On Chikazawa-Inoue ID based key system

Bae Eun Jung[1] and Hee Jean Kim[2]

Samsung Advanced Institute of Technology

14-1 Nongseo-dong, Yongin-si, 449-712, KOREA

E-mail: {be.jung[1], heejean.kim[2]}@samsung.com

Abstract

In this paper, we show that Chikazawa-Inoue ID-based key system is insecure by collusion, where Chikazawa-Inoue ID-based key system means the key parameters established during the initiation phase. We describe an algorithm factorizing a public key of Trust Center. Since our attack is based on only the key system and has no relation with specific key sharing protocols, it can be applied to all variant protocols of Chikazawa-Inoue ID based key sharing protocol. From this analysis, we obtain conclusions that Chikazawa-Inoue ID-based key system cannot be used any more for any application protocols, which means that our result puts an end to discussion of related key sharing protocols.

1 Introduction

In 1990, since Chikazawa and Inoue proposed a new ID based key sharing system for secure communication among multiple users, there have been some publications showing and improving the security flaws of Chikazawa-Inoue ID based key sharing protocols. Chikazawa-Inoue ID based key sharing protocol consists of two parts. The first part is the initiation phase that Trusted Center(TC) sets up parameters and permanent keys of each entity. The second part is a key sharing procedure for secure group communication [1]. They also proposed another Chikazawa-Inoue ID based cryptosystem [2]. The key sharing protocol in [1] and the cryptosystem in [2] are based on the same system parameters. For simplicity, the system parameters established during the initiation phase is called Chikazawa-Inoue ID based key system. In [1] and [2], the authors stated that it is impossible for any number of users to conspire because the security of the system is based on the difficulty of both factoring a large number and computing discrete logarithms over large finite fields.

However, Simbo and Kawamura showed that two participants can reveal another participant's secret key by collusion [3]. The attack in [3] is based on the key sharing protocol, i.e., they showed that the weakness was caused by key sharing procedures. Until now, it has been assumed that Chikazawa-Inoue ID based key system is secure and some key sharing protocols based on it have been proposed, analyzed and improved [4], [5], [6], [7] and [8].

In this paper, we show that the basic key system is insecure by collusion attack independently of key sharing protocols. So, we obtain the result that key sharing schemes and cryptosystem using the Chikazawa-Inoue ID based key system are also insecure.

2 Review of Chikazawa-Inoue ID based key system

Since we show that the key system is not secure as a cryptographic system, we briefly state parameters and keys of Chikazawa-Inoue ID based key system.

The trusted center (TC) selects two large prime numbers p and q, selects an arbitrary prime number e and generates an integer d such that $N = pq$, $L = lcm(p-1, q-1)$ and $ed = 1 \mod L$, where $lcm(p-1, q-1)$ denotes the least common multiple of $p-1$ and $q-1$. TC also selects an integer g that is a primitive root modulo p and modulo q, then TC generates $n-$dimensional vectors A and G as follows;

$$A = (a_1, a_2, \ldots, a_n), \text{where } 2 \leq a_i \leq L-1, (1 \leq i \leq n),$$

$$G = (g^{a_1} \mod N,\ g^{a_2} \mod N,\ \ldots,\ g^{a_n} \mod N).$$

A one-to-one one-way function f is used to convert a user U_i's identification information ID_i into an $n-$dimensional binary vector

$$f(ID_i) = (y_{i1}, y_{i2}, \ldots, y_{in}), y_{il} \in \{0, 1\} (1 \leq l \leq n).$$

Next, for each user U_i, TC calculates (u_i, v_i, s_i) satisfying

$$u_i \equiv A \cdot f(ID_i) \mod L,$$

$$u_i \cdot v_i \equiv 1 \mod L,$$

$$s_i \equiv {ID_i}^d \mod N.$$

Then TC keeps (p, q, L, A, d, u_i) as secret information, sends (s_i, v_i) to each user U_i over a secure channel and publishes $(N, g, f(\cdot), G, e)$ to all users. Here, G is used in the stage of key sharing protocol and (s_i, v_i) is the permanent secret key of a user U_i.

Remark. Since L is not a prime number, there might be u_i such that $\gcd(u_i, L) \neq 1$, where $\gcd(x, y)$ denotes the greatest common divisor of x and y. So, it should be described how to design f and how to choose a_i in order to make arbitrary u_i have its multiplicative inverse. However, we do not deal with it in this paper because we show that the key scheme is insecure even though the step is made up.

3 On the security of Chikazawa-Inoue ID based key system

We need the following well-known lemma to prove our theorem.

Lemma 1 *Let $N = pq$ and $L = lcm(p-1, q-1)$, where p and q are relatively prime numbers. Then $g^L \equiv 1 \mod N$ for all $g \in \mathbb{Z}_N^*$.*

Proof Since $g \in \mathbb{Z}_N^*$, $\gcd(g, N) = 1$. So, we have $\gcd(g, p) = 1$ and $\gcd(g, q) = 1$. Then, $g^{p-1} \equiv 1 \mod p$ and $g^{q-1} \equiv 1 \mod q$. By definition of L, we have $g^L \equiv 1 \mod p$ and $g^L \equiv 1 \mod q$, it means that $p|(g^L - 1)$ and $q|(g^L - 1)$. Since p and q are relatively prime numbers, $pq|(g^L - 1)$. Therefore $g^L \equiv 1 \mod N$. □

Now we have the following theorem.

Theorem 1 *In Chikazawa-Inoue ID based key system, arbitrary $n+1$ participants can efficiently factorize N by the following algorithm.*

1. *Compute non zero vector*

$$(c_1, c_2, \ldots, c_{n+1})$$

such that

$$c_1 f(ID_1) + c_2 f(ID_2) + \cdots + c_{n+1} f(ID_{n+1}) = (0, \ldots, 0).$$

2. *Let*

$$v = \sum_{i=1}^{n+1} c_i \Big(\prod_{j=1, j\neq i}^{n+1} v_j \Big) \mod N$$

and compute t and k such that $v = 2^t k$, where $t \geq 1$ and k is odd.

3. *Attackers repeat the following step; Choose an element $\hat{g} \in \mathbb{Z}_N^*$ randomly, then compute $x = \hat{g}^{v/2^j} \mod N$ and $y = \gcd(x-1, N)$ for $j = 1, \ldots, t$. If $y \neq 1$ and $y \neq N$, then y is p or q.*

Proof Since $f(ID_i)$ is an $n-$dimensional binary vector, any $n+1$ vectors are linearly dependent. So, there are many solutions $(c_1, c_2, \ldots, c_n, c_{n+1})$, where $c_i \in Z$ such that

$$\sum_{i=1}^{n+1} c_i f(ID_i) = (0, \ldots, 0).$$

It is not difficult to solve such $(c_1, \ldots, c_{n+1})$. Also, by definition of v_i, for each i, we have the equation

$$c_i(A \cdot f(ID_i))v_i \equiv c_i \mod L.$$

So, for each i, we obtain

$$c_i(A \cdot f(ID_i))(\prod_{j=1}^{n+1} v_j) \equiv c_i \prod_{j=1, j\neq i}^{n+1} v_j \mod L.$$

Then if we sum left sides of $n+1$ equations, we have

$$\begin{aligned}
&\sum_{i=1}^{n+1}((c_i(A \cdot f(ID_i))(\prod_{j=1}^{n+1} v_j)) \\
&= (\prod_{j=1}^{n+1} v_j) \sum_{i=1}^{n+1}(c_i(A \cdot f(ID_i)) \\
&= (\prod_{j=1}^{n+1} v_j)(A \cdot (\sum_{i=1}^{n+1} c_i f(ID_i)) \\
&= (\prod_{j=1}^{n+1} v_j)(A \cdot (0, \ldots, 0)) \\
&= 0.
\end{aligned}$$

On the other hand, if we sum right sides of $n+1$ equations, we have

$$\sum_{i=1}^{n+1}(c_i \prod_{j=1, j\neq i}^{n+1} v_j) \mod L.$$

Even though the participants have no knowledge about A, they can obtain the following relation of v_i

$$\sum_{i=1}^{n+1}(c_i \prod_{j=1, j\neq i}^{n+1} v_j) \equiv 0 \mod L.$$

It is well-known that if one knows e and d such that $ed = 1 \mod \phi(N)$, he/she can factorize N. Now, we complete our proof similarly to the proof described in [9]. If we let

$$v = \sum_{i=1}^{n+1}(c_i \prod_{j=1, j\neq i}^{n+1} v_j),$$

then v is multiple of L. Also, since L is even, we can represent v as $2^t \cdot k$ with $t \geq 1$ and odd k.

On the other hand, since $\hat{g}$ is from $\mathbb{Z}_N^*$, by Lemma 1

$$\hat{g}^L \equiv 1 \mod N.$$

So, we have

$$\hat{g}^v \equiv 1 \mod N.$$

Therefore, $\hat{g}^{v/2}$ is a square root of unity modulo N. By Chinese Remainder Theorem, there are four square roots of unity modulo $N = pq$. Two of these square roots are ± 1. The other two are $\pm x$, where x satisfies $x \equiv 1 \mod p$ and $x \equiv -1 \mod q$. Using either one of these last two square roots, one can reveal the factorization of N by computing $\gcd(x-1, N)$. If $\hat{g}$ is chosen at random from $\mathbb{Z}_N^*$, then with probability at least $1/2$, one of the elements in the sequence $\hat{g}^{v/2}, \hat{g}^{v/4}, \ldots, \hat{g}^{v/2^t} \mod N$ is a square root of unity that reveals the factorization of N. $\square$

4 Conclusions

In this paper, we have showed that Chikazawa-Inoue ID based key system is not secure. If at most $n+1$ participants collude, they can reveal the TC's secret key. We have presented the algorithm that finds out relations of user's secret information v_i used in collusion attack. Since attackers use only public information $f(ID_i)$ to obtain the relations, it is not difficult to choose the participants needed in attack.

Since the attack method is based on only the basic key system, we conclude that key sharing protocols and cryptosystems defined over Chikazawa-Inoue ID based key system are also insecure.

References

[1] T. Chikazawa and T. Inoue, *A new key sharing system for global telecommunications,* in Proc. Globecom'90, (1990) 1069–1072.

[2] T. Chikazawa and T. Inoue, *An Identity-based Cryptosystem without entities' consipiring,* IEEE International Symposium on Information Theory, (1991) 129.

[3] A. Simbo and A. Kawamura, *Cryptanalysis of several conference key distribtuion systems,* in Proc. Asiacrypt'91, (1991) 265–276.

[4] T. Chikazawa and A. Yamagishi, *An improved Identity-based one-way conference key sharing system,* Singapore ICCSllSlTA '92, (1992) 270–273.

[5] T. Chikazawa and A. Yamagishi, *Improvement of Chikazawa-Tamagishi identity-based key sharing system for a multiaddress communication,* Electron. Lett., vol. 28, no. 11, (1992) 1015–1017.

[6] B. Jung, *On the forward secrecy of chikazawa-Yamagishi ID-based key sharing scheme,* IEEE Comm.Lett., vol. 8, no. 2, (2004) 114–115.

[7] K. Shim, *Some attacks on Chikazawa-Yamagishi ID-based key sharing scheme,* IEEE Comm.Lett., vol. 7, no. 3, (2003) 145–147.

[8] Y. Tseng and J. Jan, *Improvement of Chikazawa-Tamagishi ID-based key sharing system,* Electron. Lett., vol. 34, no. 12, (1998) 1221–1222.

[9] D. Boneh, *Twenty Years of Attacks on the RSA Cryptosystem,* Notices of the AMS, (1999) 203–213.