_2 = 1$ in the formula for x_3.

In the above, we may not assume the assumption that the z-coordinate of $(2m + 1)P$ is 1 for any m, even though we take the z-coordinate of P to be 1. In this section, we clear that.

For avoiding the collision of the notation, we set $P = (x_P, y_P, z_P)$ which is used in "kP". We substitute P and Q for $(m+1)P$ and mP, respectively, at the equation $P - Q = (x_4, y_4, z_4)$ above. Since the difference between $(m+1)P$ and mP is P, the point P is equal to the point (x_4, y_4, z_4) as a point, and *there exists some* $\lambda \neq 0$ *such that* $(x_4, y_4, z_4) = (\lambda x_P, \lambda y_P, \lambda z_P)$ *as a triple.* ((x_4, y_4, z_4) is the consequence of the substraction using the method above.) Thus, if we assume $z_P = 1$, we find $z_3 = z_4 = \lambda$, and it is not always equal to 1.

Remark 7. The computing method such as Montgomery scalar multiplications without assuming either $z_1 = 1$ or $z_2 = 1$ in the formula for x_3 works and prevents timing-attacks. However, it is not efficiently fast. For a fast computation, we should combine the following relation between $P + Q$ and $P - Q$ with the formula above:

$$x_3 + x_4 = \frac{x_1x_2}{(x_1 + x_2)^2},$$

where $P = (x_1, y_1), Q = (x_2, y_2), P+Q = (x_3, y_3)$ and $P-Q = (x_4, y_4)$ are points in affine coordinates. We omit the detailed descriptions for the fast computation.

B Numerical Examples

1. $\lceil \log_2 p \rceil = 224$
   p = d0e7f3fc 9ed2398a 14ae970b db7b3d22 deb7715c 4ac259ca 2c9ba8c3
   a = 43ffe524 e92c14e8 c730f6cb e9dae99f 3bd1509b bcdd17bf 330c1ca1
   b = 07023dff eae7799e cea4c0ac a19b24fd 4ed0011f 4c7df255 a9c22143
   $\#E$ = 3439fcff 27b48e62 852ba5c2 f6def716 b3f4467d 0a57b6d8 965f69df · 4
   A = c7c856c0 8e60a802 45305c51 d49bfee1 fd5bfa7d 3a314a69 f0f978e1
   B = 8610c7be cb6d5f24 d10c6849 eb772f2b 181f4b05 2777d7fa a0828206
   α = a6b6fcc2 51d65ccf 2c87630b c24f2827 a289a840 edfbe70b ce27ff2b
2. $\lceil \log_2 p \rceil = 256$
   p = cff4508c b3e663a9 add65372 60ec1764 f633c64a da218c79 e4f43d31 dd86b4f7
   a = 303b6d25 e33dc651 edd322da 06b47d5c 1d57268b dbe0b152 c1ae7731 4d8be56d
   b = 5487b25a f80dcc71 428cee96 008dcdae 60ef4183 b8a91716 9b6110d5 c9a4016c
   $\#E$ = 33fd1423 2cf998ea 6b7594dc 983b05d9 4a5404fa 3332b622 6ebabe0a 267c26fb · 4
   A = 89f2a557 a80e151b 71963690 bf40a5e0 047c6d54 1f535115 93e11b1c 99bcec6d
   B = b69ff084 e42feff3 2f22b6cf 27ff2443 5d755e5a f4ca7f40 c53a70a4 afaa1953
   α = 474ff280 cfa17e98 9f39d4a0 9e9119a9 b39606f2 fcbc6b22 3f260ca3 8ceb0291

The following elliptic curve defined over $\mathbf{F}_p$ where $\lceil \log_2 p \rceil = 162$ has the base point order size 160. This is equal to the base point order size of the elliptic curve with cofactor 1 defined over $\mathbf{F}_{p'}$ where $\lceil \log_2 p' \rceil = 160$.

3. $\lceil \log_2 p \rceil = 162$
   p = 00000003 f224b887 e3fc28b7 f9a06aed f5da889e 032b3e37
   a = 00000002 f700a850 72e6e12e dd8494c7 9ac083c2 a4bec8e0
   b = 00000000 a1ad176a bb498420 27ac4b16 7ddd377d 6d2f8f02
   $\#E$ = 00000000 fc892e21 f8ff0a2d fe687e72 84574b83 f79c0b73 · 4
   A = 00000002 4852eaee 28edc219 6f3c9b3e 86f00972 1fa895af
   B = 00000000 8d997623 607ebadb bfd2d7c3 9ee19a16 50f63e64
   α = 00000000 271cf03a 8cb9c19f 82fb9840 5fe9e698 458750b7