New Operation and Problems on Elliptic curve and Their Application

Masaaki Shirase
Future University Hakodate, Hakodate, Hokkaido, Japan.

***Abstract*—In this paper, a new operation Me(P,Q) or $P \oplus Q$ and Me-scalar multiplication $P_{n,Z}$ with auxiliary Z are defined for $P,Q,Z \in E(\mathbb{F}_p)$ and $n \in \mathbb{N}$, where E is an elliptic curve over $\mathbb{F}_p$. Although $(E(\mathbb{F}_p),\oplus)$ does not form a group, it is shown that Me-scalar multiplication has properties suitable for constructing cryptosystems such as $(P_{n,Z})_{m,Z} = (P_{m,Z})_{n,Z}$. Next, the MeDLP and the MeCDH, which are Me-scalar multiplication version of the ECDLP and the ECCDH, are defined. Last, under the assumption that MeCDH is hard, cryptosystems using Me-scalar multiplication are proposed.**

I. INTRODUCTION

Elliptic curve cryptosystems (ECCs) are based on the elliptic curve discrete logarithm problem (ECDLP). In recent years, ECCs have been popular, for example, in the SSL/TLS communication, ECDHE and ECDSA, which are a key agreement and a digital signature using an elliptic curve, respectively, are used in many cases. However, if quantum computer of a sufficient number of bits would be realized, then ECCs (and RSAs) could be attacked in polynomial time. Therefore, researches on post-quantum cryptosystems (PQCs), which keep secure even if such quantum computer is realized, are thriving.

This paper proposes a new operation Me(P,Q) or $P \oplus Q$ on $E(\mathbb{F}_p)$, where $\mathbb{F}_p$ is a finite field and E is an elliptic curve over $\mathbb{F}_p$. **Me** means the **M** operation [1] for **e**lliptic curves. This paper defines Me-scalar multiplication $P_{n,Z}$ with auxiliary Z for $P,Z \in E(\mathbb{F}_p)$ and $n \in \mathbb{N}$. Although $(E(\mathbb{F}_p),\oplus)$ does not form a group because $\oplus$ does not satisfy the associative low, Me-scalar multiplication has properties that can be used to construct cryptosystems. Next, this paper defines the MeDLP and the MeCDH, which are Me-scalar multiplication version of the ECDLP and the ECCDH, respectively. Last, this paper provides a key agreement (MeDH) and a public key cryptography (MeElGamal) using Me-scalar multiplication under the assumption that the MeCDH is hard. It is not known whether the MeDLP and the MeCDH are difficult, however, the authors would like to expect them to be a member of PQCs.

II. ELLIPTIC CURVE

Let K be a field, E an elliptic curve over K, and $E(K)$ the set of K-rational points of E. Then, it is known that an operation $+$ is defined in $E(K)$ and $(E(K),+)$ forms a group [2]. Scalar multiplication $nP = P + P + \cdots + P$ is defined for $P \in E(K)$ and $n \in \mathbb{N}$.

Let K be a finite field $\mathbb{F}_p$. The elliptic curve discrete logarithm problem (ECDLP) is: given $P,Q \in E(\mathbb{F}_p)$, find $n \in \mathbb{N}$ such that $Q = nP$ if it exists. The elliptic curve computational Diffie-Hellman (ECCDH) problem is: given $P, nP, mP \in E(\mathbb{F}_p)$, compute nmP. Many ECCs are based on the hardness of ECDLP or ECCDH.

This work was supported by JSPS KAKENHI Grant Number 16K00188.

III. ME OPERATION AND ME-SCALAR MULTIPLICATION

Let p be a prime such that

$$p \equiv 3 \pmod 4 \tag{1}$$

and E an elliptic curve given by $E: y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ such that

$$\#E(\mathbb{F}_p) \text{ is odd.} \tag{2}$$

A function sign is defined as

$$\text{sign} : E(\mathbb{F}_p) \setminus \{O\} \to \{\pm 1\},\ (x_0, y_0) \mapsto \left(\frac{x_0}{p}\right),$$

where O is the point at infinity and $\left(-\right)$ is the Legendre symbol. Note that $\text{sign}(P) \cdot \text{sign}(-P) = -1$ is held from the conditions (1) and (2). The Me operation is defined as

$$\text{Me}(P,Q) = \begin{cases} P, & \text{if } P = Q \\ kP - (k-1)Q, & \text{if sign}(P-Q) = 1 \\ kQ - (k-1)P. & \text{if sign}(P-Q) = -1 \end{cases}$$

We write $P \oplus Q \coloneqq \text{Me}(P,Q)$. Then, we have the following proposition.

Proposition 1

Let $P,Q,R \in E(\mathbb{F}_p)$.

(a)	$P \oplus P = P$.	(idempotence)
(b)	$P \oplus Q = Q \oplus P$.	(commutativity)
(c)	$(P \oplus Q) + R = (P + R) \oplus (Q + R)$, $P + (Q + R) = (P + Q) \oplus (P + R)$.	(distributive)
(d)	$(P \oplus Q) \oplus R \neq P \oplus (Q \oplus R)$ in general	(anti-associative)

Due to Proposition 1-(d), $(E(\mathbb{F}_p),\oplus)$ does NOT form a group. Hence, simple repetitions of $\oplus$ has no meaning by Proposition 1-(a) because $P \oplus P \oplus \cdots \oplus P = P$. We define Me-scalar multiplication $P_{n,Z}$ for $P \in E(\mathbb{F}_p)$ and $n \in \mathbb{N}$ with auxiliary $Z \in E(\mathbb{F}_p)$ as the output of Algorithm 1.

Algorithm 1

Input : $P, Z \in E(\mathbb{F}_p)$, $n = (n_{l-1}, n_{l-2}, n_{l-3}, \ldots, n_0)_2 \in \mathbb{N}$
Output : $P_{n,Z} \in E(\mathbb{F}_p)$

1. $Y = P$
2. **for** $i = l-2$ **down to** 0
3. $\quad Y = (Z + Y) \oplus Y$
4. $\quad$**if** $n_i = 1$ **then** $Y = Y \oplus P$
5. **end for**
6. **return** Y

Note that if Step 3 is "$Y = Y \oplus Y$" without Z then Algorithm 1 is same as the left-to-right binary method. Note that $P_{n,Z}$ shoud not be defined as $(Z \oplus P) \oplus P \oplus \cdots \oplus P$ or $(Z + P) \oplus P \oplus \cdots \oplus P$ because $\oplus$ is anti-associative.

A. Property

Me-scalar multiplication has the following properties.

Theorem 2
Let $P, Q, Z \in E(\mathbb{F}_p), n, m \in \mathbb{N}$.
(a) $P_{n,Z} + Q = P + Q_{n,Z} = (P + Q)_{n,Z}$
(b) $(P_{n,Z})_{m,Z} = (P_{m,Z})_{n,Z} = P_{n,Z} + P_{m,Z} - P$
$\because$)(a) Let $[Y(P_{n,Z})]_{j,t}$ denote an intermediate value of Y of Algorithm 1 at iteration $i = j$ and step t. Then, it is easily seen that $[Y(P_{n,Z})]_{j,t} + Q = P + [Y(Q_{n,Z})]_{j,t} = Y[(P + Q)]_{j,t}$ for every j and t due to the distributive law of $\oplus$ and $+$.
(b) Due to (a). □

The property of Theorem 2-(b) is similar to $n(mP) = m(nP)$ of scalar multiplication, which is often used for ElGamal type public key cryptosystems.

B. MeDLP and MeCDH

We define Me-scalar multiplication version of the ECDLP and the ECCDH in this section. The MeDLP is naturally defined. The MeDLP is: given $P, Q, Z \in E(\mathbb{F}_p)$, find $n \in \mathbb{N}$ such that $Q = P_{n,Z}$ if it exists.

Defining the MeCDH is difficult. If the MeCDH is naturally defined then it is:

$$\text{given } P, Z, P_{n,Z}, P_{m,Z} \in E(\mathbb{F}_p), \text{ compue } (P_{n,Z})_{m,Z} \tag{3}$$

However, it is very easy to solve it because $(P_{n,Z})_{m,Z} = P_{n,Z} + P_{m,Z} - P$ due to Theorem 2-(b).Next, let consider the following.

$$\begin{gathered}\text{Given } n \in \mathbb{N} \text{ and } Z, P_{n,Z}, Q_{n,Z} \in E(\mathbb{F}_p), \\ \text{compute } (P + Q)_{n,Z}\end{gathered} \tag{4}$$

(4) is also solved. Picking up $R \in E(\mathbb{F}_p)$ at random, and computing $X = P_{n,Z} + R - R_{n,Z}$. Then, X is equal to P due to Theorem 2-(a). As well, Q is obtained. Therefore, $(P + Q)_{n,Z}$ is obtained. Hence, define the MeCDH as mixing (3) and (4):

$$\begin{gathered}\text{given a hash function } h: E(\mathbb{F}_p) \to \mathbb{N}, \text{ and given} \\ n \in \mathbb{N}, G, Z, G_{h(P),Z} + P_{n,Z}, G_{h(Q),Z} + Q_{n,Z} \in E(\mathbb{F}_p), \\ \text{compute } (G_{h(P),Z})_{h(Q),Z} + (P + Q)_{n,Z} \in E(\mathbb{F}_p).\end{gathered}$$

Proposition 3
A person knowing secret information P or Q can solve the MeCDH.
$\because$) A person knowing P can obtain $P_{h(P),Z}$ and compute the following using Theorem 2-(a) to solve the MeCDH.

$$\begin{aligned}(G_{h(Q),Z} + Q_{n,Z}) + P_{h(P),Z} &= (G_{h(Q),Z} + Q_{n,Z})_{h(P),Z} + P \\ &= (G_{h(Q),Z})_{h(P),Z} + Q_{n,Z} + P \\ &= (G_{h(P),Z})_{h(Q),Z} + (P + Q)_{n,Z}\end{aligned}$$

As well, another person knowing Q can also solve MeCDH. □

Open Problem 4
(a) Is the MeDLP hard?
(b) Does a quantum algorithm solving the MeDLP exist?
(c) Is the MeCDH hard?
(d) Does a quantum algorithm solving the MeCDH exist?

The MeDLP may be harder than the ECDLP because $(E(\mathbb{F}_p), \oplus)$ does not form a group, which means the rho method that is a general method for solving the ECDLP cannot be used to solve the MeDLP. Note that a target of a quantum algorithm is also a group. MeCDH uses a hash function, so (c) and (d) may be right. Of course, a new way solving the MeDLP and/or the MeCDH may exist.

IV. APPLICATION OF ME-SCALAR MULTIPLICATION

Suppose that MeCDH is hard. Then, we can construct some cryptographic applications of ElGamal type using the Me-scalar multiplication.

A. Me-DH Key Agreement

System Parameter: A hash function $h: E(\mathbb{F}_p) \to \mathbb{N}$, and $G, Z \in E(\mathbb{F}_p), n \in \mathbb{N}$.
Key Generation: User A selects $P \in E(\mathbb{F}_p)$ at random, compute $K_A = G_{h(P),Z} + P_{n,Z} \in E(\mathbb{F}_p)$, sends K_A to User B, and keeps P secret. User B selects $Q \in E(\mathbb{F}_p)$ at random, compute $K_B = G_{h(Q),Z} + Q_{n,Z} \in E(\mathbb{F}_p)$, sends K_B to User A, and keeps Q secret.
Key Agreement: User A computes $K_B + P_{h(P),Z}$ and User B computes $K_A + Q_{h(Q),Z}$. Both values are same.

B. Me-ElGamal Encryption

Key Generation: User A specifies a hash function $h: E(\mathbb{F}_p) \to \mathbb{N}$ and selects $G, Z \in E(\mathbb{F}_p), n \in \mathbb{N}$ at random. Next, user A computes $K = G_{h(P),Z} + P_{n,Z}$. Then, (G, Z, K, n) is a public key of user A and P is a secret key of user A.
Encryption of a plan text $m \in \mathbb{F}_p$: A sender selects $R \in E(\mathbb{F}_p)$ at random, computes $C_1 = G_{h(R),Z} + R_{n,Z}$ and $c_2 = x(K + R_{h(R),Z}) + m$. A pair (C_1, c_2) is the cipher text of m.
Decryption: User A computes $m' = c - x(C_1 + P_{h(P),Z})$.

V. CONCLUSION

This paper proposed a new operation $\oplus$ of elliptic curve over a finite field and presented open problems about it. If answers of (a) and (c) of Open Problem 4 would be yes, then we could obtain new cryptosystems. If answers of (b) and (d) of Open Problem 4 would be yes, then we could obtain efficient PQCs. Even if the answers are no, the operation may be useful in some area. Answering the open problem is a future work.

REFERENCE

[1] F. Yura, "Solitons with nested structure over finite fields," *Journal of Physics A: Mathematical and Theoretical,* vol. 47, pp. 1-23, 2014.
[2] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Springer, 1985.