International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 10, Number 2, pages 144–158, July 2020

# Evaluating Side-Channel Resistance Using Low Order Rational Points Against Curve25519 and an Associated Quadratic Twist

Keiji Yoshimoto, Yoshinori Uetake, Yuta Kodera, Takuya Kusaka, Yasuyuki Nogami
Graduate School of Natural Science and Technology, Okayama University,
3-1-1 Tsushima-naka, Kita-ku, Okayama-city, 700-8530, Japan

Received: February 14, 2020
Revised: April 30, 2020
Accepted: June 2, 2020
Communicated by Toru Nakanishi

**Abstract**

IoT devices contribute to improving the mechanism of a system as edge devices for data sharing and automation of industrials. However, such devices are often being a target of an attacker due to their simple architecture and the lack of resources so as to protect data confidentiality using cryptosystems. In addition, although Curve25519 has been used in various security protocols and known to work even on IoT devices efficiently, the curve inherits the low order points hidden inside of the Edward curves. In this paper, the authors demonstrate side-channel attacks against Curve25519 by focusing on the points of order 4 and 8. We choose the order 4 point which does not exist on Curve25519, that exists on the twisted curve of Curve25519. More precisely, the rational point used in this paper is given by $(x, y) = (-1, 0)$ in affine coordinates. In addition, the order 8 point appears to be a high order rational point. The results reveal that the rational points might be a threat to key extraction and it demands us to find further countermeasures.

*Keywords:* Curve25519, Side-channel attack, Invalid curve attack, Twisted Montgomery Curve, Montgomery ladder

## 1 Introduction

In the IoT era, various things are connected to each other via the Internet. The importance of security has become an inseparable part of reliable secure communication systems because there exist some possibilities of cyberattacks that attempt to steal, destroy, and expose our assets.

Elliptic curve cryptography (ECC) is introduced by Miller [1] and Koblitz [2] in 1985 as a practical public key cryptography. The hardness of recovering the plaintext from a ciphertext is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP), which allows the key size to be smaller. More precisely, ECC is considered that ECC with 256-bit is the same security level of RSA [3] with 3000-bit in [4]. Since the IoT devices have limited resources and the key size is one of the parameters that affect calculation processing time, ECC is often implemented in even low-resource devices. In 2006, Bernstein proposed Curve25519 as an elliptic curve for performing Elliptic Curve Diffie-Hellman key exchange (ECDH) [5]. Curve25519 offers 128-bit security with 256-bit key values, and is designed to compute efficiently. Since IETF had selected Curve25519 as the recommendation for a new elliptic curve in 2014, some protocols including OpenSSH [6] and SSL/TLS [7] have adopted Curve25519. However, there exist some attack methods against ECC to

recover a secret-key such as Pollard-Rho method [8] which solves the ECDLP by using the Birthday paradox . Moreover, Lim proposed a method based on the Pollard-Rho algorithm with Chinese Remainder Theorem using some prime order subgroups in [9].

On the other hand, these methods that calculate ECDLP mathematically, it is important to consider physical attacks that take advantage of physical phenomena called *side-channel* information such as timing, power consumption, and electromagnetic emanation during cryptographic calculations. A side-channel attack (SCA) is proposed by Kocher in [10] as one of the methods that estimate a secret-key using side-channel information. Genkin et al. have reported a vulnerability against Curve25519 with an attack based on software using order 4 elements in [11]. In addition, our group has also succeeded a hardware-based attack against Curve25519 by introducing an order 4 rational point into a scalar multiplication algorithm in [12].

In this paper, the authors conduct power analysis attacks against Curve25519 with order 4 and 8 rational points. Especially, this research differs from the previous ones in the point that we use a specific rational point of order 4 sampled from the twisted Montgomery curve. The rational point used in this paper is of the form $(-1, 0)$ in affine coordinate. More precisely, though the selected rational point of order 4 is not involved in the regular Curve25519, the existence of such rational points is widely known through an invalid curve attack concerning the Pollard-Rho method.

On the other hand, since the approach is rarely used for SCAs, the authors examine to utilize the concept of the invalid curve attack for revealing the effectiveness in this field. As a result, we clarify that the points of order 4 and 8 employed in this research allow us to distinguish the difference hidden inside of the power consumption. It tells the necessity of considering the risk of low order points existing in both the regular curve and its twisted curves when we implement the Curve25519.

This paper is organized with five sections as follows. In section 2, we briefly review the mathematical background concerning the finite field, elliptic curves, and side-channel attacks. Next, we describe the relations of power consumption and secret-key information in case of injecting order 4 and 8 rational points in section 3. After that, in section 4, we show the result of the waveform and the secret-key extraction methods from that. Moreover, we discuss countermeasures against our proposed attacks. Finally, we summarize our work and the outcomes in this paper and discuss countermeasures against our proposed attacks.

# 2 Fundamentals

This section describes finite field, elliptic curve, Montgomery ladder, Montgomery curve, and fault attack against Montgomery ladder.

## 2.1 Finite Field

In this paper, although we treat elliptic curves that are constructed on finite fields, we don't concern finite fields detail. Thus, we denote the symbols that relate with finite fields foremost.

Let $\mathbb{G}$ be a commutative group under the binary operation $\circ$ and $\mathbb{H}$ be a subgroup of the group. In addition, $\mathbb{F}_q$ means a field with a prime number $q$.

### 2.1.1 Subgroup

**Definition 2.3** (Left Coset and Right Coset). Let $g$ be an element of $\mathbb{G}$. Then, the set $g \circ \mathbb{H} = \{g \circ h \mid h \in \mathbb{H}\}$ and $\mathbb{H} \circ g = \{h \circ g \mid h \in \mathbb{H}\}$ is said to be a left coset of $\mathbb{H}$ and a right coset of $\mathbb{H}$ respectively.

If the group $\mathbb{G}$ is a commutative group, every left coset $g \circ \mathbb{H}$ equals to be every right coset $\mathbb{H} \circ g$ for any $g \in \mathbb{G}$. In this paper, we discuss commutative groups, so, we don't distinguish left and right cosets. We describe them as cosets. The number of cosets of $\mathbb{H}$ is called the index of $\mathbb{H}$ in $\mathbb{G}$ and denoted by $|\mathbb{G} : \mathbb{H}|$.

**Theorem 2.1** (Lagrange's Theorem). Let $\mathbb{G}$ be a finite group and $\mathbb{H}$ be a subgroup of $\mathbb{G}$. The order of $\mathbb{G}$ is represented by the product of the order of $\mathbb{H}$ and the index $|\mathbb{G} : \mathbb{H}|$.

### 2.1.2 Quadratic Residue/Quadratic Non-Residue

Let $a$ be a non-zero element of $\mathbb{F}_q$. If there exists $x \in \mathbb{F}_q$ satisfying $x^2 = a$, then the element $a$ is called a quadratic residue modulo $q$. The following equality, which is called the *Legendre symbol*, endowed by Fermat's Little Theorem.

$$a^{(q-1)/2} = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue in } \mathbb{F}_q, \\ -1 & \text{if } a \text{ is a quadratic non-residue in } \mathbb{F}_q. \end{cases}$$

## 2.2 Elliptic Curve

An elliptic curve $E$ over the prime field $\mathbb{F}_q$ for $q \neq 2, 3$ is defined as follows.

$$E/\mathbb{F}_q : y^2 = x^3 + ax + b, \quad (a, b \in \mathbb{F}_q). \tag{1}$$

An elliptic curve represented by Eq. (1) is said to be a non-singular curve if the curve satisfies the following condition concerning its coefficient $a$ and $b$.

$$4a^3 + 27b^2 \neq 0.$$

Let $E/\mathbb{F}_q$ be a non-singular elliptic curve and note that the curves dealt in what follows are non-singular. For rational points $P(x_P, y_P)$ and $Q(x_Q, y_Q)$ on $E/\mathbb{F}_q$, the addition $R(x_R, y_R) = P + Q$ is defined as follows.

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{if } P \neq Q \text{ and } x_P \neq x_Q, \\ \dfrac{3{x_P}^2 + a}{2y_P} & \text{if } P = Q \text{ and } y_P \neq 0, \\ \phi & \text{otherwise.} \end{cases} \tag{2a}$$

$$(x_R, y_R) = \begin{cases} (\lambda^2 - x_P - x_Q,\ \lambda(x_P - x_R) - y_P) & \text{if } \lambda \neq \phi, \\ \mathcal{O} & \text{if } \lambda = \phi. \end{cases} \tag{2b}$$

When $\lambda = \phi$, the result of the addition becomes the point at infinity which corresponds to the identity element as $P + \mathcal{O} = \mathcal{O} + P = P$. The scalar multiplication (SCM) for a rational point $P$ and a scalar $s$ is denoted by $[s]P = \sum_{i=0}^{s-1} P$. Furthermore, the set of rational points including the point at infinity and the binary operation defined by the Eqs. (2a), (2b) forms a commutative group $E(\mathbb{F}_q)$.

$$E(\mathbb{F}_q) = \{\mathcal{O}\} \cup \{(x, y) \mid y^2 = x^3 + ax + b\}. \tag{3}$$

Let $\#E(\mathbb{F}_q)$ be an order of $E(\mathbb{F}_q)$. Then, the order is calculated as follows.

$$\#E(\mathbb{F}_q) = p + 1 - t, \tag{4}$$

where $t$ is Frobenius trace of $E/\mathbb{F}_q$. Let $l$ be the largest prime order of the subgroup of $E(\mathbb{F}_q)$. Since $l$ divides $E(\mathbb{F}_q)$ according to the Theorem 2.1, there exists the variable $h = E(\mathbb{F}_q)/l$ that is called cofactor.

The quadratic twist of an elliptic curve represented by Eq. (1) is defined as follows.

$$\tilde{E}/\mathbb{F}_q : y^2 = x^3 + av^2x + bv^3, \tag{5}$$

where $v$ is a quadratic non-residue element in $\mathbb{F}_q$. As a well-known fact, the right-hand side of Eq. (5) can be estimated as quadratic residue if the result obtained by substituting an element $x_0$ into the right-hand side of Eq. (1) becomes a quadratic non-residue over $\mathbb{F}_q$. Thus, it is found that there exists the rational point using $x_0$ on the quadratic twist $\tilde{E}/\mathbb{F}_q$. When the order of an elliptic curve is calculated by Eq. (4), the order of the quadratic twist is given by

$$\#\tilde{E}(\mathbb{F}_q) = p + 1 + t. \tag{6}$$

## 2.3 Montgomery Ladder

Although a binary method-like calculation is the most efficient technique for handling SCMs, it is required to be resistant against a side-channel attack. Montgomery ladder is the calculation method introduced in [13] as an efficient SCM algorithm and it is considered to have a side-channel resistance. SCM with Montgomery ladder is calculated as follows Alg. 1.

**Algorithm 1** SCM with Montgomery ladder

**Input:** $P$, $s = \sum_{j=0}^{n-1} s_j 2^j,\ s_j \in \{0, 1\}$
**Output:** $T_1 = [s]P$
1: $T_1 \leftarrow \mathcal{O}$
2: $T_2 \leftarrow P$
3: **for** $j = n - 1$ to 0 **do**
4: **if** $s_j = 1$ **then**
5: $T_1 \leftarrow T_1 + T_2$
6: $T_2 \leftarrow T_2 + T_2$
7: **else**
8: $T_2 \leftarrow T_1 + T_2$
9: $T_1 \leftarrow T_1 + T_1$
10: **end if**
11: **end for**
12: **return** $T_1$

## 2.4 Montgomery Curve

The Montgomery curve is introduced by Montgomery in [13] and defined as follows.

$$E_{AB}/\mathbb{F}_q : By^2 = x^3 + Ax^2 + x, \quad (A, B \in \mathbb{F}_q), \tag{7}$$

where $B(A^2 - 4) \neq 0 \pmod q$.

Since the order $\#E_{AB}(\mathbb{F}_q)$ is always divided by 4, $E_{AB}(\mathbb{F}_q)$ has a subgroup of order 4 whose structure is $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. If $B(A+2)$ is quadratic residue in $\mathbb{F}_q$, the rational points $(1, \pm\sqrt{(A+2)/B})$ become generator of the order 4 group. In a similar way, if $B(A-2)$ is quadratic residue in $\mathbb{F}_q$, the rational points $(-1, \pm\sqrt{(A-2)/B})$ forms the order 4 cyclic subgroup. Moreover, if $A^2 - 4$ is quadratic residue in $\mathbb{F}_q$, there exist three different rational points whose $y$-coordinate is 0 and these points forms the $\mathbb{Z}_2 \times \mathbb{Z}_2$ subgroup.

For a prime $q \equiv 1 \pmod 4$, the pair of the minimal cofactors of $\#E(\mathbb{F}_q)$ and $\#\tilde{E}(\mathbb{F}_q)$ are either $\{4, 8\}$ or $\{8, 4\}$. On the other hands, for a prime $q \equiv 3 \pmod 4$, both cofactors are 4. Thus, it is said that the order 4 rational points that $x = \pm 1$ exist on the curve $E_{AB}/\mathbb{F}_q$ or $\tilde{E}_{AB}/\mathbb{F}_q$.

Let $\overline{P}(X : Y : Z)$ be a rational point on a Montgomery curve represented by projective coordinates. The relation between a point $\overline{P}(X : Y : Z)$ and $P(x, y)$ is $x = X/Z,\ y = Y/Z, Z \neq 0$. For two different rational points $\overline{P}(X_{\overline{P}} : Y_{\overline{P}} : Z_{\overline{P}})$ and $\overline{Q}(X_{\overline{Q}} : Y_{\overline{Q}} : Z_{\overline{Q}})$, consider a point $\overline{R}(X_{\overline{R}} : Y_{\overline{R}} : Z_{\overline{R}}) = \overline{P} + \overline{Q}$. Using the point $\overline{S}(X_{\overline{S}} : Y_{\overline{S}} : Z_{\overline{S}}) = \overline{P} - \overline{Q}$, the result is calculated as follows.

$$X_{\overline{R}} = Z_{\overline{S}} \{(X_{\overline{P}} + Z_{\overline{P}})(X_{\overline{Q}} - Z_{\overline{Q}}) + (X_{\overline{P}} - Z_{\overline{P}})(X_{\overline{Q}} + Z_{\overline{Q}})\}^2, \tag{8a}$$

$$Z_{\overline{R}} = X_{\overline{S}} \{(X_{\overline{P}} + Z_{\overline{P}})(X_{\overline{Q}} - Z_{\overline{Q}}) - (X_{\overline{P}} - Z_{\overline{P}})(X_{\overline{Q}} + Z_{\overline{Q}})\}^2, \tag{8b}$$

The point $\overline{S}$ corresponds to be an input point when we calculate SCM with Alg. 1.

On the other hand, the result of addition with the same point $\overline{R} = \overline{P} + \overline{P}$ is calculated as follows.

$$T = (X_{\overline{P}} + Z_{\overline{P}})^2 - (X_{\overline{P}} - Z_{\overline{P}})^2, \tag{9a}$$

$$X_{\overline{R}} = (X_{\overline{P}} + Z_{\overline{P}})^2 (X_{\overline{P}} - Z_{\overline{P}})^2, \tag{9b}$$

$$Z_{\overline{R}} = T \{(X_{\overline{P}} - Z_{\overline{P}})^2 + T \cdot (A+2)/4\}. \tag{9c}$$

According to these equations, it is found that we can omit $Y$-coordinates and inverse operations, which are much heavier than the other operations over $\mathbb{F}_q$. Thus, two rational points $P(x, y)$ and $-P(x, -y)$ are treated as the same point in projective coordinates $\overline{P}(X : Z)$ and a Montgomery curve enable us to implement ECC efficiently.

### 2.5 Curve25519

Curve25519 is a kind of Montgomery curve introduced by Bernstein in [5], and defined over $\mathbb{F}_{2^{255}-19}$ as follows:

$$E_{25519} \ : \ y^2 = x^3 + 486662x^2 + x. \tag{10}$$

Curve25519 is used for Elliptic Curve Diffie-Hellman key exchange (ECDH) since the curve is efficiently implemented even for resource-constrained devices, and Curve25519 ensures 128-bit security with 256-bit integer space. These advantages are realized by a specific modular equation as follows:

$$2^{255} \equiv 19 \equiv 2^4 + 2^1 + 2^0 \pmod{2^{255} - 19}. \tag{11}$$

As seen from Eq. (11), the modular operation is carried out by bit shift operations when values that exceed 255-bit.

### 2.6 Side-channel Attack (SCA)

A side-channel attack [10] is a method to retrieve a secret-key by analyzing physical phenomena such as computation timing, power consumption, and electromagnetic emanation. This paragraph describes the SCA by focusing on the power consumption.

An integrated circuit (IC) having cryptographic modules is composed of numerous CMOS circuits. A CMOS circuit possesses one-bit information as on or off depending on a gate voltage. When the value of the CMOS changes, on to off states and the other way around, a current to switch a MOS transistor is generated. Thus, the current depending on the number of CMOS circuits changing the values causes a power supply voltage which is closely related to a scalar value used in SCM algorithms such as a binary method. More precisely, if there is a physical bias, the number of changing CMOS circuits, we can retrieve a secret-key by observing phenomena caused by the bias. In this research, we use simple power analysis (SPA) which is one of the side-channel attack methods with monitoring and analyzing the power consumption [14].

## 3 Discussion for attacking Curve25519

This section describes how to retrieve a secret-key by the SCA using order 4 and 8 rational points as a chosen-ciphertext against SCM on Curve25519.

### 3.1 Target Algorithm

Although there are no differences in classes and the number of procedures in the SCM algorithm described in Alg. 1, the ECD requires a different argument $T_1$ or $T_2$ depending on a secret-key. To perform a constant sequence of operations without any divergences which are driven by the secret-key is said to be an important matter in [15]. Based on this concept, RFC 7748 [16] describes a Montgomery ladder algorithm that employs a swapping function.

In this paper, the authors especially focus on the Montgomery ladder algorithm using the cswap function as shown in Alg. 3. By employing the cswap function, the Montgomery ladder algorithm is carried out as shown in Alg. 2. In Alg. 3, it is noted that the length of variables *mask* and *dummy* is the same as $A$ and $B$. In addition, the hamming weight of the variable *mask* is $\log_2 A$ or 0 if *swap* is 1 or 0, respectively. As shown in Alg. 3 this algorithm carries out different operations depending on swap values. For example, Although Alg. 3 has no conditional branch instructions such as if, outputs $A$ and $B$ have itself values when $swap = 0$ and have each other's values when $swap = 1$. Thus, Alg. 2 and Alg. 3 are suitable for ideal algorithms because they perform as if they are constructed

with conditional branch instructions without those instructions. By this feature, it has shown that these algorithms protect the secret information from unintended physical attacks.

**Algorithm 2** Montgomery ladder with cswap

**Input:** $\overline{P}$ $x$-coordinate $X_p, s = (s_{n-1}, s_{n-2} \dots s_1, s_0)_2$
**Output:** $\overline{T_1} = s\overline{P}$
1: $\overline{T_1} = (X_1 : Z_1) \leftarrow (1 : 0)$ $(= \mathcal{O})$
2: $\overline{T_2} = (X_2 : Z_2) \leftarrow (X_p : 1)$ $(= \overline{P})$
3: $swap \leftarrow 0$
4: $A_{24} \leftarrow (A + 2)/4$
5: **for** $i = n - 1$ to 0 **do**
6: $\quad k \leftarrow (s \gg i)$ & 1
7: $\quad swap \leftarrow swap \oplus k$
8: $\quad (X_1 : X_2) \leftarrow \mathrm{cswap}(swap, X_1, X_2)$
9: $\quad (Z_1 : Z_2) \leftarrow \mathrm{cswap}(swap, Z_1, Z_2)$
10: $\quad swap \leftarrow k$
11: $\quad (\overline{T_1}, \overline{T_2}) \leftarrow \mathrm{ladderstep}(\overline{T_1}, \overline{T_2}, X_p, A_{24})$
12: **end for**
13: $(X_1 : X_2) \leftarrow \mathrm{cswap}(swap, X_1, X_2)$
14: $(Z_1 : Z_2) \leftarrow \mathrm{cswap}(swap, Z_1, Z_2)$
15: **return** $\overline{T_1}$

**Algorithm 3** cswap

**Input:** $swap = 0$ or $1, A, B, (\log_2 A = \log_2 B)$
**Output:** $A, B$
1: $mask \leftarrow 0$
2: **for** $i = \log_2 A$ to 0 **do**
3: $\quad mask \leftarrow mask + swap$
4: $\quad mask \leftarrow 2 \cdot mask$
5: **end for**
6: $dummy \leftarrow mask$ & $(A \oplus B)$
7: $A \leftarrow A \oplus dummy$
8: $B \leftarrow B \oplus dummy$
9: **return** $A, B$

## 3.2 Attack with Order 4 Point

Let $\overline{P}$ be a rational point of order 4. Since the projective coordinates enable us to regard rational points having a similar coefficient $X/Z$ as the same point, $\overline{P}$ is represented by such as $\overline{P}(\alpha : \alpha)$ using a non-zero element $\alpha$ in $\mathbb{F}_p$. The ECD result of the $\overline{P}$ is represented as $\overline{2P}(0 : \alpha)$, and the coordinates of the point at infinity is $\mathcal{O}(\alpha : 0)$. Since a point and the inverse of the point are treated as the same point in projective coordinates using Montgomery ladder, the point $\overline{3P}$ which is the result of $\overline{P} + \overline{2P}$ is represented by a similar coordinates of $\overline{P}$. Therefore, without loss of generality, we denote $\overline{3P}$ as $\overline{P}$. As a result, outputs of $T_1$ and $T_2$ in each step are classified into only three patterns $\overline{P}(\alpha : \alpha)$, $\overline{2P}(0 : \alpha)$, and $\mathcal{O}(\alpha : 0)$ throughout the Montgomery ladder.

In this paper, we focused on $T_1$ in Alg. 2, the ECD Eq. (9a), and it becomes two patterns: "*Case* A" is the calculation of $\overline{P}$, "*Case* B" is the calculation of $\overline{2P}$ and $\mathcal{O}$.

- *Case* A

$$\begin{aligned} X_{\overline{R}} &= (\theta + 0)^2(\theta - 0)^2 = \theta, \\ T &= (\theta + 0)^2 - (\theta - 0)^2 = 0, \\ Z_{\overline{R}} &= 0\{(\theta - 0)^2 + \tfrac{A+2}{4} \cdot 0\} = 0, \end{aligned} \tag{12}$$

**Algorithm 4** ladderstep

**Input:** $\overline{T_1}(X_1 : Z_1), \overline{T_2}(X_2 : Z_2), X_p, A_{24}$
**Output:** $\overline{T_1}, \overline{T_2}$
1: $A \leftarrow X_1 + Z_1$
2: $AA \leftarrow A^2$
3: $B \leftarrow X_1 - Z_1$
4: $BB \leftarrow B^2$
5: $C \leftarrow X_2 + Z_2$
6: $D \leftarrow X_2 - Z_2$
7: $E \leftarrow AA - BB$
8: $DA \leftarrow D \cdot A$
9: $CB \leftarrow C \cdot B$
10: $X_2 \leftarrow (DA + CB)^2$
11: $Z_2 \leftarrow X_p \cdot (DA - CB)^2$
12: $X_1 \leftarrow AA \cdot BB$
13: $Z_1 \leftarrow E \cdot (AA + A_{24} \cdot E)$
14: **return** $\overline{T_1}, \overline{T_2}$

- *Case* B

$$\begin{aligned} X_{\overline{R}} &= (\theta + \theta)^2(\theta - \theta)^2 = 0, \\ T &= (\theta + \theta)^2 - (\theta - \theta)^2 = \theta, \\ Z_{\overline{R}} &= \theta\{(\theta - \theta)^2 + \tfrac{A+2}{4} \cdot \theta\} = \theta. \end{aligned} \tag{13}$$

$\theta$ is a large positive integer that represents coordinates for convenience. Figure 1 shows transitions of the states $[T_1, T_2]$ at fifth line in Alg. 2. The number of states is two. The arrow symbols in the figure show state transitions. In the "$Case : s_{j+1} \oplus s_j$", $Case$ indicates the ECD calculation patterns which are A or B, and $s_{j+1} \oplus s_j$ means an XOR value with current $j$th bit and previous $(j+1)$th bit of a secret-key $s$. For example, assume that the current state is $[\mathcal{O}, \overline{P}]$, current bit is 1, and "$Case$ B" is occurred, then the next state and next bit are $[\overline{2P}, \overline{P}]$ and 0 because $1 \oplus 0 = 1$.

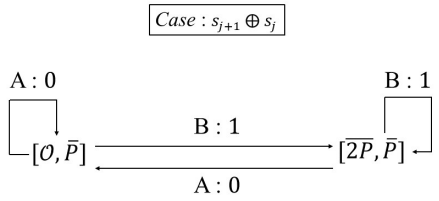


Figure 1: Transition flow based on the order 4 points.

In this paper, we use the order 4 point $(-1 : 1)$ which is a point on the twist of Curve25519. We suppose that $\theta$ is approximately 254-bits. However, when we use the order 4 point $(1 : 1)$ which is on Curve25519, $\theta$ of the $Z_R$ calculation is not sufficient in the first few ladder steps. More precisely, the variables used in ECD calculation Eq. (9a) are smaller than 128-bits in the first three ladder steps. During those first steps, the power consumption does not be large enough to differentiate the operations. Thus, we use the point $(-1 : 1)$ to overcome that point by inducing multiplications with 254-bits values in the first ladder step. It is noted that the state transition diagram and the method to retrieve a secret-key do not change for the choice of a point having order 4.

### 3.3 Attack with Order 8 Point

We can introduce the scenario of the order 4 point into the order 8 point. The coordinates of the order 8 point which is shown in Table 6 pretend to be regular rational points compared to the order

4 point which has the same coordinates in $X = Z$. Therefore, it is not reasonable to evaluate all points whether the points are order 8 or not.

Let $\overline{Q} = (\alpha : \beta)$ be a point of order 8, where $\beta \neq \alpha, \alpha \neq 0, \beta \neq 0$. In projective coordinates using Montgomery ladder, since a point and its additive inverse have the same coordinates, we denote $\overline{7Q}$, $\overline{5Q}$, and $\overline{6Q}$ as $\overline{Q}$, $\overline{3Q}$, and $\overline{2Q}$, respectively. It is noted that the points $\overline{2Q}$ and $\overline{4Q}$ are order 4 and 2 points, respectively. Thus, these points can be considered as $\overline{P}$ and $\overline{2P}$ in section 3.2. By using this relation, the ECD calculation of $\overline{2Q}$ and $\overline{4Q}$ are classified into the "*Case* A" and "*Case* B". Following the "*Case* A, B" and later description, the important thing for our attacks is whether the value is zero or non-zero. In this sense, we place importance on not exact values but whether the values are zero or non-zero values. Consequently, $\overline{Q}$ and $\overline{3Q}$ are the same in that both are points with projective coordinates that can be represented with two different large positive integers. Thus, we unite these points to $\overline{Q'} = \{\overline{Q}, \overline{3Q}\}$. As a result, during SCM with Montgomery ladder, the outcomes of $T_1$ and $T_2$ are within four elements $\overline{Q'}$, $\overline{2Q}$, $\overline{4Q}$, and $\mathcal{O}$.

For the order 8 points, the ECD calculation is classified into the new patterns "*Case* C".

- *Case* C

$$\begin{aligned} X_{\overline{R}} &= (\theta + \lambda)^2(\theta - \lambda)^2 = \omega, \\ T &= (\theta + \lambda)^2 - (\theta - \lambda)^2 = \omega, \\ Z_{\overline{R}} &= \omega\{(\theta - \lambda)^2 + \tfrac{A+2}{4} \cdot \omega\} = \omega, \end{aligned} \tag{14}$$

where $\lambda$ and $\omega$ are large positive integers such that $\lambda, \omega \neq 0$, and $\lambda \neq \theta$. Figure 2 shows transitions of the states $[T_1, T_2]$ at the beginning of each ladder step in Alg. 2 when we input the order 8 point.

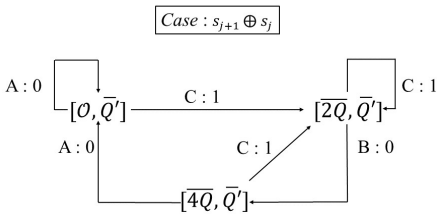


Figure 2: Transition flow based on the order 8 points.

We suppose that the power consumption of the multiplication with zero is smaller than that with each non-zero element. By observing the differences in voltage during the multiplication, it is possible to determine whether the multiplication with zero is performed or not. Furthermore, we can associate *Case*s with power consumption. For instance, consider the case that the calculation of $X_{\overline{R}}$ is low and the calculation of $Z_{\overline{R}}$ is high, then it is presumed that *Case* B occurs. This is because the multiplication with zero in $X_{\overline{R}}$ calculation and the multiplication with non-zero in $Z_{\overline{R}}$ calculation occur in *Case* B. The relations between *Case*s and power consumption are defined in Table 1. As a result, focusing on the multiplications of $X_{\overline{R}}$ and $Z_{\overline{R}}$, we can retrieve secret-key from power consumption and Table 1.

Table 1: Relations between *Case*s and power consumption

| | *Case* A | *Case* B | *Case* C |
|---|---|---|---|
| $X_{\overline{R}}$ | *High* | *Low* | *High* |
| $Z_{\overline{R}}$ | *Low* | *High* | *High* |

# 4 Experimental Result

## 4.1 Experimental results and a consideration concerning countermeasures

In this paper, we used an oscilloscope, Agilent Technologies DSOS104A, to measure a power consumption during a SCM calculation with Alg. 2. The secret-key $s$ is a 255-bits value. We target Arduino Uno [17] since it is expected that the practical use of ECC for IoT devices will expand in the future and implementations and evaluations of ECC for Arduino have been reported in some research (e.g. [18], [19]).

The authors used Arduino Cryptography Library [20], an open-source cryptography library for Arduino devices, for implementing SCM of Curve25519 with Montgomery ladder algorithm Alg. 2. The input points of order 4 and 8 for SCM are shown in Table 5, 6.

The authors remodel an Arduino Uno to measure the power consumption. More precisely, we cut the GND pins of microcontroller and insert a 50 Ω register between $V_{cc}$ pin and the ground. Then, we observe the voltage drop across the resistance using a passive probe. Since a single trace is much noisy to observe, we carry out the same SCM calculation 25 times and take the average. Thus, it can be possible that we observe the power consumption and detect as High or Low easily.

In other words, though the proposed attack enables an attacker to retrieve the secret-key from a waveform based on our pattern recognition technique even if the one does not use the averaging option. (See Figures 9 and 10 in Appendix for the reference.) However, it would be considered to be hard for distinguishing the cases visually. Therefore, the authors list up and mention the results by using the averaging option hereafter.

## 4.2 Experimental Results

This section describes the experimental results of the attack based on Sec. 3. Moreover, we show that we can classify the voltage visually and the models that is created from waveform of each cases mechanically.

### 4.2.1 Key Extraction with Order 4 of the Quadratic Twist

Figure 3 shows the voltage of SCM with the order 4 rational point during first five ladder steps. We use black colored trigger surrounding line 13 in Alg. 4 and retrieve the secret-key using Figure 1 and Table 1. The authors distinguish the surrounded waveform by red lines, auxiliary lines.

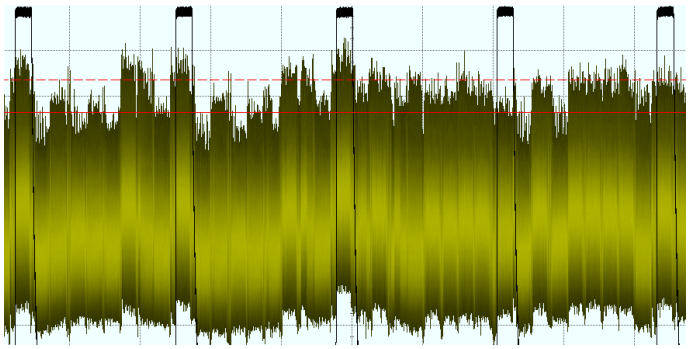

Figure 3: Waveform of SCM using the order 4 point of quadratic twist curve.

We can classify the all waveforms except for 4th waveform as High. For the first waveform, it represents the voltage of MSB whose state transition is classified as $Case$ B always. Therefore, the first waveform will be high and we can verify the phenomenon in Figure 3. After this waveform, we retrieve the secret-key in accordance with the following: When we classify a waveform as $Case$ A, the current bit is same as the previous bit, which means the value of XOR is 0. On the other hand, when we classify a waveform as $Case$ B, the current bit is different from the previous bit, which means the value of XOR is 1. According to the above procedure, we obtain the Table 2 which shows the trace of $Z_{\overline{R}}$, $Case$, state, and secret-key bits.

Table 2: Status and secret-key in each loop with the order 4 point

| Loop | 1st | 2nd | 3rd | 4th | 5th |
|---|---|---|---|---|---|
| $Z_{\overline{R}}$ | $High$ | $High$ | $High$ | $Low$ | $High$ |
| $Case$ | $B$ | $B$ | $B$ | $A$ | $B$ |
| State | $[\overline{2P}, \overline{P}]$ | $[\overline{2P}, \overline{P}]$ | $[\overline{2P}, \overline{P}]$ | $[\mathcal{O}, \overline{P}]$ | $[\overline{2P}, \overline{P}]$ |
| $s_i$ | 1 | 0 | 1 | 1 | 0 |

#### 4.2.2 Comparison waveform with Order 4 and Quadratic Twist

Figure 4 shows the voltage of SCM during the same time as Figure 3. Furthermore, we use the same secret-key, thus, the waveform should be the same behavior. However, the voltage for the first two loops appears to be low, it should be high. In this way, when we use an order 4 point on the quadratic twist shown in Table 5, it is more dangerous to retrieve a secret-key. More precisely, when we use an order 4 point on the curve, the hamming weight of variables for SCM, $X_{\overline{R}}$, $Z_{\overline{R}}$, and $T$, is smaller than the half of 255-bit in the first three loops. In contrast, when we use an order 4 point on the quadratic twist, the hamming weight of variables becomes 255-bit from the first loop.

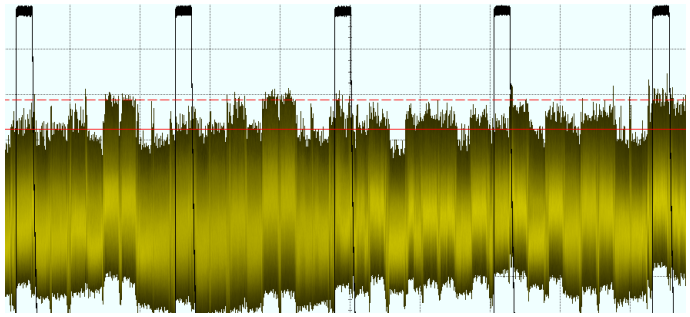

Figure 4: Waveform of SCM using the order 4 point.

#### 4.2.3 Key Extraction with Order 8

Figure 5 shows the voltage of SCM with the order 8 rational point during first five ladder steps. We use a different secret-key from section 4.2.1 and show that it is possible to retrieve the secret-key using Figure 2 and Table 1. We set black colored trigger for overall ECD calculations, line 12 and 13 in Alg. 4.

For the first waveform, the voltage for $X_{\overline{R}}$ and $Z_{\overline{R}}$ are high. It is the $Case$ C and for MSB behavior. After this waveform, we retrieve the secret-key in accordance with the following: For the ECA and the ECD waveforms, when we classify both of a $X_{\overline{R}}$ and $Z_{\overline{R}}$ waveform as high, it is $Case$ C and the current bit is different from the previous bit. On the other hand, when the degree of voltage of a $X_{\overline{R}}$ and $Z_{\overline{R}}$ are different, the current bit is the same as previous bit. According to the above procedure, we obtain the Table 3 which shows the trace of $X_{\overline{R}}$, $Z_{\overline{R}}$, $Case$, state, and secret-key bits.

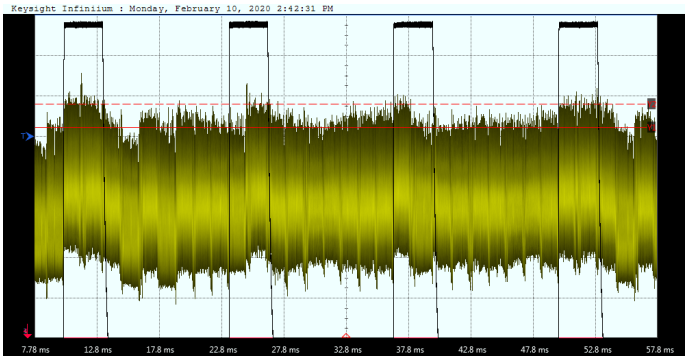


Figure 5: Waveform of SCM using the order 8 point.

Table 3: Status and secret-key in each loop with the order 8 point

| Loop | 1st | 2nd | 3rd | 4th |
|---|---|---|---|---|
| $X_{\overline{R}}$ | $High$ | $Low$ | $High$ | $High$ |
| $Z_{\overline{R}}$ | $High$ | $High$ | $Low$ | $High$ |
| $Case$ | $C$ | $B$ | $A$ | $C$ |
| State | $[\overline{2Q}, \overline{Q'}]$ | $[\overline{4Q}, \overline{Q'}]$ | $[\mathcal{O}, \overline{Q'}]$ | $[\overline{4Q}, \overline{Q'}]$ |
| $s_i$ | 1 | 1 | 1 | 0 |

### 4.2.4 Pattern Recognition of Each *Case*s

Next, we show that there exist differences in power consumption models of each *Case*. We focus on the power consumption during each ladder steps described in Alg. 4 by raising analog pins. Figure 6 shows the one SCM operation with 256 ladder steps using the order 8 rational point. Red colored trigger represents the one ladder step. We conduct the same experiment using the order 4 rational points. Figure 7 and 8 show the power consumption models using the order 4 and 8 points respectively. When we make a model of power consumption, we choose a secret-key intentionally so that we have to correlate the power with each *Case*s based on the XOR value of the secret-key. From these figures, we can classify the ladder steps into each *Case*s and retrieve the secret-key by using correlation analysis, pattern matching, and machine learning.

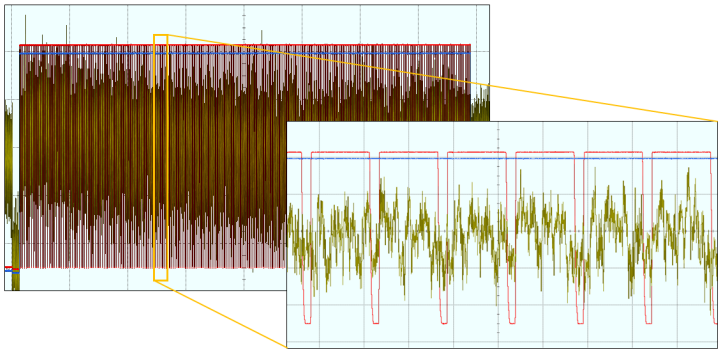

Figure 6: Overall and the part of the power consumption waveform with an order 8 point.

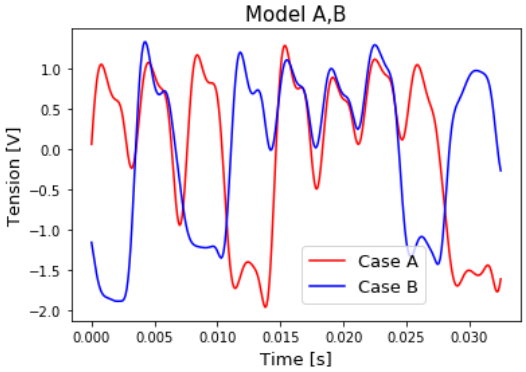


Figure 7: Two models in each *Case* with the order 4 point.

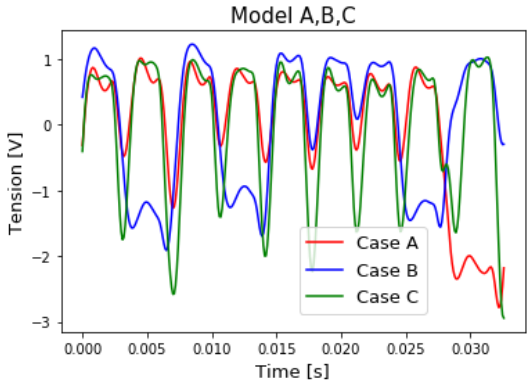


Figure 8: Three models in each *Case* with the order 8 point.

### 4.3 A consideration concerning countermeasures

Though the proposed pattern recognition technique works more powerfully in the sense that an attacker can automatically retrieve the secret-key from a waveform, there are several techniques available as countermeasures. As one of the straightforward ways is to build a blacklist by listing up every corresponding rational point since the number of such available points is relatively small. Another way is to check the input and the output of SCM calculation whether the points are on the specified curve or not. It works effectively against invalid curve attacks. Furthermore, the cofactor multiplication technique is considered to be effective against the proposed attack. The technique is proposed by Smart in [21] and the approach is as follows. First, we generate a temporary rational $P$ point randomly. After that, we adopt $[h]P$ where $h$ is cofactor as a secret-key if $[h]P$ is not a point at infinity, else start over from generating a rational point once again. Then, we can detect the error point as the output of SCM calculation is sure to be a point at infinity when an attacker input a low order rational point maliciously.

## 5 Conclusion

In this work, we have focused on Curve25519 with Montgomery ladder implementation using cswap function. Moreover, we have shown that attacking this implementation using low order rational points is possible with power consumption analysis on Arduino Uno. Injecting points of order 8 and order 4 of the twist curve are highly dangerous because it is possible to retrieve the secret-key from it entirely. It is noted that the order 8 points appear normal order points, and the order 4 points of the twist are not on the Curve25519. We also introduced the pattern recognition techniques for SCA

and show that each *Case*s are distinguished into different patterns. When we design a cryptosystem based on Curve25519, it is important to consider this kind of attack using low order points including the twist. We can avoid our proposed method with some countermeasures: blacklist, checking on the curve, and cofactor multiplication. As future work, we are planning to verify the safety of Curve448 which does not have order 8 points against the chosen-ciphertext attack.

## 6 Acknowledgment

This work is partially supported by a JSPS KAKENHI Challenging Research (Pioneering) 19H05579.

## References

[1] V. S. Miller, "Use of Elliptic Curves in Cryptography", CRYPTO '85, LNCS, vol. 218, pp. 417–426, Springer, Berlin, Heidelbelg, 1985.

[2] N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of computation, 48(177):203–209, 1987.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, 21(2):120–126, 1978.

[4] BlueKrypt Cryptographic KeyLength Recommendation, `https://www.keylength.com/en/4/`, Accessed: Jan. 22, 2020.

[5] D. J. Bernstein, "Curve25519: New Diffie-Hellman Speed Records", PKC 2006, LNCS, vol. 3985, pp. 207–228, Springer, Berlin, Heidelbelg, 2006.

[6] OpenSSH Specifications, `https://www.openssh.com/specs.html`, Accessed: Jan. 22, 2020.

[7] OpenSSL Cryptography and SSL/TLS Toolkit, `https://www.openssl.org/docs/manmaster/man7/Ed25519.html`, Accessed: Jan. 22, 2020.

[8] J. M. Pollard, "Monte Carlo Methods for Index Computation (mod p)", Mathematics of computation, 32(143):918–924, 1978.

[9] C. H. Lim and P. J. Lee, "A Key Recovery Attack on Discrete Log-based Schemes Using a Prime Order Subgroup", CRYPTO '97, LNCS, vol. 1294, pp. 249–263, Springer, Berlin, Heidelbelg, 1997.

[10] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", CRYPTO '96, LNCS, vol. 1109, pp. 104–113, Springer, Berlin, Heidelbelg, 1996.

[11] D. Genkin, L. Valenta, and Y. Yarom, "May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519", Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 845–858, 2017.

[12] Y. Uetake, A. Sanada, T. Kusaka, Y. Nogami, L. Weissbart, and S. Duquesne, "Side-Channel Attack using Order 4 Element against Curve25519 on ATmega328P", 2018 International Symposium on Information Theory and Its Applications (ISITA), pp. 618–622, IEEE, 2018.

[13] P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization", Mathematics of computation, 48(177):243–264, 1987.

[14] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", CRYPTO '99, LNCS, vol. 1666, pp. 388–397, Springer, Berlin, Heidelbelg, 1999.

[15] D. J. Bernstein and T. Lange, "Montgomery Curves and The Montgomery Ladder", IACR Cryptology ePrint Archive, 2017:293, 2017.

[16] "Elliptic Curves for Security, `https://tools.ietf.org/html/rfc7748`, Accessed: Jan. 22, 2020.

[17] Arduino Uno Rev3, `https://store.arduino.cc/usa/arduino-uno-rev3`, Accessed: Nov. 10, 2019.

[18] Y. Hashimoto, M. A.-A. Khandaker, Y. Kodera, T. Park, T. Kusaka, H. Kim, and Y. Nogami, "An Implementation of ECC with Twisted Montgomery Curve over 32nd Degree Tower Field on Arduino Uno", International Journal of Networking and Computing, 8(2):341–350, 2018.

[19] Y. Romailler and S. Pelissier, "Practical fault attack against the Ed25519 and EdDSA signature schemes", 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 17–24, IEEE, 2017.

[20] Arduino Cryptography Library, `https://rweather.github.io/arduinolibs/crypto.html`, Accessed: Dec. 30, 2019.

[21] N. P. Smart, "An Analysis of Goubin's Refined Power Analysis Attack", CHES 2003, LNCS, vol. 2779, pp. 281–290, Springer, Berlin, Heidelbelg, 2003.

# 7 Appendix

Tables 4, 5, and 6 show the parameters of Curve25519, order 4 rational point concerning Curve25519, and an order 8 rational point, respectively. Figures 9 and 10 show the result of pattern recognition using an order 4 and an 8 rational point without averaging.

Table 4: Parameters of Curve25519

| Curve25519 | |
|---|---|
| $p$ (prime number) | $2^{255} - 19$ |
| Group order $\#E_{25519}$ | $2^{255} + 221938542218978828286815502327069187944$ |
| cofactor $h$ | 8 |

Table 5: Parameters of the order 4 rational point on the Curve and Quadratic Twist

| Order 4 rational point $\overline{P} = (X : Z)$ | | |
|---|---|---|
| On the Curve | $X$ | 1 |
| | $Z$ | 1 |
| On the Quadratic Twist | $X$ | -1 |
| | $Z$ | 1 |

Table 6: Parameters of the order 8 rational point on the Curve

| Order 8 rational point $\overline{Q} = (X : Z)$ | |
|---|---|
| $X$ | 31740719336846463935661295117418533467147061622493166019063263804243205893678 |
| $Z$ | 41737339704642262903321258117524176596849662212122228668073959407940653183394 |

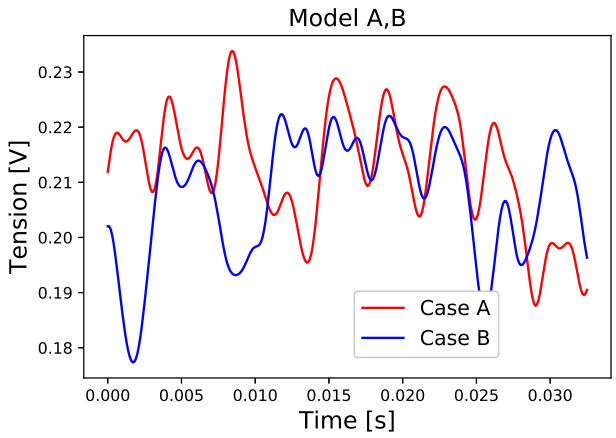


Figure 9: Two models in each *Case* with the order 4 point without averaging.

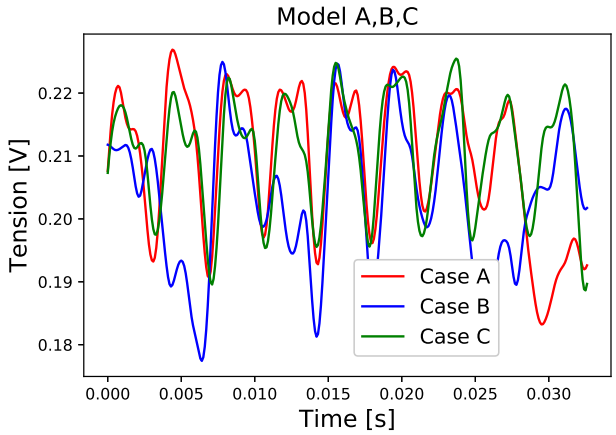


Figure 10: Three models in each *Case* with the order 8 point without averaging.