社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30（36）
2005／7／22

村上-笠原 ID 鍵共有方式について

— Maurer-Yacobi 方式との比較 —

村上　恭通†　　笠原　正雄††

† 大阪電気通信大学
大阪府寝屋川市初町 18-8
†† 大阪学院大学
大阪府吹田市岸部南 2-36-1
E-mail: †yasuyuki@isc.osakac.ac.jp, ††kasahara@utc.osaka-gu.ac.jp

あらまし　1990 年 9 月，筆者らは合成数を法とする既約剰余類に属する任意の元を，法により一意に決定される数によってべき乗したものは，必ず対数を有することを示し，ID 情報に基づく予備通信不要な鍵共有方式 (MK1 方式) を提案した．同様の方式が Eurocrypt' 91 にて Maurer-Yacobi により提案されている (MY 方式)．しかしながら，これら両方式ともに安全ではなかった．1990 年 12 月，筆者らは合成数を法とする離散対数問題を安全に暗号技法へ応用するために必要な条件について明らかにし，安全な ID 鍵共有方式 (MK2 方式) を提案した．MK1 方式を含めたこれらの方式は発表当時，演算能力に限界があり実用化は必ずしも容易ではなかった．しかしながら，その後におけるコンピュータの目覚しい発達により，最近においては十分実用化できる可能性が出てきている．筆者らは，これらの方式の有用性を改めて認識するものであるが，(i) MY 方式，MK1 方式が安全ではないこと，(ii) 安全である MK2 方式が存在することが，必ずしも広く知られていないようであるため，本論文では，再びこの問題を取り上げることとし，MK2 方式の可能性を MY 方式や他の種々の方式と比較しつつ，議論することとしたい．

キーワード　離散対数問題，素因数分解問題，ID 暗号，予備通信不要な鍵共有方式

Murakami-Kasahara ID-based Key Sharing Scheme Revisited

— In Comparison with Maurer-Yacobi Schemes —

Yasuyuki MURAKAMI† and Masao KASAHARA††

† Osaka Electoro-Communication University
18-8, Hatsu-cho, Neyagawa-shi, Osaka, 572-8530
†† Osaka Gakuin University
2-36-1, Kishibe Minami, Suita-shi, Osaka, 564-8511
E-mail: †yasuyuki@isc.osakac.ac.jp, ††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 the similar 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 a last 15 years, our proposed scheme would have more chance to be applied practically. Regrettably, it is not widely known the fact that (i) the schemes MY and MK1 are not secure, (ii) there exists a secure scheme, MK2. At this time, present authors review MK2 and clarify the difference between MK2 and other schemes from the standpoint of security.

Key words　Discrete logarithm problem; prime factorization problem; ID-based cryptosystem; non-interactive key sharing scheme.

1. Introduction

Modern cryptography is based on information theory, the theory of computational complexity, the theory of finite field and etc. Typical problems in the theory of integers used in cryptography would be the prime factorization problem.

A Discrete Logarithm Problem(DLP) has been also extensively studied and successfully applied to the various cryptographic technologies.

In the conventional DLP, usually, a prime number is used for the modulus. However, DLP can be considered in a more general standpoint where the modulus is a composite number, although in such case 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 [1]. In Dec. 1990, they presented an improved version of MK1, referred to as MK2 [2].

In 1991, Maurer and Yacobi presented the similar scheme [5], referred to as MY, which is similar to our scheme, MK1. In 1992, Maurer and Yacobi proposed some schemes as as improved version of their schemes [6]. Unfortunately the schemes MK1 and MY are not secure, although MK2 is considered secure.

With a rapid progress of computer power for a last 15 years, our proposed scheme would have more chance to be applied practically. In SCIS2005, Abe, Kunihiro and Ohta discussed the practical parameters of ID-based key sharing scheme using DLP over n [9]. Tanaka proposed a similar ID-based key sharing scheme of ours [8].

This paper discusses the problems presented in Ref. [1] 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:

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

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
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$g^{\pi(n)-1}H_n$	$g^{\pi(n)-1}$	$g^{\pi(n)-1}h_2$	$\cdots$	$g^{\pi(n)-1}h_d$

[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 generating element and etc., are defined as follows:

Maximum generating element: element with the maximum order with an arbitrary positive integer as the modulus;

S_n: set of maximum generating element with a positive integer n as the modulus;

$\lambda(n)$: Carmichael function which represents the order of the maximum generating element with a positive integer n as the modulus.

2.2 Theorems on DLP over n

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

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

[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

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

Proof: Let $i \neq j (i, j \in \mathbb{Z}_\pi(n))$. For any element a belonging to H_n, there holds $ag^i \not\equiv g^j \pmod{n}$ and $G_n(g)$ can be used as the coset leaders. There hold $|H_n| \cdot |G_n(g)| = \varphi(n)$. Consequently, all elements are exhausted. □

[Lemma 2] Let the maximum generating element be g. Then the cyclic multiplication 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.

Proof: Let the set of $\delta(n)$-th power residues modulo-n be R_n, i.e.,

$$R_n = \{x \mid x \equiv e^{\delta(n)} \pmod{n}, \quad e \in \mathbb{Z}_n^*\}.$$

It follows from Lemma 1 that for any e belonging to $\mathbb{Z}_n^*$, there exist $x \in H_n$ and $y \in G_n(g)$ such that $e = xy$. The relation $e^{\delta(n)} \equiv x^{\delta(n)} y^{\delta(n)} \equiv y^{\delta(n)} \pmod{n}$ also holds. Consequently, $R_n = \langle g^{\delta(n)} \rangle_n$ holds. □

The following theorem is 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. □

Thus, it is shown that the $\delta(n)$-th power of any element has a logarithm with a composite number n as modulus.

2.3 DLP over Composite Number n

The problem to determine x such that $y \equiv g^x$ from given y and g is called the discrete logarithm problem. In this problem, a prime number usually is considered as the modulus. However, it is possible to consider a more general discrete logarithm problem with the composite number as the modulus.

As is well known, the multiplication group $\mathbb{Z}_n^*$ is a cyclic multiplication group only when n is 2, 4, odd prime number, or an exponent of an odd prime number. The primitive element exists only in those cases. When the composite number is used as the modulus, the maximum generating element is defined to replace the role of the primitive element.

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

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

In general, for any x such that $x \in \mathbb{Z}_{\lambda(n)}$ there corresponds $y \in \mathbb{Z}_n^*$ 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 call the problem to determine x from given y and g over n as DLP over n.

2.4 Square-root attack

If the discrete logarithm problem over n can be solved with the base g, then the factoring problem of n can be solved. 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.

In the case applying DLP over 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 over n. The attacker requests TC to join the system as his/her ID as a spurious ID to obtain the discrete logarithm of the wanted value. The example of the square-root attack for MK1 and MY is given in Table 3.

Using one-way hash function is very important to avoid this attack. 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 construct a secure application using DLP over n.

3.1 DLP over 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 $\delta(n) \geqq 2$ holds for general n. To prevent the square-root attack, we clarify the conditions. and propose another method that any element $e \in \mathbb{Z}_n^*$ corresponds with a discrete logarithm without powering by $\delta(n)$.

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

[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 generating element as the base.

Further, the following condition is assumed.

[Condition 2] The maximum generating element 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 $q \equiv 1 \pmod 4$,

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

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

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

where $(\frac{a}{b})$ 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 for cases of (a) and (b), 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 $(\frac{e}{n}) = 1$ 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 generating element 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 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 decompose 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 generating element g satisfies Condition 2, either e or $-e$, where e is an arbitrary element belonging to $\mathbb{Z}_n^*$ has a discrete logarithm with g as the base and n as the modulus.

Table 2 Residue class decomposition 2

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

4. ID-based Key Sharing Schemes

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

We shall 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 factors 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. $h(\cdot)$ denotes a public one-way hash function defined by TC.

4.1 Trivial Scheme

We shall describe the trivial scheme of ID-based key sharing system based on Diffie-Hellman key distribution scheme [10], as an application of the discrete logarithm problem over composite modulus.

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

The trivial schemes are not secure against the $\delta(n)$-th root attack because s_k is divisible by $\delta(n)$, which is a similar attack as the square-root attack. That is, there is a case that factors of 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, we proposed the scheme as an application of the discrete logarithm problem over composite modulus [1]. In this paper, this scheme will be referred to as MK1.

$$\begin{aligned} n &= pq \quad \text{where } \delta(n) = 2, \quad (m = 2), \\ g &\in S_n, \\ e_k &= h(ID_k), \end{aligned}$$

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	10	11	12	13	14	15	16	17	18	19	20	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

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

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	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

Table 7 Various Schemes

Scheme	n	Public key: e_A	Secret key: s_A	Shared key: K_{AB}	Type	Secure
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)	—	No
MK1 ('90)	pq	$h(ID_A)$	$\log_g e_A^2$	$e_B^{s_A} \equiv g^{s_A s_B/2}$	Type1	No
MK2 ('90)	pq	$h(ID_A)$	$\log_g e_A / \log_g -e_A$	$e_B^{2s_A} \equiv g^{2 s_A s_B}$	—	Yes
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	No
AMY ('91)	pq	$ID_A + \varepsilon$ s.t. $(\frac{ID_A+\varepsilon}{n}) = 1$	$\log_g e_A$	$e_B^{s_A} \equiv g^{s_A s_B}$	—	No
MMY ('92)	$p_1 \ldots p_m$	ID_A	$\log_{g'} e_A^2$ $(g' \equiv g^v)$	$e_B^{2s_A} \equiv g'^{s_A s_B}$	Type2	No
MAMY ('92)	pq	ID_A if $(\frac{ID_A}{n}) = 1$ $2ID_A$ if $(\frac{ID_A}{n}) = -1$	$\log_g e_A$	$e_B^{s_A} \equiv g^{s_A s_B}$	—	No
MK3 ('05)	pq	$h(ID_A)$ if $(\frac{h(ID_A)}{n}) = 1$ $-h(ID_A)$ if $(\frac{h(ID_A)}{n}) = -1$	$\log_g e_A$	$e_B^{s_A} \equiv g^{s_A s_B}$	—	Yes

$$s_k \equiv \log_g e_k^2 \pmod{\lambda(n)},$$
$$K_{AB} \equiv e_B^{s_A} \equiv g^{s_A s_B/2} \pmod{n}.$$

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 $\boxed{\boxed{23}}$ by requesting TC as ID_X. Thus, X can calculate $g^{20/2} \equiv g^{10} \equiv \boxed{67}$. Finally, the factors can be disclosed by $\gcd(\boxed{67} \pm \boxed{45}, n) = 7, 11$.

4.3 Murakami-Kasahara Scheme Ver.2

In 1990, we also proposed the scheme as an application of the discrete logarithm problem over composite modulus [2]. In this paper, this scheme will be referred to as MK2.

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

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 $-\boxed{45} \equiv \boxed{32}$ by requesting 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 proposed a similar scheme [5] of our scheme MK1. This scheme will be referred to as MY.

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

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

4.4.2 Practical Parameters

In 2005, Abe, Kunihiro and Ohta suggested the using of $n = p_1 p_2 p_3$ in MY [9] for a practical realization. Unfortunately, their suggestion would not be meaningful, because the scheme MY is not secure.

4.4.3 Alternative Maurer-Yacobi Scheme

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

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

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

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 enduring the square root attack [6]. This scheme will be referred to as MMY.

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

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

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

The 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.

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

This scheme is not secure. The 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 $(\frac{ID_X}{n}) = -1$. 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 $m \geqq 3$ [6]. In this paper, we shall not treat with this scheme because it is not non-interactive.

4.6 Tanaka's Scheme

In 2005, Tanaka proposed a similar scheme [8].

$$
\begin{aligned}
n &= pq \quad \text{where } \delta(n) = \gcd(\gamma, \delta), \quad (m = 2), \\
p - 1 &= \alpha\gamma = \alpha\gamma' \delta(n), \\
q - 1 &= \beta\delta = \beta\delta' \delta(n), \quad \text{where } \gcd(\gamma', \delta') = 1, \\
g &\quad \text{such that } (g \bmod p) \in S_p \text{ and } (g \bmod q) \in S_q, \\
e_k &= ID_k, \\
s_k &: \text{such that } e_k^{\alpha} \equiv g^{\alpha s_k} \pmod{p}, \\
y_k &: \text{such that } e_k^{\beta} \equiv g^{\beta y_k} \pmod{q}, \\
d_k &\equiv \alpha\beta(\delta' s_k + \gamma' y_k) \pmod{\lambda(n)}, \\
K_{AB} &\equiv e_B^{d_A} \pmod{n}.
\end{aligned}
$$

From Lemma 1, it is easy to see that e_k can be represented

as

$$e_k \equiv r_k g'^{s_k} \pmod{n},$$

where $r_k \in H_n$, $g' \in S_n$ and $s_k = \delta' s_k + \gamma' y_k$. Then, it can be shown that $g' \equiv g^v \pmod{n}$, where $v \equiv (\gamma' + \delta')^{-1} \pmod{\gamma'\delta'}$.

Proof: By powering with $\alpha\beta$ to extinguish r_k, we have

$$\begin{aligned} e_k^{\alpha\beta\delta(n)} &\equiv r_k^{\alpha\beta\delta(n)} g^{v\alpha\beta\delta(n)(\delta' s_k + \gamma' + y_k)} \pmod{n} \\ &\equiv g^{v\alpha\beta\delta s_k} \cdot g^{v\alpha\beta\gamma y_k} \pmod{n} \\ &\equiv \begin{cases} g^{v\alpha\beta\delta s_k} \equiv e_A^{v\alpha\beta\delta} \pmod{p} \\ g^{v\alpha\beta\gamma y_k} \equiv e_A^{v\alpha\beta\gamma} \pmod{q} \end{cases} \end{aligned}$$

Thus, the following relations hold:

$$\begin{aligned} v^{-1} &\equiv \begin{cases} \delta' \pmod{\gamma'} \\ \gamma' \pmod{\delta'} \end{cases}, \\ &\equiv \gamma' + \delta' \pmod{\gamma'\delta'}. \end{aligned}$$

This means that $v \equiv (\gamma' + \delta')^{-1} \pmod{\gamma'\delta'}$. □

Consequently, we have

$$\begin{aligned} K_{AB} &\equiv e_B^{d_A} \equiv r_B^{\alpha\beta s_A} g'^{\alpha\beta s_A s_B} \pmod{n} \\ K_{BA} &\equiv e_A^{d_B} \equiv r_A^{\alpha\beta s_B} g'^{\alpha\beta s_A s_B} \pmod{n}. \end{aligned}$$

In general, $r_B^{\alpha\beta s_A} \not\equiv r_A^{\alpha\beta s_B}$. Consequently, K_{AB} is not always equal to K_{BA} in this scheme.

For example, $\alpha = 23$, $\beta = 13$, $\gamma = 6$, $\delta = 10$, i.e., $p = 139$, $q = 131$, $n = pq = 18209$ and $g = 2$.

$$\begin{aligned} e_A &= 17699, \\ d_A &= 5083, \quad s_A = 4, \quad y_A = 9 \\ e_B &= 7332, \\ d_B &= 7774, \quad s_B = 1, \quad y_B = 7 \\ K_{AB} &\equiv e_B^{d_A} = 16584 \\ K_{BA} &\equiv e_A^{d_B} = 1625 \end{aligned}$$

In this way, it is seen that $K_{AB} \not\equiv K_{BA} \pmod{n}$. It should be noted that $K_{AB}^2 \equiv K_{BA}^2 \equiv 320 \pmod{n}$ holds. Then, this scheme is regarded as a scheme of Type2 of the trivial scheme in which $g^{\alpha\beta}$ is used instead of the maximum generating element g.

4.7 Proposed Scheme

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

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

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

5. Secure and Practical Parameters

In this section, we shall discuss secure and practical parameters of MK2 and MK3.

5.1 Secure parameters

As is described in Section 3., On the condition of the composite number n, $n = pq$ such that $p = 2p' + 1, q = 2q' + 1$ where $\gcd(p', q') = 1$ is required in order to avoid the square-root attack. On the base $g \in S_n$, $-1 \notin \langle g \rangle_n$ is also required to avoid the square-root attack.

5.2 Practical parameters

To realize these schemes in practical, TC need to calculate the discrete logarithm of any element $e \in \mathbb{Z}_n^*$ in a practical time. So, p' and q' need to be factored into some prime factors. However, if the factors are small, it is well known that n can be factored by the $P - 1$ method.

Let

$$\begin{aligned} p - 1 &= 2p_1'^{a_1} p_2'^{a_2} \cdots p_u'^{a_u}, \\ q - 1 &= 2^{b_0} q_1'^{b_1} q_2'^{b_2} \cdots q_v'^{b_v}, \end{aligned}$$

where p_k', q_k' are prime numbers such that $p_1' < p_2' < \cdots < p_u'$, $q_1' < q_2' < \cdots < q_v'$, and a_k, b_k are positive integers, $b_0 \in \{1, 2\}$.

In the $P - 1$ method, if $p \mid K$ and $q \not\mid K$, then

$$p = \gcd(a^K - 1, n) \tag{3}$$

for any base $a \in \mathbb{Z}_n^*$.

At the first stage in the $P - 1$ method, Eq.(3) is usually calculated by using the prepared K such as $K = \prod_{i=1}^{w} P_i^{C_i}$, where P_i is i-th prime number and C_i is an adequate positive integer. It is reasonable to set $C_i = \lfloor \log_2 P_w / \log_2 P_i \rfloor$.

At the second stage, Let $P' = P_{w+1}, A \equiv a^{KP'}$ at the beginning and the A and P' are updated by $A \leftarrow Aa^2 \bmod n, P' \leftarrow P' + 2$ while $P' < P_{w'}$, where $w' > w$. The second stage can factor n when $p - 1$ has only one large prime factor p_u' such that $p_u' < P_{w'}$ and all of other prime factors are less than P_w.

As a special case of $P - 1$ method, we can consider the case $K = P_z!$. This case is implemented as follows: Let $A = a, Q = 2$ at the beginning and the A is updated by $A \leftarrow A^Q \bmod n, Q \leftarrow Q + 1$ while $Q \leqq P_z$. When this K is used, the $P - 1$ method is very strong but it takes much

longer time to execute.

It is reasonably assumed that $P_w < P_z < P_{w'}$. In order to be difficult to factor n by the first stage, $p'_u < P_w$ should be satisfied. In order to be difficult to factor n by the second stage, at least two of p'_k's should be greater than P_w or $p'_u > P_{w'}$ should be satisfied. In order to be difficult to a special case that $K = P_z!$, $p'_u > P_z$ should hold. Consequently, at least two of p'_k's should be greater than P_z, or $p'_u > P_{w'}$ should be satisfied.

So, we shall give several guideline to determine p which is secure and practical as follows:

- Some of p'_ks are small so that it is easy to calculate a discrete logarithm,
- Some of p'_ks have the exponent $a_k \geqq 2$ in order to reduce the database to solve the discrete logarithm,
- At least two of p'_k's are larger than P_z. in order to be secure against both the second stage and when the $K = P_z!$ is used.
- $p'_u > P_{w'}$ should hold in order to be secure against the second stage of the $P-1$ methods.

The q'_k is defined in a similar manner as p'_k.

For example, the following p and q satisfy the conditions.

$$p - 1 = 2p_1'^{a_1} p_2'^{a_2} \cdots p_{u-2}'^{a_{u-2}} p_{u-1}'^{2} p'_u, \tag{4}$$

$$q - 1 = 2^2 q_1'^{b_1} q_2'^{b_2} \cdots q_{v-2}'^{b_{v-2}} q_{v-1}'^{2} q'_v, \tag{5}$$

where $P_z < p'_{u-1} < P_{w'}$ and $p'_k < P_z$ for $k = 1, 2, \ldots, u-2$.

Under present circumstances, the size of P_w, P_z, $P_{w'}$ are respectively considered as 30, 50, 70-bit, as an example.

Of course, the size of n is set to be large enough to be secure against other general factoring method such as the number field sieve method.

6. Conclusions

This paper has discussed the discrete logarithm problem over composite number presented in Ref. [1] again. Also, this paper has reviewed MK2 and clarified the difference between MK2 and other schemes from the standpoint of the security.

It will be necessary in the future to investigate the discrete logarithm problem from a more general viewpoint. We hope that a new security technique will be considered based on this paper.

REFERENCES

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

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

[3] 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).

[4] 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).

[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] 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).

[8] H.Tanaka, "Identity-based non-interactive key sharing equivalent to RSA deciphering," Proc. of the 2005 symposium on cryptography and information security. pp.1135–1140 (2005).

[9] W.Abe, N.Kunihiro and K.Ohta, "Maurer-Yacobi ID-based encryption scheme revisited," Proc. of the 2005 symposium on cryptography and information security. pp.2011–2016 (2005).

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

[11] 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).