Delft University of Technology

# A Side-Channel Attack Using Order 8 Rational Points against Curve25519 on an 8-Bit Microcontroller

Uetake, Yoshinori; Yoshimoto, Keiji; Kodera, Yuta; Weissbart, Leo; Kusaka, Takuya; Nogami, Yasuyuki

**DOI**
10.1109/CANDAR.2019.00037

**Publication date**
2019

**Document Version**
Final published version

**Published in**
Proceedings - 2019 7th International Symposium on Computing and Networking, CANDAR 2019

**Citation (APA)**
Uetake, Y., Yoshimoto, K., Kodera, Y., Weissbart, L., Kusaka, T., & Nogami, Y. (2019). A Side-Channel Attack Using Order 8 Rational Points against Curve25519 on an 8-Bit Microcontroller. In *Proceedings - 2019 7th International Symposium on Computing and Networking, CANDAR 2019* (pp. 225-231). Article 8958444 IEEE. https://doi.org/10.1109/CANDAR.2019.00037

**Important note**
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

**Copyright**
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

**Takedown policy**
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

*This work is downloaded from Delft University of Technology.*
*For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.*

# A Side-Channel Attack using Order 8 Rational Points against Curve25519 on an 8-Bit Microcontroller

1st Yoshinori Uetake
*Graduate School of Natural Science and Technology, Okayama University*
Okayama, Japan
yoshinori.uetake@s.okayama-u.ac.jp

2nd Keiji Yoshimoto
*Department of Electrical and Communication Enjineering, Okayama University*
Okayama, Japan
keiji_yoshimoto@s.okayama-u.ac.jp

3rd Yuta Kodera
*Graduate School of Natural Science and Technology, Okayama University*
Okayama, Japan
yuta.kodera@s.okayama-u.ac.jp

4th Léo Weissbart
*Delft University of Technology, and Digital Security Group, Radboud University*
The Netherlands
l.weissbart@cs.ru.nl

5th Takuya Kusaka
*Graduate School of Natural Science and Technology, Okayama University*
Okayama, Japan
kusaka-t@okayama-u.ac.jp

6th Yasuyuki Nogami
*Graduate School of Natural Science and Technology, Okayama University*
Okayama, Japan
yasuyuki.nogami@okayama-u.ac.jp

***Abstract*—Among the increasing evolution of IoT devices, practical applications need reliable secure protocols to communicate with each other. A major issue for modern cryptosystems is an implementation of secure and trustworthy mechanisms to rely on. A side-channel attack against these cryptosystems may overturn the guarantee of security against conventional cyber-attacks. Elliptic curve cryptography is public-key cryptography based on elliptic curves, and one of the well-known curves is Curve25519 which is used for TLS protocols as a recommended curve. This curve is mainly implemented on limited resource devices such as microcontrollers. However, this curve poses a weakness for low-order points during a Diffie-Hellman key exchange is employed. This research demonstrates possible exploitation of a threat of order 8 rational points of Curve25519 and shows results of the side-channel attacks using order 8 rational points on an embedded system. The results indicate the order 8 rational points might be applied to key extraction as attacker sides.**

***Index Terms*—order 8 rational point, side-channel attack, Curve25519, microcontroller**

## I. Introduction

In the IoT (Internet of Things) era, many devices are connected to the Internet, and many application services are provided. A large number of IoT devices that surround us are linked to each other on the network and thus, reliable communication technology is required to transmit secret information over the network. Cryptography is used to protect information in the most cases, on the other hand, there exist many reports which try to break cryptography or eavesdrop the secret information over the network at the same time.

Conversely, in the IoT era, we need to consider physical attacks along with the above cyber-attacks. Moreover, in embedded hardware architectures, the resource is constrained, hence designing an enough secure cryptosystem within the limitations is necessary. There is some efficient algorithm that allows us to implement cryptography as software on resource constraint devices. However, sometimes they lack security from the aspect of hardware implementation. Side-channel attack (SCA) introduced in [1] is the method of exploiting information leakage of cryptographic modules to extract secret information as *side-channels*. As the physical side-channels, timing, data dependency, power, and electromagnetic emanation are well-known.

In this work, we focus on power analysis attacks that take out significant information by analyzing power consumption from a device processing some cryptographic data and algorithm. As the target cryptography, we work with elliptic curve cryptography (ECC) whose security depends on the difficulty of the elliptic curve discrete logarithm problem. The ECC has been introduced in 1985 by Koblitz [2] and Miller [3] and is nowadays a promising alternative to overly used public-key cryptography such as RSA [4] because it can offer the same security level with a shorter public key. Internet Engineering Task Force (IETF) has adopted the elliptic curve Curve25519 proposed by Berstein in 2006 [5] as one of the next generation curves for the widely used cryptography standard on the Internet TLS [6] because of its efficiency and security for ECC. While this cryptography can be considered trustful, it is not exempted of the threat and one of them is order 4 rational points, has been pointed out by Genkin, Valenta, and Yarom [7]. This attack is a side-channel attack taking advantage of the few possibilities of intermediates calculations during scalar multiplication (SCM) for ECC.

As another threat to this kind of cryptosystems, the authors introduce the SCA scheme based on the features of order 8 rational points in this research. The order 8 rational points attack could be the same principle as the order 4 attacks although

2379-1896/19/$31.00 ©2019 IEEE
DOI 10.1109/CANDAR.2019.00037

there have not been reported that confirm the vulnerability of side-channel attacks using order 8 rational points on embedded devices. This research reveals the threat of order 8 rational points of Curve25519 in an ECC secure algorithm against a side-channel attack. After a brief introduction to mathematical fundamentals used in ECC, this paper exposes the principle of the order 8 rational points side-channel attack, then gives the results of such attacks on an ATmega 8-bit microcontroller and presents a consideration for applying pattern recognition to the attack.

## II. Preliminaries

This section introduces some fundamentals such as elliptic curve, Curve25519, Montgomery curve, and Montgomery ladder.

### A. Elliptic Curve

For a prime number $p$, let $\mathbb{F}_p$ be a prime field. An elliptic curve $E$ over $\mathbb{F}_p$ is defined as the simplified Weierstrass form [8] as below,

$$E: \ y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_p, \tag{1}$$

where $a, b \in \mathbb{F}_p$ such that $4a^3 + 27b^2 \neq 0$. A pair of coordinates $x$ and $y$ which satisfy Eq. (1) on affine coordinates is called a rational point including the point at infinity denoted by $\mathcal{O}$. The number of rational points in this group is called *group order* and there are two types of operation for the set of rational points; elliptic curve addition (ECA) and elliptic curve doubling (ECD). By combining these operations, SCM is defined so that one can compute the resultant rational points for a given scalar efficiently. Typically, an ECC using a general type of elliptic curve for cryptographic systems requires complicated arithmetic operations. Indeed, the computations for ECA and ECD involve inversions which is a heavy operation over the definition field. In contrast, there is a particular type of elliptic curve, which allows us to omit the inverse operation. In the following section, we introduce Montgomery curve as such an efficient elliptic curve for the ECC.

### B. Montgomery Curve

Montgomery curves are introduced in [9] and it is represented as follows:

$$E : By^2 = x^3 + Ax^2 + x,$$

where $A, B \in \mathbb{F}_p$ and $B(A^2 - 4) \neq 0 \pmod{p}$.

By using projective coordinates, although a rational point $P = (x, y)$ on Montgomery curve is expressed by coordinates $P = (X : Y : Z)$ where $x = X/Z$ for $Z \neq 0$, we can omit the $Y$-coordinates when the SCM is carried out. Therefore, $P$ is represented as $\overline{P} = (X : Z)$ throughout the paper for the sake of convenience.

- ECA of Montgomery Curve

For two different elements, $\overline{P} = (X_i : Z_i)$ and $\overline{Q} = (X_j : Z_j)$, define their addition $\overline{R} = \overline{P} + \overline{Q}$ that have coordinates $\overline{R} = (X_R : Z_R)$. Also prepare the point $\overline{U} = \overline{P} - \overline{Q}$, which is $\overline{U} = (X_{i-j} : Z_{i-j})$. Then, $\overline{R}$ is calculated as follows:

$$\begin{aligned} X_R &= Z_{i-j}[(X_i - Z_i)(X_j + Z_j) + (X_i + Z_i)(X_j - Z_j)]^2, \\ Z_R &= X_{i-j}[(X_i - Z_i)(X_j + Z_j) - (X_i + Z_i)(X_j - Z_j)]^2. \end{aligned}$$

As the above equations show, the pre-computation $\overline{U}$ enables us to process the addition efficiently. In addition, the $Y$-coordinates in the ECA with projective coordinates can ignore by combining the Montgomery ladder algorithm described in II-D. Therefore, we treat the affine cordinates points $(x, y)$ and $(x, -y)$ as the same point in the projective coordinates representation in what follows.

- ECD of Montgomery Curve

For a $\overline{P} = (X_i : Z_i)$, let us consider the doubling operation $\overline{R} = \overline{P} + \overline{P}$, where $\overline{R} = (X_R : Z_R)$ is defined as follows:

$$\begin{aligned} X_R &= (X_i + Z_i)^2 (X_i - Z_i)^2, \\ T &= (X_i + Z_i)^2 - (X_i - Z_i)^2, \\ Z_R &= T \cdot [(X_i - Z_i)^2 + A_{24} \cdot T], \end{aligned} \tag{2}$$

where $A_{24}$ denotes a precomputed constant value $\frac{A+2}{4}$.

Since ECA and ECD do not involve any inverse operations which are time-consuming operations much lager than multiplications, Montgomery curve allows more efficient imoplementation.

### C. Curve25519

Curve25519 is an elliptic curve introduced by Bernstein [5] in 2006. Let $p$ be the fixed prime number $2^{255} - 19$, then, Curve25519 over $\mathbb{F}_p$ is given as follows:

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

Curve25519 is used for Elliptic Curve Diffie-Hellman (ECDH) protocols which are adopted in TLS with offering the 128-bit security with 32-byte secret key. Since the definition field is given by $p = 2^{255} - 19$, we have $2^{255} \equiv 19 = 2^4 + 2^1 + 2^0$ and the modulo operations required in multiplication are carried out by some shift operations and additions. Moreover, Montgomery ladder which is described in the following section also contributes to its efficiency. Considering the above features, Curve25519 have been paid much attention as practical elliptic curve cryptosystem.

However, the readers need to remember that there exist low-order rational points in affine coordinates as reported in [7]. More precisely, the rational points with affine coordinates $(0, 0)$ and $(1, \pm\sqrt{486664})$ are known to have the order 2 and 4, respectively.

### D. Montgomery Ladder

ECDH based cryptography relies on SCM over the elliptic curve to generate a session key. During this operation, there potentially exist weaknesses which allow an attacker to retrieve the secret key via side-channel information.

To address the weaknesses, Montgomery ladder algorithm [9], [10] is adopted as an side-channel attack (SCA) resistant algorithm for handling SCM without leaking information.

Montgomery ladder algorithm is shown in Alg. 1. If a conditional branching of SCM algorithm is driven by secret scalar $s$ and the side-channel data such as timing or power are observed regarding the branches, an attacker could obtain secret data. In contrast, Montgomery ladder always processes addition and doubling in all branches, thus any differences would not occur and we say that it has durability for SCA [11].

**Algorithm 1** Montgomery Ladder

```
Input: $\overline{P}, s = (s_{n-1}, s_{n-2} \ldots s_1, s_0)_2$
Output: $\overline{T_1} = [s]\overline{P}$
$\overline{T_1} \leftarrow \mathcal{O}$
$\overline{T_2} \leftarrow \overline{P}$
for $i = n - 1$ to $0$ do
    if $s_i = 1$ then
        $\overline{T_1} \leftarrow \overline{T_1} + \overline{T_2}$
        $\overline{T_2} \leftarrow 2\overline{T_2}$
    else
        $\overline{T_2} \leftarrow \overline{T_1} + \overline{T_2}$
        $\overline{T_1} \leftarrow 2\overline{T_1}$
    end if
end for
return $\overline{T_1}$
```

In the rest of this paper, a loop of the FOR statement of Montgomery ladder algorithm is reffered to as a *ladder step*.

## III. Attacking Method

This section describes the scenario of SCA against Curve25519 implemented on a microcontroller using order 8 rational points. This is our critical proposal that points of order 8 pose a noteworthy threat on Curve25519.

The authors have reported a related work about SCA using order 4 rational points in [12]. Although the attacks using order 4 points have been reported, the threat of the attack that points of order 8 can be used as a chosen-ciphertext still has not been enough considered. Even if countermeasures are introduced for order 4 rational points, it will be a serious problem, when other specific ciphertexts are chosen and used. In this research, the authors confirm order 8 rational points can be used for the SCA to extract a secret key and point out its vulnerability.

Let $\overline{P} = (X = \alpha : Z = \beta)$ be a rational point of order 8 and consider that $\overline{P}$ is used as a chose-ciphertext in what follows, where $\alpha \neq \beta$ and both $\alpha$ and $\beta$ are not 0. It is noteworthy that though the order 4 elements have the same values in both $X$ and $Z$-coordinates, the order 8 elements pretend to be regular rational points as different values of both coordinates. Therefore, it is not difficult to point out whether a rational point belongs to the order 4 group by evaluating the coordinates of the element. On the other hand, it is not a reasonable choice to evaluate the order of all elements to know whether the element has order 8. Thus, we focus on explaining how to employ the feature of rational points of order 8 into the SCA hereafter.

Since the order of $\overline{P}$ is 8, the doubling for $\overline{P}$ and $\overline{2P}$ have to result in the rational points of order 4 and 2, respectively. Besides, recall that the inverse of $(x, y)$ is given by $(x, -y)$ in affine coordinates and we can omit the $Y$-coordinate in projective coordinates. Hence, we have $\overline{5P} = \overline{3P}$, $\overline{6P} = \overline{2P}$, $\overline{7P} = \overline{P}$. Following the later description, the important thing for our attacks is that the value is whether zero or non-zero, it doesn't matter what the exact number is. Consequently, $\overline{P}$ and $\overline{3P}$ are the same in that both are points with projective coordinates that can be represented with two different large positive integers, for instance, $\overline{P} = (\alpha; \beta), \overline{3P} = (\nu; \upsilon)$. Thus, we can consider $\overline{P}$ and $\overline{3P}$ are the same set. We define this set as $\overline{P'}$ and point at infinity $\mathcal{O}$ is defined as $\mathcal{O} = (X \neq 0 : Z = 0)$. The relations between these points are obtained with every combination of $\overline{P}$ through addition and doubling.

As a result, during SCM with Montgomery ladder, the outcomes of every operation are within 4 elements including point at infinity:

$$\overline{P'} = \{\overline{P}, \overline{3P}\},\ \overline{2P},\ \overline{4P}, \text{and } \mathcal{O}.$$

In Fig. 1, each state represents the pair of value $[\overline{T_1}, \overline{T_2}]$ which is indicated in Alg. 1. The results of Montgomery ladder are divided into six states when $\overline{P}$ is used as a base point for attacks. The arrow symbols in the figure show the transition of these states. In the *Case : Key*, *Case* indicates three groups of *Case A* to *C* which give us information to recover a secret key and *Key* means a bit of the current secret key. For example, the sequence from $[\mathcal{O}, \overline{P'}]$ to $[\overline{P'}, \overline{2P}]$ belongs to *Case C*, and we have the current secret key bit is 1.

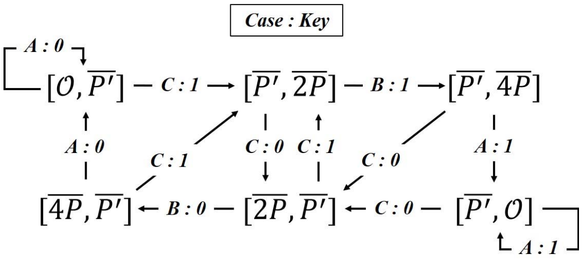

Fig. 1. State transition diagram of SCM using order 8 rational points

In each case, Eq. (2) becomes,

- *Case A*

$$\begin{aligned} X_R &= (0 + \theta)^2 \cdot (0 - \theta)^2 \equiv \omega, \\ T &= (0 + \theta)^2 - (0 - \theta)^2 = 0, \\ Z_R &= 0 \cdot [(0 - \theta)^2 + A_{24} \cdot 0] = 0, \end{aligned} \tag{4}$$

- *Case B*

$$\begin{aligned} X_R &= (\theta + \theta)^2 \cdot (\theta - \theta)^2 = 0, \\ T &= (\theta + \theta)^2 - (\theta - \theta)^2 \equiv \omega, \\ Z_R &= \omega \cdot [(\theta - \theta)^2 + A_{24} \cdot \omega] \equiv \omega, \end{aligned} \tag{5}$$

- *Case C*

$$\begin{aligned} X_R &= (\theta+\lambda)^2 \cdot (\theta-\lambda)^2 \equiv \omega, \\ T &= (\theta+\lambda)^2 - (\theta-\lambda)^2 \equiv \omega, \\ Z_R &= \omega \cdot [(\theta-\lambda)^2 + A_{24} \cdot \omega] \equiv \omega, \end{aligned} \tag{6}$$

where $\theta$, $\lambda$, and $\omega$ different large positive integers that generate elements such as $\overline{P'}$ for convenience.

When the value 0 is used for multiplication in $X_R$ or $Z_R$, the power needed to compute the result is quite small compared to a multiplication involving two large integers. By observing the differences in voltage throughout the multiplication, it is possible to determine whether the zero calculation has been performed. Additionally, the *Case* can be identified from these differences. For instance, *Case A* is non-zero calculation in $X_R$, conversely, the multiplication of $Z_R$ is zero which is considered low power consumption. Thus, if only the power consumption in the multiplication of $Z_R$ is small, it can be specified to be *Case A*. The relationship between each *Case* and the power consumption is defined in TABLE I. As a result, focusing on the multiplication of $X_R$ and $Z_R$ and using Fig. 1 and TABLE I, we can retrieve the secret key from the transition of the states.

TABLE I
RELATIONS BETWEEN *Case*S AND POWER CONSUMPTION

| | *Case A* | *Case B* | *Case C* |
|---|---|---|---|
| $X_R$ | *High* | *Low* | *High* |
| $Z_R$ | *Low* | *High* | *High* |

# IV. EXPERIMENT

## A. Computation Environment

This experiment has been performed using an Agilent Technologies DSOS104A oscilloscope synchronized with the execution of the SCM through a provoked trigger signal. Since it is expected that the practical use of ECC with IoT devices will further expand in the future, we choose Arduino UNO for the target. Simultaneously, implementations and evaluations of ECC for Arduino have been extensively reported in [13], [14], for example.

The authors use $\mu NaCl$ [15], the networking and cryptography library for microcontrollers, for implementing curve25519 with Montgomery ladder algorithm over the prime field $2^{255} - 19$. The base point $\overline{P}$ used for SCM is an order 8 rational point and the secret key $s$ is a randomly initialized by 256-bit size integer. The readers can refer to further details of $\overline{P}$ and $s$ in the Appendix. TABLE II shows the specifications of Arduino UNO.

TABLE II
ARDUINO UNO SPECIFICATIONS

| | |
|---|---|
| Microcontroller | ATmega328P |
| Flash Memory | 32K bytes |
| SRAM | 2K bytes |
| Clook Speed | 16 MHz |
| Language | Arduino functions based on C/C++ |
| Compiler | avr-gcc |

## B. Experimental Results

This section introduces the experimental results of the attack based on Sec. III scenario. Furthermore, we conduct another experiment which uses a standard rational point as a base point used to compute SCM to compare these results and to make the threat of the order 8 rational point much clear.

The point of order 8 is initially chosen so that the coordinates are made up of large integers because if the base point has small coordinates, the first a few loops of Montgomery ladder do not show sufficient differences in power consumption between zero and non-zero multiplications. To make the lecture of the trace easier, a signal is raised with an analog pin during the target multiplications which are $X_R$ and $Z_R$ calculations of Eq. (4) to Eq. (6). As the complete SCM is about 6.5 seconds long, we focus on only the first six bits calculation in this section, however, it is noted that the same result is confirmed for the whole bits of the secret key. In the next paragraph, the result of the attack is represented in Fig. 2.

Since a single trace is too noisy to observe, we carry out the same SCM 50 times and takes the average of the traces so that the differences between zero and non-zero multiplications can be visible more clearly. To measure the power consumption, a 50 $\Omega$ resistor is inserted between the GND pin of the microcontroller and the ground. Then, we observe the voltage across the resistor with a passive probe. The larger the power consumption, the larger the amplitude of the voltage waveform measured on the oscilloscope. Conversely, the amplitude is smaller in the case of low power consumption.

During the marked sets of multiplication, the first trigger signal indicates $X_R$ calculations, then the next signal shows $Z_R$ calculations of the above equations, respectively. First, let us focus on the part of $X_R$. We can see for the first loop that the power consumption is high and on the next loop, we can see a lower power consumption. Since the first invocation of multiplication is non-zero multiplication, the energy to set the final value is large. It means that the energy is greater than a zero multiplication. In contrast, the second invocation of the function, we have a zero multiplication, therefore it is considered that energy is not so much large compared to a non-zero multiplication.

Second, we focus on the $Z_R$ computations to determine the *Case*s on each loop. In the $Z_R$, the differences of waveforms can be clearly seen than in the $X_R$, the power consumption of the fifth loop is exactly low compared to the others.

From the above observations, we can recover the secret key using Fig. 1 and TABLE I. The status of power consumption in $X_R$ and $Z_R$ of each loop and the *Case*s determined from TABLE I are shown in TABLE III. TABLE III also shows the current state within the transition diagram and secret key bits $s_i$ which we try to obtain. Initially, the state is $[\mathcal{O}, \overline{P'}]$ and the *Case* is *C*, therefore the key bit is 1 and the next state is $[\overline{P'}, \overline{2P}]$. The second loop is *Case B*, thus the next key bit is also 1. Then, third and fourth loops are as same as first and second loops. The fifth *Case* is *A* and the current state is $[\overline{4P}, \overline{P'}]$. Consequently, we can decide its key value is 0 in the same way as previous processes. These values are ultimately the same as the secret key $s$.

TABLE III
STATUS AND SECRET KEY IN EACH LOOP

| Loop | 1st | 2nd | 3rd | 4th | 5th | 6th |
|---|---|---|---|---|---|---|
| $X_R$ | *High* | *Low* | *High* | *Low* | *High* | *High* |
| $Z_R$ | *High* | *High* | *High* | *High* | *Low* | *High* |
| *Case* | *C* | *B* | *C* | *B* | *A* | *C* |
| State | $[\mathcal{O}, \overline{P'}]$ | $[\overline{P'}, \overline{2P}]$ | $[\overline{P'}, \overline{4P}]$ | $[\overline{2P}, \overline{P'}]$ | $[\overline{4P}, \overline{P'}]$ | $[\mathcal{O}, \overline{P'}]$ |
| $s_i$ | 1 | 1 | 0 | 0 | 0 | 1 |

Fig. 3 shows a power trace using a standard rational point which is used to compare the chosen-ciphertext attack of the order 8 rational point and general plaintext attack with a standard rational point (see Appendix). This element is on the Curve25519, however, the order is not small such as low-order points. The power traces are irregular, and there are no relations between waveforms and key values.

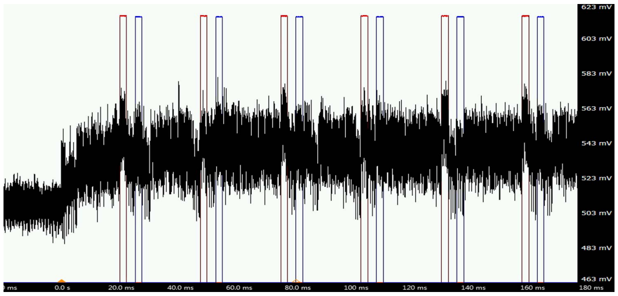

Fig. 2. Power trace using an order 8 rational point

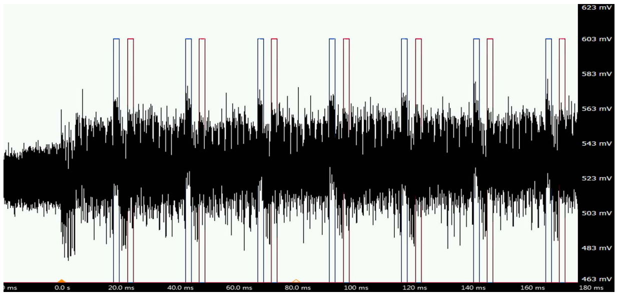

Fig. 3. Power trace using a standard rational point

### C. Pattern Recognition for SCA of order 8 rational points

There have been many studies about machine learning [16] and template attacks [17] which are two popular side-channel attacks to evaluate the side-channel resistance of cryptography. For the further step, we tried to introduce pattern recognition [18] to our order 8 attack. As a result, it was found that the secret key can be analyzed more rapidly by applying pattern recognition. In the method of IV-B, since the differences in power consumption is confirmed manually, it has taken a great deal of time to analyze secret information. However, the analyses are completed within a second by using that approach.

In our experiments, the obtained measure contains the 256 ladder steps of the Montgomery ladder algorithm. The attacks introducing pattern recognition are divided into two phases: training phase and test phase. In the training phase consists of classifying the ladder steps in the three patterns according to TABLE I when attacked with an order 8 rational point which secret key is known. From the classified ladder step traces, three models are created by averaging the traces of each *Case*. The test phase consists of comparing ladder steps from an unknown attack with the obtained models and decide which one fits the most for each ladder step. It means that another measure is taken from another secret key. By cutting the signal in ladder steps and comparing each ladder step with the three models using correlation, it is possible to determine the most possible *Case* for every ladder step by applying correlation. Finally, we can retrieve the secret key by applying the state transition shown in Fig. 1.

Fig. 4 illustrates the 256 ladder steps of the Montgomery ladder algorithm used with the 256-bit secret key and Fig. 5 shows the three models in each *Case*. From the training phase, it is clear that the three obtained models are different and thus identifiable as shown. If this phase was not correct because the measure is not effective or the secret key is wrong, the three models would be the same because of the averaging. The models of the *Case A*, *B*, and *C* obtained from the training phase, to classify the ladder steps of the test set into the corrects pattern model is almost 100 % for a measure which is taken in the same conditions as the training set. The experiments have been made with different secret keys and on different Arduino UNO from the batch of manufacture to prove those results.

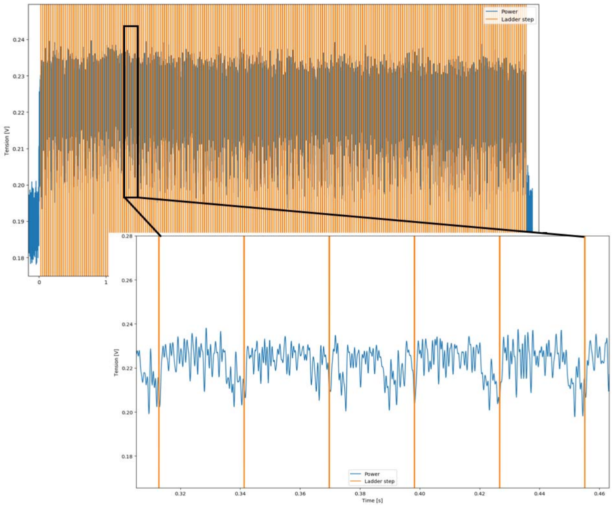

Fig. 4. Waveforms of power consumption in each ladder step

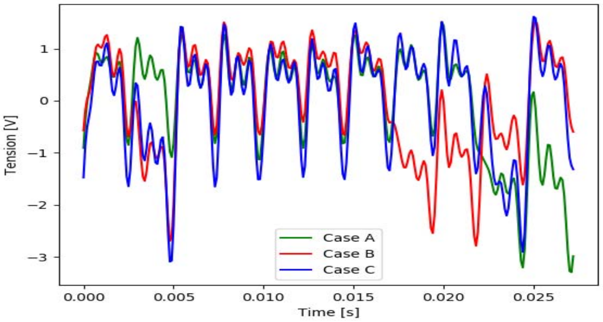

Fig. 5. Three models in each *Case*

## V. Conclusion

In our work, we have shown that attacking Curve25519 with Montgomery implementation using an order $8$ rational point is possible with analyzing power consumption on Arduino UNO. Injecting a point of order $8$ as a base point of Montgomery ladder algorithm for Curve25519 is highly dangerous because it is possible to extract the ECC secret key from it entirely. This makes every secure protocol using Curve25519 potentially vulnerable to SCA. We also introduced the pattern recognition techniques for SCA, it indicates that attackers potentially have advanced physical attack methods. When designing a cryptosystem based on ECC and Curve 25519, it is important to consider implementing countermeasures to this kind of attack. It may be the easiest way to prohibit performing order $8$ rational points for the input, similarly, also in case of order $4$ rational points should be constrained. We are planning to introduce machine learning into this side-channel attack to confirm the impact of AI (Artificial Intelligence) on cryptography. Furthermore, the authors would like to verify the safety of Curve448 [19] against chosen-ciphertext attack as future work.

## Acknowledgement

This work was partially supported by the JSPS KAKENHI Challenging Research (Pioneering) 19H05579.

## Apendix

TABLE IV to TABLE VI shows the parameters of Curve25519 and experiments.

TABLE IV
Parameters of Curve25519

| Curve25519 | |
|---|---|
| $p$ (prime number) | $2^{255} - 19$ |
| $A$ | 486662 |
| Group order $\#E_{25519}$ | $2^{255}$ + 221938542218978828286815502327069187944 |
| Order of the base point | $2^{252}$ + 27742317777372353535851937790883648493 |

TABLE V
Parameters of the order 8 point

| Order 8 rational point $\overline{P} = (X : Z)$, secret key $s$ | |
|---|---|
| $X$ | 31740719336846463935661295117418533467147061622493166019063263804243205893678 |
| $Z$ | 41737339704642262903321258117524176596849662212122228668073959407940653183394 |
| $s$ | 89983078833945199161666674335136204525775460278787651032884970583523388749624 |

TABLE VI
Parameters of the standard point

| Standard point $\overline{P} = (X : Z)$, secret key $s$ | |
|---|---|
| $X$ | 67138413771517688612956901188372058122069988307910720957457332373321210586 |
| $Z$ | 7459823752390854290328544576485784235785455425643452550828592485924578954 |
| $s$ | 89983078833945199161666674335136204525775460278787651032884970583523388749624 |

## References

[1] E. Peeters, "Side-channel cryptanalysis: A brief survey," in *Advanced DPA Theory and Practice*. Springer, 2013, pp. 11–19.

[2] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[3] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*. Springer, 1985, pp. 417–426.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[5] D. J. Bernstein, "Curve25519: new diffie-hellman speed records," in *International Workshop on Public Key Cryptography*. Springer, 2006, pp. 207–228.

[6] K. P., "Formal request from TLS WG to CFRG for new elliptic curves," 2014. [Online]. Available: http://www.ietf.org/mail-archive/web/cfrg/current/msg04655.html

[7] 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," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 845–858.

[8] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*. Cambridge university press, 1999, vol. 265.

[9] P. L. Montgomery, "Speeding the pollard and elliptic curve methods of factorization," *Mathematics of computation*, vol. 48, no. 177, pp. 243–264, 1987.

[10] D. J. Bernstein and T. Lange, "Montgomery curves and the montgomery ladder." *IACR Cryptology ePrint Archive*, vol. 2017, p. 293, 2017.

[11] M. Joye and S.-M. Yen, "The montgomery powering ladder," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2002, pp. 291–302.

[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," in *2018 International Symposium on Information Theory and Its Applications (ISITA)*. IEEE, 2018, pp. 618–622.

[13] 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*, vol. 8, no. 2, pp. 341–350, 2018.

[14] Y. Romailler and S. Pelissier, “Practical fault attack against the ed25519 and eddsa signature schemes,” in *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2017, pp. 17–24.

[15] M. Düll, B. Haase, G. Hinterwälder, M. Hutter, C. Paar, A. H. Sánchez, and P. Schwabe, “High-speed curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers,” *Designs, Codes and Cryptography*, vol. 77, no. 2-3, pp. 493–514, 2015.

[16] G. Hospodar, B. Gierlichs, E. De Mulder, I. Verbauwhede, and J. Vandewalle, “Machine learning in side-channel analysis: a first study,” *Journal of Cryptographic Engineering*, vol. 1, no. 4, p. 293, 2011.

[17] S. Chari, J. R. Rao, and P. Rohatgi, “Template attacks,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2002, pp. 13–28.

[18] C. M. Bishop, *Pattern recognition and machine learning*. springer, 2006.

[19] Y. Nir and S. Josefsson, “Curve25519 and curve448 for the internet key exchange protocol version 2 (ikev2) key agreement,” Tech. Rep., 2016.