Murakami-Kasahara ID-based Key Sharing Scheme Revisited — In Comparison with Maurer-Yacobi Schemes —

Yasuyuki MURAKAMI[*]
yasuyuki@isc.osakac.ac.jp

Masao KASAHARA[†]
kasahara@utc.osaka-gu.ac.jp

Abstract. In Sept. 1990, the present authors firstly discussed DLP over composite number and presented an ID-based Key Sharing Scheme referred to as MK1. In 1991, Maurer and Yacobi presented a scheme, referred to as MY, which is similar to our scheme, MK1. Unfortunately the schemes MK1 and MY are not secure. In Dec. 1990, the present authors presented a secure ID-based key sharing scheme referred to as MK2. With a rapid progress of computer power for the last 15 years, our proposed scheme would have more chance to be applied practically. Regrettably, it has not been widely known that (i) the schemes MY and MK1 are not secure, (ii) there exists a secure scheme, MK2. In this paper, we shall review MK2 and clarify the difference between MK2 and other schemes from the standpoint of security.

Keywords: discrete logarithm problem, prime factorization problem, ID-based cryptosystem, non-interactive key sharing scheme, Diffie-Hellman problem

1 Introduction

Modern cryptography is based on information theory, computational theory, finite field theory and etc. Typical problems in integer theory used in cryptography would be the prime factorization problems. A Discrete Logarithm Problem(DLP) has been also extensively studied and successfully applied to the various cryptographic technologies such as Diffie-Hellman public key distribution scheme[1].

In the conventional DLP, usually, a prime number is used for the modulus. However, DLP can be considered in a more general issue where the modulus is a composite number, although in such case discrete logarithm(DL) does not necessarily exist. Hereinafter we shall refer to DLP with a composite number as DLP over composite number.

In Sept. 1990, the present authors firstly discussed DLP over composite number and presented an ID-based Key Sharing Scheme referred to as MK1[3][1]. In Dec. 1990, they presented an improved version of MK1, referred to as MK2[4]. In 1991, Maurer and Yacobi presented a scheme[5], referred to as MY, which is similar to our scheme, MK1. In 1992, Maurer and Yacobi proposed some schemes as improved version of their schemes[6], MK2. Unfortunately the schemes MK1 and MY are not secure, although MK2 is considered secure.

---

[*]Department of Telecommunications and Computer Networks, Osaka Electro-Communication University, 18-8, Hatsu-cho, Neyagawa-shi, Osaka, 572-8530 Japan.

[†]Faculty of Informatics, Osaka Gakuin University, 2-36-1, Kishibe-Minami, Suita-shi, Osaka, 564-8511 Japan.

[1]ID-based cryptosystem was first proposed by A. Shamir[2].

This paper discusses the problems presented in Ref.[3] again. At this time, present authors review MK2 and clarify the difference between MK2 and other schemes from the standpoint of security.

2 Discrete Logarithm Problem over Composite Number

2.1 Definitions

Several definitions are given first.

Definition 1 *The composite number n can be uniquely represented as follows:*

$$n = \prod_{k=1}^{m} p_k^{c_k},$$

where p_k's are prime numbers such that $p_1 < p_2 < \ldots < p_m$ and c_k's are positive integers.

Definition 2 *Sets $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$ are defined as follows:*

$$
\begin{aligned}
\mathbb{Z}_n &= \{0, 1, 2, \ldots, n-1\} \\
\mathbb{Z}_n^* &= \{x \mid x \in \mathbb{Z}_n, \gcd(x, n) = 1\}
\end{aligned}
$$

Definition 3 *The cyclic multiplication group generated by g with modulus n is denoted by $\langle g \rangle_n$. That is, the cyclic multiplication group $\langle g \rangle_n$ for an arbitrary element $g \in \mathbb{Z}_n^*$ is represented as follows:*

$$\langle g \rangle_n = \{y \mid y \equiv g^x \pmod{n}, g \in \mathbb{Z}_n^*, x \in \mathbb{Z}_{|g|_n}\},$$

where $|g|_n$ is the order of g.

Definition 4 *The maximum generator and etc., are defined as follows:*

Maximum generator: *element with the maximum order in $\mathbb{Z}_n^*$;*

S_n**:** *set of maximum generators in $\mathbb{Z}_n^*$;*

$\lambda(n)$**:** *Carmichael function representing the order of the maximum generator in $\mathbb{Z}_n^*$;*

2.2 DLP over Composite Number n

From Definition 3, the following relations hold, where g is a maximum generator:

$$
\begin{cases}
g \in S_n \\
y \in \langle g \rangle_n
\end{cases}
$$
$$y \equiv g^x \pmod{n}$$

In general, for any x such that $x \in \mathbb{Z}_{\lambda(n)}$ there exists $y \in \mathbb{Z}_n^*$ satisfying $y \equiv g^x \pmod{n}$. Conversely, it is not always true that, for any y such that $y \in \mathbb{Z}_n^*$ there exists $x \in \mathbb{Z}_{\lambda(n)}$. We shall refer the problem to determine x from given y and g over n as DLP(n).

Table 1: Residue class decomposition

H_n	$h_1 = 1$	h_2	$\cdots$	h_d
gH_n	g	gh_2	$\cdots$	gh_d
g^2H_n	g^2	g^2h_2	$\cdots$	g^2h_d
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$g^{\pi(n)-1}H_n$	$g^{\pi(n)-1}$	$g^{\pi(n)-1}h_2$	$\cdots$	$g^{\pi(n)-1}h_d$

2.3 Theorems on DLP(n)

Definition 5 *Define $\delta(n)$ and $\pi(n)$ as follows:*

$$\begin{aligned} \delta(n) &= \operatorname*{lcm}_{i \neq j}(\gcd(\lambda(p_i^{c_i}), \lambda(p_j^{c_j}))), \\ \pi(n) &= \lambda(n)/\delta(n). \end{aligned}$$

Definition 6 *Let the set of $\delta(n)$-th root of 1 with n as the modulus be H_n:*

$$H_n = \{x \mid x^{\delta(n)} \equiv 1 \pmod{n}\}$$

The group H_n obviously forms a subgroup of $\mathbb{Z}_n^*$. Consequently, $\mathbb{Z}_n^*$ can be decomposed into residue classes on H_n.

Lemma 1 *All the elements of $\mathbb{Z}_n^*$ can be decomposed into residue classes on H_n with $G_n(g)$ as coset leaders, where*

$$G_n(g) = \{y \mid y \equiv g^x \pmod{n}, \quad g \in S_n, x \in \mathbb{Z}_{\pi(n)}\}.$$

Lemma 2 *Let the maximum generator be g. Then the cyclic multiplicative group $\langle g^{\delta(n)} \rangle_n$ generated by $g^{\delta(n)}$ is the same as the set of $\delta(n)$-th power residues modulo-n.*

The following theorem can be derived directly from Lemma 2, which has an important role in this paper.

Theorem 1 *If $e \in \mathbb{Z}_n^*$, $e^{\delta(n)}$ has a logarithm with the maximum generating element g as the base and n as the modulus.*
Proof: It follows from Lemma 2 that $e^{\delta(n)} \in \langle g^{\delta(n)} \rangle_n$. Consequently, $e^{\delta(n)}$ has a discrete logarithm with g as the base and n as the modulus. $\square$

Thus, it is shown that the $\delta(n)$-th power of any element in $\mathbb{Z}_n^*$ has a logarithm.

2.4 Square-root attack

If the DLP(n) can be solved with the base g in polynomial time, then the factoring problem of n can be solved in expected polynomial time[7]. In other words, if one can calculate the discrete logarithm x of an arbitrary element $e \in \mathbb{Z}_n^*$, he/she can find a factor of n with the following algorithm:

———— Square-Root Attack ————

Step 1: Choose e' randomly from $\mathbb{Z}_n^*$.

Step 2: Let $e \equiv e'^2 \pmod{n}$.

Step 3: Calculate the discrete logarithm x of e with the base g. If e does not have a discrete logarithm then goto Step 1.

Step 4: If $g^{x/2} \equiv \pm e' \pmod{n}$ then goto Step 1.

Step 5: Factors of n can be obtained as $\gcd(g^{x/2} \pm e', n)$.

This attack will be referred to as the square-root attack.

When applying DLP(n) to ID-based key sharing scheme, it should be noted that the trusted center (TC) can be used as an oracle of solving DLP(n). The attacker requests TC to join the system as his/her ID as a forged ID to obtain the discrete logarithm of the wanted value. The example of the square-root attack on MK1 and MY is given in Table 3.

Using one-way hash function is very important to be secure against this square-root attack[3]. However, it should be noted that the scheme which uses one-way hash function is not always secure.

3 Secure Conditions

This section gives the conditions that n and g should satisfy in order to realize a secure scheme when using DLP(n).

3.1 DLP(n) under secure conditions

As was discussed in Section 2, $\mathbb{Z}_n^*$ is not a cyclic multiplication group, except for the case where a special composite number n is used. This implies that the relation $\delta(n) \geq 2$ holds for general n. We thus clarify the conditions for being secure against the square-root attack and propose another method where any element $e \in \mathbb{Z}_n^*$ yields a discrete logarithm without powering by $\delta(n)$.

In the following, the case where the composite number n is a product of two prime numbers p and q satisfying the following conditions is considered.

Condition 1 *Odd prime numbers p and q satisfy the following relations:*

$$\begin{cases} p = 2p' + 1 \\ q = 2q' + 1 \end{cases}$$
$$\gcd(p', q') = 1.$$

By defining n in this way, we see that $\delta(n) = 2$ holds. From Theorem 1, the square of any element belonging to $\mathbb{Z}_n^*$ has a logarithm with the maximum generator as the base.

Further, the following condition is assumed.

Condition 2 *The maximum generator g is assumed to satisfy the following condition:*

$$-1 \notin \langle g \rangle_n.$$

Relating to Condition 2, the following lemma is important.

Lemma 3 *The necessary and sufficient condition for the maximum generating element g to satisfy Condition 2 is the following:*
(a) When $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$,

$$
\begin{cases} \left(\frac{g}{p}\right) = -1 \\ \left(\frac{g}{q}\right) = -1 \end{cases} \quad or \quad \begin{cases} \left(\frac{g}{p}\right) = 1 \\ \left(\frac{g}{q}\right) = -1 \end{cases} \tag{1}
$$

(b) When $p \equiv q \equiv 3 \pmod 4$,

$$
\begin{cases} \left(\frac{g}{p}\right) = 1 \\ \left(\frac{g}{q}\right) = -1 \end{cases} \tag{2}
$$

where $\left(\frac{a}{b}\right)$ denotes Jacobi symbol.
Proof: The following relation holds:

$$
\begin{aligned}
g^{\lambda(n)/2} &\equiv g^{p'q'} \pmod n \\
&\equiv \begin{cases} 1 \pmod p \\ -1 \pmod q \end{cases}
\end{aligned}
$$

If Eq.(1) or (2) is satisfied, then $g^{\lambda(n)/2}$ is $1 \pmod p$ and $-1 \pmod q$, respectively. Consequently, $g^{\lambda(n)/2} \not\equiv -1 \pmod n$. Since the square root of 1 is limited to $g^{\lambda(n)/2}$ and 1 in $\langle g \rangle_n$, there holds $-1 \notin \langle g \rangle_n$. □

Corollary 1 *There holds $(g \bmod p) \in S_p$ and $(g \bmod q) \in S_q$, if and only if $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$.*

Lemma 4 *In this case, an element e satisfying $\left(\frac{e}{n}\right) = 1$ has a discrete logarithm over n.*

The cyclic multiplication group $\langle g \rangle_n$ obviously forms a subgroup of $\mathbb{Z}_n^*$. Consequently, $\mathbb{Z}_n^*$ can be decomposed into residue classes on $\langle g \rangle_n$. Since Condition 2 is satisfied, the following lemma is derived.

Lemma 5 *When the maximum generator g satisfies Condition 2, $\mathbb{Z}_n^*$ can be decomposed into residue classes on $\langle g \rangle_n$ with $\{1, -1\}$ as coset leaders (see Table 2).*
Proof: Since Condition 2 is satisfied, $\{1, -1\}$ can be used as coset leaders. Since $\lambda(n) = \varphi(n)/2$ follows from Condition 1, there holds $2|\langle g \rangle_n| = \varphi(n)$. Then all elements are exhausted. □

The fact that the residue class decomposition is possible with the obvious two square-roots of 1 as the coset leaders is very important to maintain the security of the prime factorization of n. The example of the decomposition is shown in Table 4. It should be noted that we can not complete the decomposing with the obvious two square-roots of 1 as the coset leader when $m \geq 3$. The example of the decomposition when $m = 3$ is shown in Table 5. The following theorem can be derived directly from Lemma 5.

Theorem 2 *When the maximum generator g satisfies Condition 2, letting $e \in \mathbb{Z}_n^*$, either e or $-e$ has a discrete logarithm with g the base.*

5

Table 2: Residue class decomposition 2

$\langle g \rangle_n$	1	g	g^2	$\cdots$	$g^{\lambda(n)-1}$
$-\langle g \rangle_n$	-1	$-g$	$-g^2$	$\cdots$	$-g^{\lambda(n)-1}$

Table 3: Residue class decomposition in MK1, MY ($n = 7 \cdot 11, g = 24$)

i	0	1	2	3	4	5	6	7	8	9	<u>10</u>	11	12	13	14	15	16	17	18	19	<u>20</u>	21	22	23	24	25	26	27	28	29
g^i	1	24	37	41	60	54	64	73	58	6	67	68	15	52	16	76	53	40	36	17	23	13	4	19	71	10	9	62	25	61
rg^i	34	46	26	8	38	65	20	18	47	50	45	2	48	74	5	43	31	51	69	39	12	57	59	30	27	32	75	29	3	72

4 ID-based Key Sharing Schemes

The trusted center (TC) generates a composite modulus n and a maximum generator g. It should be noted that g need not to be publicized. However, g (or an element doing the same working as g) can be easily revealed.

Let us denote identity information of User k as ID_k. Let $e_k \in \mathbb{Z}_n^*$ and s_k be the public key and the personal secret key corresponding to ID_k, respectively. We assume that TC can calculate s_k from e_k by calculating the discrete logarithms of e_k over each prime factor of n. We also assume that anyone can calculate e_k from ID_k with a public algorithm which is publicized by TC.

K_{AB} denotes the shared key between Users A and B. We shall often use p and q instead of p_1 and p_2 when $n = p_1 p_2$, for simplicity. The $h(\cdot)$ denotes a public one-way hash function defined by TC.

4.1 Trivial Scheme

We shall describe the trivial ID-based key sharing scheme based on Diffie-Hellman problem over n, as an application of the discrete logarithm problem over composite modulus.

$$
\begin{aligned}
n &: \text{ composite number,} \\
g &\in S_n, \\
e_k &= h(ID_k), \\
s_k &\equiv \log_g e_k^{\delta(n)} \pmod{\lambda(n)}, \\
K_{AB} &\equiv e_B^{s_A} \equiv g^{s_A s_B / \delta(n)} \quad \text{(Type1)}, \\
K_{AB} &\equiv e_B^{\delta(n)s_A} \equiv g^{s_A s_B} \quad \text{(Type2)}.
\end{aligned}
$$

Because s_k is divisible by $\delta(n)$, the trivial schemes are not secure against the $\delta(n)$-th root attack which is a similar attack as the square-root attack. That is, there is a case where the factors of

Table 4: Residue class decomposition in MK2 ($n = 7 \cdot 11, g = 2$)

i	0	1	2	3	4	<u>5</u>	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
g^i	1	2	4	8	16	32	64	51	25	50	23	46	15	30	60	43	9	18	36	72	67	57	37	74	71	65	53	29	58	39
$-g^i$	76	75	73	69	61	45	13	26	52	27	54	31	62	47	17	34	68	59	41	5	10	20	40	3	6	12	24	48	19	38

Table 5: Residue class decomposition when $m = 3$ ($n = 3 \cdot 5 \cdot 11, g = 2$)

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
g^i	1	2	4	8	16	32	64	128	91	17	34	68	136	107	49	98	31	62	124	83
$-g^i$	164	163	161	157	149	133	101	37	74	148	131	97	29	58	116	67	134	103	41	82
$r_1 g^i$	56	112	59	118	71	142	119	73	146	127	89	13	26	52	104	43	86	7	14	28
$r_2 g^i$	109	53	106	47	94	23	46	92	19	38	76	152	139	113	61	122	79	158	151	137

Table 6: Residue class decomposition in MMY ($n = 7 \cdot 11, g = 73$)

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
g^i	1	73	16	13	25	54	15	17	9	41	67	40	71	24	58	76	4	61	64	52	23	62	60	68	36	10	37	6	53	19
rg^i	34	18	5	57	3	65	48	39	75	8	45	51	27	46	47	43	59	72	20	74	12	29	38	2	69	32	26	50	31	30

n can be obtained by $\gcd(g^{s_k/\delta(n)} \pm e_k, n)$.

It should be noted that $\delta(n)$ is publicized in Type2.

4.2 Murakami-Kasahara Scheme Ver.1

In 1990, present authors proposed the scheme, MK1, as an application of the discrete logarithm problem over composite modulus[3].

$$
\begin{aligned}
n &= pq \quad \text{where } \delta(n) = 2, \quad (m = 2), \\
g &\in S_n, \\
e_k &= h(ID_k), \\
s_k &\equiv \log_g e_k^2 \pmod{\lambda(n)}, \\
K_{AB} &\equiv e_B^{s_A} \equiv g^{s_A s_B/2} \pmod{n}.
\end{aligned}
$$

MK1 is not secure because it belongs to Type1 of the trivial scheme.

For example, in Table 3, let ID (or hashed ID) of the attacker X be $e_X = \boxed{45}$. Since $e_X^2 \equiv \boxed{\boxed{23}}$, X obtains a logarithm $s_x = 20$ of $\boxed{\boxed{23}}$ on request to TC as $ID_X = 23$. Thus, X can calculate $g^{20/2} \equiv g^{10} \equiv \boxed{67}$. Finally, the factors can be disclosed by $\gcd(\boxed{67} \pm \boxed{45}, n) = 7, 11$.

Table 7: Various Schemes

Scheme	n	Public key: e_A	Secret key: s_A	Shared key: K_{AB}	Type
Trivial scheme	General	$h(ID_A)$	$\log_g e_A^{\delta(n)}$	$e_B^{s_A} \equiv g^{s_A s_B/\delta(n)}$ (Type1) $e_B^{\delta(n)s_A} \equiv g^{s_A s_B}$ (Type2)	—
MK1 ('90)	pq	$h(ID_A)$	$\log_g e_A^2$	$e_B^{s_A} \equiv g^{s_A s_B/2}$	Type1
MK2 ('90)	pq	$h(ID_A)$	$\log_g e_A/\log_g -e_A$	$e_B^{2s_A} \equiv g^{2s_A s_B}$	—
MY ('91)	$p_1 \ldots p_m$	ID_A	$\log_g e_A^2$	$e_B^{2s_A} \equiv g^{s_A s_B}$	Type2
AMY ('91)	pq	$ID_A + \varepsilon$ s.t. $\left(\frac{ID_A + \varepsilon}{n}\right) = 1$	$\log_g e_A$	$e_B^{s_A} \equiv g^{s_A s_B}$	—
MMY ('92)	$p_1 \ldots p_m$	ID_A	$\log_{g'} e_A^2 \quad (g' \equiv g^v)$	$e_B^{2s_A} \equiv g'^{s_A s_B}$	Type2
MAMY ('92)	pq	ID_A if $\left(\frac{ID_A}{n}\right) = 1$ $2ID_A$ if $\left(\frac{ID_A}{n}\right) = -1$	$\log_g e_A$	$e_B^{s_A} \equiv g^{s_A s_B}$	—

4.3 Murakami-Kasahara Scheme Ver.2

In 1990, present authors also proposed the scheme, MK2, as an application of the discrete logarithm problem over composite modulus[4].

$$
\begin{aligned}
n &= pq \quad \text{where } \delta(n) = 2, \quad (m = 2), \\
g &\in S_n \quad \text{where} -1 \notin \langle g \rangle_n, \\
e_k &= h(ID_k), \\
s_k &\equiv \begin{cases} \log_g e_k \pmod{\lambda(n)} & \text{if } e_k \in \langle g \rangle_n \\ \log_g -e_k \pmod{\lambda(n)} & \text{if } e_k \notin \langle g \rangle_n \end{cases}, \\
K_{AB} &\equiv e_B^{2s_A} \equiv g^{2s_A s_B} \pmod{n}.
\end{aligned}
$$

For example, in Table 4, Let hashed ID of the attacker X be $e_X = \boxed{45}$. Since $e_X \notin \langle g \rangle_n$, X obtains a logarithm $s_x = 5$ of $-\boxed{45} \equiv \boxed{32}$ on request to TC as ID_X Thus, X can calculate $g^5 \equiv \boxed{32}$. However, any factor of n can not be disclosed by $\gcd(\boxed{32} \pm \boxed{45}, n)$.

In this way, MK2 is considered to be secure when n is difficult to be factored.

4.4 Maurer-Yacobi Scheme

4.4.1 Maurer-Yacobi Scheme

In 1991, Maurer and Yacobi[5] proposed a similar scheme to MK1. This scheme will be referred to as MY.

$$
\begin{aligned}
n &= p_1 p_2 \ldots p_m \quad \text{where } \delta(n) = 2, \\
g &: \quad \text{maximum generator such that } (g \bmod p_i) \in S_{p_i} \text{ for } i = 1, 2, \ldots, m, \\
e_k &= ID_k, \\
s_k &\equiv \log_g e_k^2 \pmod{\lambda(n)}, \\
K_{AB} &\equiv e_B^{2s_A} \equiv g^{s_A s_B} \pmod{n}.
\end{aligned}
$$

MY is not secure because it belongs to Type2 of the trivial scheme.

4.4.2 Alternative Maurer-Yacobi Scheme

Maurer and Yacobi also proposed an alternative implementation in [5]. This scheme will be referred to as AMY.

$$
\begin{aligned}
n &= pq \quad \text{where } \delta(n) = 2, \quad (m = 2), \\
g &: \quad \text{maximum generator such that } (g \bmod p) \in S_p \text{ and } (g \bmod q) \in S_q, \\
e_k &: \quad \text{the smallest integer greater than } ID_k \text{ such that } \left(\frac{e_k}{n}\right) = 1. \\
s_k &\equiv \log_g e_k \pmod{\lambda(n)}, \\
K_{AB} &\equiv e_B^{s_A} \equiv g^{s_A s_B} \pmod{n}.
\end{aligned}
$$

AMY is not secure against the square root attack because one-way hash function is not used[2].

---

[2]We stress that using one-way hash function is essential in order to securely apply DLP over composite modulus for ID-based key sharing schemes.

4.5 Modified Maurer-Yacobi Scheme

4.5.1 Modified Maurer-Yacobi Scheme

In 1992, Maurer and Yacobi proposed a modified version of their scheme for the purpose of being invulnerable to the square root attack[6]. This scheme will be referred to as MMY.

$$
\begin{aligned}
n &= p_1 p_2 \ldots p_m \quad \text{where } \delta(n) = 2, \\
g &: \quad \text{maximum generator such that } (g \bmod p_i) \in S_{p_i} \text{ for } i = 1, 2, \ldots, m, \\
e_k &= ID_k, \\
s'_k &\equiv \log_g e_k^2 \pmod{\lambda(n)}, \\
s_k &\equiv ts'_k \pmod{\varphi(n)} \quad \text{where } t \in \mathbb{Z}^*_{\varphi(n)} \text{ is a secret of the center}, \\
K_{AB} &\equiv e_B^{2s_A} \equiv g^{vs_A s_B} \quad \text{where } vt \equiv 1 \pmod{\lambda(n)},
\end{aligned}
$$

By substituting $g' = g^v$, s_k and K_{AB} can be represented as follows:

$$
\begin{aligned}
s_k &\equiv \log_{g'} e_k^2 \pmod{\varphi(n)}, \\
K_{AB} &\equiv e_B^{2s_A} \equiv g'^{s_A s_B} \pmod{n}.
\end{aligned}
$$

Attackers A and B such that $\gcd(s_A, s_B) = 2$ can calculate α, β satisfying $\alpha s_A + \beta s_B = 2$ by extended Euclidean algorithm. Then, g' can be easily disclosed as follows:

$$
g' \equiv e_A^{\alpha} e_B^{\beta} \pmod{n}.
$$

For example, in Table 6, $s_A = 14$ and $s_B = 22$ are given for $e_A = \boxed{39}$ and $e_B = \boxed{40}$, respectively. Then, $\alpha = 8$ and $\beta = -5$ satisfies $\alpha s_A + \beta s_B = 2$. Consequently, $g \equiv e_A^{\alpha} e_B^{\beta} \equiv 39^8 \cdot 40^{-5} \equiv 73 \pmod{n}$ can be disclosed.

Thus, it is clarified that MMY belongs to Type2 of the trivial scheme. Consequently, we can conclude that MMY is not secure against the square root attack.

4.5.2 Modified Alternative Maurer-Yacobi Scheme

They also proposed a modified version of their alternative implementation[6]. This scheme will be referred to as MAMY.

$$
\begin{aligned}
n &= pq \quad \text{where } \delta(n) = 2, \quad (m = 2), \\
&\qquad p \equiv 3 (\bmod 8), \quad q \equiv 7 (\bmod 8), \\
g &: \quad \text{maximum generator such that } (g \bmod p) \in S_p \text{ and } (g \bmod q) \in S_q, \\
e_k &= \begin{cases} ID_k & \text{if } \left(\frac{ID_k}{n}\right) = 1 \\ 2ID_k & \text{if } \left(\frac{ID_k}{n}\right) = -1 \end{cases}, \\
s_k &\equiv \log_g e_k \pmod{\lambda(n)}, \\
K_{AB} &\equiv e_B^{s_A} \equiv g^{s_A s_B} \pmod{n}.
\end{aligned}
$$

This scheme is not secure. Attacker X requests to TC to join the system as $ID_X \equiv 2a^2 \pmod{n}$, where a is an arbitrary integer. Then, there clearly holds $\left(\frac{ID_X}{n}\right) = -1$. So, TC gives $s_X = \log_g 2ID_X = \log_g(2a)^2$. Thus, it is clear that the square root attack can be applied. Consequently, MAMY is not secure. This deficiency can be recovered by using a secure hash function.

4.5.3 Another Maurer-Yacobi Scheme

They proposed the improvement scheme of $m \geq 3$ [6]. In this paper, we shall not treat with this scheme because it seems not non-interactive.

4.6 Proposed Scheme

We shall propose a new scheme of non-interactive key sharing. This scheme will be referred to as MK3.

$$
\begin{aligned}
n &= pq \quad \text{where } \delta(n) = 2, \quad (m = 2), \\
&\quad p \equiv 3 \pmod{4}, \quad q \equiv 1 \pmod{4}, \\
g &: \quad \text{maximum generator such that } (g \bmod p) \in S_p \text{ and } (g \bmod q) \in S_q, \\
e_k &= \begin{cases} h(ID_k) & \text{if } \left(\frac{h(ID_k)}{n} \right) = 1 \\ -h(ID_k) & \text{if } \left(\frac{h(ID_k)}{n} \right) = -1 \end{cases}, \\
s_k &\equiv \log_g e_k \pmod{\lambda(n)}, \\
K_{AB} &\equiv e_B^{s_A} \equiv g^{s_A s_B} \pmod{n}.
\end{aligned}
$$

This scheme is also considered to be secure when n is difficult to be factored. From Lemma 4, e_k has a discrete logarithm over n. It should be noted that anyone can easily calculate Jacobi symbol without a knowledge of factors of n. The difference between MK2 and MK3 is as follows:

- The calculation of Jacobi symbol is not necessary in MK2.

- The space of shared keys in MK3 is $\mathbb{Z}_n^*$, whose order is twice larger than that in MK2.

5 Conclusions

This paper has discussed the ID-based non-interactive key sharing schemes based on DLP(n). Also, this paper has reviewed MK2[4] and clarified the difference between MK2 and other schemes from the standpoint of the security.

It will be necessary in the future to investigate DLP(n) from a more general viewpoint. We sincerely wish a new security technique be developed based on the present paper.

References

[1] W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Trans, Inf. Theory, IT-22, 6, pp.644–654 (Nov.1976).

[2] A.Shamir, "Identity-Based Cryptosystems and Signature Schemes," Advances in Cryptology – CRYPTO'84, Lecture Notes in Computer Science, Springer-Verlag, vol.196, pp.47–53, (1985).

[3] Y.Murakami and M.Kasahara, "An ID-based key distribution system," Technical Report of IEICE, ISEC90-26, pp.29–36 (Sept. 1990).

[4] Y.Murakami and M.Kasahara, "The discrete logarithm problem under a composite modulus," Technical Report of IEICE, ISEC90-42, pp.33–40 (Dec. 1990).

[5] U.M.Maurer and Y.Yacobi, "Non-interactive public key cryptography," Advances in Cryptology – EUROCRYPT'91, Lecture Notes in Computer Science, Springer-Verlag, vol.547, pp.498–507 (1991).

[6] U.M.Maurer and Y.Yacobi, "A remark on non-interactive public-key distribution system," Advances in Cryptology – EUROCRYPT'92, Lecture Notes in Computer Science, Springer-Verlag, vol.658, pp.458–460 (1992).

[7] A.Menezes, P.C.Oorschot, S.A.Vanstone, "Handbook of Applied Cryptography," CRC Press, (1997).

[8] Y.Murakami and M.Kasahara, "Discrete logarithm problem with composite number as modulus," Proc. of the 13-th Symposium on Information Theory and Its Applications (SITA '90), pp.17–22 (Jan. 1991).

[9] Y.Murakami and M.Kasahara, "Discrete logarithm problem with composite number as modulus," IEICE Trans. on Fundamentals, vol.76-A, No.4, pp.649–655 (1993).

[10] U.M.Maurer and Y.Yacobi, "A non-interactive public-key distribution system," Designs, Codes and Cryptography 9, Kluwer Academic Publishers, pp.305–316 (1996).