# A New ID-Based Key Sharing System

Shigeo TSUJI
Dept. of Electrical and Electronic Eng.
Tokyo Institute of Technology

Jinhui CHAO
Dept. of Electrical and Electronic Eng.
Tokyo Institute of Technology
jchao@ss.titech.ac.jp

## Abstract

Non-interactive ID-based key sharing schemes are convenient in practice since they do not need preliminary communication. However, they are vulnerable to entities conspiracy. This paper proposes a new ID-based non-interactive key sharing scheme with high security against conspiracy of entities.

## 1 Background

This paper addresses the ID information based key sharing systems in secret communication. The ID-based key sharing scheme seems originally appeared in Blom's work [1]. This interesting idea, however, really began to attract a great deal of attention only after Shamir in 1984 proposed explicitly the concept of an ID-based system [2]. Since then, active researches have been observed, especially in Japan, to develop concrete ID-based key sharing schemes.

ID-based key sharing scheme can be categorized into interactive and non-interactive ones. The interactive schemes require preliminary communication between entities before they share their common key [3]. On the other hand, there is no need of any preliminary communication in non-interactive schemes.

In this paper, we consider the non-interactive schemes. Researches have been continuing in this field, which include T.Matsumoto and H.Imai [4], H.Tanaka [5], S.Tsujii et al [6], [7]. T.Harada and N.Matsuzaki [8] etc.. However, the non-interactive schemes suffered from the conspiracy problem. In other words, if a certain number of entities show each other their secrets given by the trusted center, they maybe able to reveal the center secrets or to forge the common secret keys between some other entities. We define "threshold of conspiracy" as the minimum number of entities in order to reveal the center secrets in such way. (Recently, another key distribution method is proposed by Y. Murakami, S.Kasahara [10][11] and a little later by U.M.Maurer and Y.Yacobi [12], which is also discussed in [13] .)

J. Feigenbaum (Ed.): Advances in Cryptology - CRYPTO '91, LNCS 576, pp. 288-299, 1992.

Thus, to find a non-interactive ID-based scheme has been a challenging problem for the researchers in this field.

Despite of extensive efforts on this subject, all the non-interactive schemes proposed so far are unable to extend their threshold beyond the number of secret parameters in the center. Therefore, it has been skeptical about whether there exist schemes without conspiracy threshold.

In this paper, a novel non-interactive key sharing schemes is presented. It is believed to be highly secure in the sense that it is free from the conspiracy problem.

# 2 Center algorithm priori to key sharing

A trusted center prepares four kinds of information, in addition to processing of ID information as followings:

1. Publicized information common to all entities;
2. Center secret information common to all entities;
3. Center secret information for each entity;
4. Entity secret information for key sharing.

## 2.1 ID information pre-processing

The center chooses an one-way function and transforms the $l$-bit ID vectors to $n$-bit random vectors, then publicizes them to all the entities.

$$\begin{aligned} h(\cdot) \quad &: \quad \text{Hash function which converts} l - \text{bit sequence of original} \\ &\quad\;\; \text{ID vector of an entity to a} n - \text{bit random sequence.} \\ \boldsymbol{ID}_A,\ \boldsymbol{ID}_B \quad &: \quad \text{Modified ID vector of entities A and B as images of} \\ &\quad\;\; \text{the original ID vectors of A and B under } h(\cdot). \end{aligned}$$

$$\begin{aligned} \boldsymbol{ID}_A &= (a_1, a_2, \ldots, a_n)^t \quad a_k \in GF(2); \\ \boldsymbol{ID}_B &= (b_1, b_2, \ldots, b_n)^t \quad b_k \in GF(2); \end{aligned}$$

We also need the binary complement of the ID vectors

$$\begin{array}{rcllll} ID_A^c & = & (a_1^c, a_2^c, \ldots, a_n^c)^t & a_k^c: & \text{binary complement of} & a_k; \\ ID_B^c & = & (b_1^c, b_2^c, \ldots, b_n^c)^t & b_k^c: & \text{binary complement of} & b_k. \end{array}$$

## 2.2 Publicized information common to all entities

The center publicizes a composite number $N$, which is determined as follows.

$$\begin{array}{rcrl} N & = & P \cdot Q \cdot R \cdot T & \\ P & = & 2p+1 & \text{80digits (250bit)} \\ Q & = & 2q+1 & \text{80digits (250bit)} \\ R & = & 2r+1 & \text{80digits (250bit)} \\ T & = & 2t+1 & \text{80digits (250bit)} \end{array}$$

Here $P$, $Q$, $R$ and $T$ are Sophie-Germain primes, and $p$, $q$, $r$, $t$ are primes. We assume that it is difficult to factorize $pq$ and $rt$.

## 2.3 Center Secret information common to all entities

The center specifies the following parameters and keeps them for its secrets.

$$\begin{array}{lrcl} (1) & \lambda(N) & = & 2pqrt \\ (2) & \boldsymbol{X}, \boldsymbol{Y} & : & n \times n \quad \text{nonsingular symmetric matrices;} \\ & \boldsymbol{X} & = & (x_{ij}), \quad x_{ij} = x_{ji}, \quad x_{ij} \in \boldsymbol{Z}_{\lambda(N)} \\ & \boldsymbol{Y} & = & (y_{ij}), \quad y_{ij} = y_{ji}, \quad y_{ij} \in \boldsymbol{Z}_{\lambda(N)} \\ & \boldsymbol{x}_i & : & i\text{-th row vector of } \boldsymbol{X}; \\ & \boldsymbol{y}_i & : & i\text{-th row vector of } \boldsymbol{Y}; \\ (3) & g & : & \text{a maximum generator in } \boldsymbol{Z}_N^*; \end{array}$$

Here, $\boldsymbol{Z}_N^*$ stands for the set of the elements in $\boldsymbol{Z}_N$ which are relatively prime to $N$ or the unit group of $\boldsymbol{Z}_N$. The maximum generator is a generator in the unit group of $\boldsymbol{Z}_N$ with the maximum order, or its order equals the Carmichael function $\lambda(N)$.

## 2.4 Center secrets for each entities

For notational simplicity, we define a scalar product operation "$\otimes$" between vectors and vectors with a matrix.

Definition: An exponential-product of a row vector $\boldsymbol{u}$ and a column vector $\boldsymbol{v}$ is defined as

$$\boldsymbol{u} \bigotimes \boldsymbol{v} = \prod_{k=1}^{n} u_k^{v_k} \tag{1}$$

$$\begin{aligned} \text{where} \quad \boldsymbol{v} &= (v_1, \ldots, v_n)^t, \quad v_k \in \boldsymbol{Z} && (2) \\ \boldsymbol{u} &= (u_1, \ldots, u_n), \quad u_k \in \boldsymbol{Z} && (3) \end{aligned}$$

The product of a $n \times n$ matrix $U$ and a column vector $\boldsymbol{v}$ are defined as

$$\begin{aligned} U \bigotimes \boldsymbol{v} &= (\boldsymbol{u}_1 \bigotimes \boldsymbol{v}, \ldots, \boldsymbol{u}_n \bigotimes \boldsymbol{v})^t && (4) \\ &= (\prod_{j=1}^{n} u_{1j}^{v_j}, \ldots, \prod_{j=1}^{n} u_{nj}^{v_j})^t && (5) \\ \text{where} \qquad U &= (\boldsymbol{u}_1^t, \ldots, \boldsymbol{u}_n^t)^t && (6) \\ \boldsymbol{u}_i &= (u_{i1}, \ldots, u_{in}), i = 1, \ldots, n && (7) \end{aligned}$$

are the row vectors of $U$. The center computes the following secrets for each entity, e.g. A;

$$\begin{aligned} (1) \qquad \alpha_{Akj} &\in \boldsymbol{Z}^*_{\lambda(N)} \quad (1 \leq j \leq n, \quad k = 1, 2) && (8) \\ \alpha_{Ak} &= \prod_{j=1}^{n} \alpha_{Akj} \quad \bmod \lambda(N) && (9) \\ c_{Aj} &= (c_{A2}, \ldots, c_{An}), \quad c_{Aj} \in \boldsymbol{Z}^*_{\lambda(N)} && (10) \\ \beta_{Ak1j} &\in \boldsymbol{Z}^*_{\lambda(N)} \quad (2 \leq j \leq n) && (11) \\ & \text{where} \quad \alpha_{A1j}\beta_{A21j} = \alpha_{A2j}\beta_{A11j} && (12) \\ \beta_{Ak2j} &= c_{Aj}\beta_{Ak1j} \quad (2 \leq j \leq n) && (13) \\ \beta_{Aki} &= \prod_{j=1}^{n} \beta_{Akij} \qquad \bmod \lambda(N) && (14) \\ & \text{here } \beta_{Aki1} \text{ are chosen to satisfy} \\ & \alpha_{A1}^{-1}\beta_{A1i} + \alpha_{A2}^{-1}\beta_{A2i} = 0 \quad \bmod \lambda(N) && (15) \\ & \qquad (i = 1, 2 \quad k = 1, 2) \\ (2) \qquad \boldsymbol{s}_{A1} &= (s_{A11}, \ldots, s_{A1n}) && (16) \\ &= (\boldsymbol{X} \otimes \boldsymbol{ID}_A)^T && (17) \\ &= (\prod_{j=1}^{n} x_{1j}^{a_j}, \ldots, \prod_{j=1}^{n} x_{nj}^{a_j}) \quad \bmod \lambda(N) && (18) \\ \boldsymbol{s}_{A2} &= (s_{A21}, \ldots, s_{A2n}) && (19) \\ &= (\boldsymbol{Y} \otimes \boldsymbol{ID}_A)^T && (20) \end{aligned}$$

$$
\begin{aligned}
&= (\prod_{j=1}^{n} y_{1j}^{a_j}, \ldots, \prod_{j=1}^{n} y_{nj}^{a_j}) \quad \bmod \lambda(N) && (21)\\
s_{Aij} &\in Z_{\lambda(N)} && (22)
\end{aligned}
$$

## 2.5 Individual secrets for each entities

The center then delivers to entity A through a secure channel the following individual secret data matrices.

$$
\begin{aligned}
(1) \quad G_{Ak} &= g^{\alpha_{Ak}^{-1}} \qquad (\bmod N) && (23)\\
(2) \quad D_{Ak} &= [\, d_{Ak}(i,j) \,], \quad k = 1,2; \quad i = 1,2; \quad j = 1, \ldots, n && (24)
\end{aligned}
$$

with row vectors as

$$
\begin{aligned}
\boldsymbol{d}_{Ak1} &= (\ d_{Ak}(1,1), \ldots, d_{Ak}(1,n)\ )\\
\boldsymbol{d}_{Ak2} &= (\ d_{Ak}(2,1), \ldots, d_{Ak}(2,n)\ )
\end{aligned}
$$

$$
d_{Ak}(i,j) = 2pq\ \alpha_{Akj}\ s_{Aij} + rt\ \beta_{Akij} \qquad (25)
$$

Notice that $d_{Ak}(i,j)$ is not computed with modulo arithmetics, e.g. mod $\lambda(N)$, but with the arithmetics over the integer ring. This is required in order to keep $\lambda(N)$ secret as explained in section 5. Thus $d_{Ak}(i,j)$ may take larger values. The increase of the length, however, is no more than twice, so it will cause little problem when fast modular exponentiation algorithms are used.

# 3 Common Key Generation

When key sharing is required between entity A and B, A computes the following parameter (we call it the key kernel) over the integer ring $\boldsymbol{Z}$, (since the Carmichael function is unknown for all entities).

$$
\begin{aligned}
H_{ABk} &= (\boldsymbol{d}_{Ak1} \bigotimes \boldsymbol{ID}_B) \cdot (\boldsymbol{d}_{Ak2} \bigotimes \boldsymbol{ID}_B^c)\\
&= \prod_{j=1}^{n} d_{Ak}(1,j)^{b_j} \prod_{j=1}^{n} d_{Ak}(2,j)^{b_j^c} && (26)
\end{aligned}
$$

and calculates the key to entity B as

$$
K_{AB} = G_{A1}^{H_{AB1}} \cdot G_{A2}^{H_{AB2}} \quad \bmod N. \qquad (27)
$$

At the same time, B calculates also his key kernel over the integer ring $\boldsymbol{Z}$

$$
H_{BAk} = (\boldsymbol{d}_{Bk1} \bigotimes \boldsymbol{ID}_A) \cdot (\boldsymbol{d}_{Bk2} \bigotimes \boldsymbol{ID}_A^c) \qquad (28)
$$

and the key to entity A

$$K_{BA} = G_{B1}^{H_{BA1}} \cdot G_{B2}^{H_{BA2}} \quad \mathrm{mod}\ N. \tag{29}$$

We note that the key kernels for A and B are not the same. However, we will show that the keys produced from the key kernels between A and B are equal. Since

$$\begin{aligned} H_{ABk} &= (2pq)^n \alpha_{Ak} S_{AB} + \prod_{j=1}^{n} rt\beta_{Akb_jj} + l\lambda(N) \\ &= (2pq)^n \alpha_{Ak} S_{AB} + (rt)^n \beta_{ABk} + l\lambda(N) && (30) \\ \text{Here,}\quad \beta_{ABk} &:= \prod_{j=1}^{n} \beta_{Akb_jj} && (31) \\ S_{AB} &= s_{A1} \bigotimes \boldsymbol{ID}_B \cdot s_{A2} \bigotimes \boldsymbol{ID}_B^c \\ &= (\boldsymbol{X} \bigotimes \boldsymbol{ID}_A)^t \bigotimes \boldsymbol{ID}_B \cdot (\boldsymbol{Y} \bigotimes \boldsymbol{ID}_A^c)^t \bigotimes \boldsymbol{ID}_B^c \\ &= \prod_{i=1}^{n} \prod_{j=1}^{n} x_{ij}^{b_i a_j} \prod_{i=1}^{n} \prod_{j=1}^{n} y_{ij}^{b_i^c a_j^c} \quad \mathrm{mod}\ \lambda(N), && (32) \end{aligned}$$

As shown at the end of this section, entity A will exponentiate $d_{Ak}(i,j)$ to $G_{Ak}$ to calculate $K_{ABk}$. The last term in Eq.(31) will vanish during these processes despite that A does not know $\lambda(N)$. In the sequel,

$$\begin{aligned} K_{ABk} &= G_{Ak}^{H_{ABk}} \\ &= g^{\alpha_{Ak}^{-1}[\alpha_{Ak}(2pq)^n S_{AB} + (rt)^n \beta_{ABk}]} \\ &= g^{[(2pq)^n S_{AB} + \alpha_{Ak}^{-1} \beta_{ABk} (rt)^n]} \qquad (\mathrm{mod}\ N) && (33) \\ K_{AB} &= G_{A1}^{H_{AB1}} \cdot G_{A2}^{H_{AB2}} \\ &= g^{[(2pq)^n S_{AB} + \alpha_{A1}^{-1} \beta_{AB1} (rt)^n]} \\ &\quad \cdot g^{[(2pq)^n S_{AB} + \alpha_{A2}^{-1} \beta_{AB2} (rt)^n]} \\ &= g^{[2(2pq)^n S_{AB} + (\alpha_{A1}{}^{-1} \beta_{AB1} + \alpha_{A2}{}^{-1} \beta_{AB2})(rt)^n]} \\ &= g^{2(2pq)^n S_{AB}} \qquad (\mathrm{mod}\ N), && (34) \end{aligned}$$

The last equality is derived as follows. We assume $b_1 = 1$, but we can prove it by the same way in the case of $b_1 = 0$. Since

$$\beta_{AB1} = \beta_{A11} \cdot \prod_{j=2}^{n} c_{Aj}{}^{b_j^c}, \qquad \beta_{AB2} = \beta_{A21} \cdot \prod_{j=2}^{n} c_{Aj}{}^{b_j^c}$$

$$\begin{aligned} \text{Thus}\quad \alpha_{A1}{}^{-1}\beta_{AB1} + \alpha_{A2}{}^{-1}\beta_{AB2} &= (\alpha_{A1}{}^{-1}\beta_{A11} + \alpha_{A2}{}^{-1}\beta_{A21}) \prod_{j=2}^{n} c_{Aj}{}^{b_j^c} \\ &= 0 \quad \mathrm{mod}\ \lambda(N) \end{aligned}$$

due to the condition equation (15).

On the other hand,

$$\begin{aligned}
H_{BAk} \quad (\text{mod } \lambda(N)) &= (2pq)^n \alpha_{Bk} S_{BA} + \prod_{j=1}^{n} rt\beta_{Bka_jj} \\
&= (2pq)^n \alpha_{Bk} S_{BA} + (rt)^n \beta_{BAk} \quad \text{mod } \lambda(N) && (35) \\
S_{BA} &= s_{B1} \bigotimes \boldsymbol{ID}_A \cdot s_{B2} \bigotimes \boldsymbol{ID}^c_A \\
&= (\boldsymbol{X} \bigotimes \boldsymbol{ID}_B)^t \bigotimes \boldsymbol{ID}_A \cdot (\boldsymbol{Y} \bigotimes \boldsymbol{ID}^c_B)^t \bigotimes \boldsymbol{ID}^c_A \\
&= \prod_{i=1}^{n} \prod_{j=1}^{n} x_{ij}^{a_i b_j} \prod_{i=1}^{n} \prod_{j=1}^{n} y_{ij}^{a^c_i b^c_j} \quad \text{mod } \lambda(N), && (36) \\
& && (37)
\end{aligned}$$

$$\begin{aligned}
K_{BA} &= G_{B1}^{H_{BA1}} \cdot G_{B2}^{H_{BA2}} \\
&= g^{[2(2pq)^n S_{BA} + (\alpha_{B1}{}^{-1}\beta_{BA1} + \alpha_{B2}{}^{-1}\beta_{BA2})]} \\
&= g^{2(2pq)^n S_{BA}} \qquad (\text{mod } N), && (38)
\end{aligned}$$

Considering that $\boldsymbol{X}$ and $\boldsymbol{Y}$ are symmetric, $(x_{ij} = x_{ji})$, $(y_{ij} = y_{ji})$,

$$\begin{aligned}
S_{AB} &= S_{BA} \qquad \text{mod } \lambda(N) && (39) \\
\text{thus,} \quad K_{AB} &= K_{BA} \qquad \text{mod } N && (40)
\end{aligned}$$

is obviously satisfied.

In fact, the entities have no knowledge of $\lambda(N)$. Thus, entity A can only compute the exponent of $K_{ABk}$, $\prod_{j=1}^{n} d_{Ak}(1,j)^{b_j} \prod_{j=1}^{n} d_{Ak}(2,j)^{b^c_j}$ over the integer ring, which may result in some very large number. A practical way for entity A to obtain $K_{AB}$ is as follows. Notice that $g^{\lambda(N)} = 1$ mod $N$, then we can calculate

$$K_{ABk} = ((((G_{A1}^{d_{Ak}(1,1)^{b_1}})^{d_{Ak}(2,1)^{b^c_1}})^{d_{Ak}(1,2)^{b_2}})^{d_{Ak}(2,2)^{b^c_2}})^{\cdots\cdots} \quad \text{mod } N$$

# 4 A Working Example

The following dummy example will facilitate the understanding of the above scheme. For simplicity, no large prime factors are included in $N$. First the center prepares the following parameters.

Let $n = 3$,

$$\begin{aligned}
\boldsymbol{ID}_A &= (1,0,1)^t \\
\boldsymbol{ID}_B &= (0,1,1)^t \\
N &= 5 \cdot 7 \cdot 11 \cdot 23 = 8855 \\
\lambda(N) &= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 11 = 660 \\
g &= 17 \\
\boldsymbol{X} &= \begin{pmatrix} 29 & 23 & 7 \\ 23 & 13 & 17 \\ 7 & 17 & 19 \end{pmatrix} \\
\boldsymbol{Y} &= \begin{pmatrix} 29 & 7 & 17 \\ 7 & 19 & 31 \\ 17 & 31 & 13 \end{pmatrix}
\end{aligned}$$

The center secrets for entities A and B are set as

$$\begin{array}{rcl@{\qquad\qquad}rcl}
s_{A1} & = & (203, 391, 133) & s_{B1} & = & (13, 17, 11) \\
s_{A2} & = & (493, 217, 221) & s_{B2} & = & (29, 29, 23) \\
\boldsymbol{c}_A & = & (7, 19) & \boldsymbol{c}_B & = & (13, 17) \\
\boldsymbol{\alpha}_{A_1} & = & (29, 17, 31) & \boldsymbol{\alpha}_{B_1} & = & (161, 221, 323) \\
\boldsymbol{\alpha}_{A_2} & = & (13, 19, 23) & \boldsymbol{\alpha}_{B_2} & = & (117, 589, 403) \\
\alpha_{A1} & = & 143 & \alpha_{B1} & = & 133 \\
{\alpha_{A1}}^{-1} & = & 487 & {\alpha_{B1}}^{-1} & = & 397 \\
\alpha_{A2} & = & 401 & \alpha_{B1} & = & 557 \\
{\alpha_{A2}}^{-1} & = & 581 & {\alpha_{B1}}^{-1} & = & 173
\end{array}$$

$$\begin{array}{rcl@{\qquad\qquad}rcl}
\boldsymbol{\beta}_{A_{11}} & = & (29, 19, 23) & \boldsymbol{\beta}_{B_{11}} & = & (13, 19, 29) \\
\boldsymbol{\beta}_{A_{12}} & = & (31, 463, 437) & \boldsymbol{\beta}_{B_{12}} & = & (37, 247, 493) \\
\boldsymbol{\beta}_{A_{21}} & = & (29, 17, 13) & \boldsymbol{\beta}_{B_{21}} & = & (29, 23, 19) \\
\boldsymbol{\beta}_{A_{22}} & = & (361, 119, 247) & \boldsymbol{\beta}_{B_{12}} & = & (381, 299, 323)
\end{array}$$

Also, the center delivers the following individual data to the entity A.

$$\begin{aligned}
G_{A1} &= 7213 \\
G_{A2} &= 5397 \\
\boldsymbol{D}_{A1} &= \begin{pmatrix} 72239 & 80809 & 50741 \\ 173269 & 69733 & 106247 \end{pmatrix}
\end{aligned}$$

$$\boldsymbol{D}_{A2} = \begin{pmatrix} 33263 & 90083 & 37423 \\ 96763 & 56021 & 74581 \end{pmatrix}$$

Based on these data and the ID information of entity B, entity A calculates the key kernel and $K_{AB}$,

$$\begin{aligned} H_{ABk} &= (2pq)^3 \alpha_{Ak} x_{21} x_{23} x_{31} x_{33} y_{12} + (rt)^3 \prod_{j=1}^{3} \beta_{Akb_j j} && (41) \\ K_{AB} &= g^{(2pq)^3 x_{21} x_{23} x_{31} x_{33} y_{12}} \quad \bmod 8855 && (42) \end{aligned}$$

At the same time, entity B receives his individual data matrix

$$\begin{aligned} G_{B1} &= 822 \\ G_{B2} &= 4352 \\ \boldsymbol{D}_{B1} &= \begin{pmatrix} 56743 & 62041 & 75239 \\ 43447 & 176149 & 118999 \end{pmatrix} \\ \boldsymbol{D}_{B2} &= \begin{pmatrix} 42619 & 51653 & 113449 \\ 30951 & 150737 & 158009 \end{pmatrix} \end{aligned} \quad .$$

Entity B then calculates the key kernel and key to entity A as

$$\begin{aligned} H_{BAk} &= (2pq)^3 \alpha_{Bk} x_{12} x_{13} x_{32} x_{33} y_{21} + (rt)^3 \prod_{j=1}^{3} \beta_{Bka_j j} && (43) \\ K_{BA} &= g^{(2pq)^3 x_{12} x_{13} x_{32} x_{33} y_{21}} \quad \bmod 8855 && (44) \end{aligned}$$

Note the second terms in $H_{AB}$ and $H_{BA}$ are eliminated during generation process of common keys in the sequel. Thus, the common key

$$K_{AB} = K_{BA} = 246 \qquad \bmod 8855 \qquad (45)$$

is obtained between A and B.

# 5 Security Consideration Against Conspiracy

## 5.1 Condition required to break the scheme

We consider the conditions for a conspired group of entities to attack any particular entity X or to forge the common keys between X and other entities.

In fact, among the center secrets, $\boldsymbol{X}$, $\boldsymbol{Y}$ and $\lambda(N) = 2pqrt$, only $rt$ may be revealed under the following conspiracy attacks.

Suppose that a conspiracy group consists of three members A,B,C. They can produce key kernels $H_{AB}, H_{BC}, H_{CA}$ by simulating the key sharings between A and B, B and C, also C and A. This circle of key sharings can also be formed in the reverse order, when the conspirators have $H_{AC}, H_{CB}, H_{BA}$. If they took the products of each triples of the key kernels, the difference $H_{AB}H_{BC}H_{CA} - H_{AB}H_{BC}H_{CA}$ will be a multiple of $rt$. By choice of several different triples of conspirators to obtain more multiples of $rt$, the $rt$ can be found as the GCD of these quantities. (We sometime call these kinds of attack as "loop attack").

Once the $rt$ is revealed, each conspirator Z can know about $pq\alpha_{Zkj}S_{Zij}$ (mod $rt$) by taking modulo $rt$ on $d_{Zk}(i,j)$. By solving a system of linear equations, $\boldsymbol{X}$, $\boldsymbol{Y}$ (mod $rt$) and $pq$ (mod $rt$) can also be obtained.

However, to forge the common keys of entity X requires values of $p, q$ or $\lambda(N)$, which cannot be derived from $pq$ (mod $rt$). In conclusion, the integrity of the proposed scheme lies on the difficulty to find $\lambda(N)$ .

## 5.2 Consideration on the Carmichael function

Now we address the possibility of revealing Carmichael function $\lambda(N)$ or $pq$ in the following three situations.

First, we suppose that entity A tries to find $pq$ or $\lambda(N)$ from its individual data matrices $\boldsymbol{D}_{Ak}$. Notice that the first and second terms of

$$d_{Ak}(i,j) = pq\alpha_{Akj}S_{Aij} + rt\beta_{Akij}$$

contain different parameters at different rows and columns, no one can eliminate the second terms in $d_{Ak}(i,j)$ in order to reach the first terms which contains $pq$.

Besides, these quantities are calculated over the integer ring without any modulo $\lambda(N)$ operations involved. Therefore, it is impossible to fabricate two different integers which are congruent modulo $\lambda(N)$. i.e., $\lambda(N)$ cannot be found by a single entity himself.

Also, the parameters in each elements of the individual data matrices are distinct for different entities. Thus, even a number of entities conspired together, there is no way to find $pq$, since the system of equations to solve these parameters always contain more unknowns than the number of the equations.

Secondly, we assume the attack is conducted by A using its key kernels to a group of entities B, C, D, $\cdots, H_{AB}, H_{AC}, H_{AD}, \cdots$. Since the second term in

$$H_{AB} = (2pq)^n \alpha_A S_{AB} + (rt)^n \beta_{ABk} + l\lambda(N)$$

is also different for different pairs of entities, it can not be removed by subtraction. Thus, the information on $pq$ will not be separated out.

Besides, numerous entities, e.g. A, B, C may conspire together by using their key kernels to implement a loop attack. If the products such as $H_{AB}H_{BC}H_{CA}$ and $H_{AC}H_{CB}H_{BA}$ had same values over $Z_{\lambda(N)}$, or congruent modulo $\lambda(N)$, they would reveal $\lambda(N)$. In our setting, however, $H_{AB}H_{BC}H_{CA}$ and $H_{AC}H_{CB}H_{BA}$ always have different values, thus nothing about $\lambda(N)$ can be revealed.

Thirdly, we consider the situations when the conspired entities show each others their common keys, e.g. $K = g^{(2pq)^n S_{AB}} \bmod N$,etc. Since the discrete logarithm problem is computationally difficult, and factorization of N are unknown to them, the scheme will remain secure under such attacks.

# 6 Conclusion

We have shown a new ID-based non-interactive key sharing scheme. It is designed to clear out all kinds of approaches used until now to break out the center secrets or implement attack to an arbitrary entity in existing non-interactive ID-based schemes. Thus, it is considered to be highly secure against the conspiracy attacks by any group of entities.

**Acknowledgment:** The authors wish to thank for Professor Hatsukazu Tanaka of Kobe University for stimulating discussions with him, and Mr. Genichi Nishio of Tokyo Institute of Technology for his helpful suggestions.

# References

[1] R. Blom " Non-public key distribution," Proceeding of Crypto'82, pp.231-236, 1982.

[2] A. Shamir "Identity-based cryptosystem and signature scheme," Proceeding of Crypto'84, pp.47-53, 1984.

[3] E. Okamoto, K. Tanaka " Key distribution system based on identification information," IEEE Journal on Selected Areas in Communications, Vol.7, No.4, pp.481-485, May, 1989.

[4] T. Matsumoto, H. Imai " On the key predistribution system: A practical solution to the key distribution problem ," Proceeding of Crypto'87, pp.185-193, 1987.

[5] H. Tanaka, " A realization scheme for the identity-based cryptosystem," Proceeding of Crypto'87, pp.340-349, 1987.

[6] S. Tsujii, T.Itoh, " ID-based cryptosystem based on the discrete logarithm problem," IEEE Journal on Selected Areas in Communications, Vol.7, No.4, pp.467-473, May, 1989.

[7] S. Tsujii, T.Itoh, " ID-based cryptosystem using discrete logarithm problem," *Electronics Letters*, Vol.23, No.24, pp.1318-1320, Nov. 1987. May, 1989.

[8] . Harada, Matsuzaki "An ID-based key sharing scheme without preliminary communication," IEICE Japan Tech. Rep. ISEC89-38, Dec. 1989

[9] H. Tanaka "Identity-based non-interactive common- information generation and its application to cryptosystems," Proceeding of Symposium on Cryptography and Information Security, SCIS91, Japan, Dec. 1990.

[10] Y. Murakami, S. Kasahara "An ID-based key distribution system," IEICE Japan Tech. Rep. ISEC90-26, Sept. 1990.

[11] Y. Murakami, S. Kasahara "The discrete Logarithm problem under a composite modulus," IEICE Japan Tech. Rep. ISEC90-42, Dec. 1990.

[12] U. M. Maurer, Y. Yacobi "Non-interactive public key cryptography," Proceeding of EUROCRYPT'91, 1991.

[13] T.Matsumoto, H.Imai "On the security of some key sharing schemes (Part 2)" IEICE Japan Tech. Rep. ISEC90-28, 1990.