JSIAM Letters Vol.2 (2010) pp.5–8 ©2010 Japan Society for Industrial and Applied Mathematics JSIAM Letters

An ID-based key sharing scheme based on discrete logarithm problem over a product of three primes

Yasuyuki Murakami[1] and Masao Kasahara[2]

Department of Telecommunications and Computer Networks, Faculty of Information and Communication Engineering, Osaka Electro-Communication University, 18-8, Hatsu-cho, Neyagawa-shi, Osaka 572-8530, Japan[1]
Faculty of Informatics, Osaka Gakuin University, 2-36-1, Kishibe minami, Suita-shi, Osaka 564-8511, Japan[2]

E-mail *yasuyuki@isc.osakac.ac.jp*

Received November 2, 2009, Accepted December 30, 2009

Abstract

In 1990, the present authors proposed the first ID-based non-interacrive key sharing scheme (ID-NIKS) based on the discrete logarithm problem (DLP) over a composite number n. With a rapid progress of computer system for the last two decades, ID-NIKS based on DLP over n would have more chance to be applied practically. However, there existed no secure ID-NIKS based on DLP over n against the square-root attack when n is a product of three prime numbers. In this paper, we propose an ID-NIKS based on DLP over a product of three prime numbers which can circumvent the square-root attack.

Keywords ID-based cryptosystem, non-interactive key sharing, discrete logarithm problem, factoring problem

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

The discrete logarithm problem (DLP) has been 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 the discrete logarithm does not necessarily exist. Hereinafter we shall denote DLP over a composite number n by DLP(n).

In Sept. 1990, the present authors firstly discussed DLP over composite number and presented an ID-based non-interactive key sharing scheme (ID-NIKS) referred to as MK1 [2]. In Dec. 1990, they presented an improved version of MK1, referred to as MK2 [3]. In 1991, Maurer and Yacobi presented a scheme referred to as MY [4], which is similar to our scheme, MK1. Maurer and Yacobi proposed improved versions of their scheme later [5, 6]. All of these schemes can be regarded as a generalized version of Diffie-Hellman key sharing scheme using ID as a public key. Unfortunately these schemes except MK2 cannot circumvent the square-root attack as was discussed in [7]. In MK2, a product of two prime numbers is used as the modulus n.

With a rapid progress of computer system for the last two decades, ID-NIKS based on DLP over a composite modulus 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 a composite modulus n [8]. They suggested that the modulus n should be a product of three prime numbers in MY for a practical realization. Their suggestion is very interesting. However, unfortunately, their suggestion could not be successful at that time, because there existed no secure ID-NIKS using DLP(n) against the square-root attack for the case where n is a product of three prime numbers. From the practical viewpoint, it is very important to construct a secure scheme against the square-root attack when using a product of three prime numbers as the modulus n.

In this paper, we shall firstly discuss in detail the discrete logarithm problem over n in the case where n is a product of three prime numbers. We give the conditions that are required for designing ID-NIKS over DLP(n). We also show that, for an arbitrary element e such that $(e/n) = 1$, either e or $-e$ has the discrete logarithm over n under the proposed conditions. We then present a new ID-NIKS based on DLP(n) over a product of three prime numbers which can circumvent the square-root attack.

2. Preliminaries

2.1 Definitions

Several definitions are given first.

Definition 1 *Additive group $\mathbb{Z}_n$, and multiplicative group $\mathbb{Z}_n^*$ and $\mathbb{Z}_n^\sharp$ are defined as follows:*

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\},$$
$$\mathbb{Z}_n^* = \{x \mid x \in \mathbb{Z}_n, \gcd(x, n) = 1\},$$
$$\mathbb{Z}_n^\sharp = \left\{x \;\middle|\; x \in \mathbb{Z}_n^*, \left(\frac{x}{n}\right) = 1\right\},$$

where (x/n) denotes the Jacobi symbol.

Definition 2 *The cyclic multiplicative group generated by $g \in \mathbb{Z}_n^*$ is denoted by $\langle g \rangle_n$. That is, the cyclic multiplicative group $\langle g \rangle_n$ for an arbitrary element $g \in \mathbb{Z}_n^*$ is represented as follows:*

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

where $\mathbb{Z}$ denotes the integer set.

Definition 3 *The maximum generator etc., are defined as follows:*

$\varphi(n)$**:** *Euler function i.e. the order of $\mathbb{Z}_n^*$,*
$\mathrm{ord}_n(a)$**:** *the minimum positive integer e, which is called the order, such that $a^e \equiv 1 \pmod{n}$ for an integer a,*
$\lambda(n)$**:** *Carmichael function of n i.e, $\max\{\mathrm{ord}_n(a) \mid a \in \mathbb{Z}_n^*\}$,*
*Maximum generator***:** *elements of order $\lambda(n)$ in $\mathbb{Z}_n^*$,*
S_n**:** *the set of maximum generators in $\mathbb{Z}_n^*$.*

2.2 DLP over composite number n

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

As is well known, the multiplicative group $\mathbb{Z}_n^*$ is a cyclic multiplicative group only when n is 2, 4, an 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 generator is used instead of the primitive element.

Let us consider the following relation,

$$y \equiv g^x \pmod{n}, \tag{1}$$

for $g \in S_n$. In general, for any $x \in \mathbb{Z}_{\lambda(n)}$ there exists $y \in \mathbb{Z}_n^*$ satisfying (1). However, it is not always true that, for any $y \in \mathbb{Z}_n^*$ there exists $x \in \mathbb{Z}_{\lambda(n)}$ satisfying (1). We shall refer to the problem for the determination of x from given y and g over n as DLP(n).

2.3 Square-root attack

If DLP(n) can be solved with the base g in a polynomial time, then the factoring problem of n can be solved in an expected polynomial time [9]. Indeed, any attacker who is able to compute the discrete logarithm x of an arbitrary element $e \in \mathbb{Z}_n^*$ 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: Compute the discrete logarithm $x = \log_g e$ determined from given e and g over n. 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 $\gcd(g^{x/2} \pm e', n)$.

It was shown that the scheme using DLP(n) with a powered element in $\mathbb{Z}_n^*$ is not secure against the square-root attack [7].

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). Namely an attacker presents his/her forged ID for TC to obtain the discrete logarithm of the wanted value. This means that the use of one-way hash function is essential for being secure against the square-root attack.

3. DLP over product of 3 primes

Here, we discuss the DLP(n) when n is written by $n = pqr$. Further, we assume that the factors of n satisfy the following condition.

Condition 4 *Odd prime numbers p, q and r satisfy the following relations:*

$$\begin{cases} p = 2p' + 1 \\ q = 2q' + 1 \\ r = 2r' + 1, \end{cases}$$

where $\gcd(p', q') = \gcd(q', r') = \gcd(r', p') = 1$.

It should be noted that p', q' and r' are not necessarily required to be prime numbers.

We also assume that the following conditions are satisfied.

Condition 5 *The modulus n satisfies the following relation:*

$$\left(\frac{-1}{n}\right) = 1. \tag{2}$$

Condition 6 *The maximum generator $g \in \mathbb{Z}_n^*$ satisfies the following relations:*

$$-1 \notin \langle g \rangle_n, \tag{3}$$

$$\left(\frac{g}{n}\right) = 1. \tag{4}$$

The following lemmas on the Legendre symbol are well-known, where p is a prime number.

Lemma 7 *For an integer a, it follows that*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Lemma 8

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Lemma 9

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Relating to Conditions 5 and 6, the following lemmas are important.

Lemma 10 *Let p, q and r be odd prime numbers that satisfy Condition 4. The necessary and sufficient condition for the composite number $n = pqr$ to satisfy Condition 5 is the following:*

$$(p, q, r) \equiv (1, 3, 3), (3, 1, 3), (3, 3, 1) \pmod 4. \tag{5}$$

Proof From (2), it follows that:

$$\left(\left(\frac{-1}{p}\right),\left(\frac{-1}{q}\right),\left(\frac{-1}{r}\right)\right) = (1,-1,-1),(-1,1,-1),\\ (-1,-1,1),(1,1,1).$$

Only the last value $(1,1,1)$ does not satisfy Condition 4 because $4|p-1$, $4|q-1$ and $4|r-1$. Consequently, (5) is obtained from Lemma 8. The converse is straightforward.

(QED)

Lemma 11 *Let $g \in \mathbb{Z}_n^*$ be a maximum generator. The necessary and sufficient condition for g satisfies the relation $(g/n) = 1$ is the following:*

$$\left(\left(\frac{g}{p}\right),\left(\frac{g}{q}\right),\left(\frac{g}{r}\right)\right) = (1,-1,-1),(-1,1,-1),\\ (-1,-1,1).$$

Proof From (4), it follows that:

$$\left(\left(\frac{g}{p}\right),\left(\frac{g}{q}\right),\left(\frac{g}{r}\right)\right) = (1,-1,-1),(-1,1,-1),\\ (-1,-1,1),(1,1,1).$$

However, it is impossible that g is a maximum generator in the last value $(1,1,1)$ for the following reason. When $(g/p) = 1$ holds, it holds that $\mathrm{ord}_p(g)|(p-1)/2$, because $g^{(p-1)/2} \equiv 1 \pmod p$ holds from Lemma 7. Similarly, $\mathrm{ord}_q(g)|(q-1)/2$ and $\mathrm{ord}_r(g)|(r-1)/2$ also hold. Thus, it follows that $\mathrm{ord}_n(g) = \mathrm{lcm}(\mathrm{ord}_p(g), \mathrm{ord}_q(g), \mathrm{ord}_r(g))| \varphi(n)/8 < \lambda(n)$. This concludes the proof. The converse is straightforward.

(QED)

Corollary 12 *Letting $g_p \in S_p$, $g_q \in S_q$ and $g_r \in S_r$, if an element $g \in \mathbb{Z}_n^*$ satisfies one of the following congruences, then g is the maximum generator that satisfies the relation $(g/n) = 1$:*

$$g \equiv \begin{cases} g_p^2 \pmod p, \\ g_q \pmod q, \\ g_r \pmod r, \end{cases}$$

$$g \equiv \begin{cases} g_p \pmod p, \\ g_q^2 \pmod q, \\ g_r \pmod r, \end{cases}$$

$$g \equiv \begin{cases} g_p \pmod p, \\ g_q \pmod q, \\ g_r^2 \pmod r. \end{cases}$$

Lemma 13 *If Conditions 4 to 6 are satisfied, the $\mathbb{Z}_n^\sharp$ can be decomposed into residue classes of $\langle g\rangle_n$ with $\{1,-1\}$ as coset leaders (see Table 1).*

Proof The $\mathbb{Z}_n^\sharp$ is a multiplicative group of order $\varphi(n)/2$. From Condition 6, $\langle g\rangle_n$ forms a subgroup of $\mathbb{Z}_n^\sharp$. Consequently, $\mathbb{Z}_n^\sharp$ can be decomposed into residue classes of $\langle g\rangle_n$. Since Conditions 5 and 6 are satisfied, $\{1,-1\}$ can be used as coset leaders. The order of $\mathbb{Z}_n^\sharp$ is $\varphi(n)/2$. Since $\lambda(n) = \varphi(n)/4$ from Condition 4, it follows that $2|\langle g\rangle_n| = |\mathbb{Z}_n^\sharp|$. Then all the elements are exhausted.

(QED)

Table 1. Residue class decomposition of $\mathbb{Z}_n^\sharp$ ($n = pqr$).

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

We show a small example of residue class decomposition of $\mathbb{Z}_n^\sharp$ in Table 2.

The following theorem can be derived from Lemma 13.

Theorem 14 *If Conditions 4 to 6 are satisfied, letting $e \in \mathbb{Z}_n^\sharp$, either e or $-e$ has a discrete logarithm over n with g as the base.*

4. Proposed scheme

We shall propose here a new ID-NIKS using DLP(n) where n is a product of three prime numbers.

Let us denote the identity information of User k as ID_k. Let $e_k \in \mathbb{Z}_n^*$ be the public key of User k which is corresponding to ID_k, and s_k, the secret key of User k. We assume that TC can solve DLP over each prime factor of n. TC can then compute the discrete logarithm of e_k over n from the discrete logarithms over all the prime factors of n with the Chinese remainder theorem. Let K_{AB} denote the shared key between Users A and B.

4.1 Preparation of TC

TC generates a composite modulus $n = pqr$ and a maximum generator g so that they may satisfy Conditions 4 to 6. TC publicizes α satisfying $(\alpha/n) = -1$. TC also publicizes a one-way hash function $h(\cdot)$ which maps bit-strings of arbitrary finite length to elements in $\mathbb{Z}_n^*$ so that anyone can compute e_k from ID_k.

4.2 Registration of User

From Theorem 14, one and only one of e_k, $-e_k$, αe_k and $-\alpha e_k$ has the discrete logarithm over $n = pqr$ for any α such that $(\alpha/n) = -1$. TC computes the secret key s_k of User k as the discrete logarithm over n as follows:

$$e_k = h(ID_k),$$

$$e'_k = \begin{cases} e_k & \text{if } \left(\frac{e_k}{n}\right) = 1, \\ \alpha e_k & \text{if } \left(\frac{e_k}{n}\right) = -1, \end{cases}$$

$$s_k \equiv \begin{cases} \log_g e'_k \pmod{\lambda(n)} & \text{if } e'_k \in \langle g\rangle_n, \\ \log_g -e'_k \pmod{\lambda(n)} & \text{if } e'_k \notin \langle g\rangle_n. \end{cases}$$

TC sends s_k to User k in a secure channel. It should be noted that s_k can be computed with the Chinese remainder theorem from the discrete logarithms of e'_k over p, q and r.

4.3 Non-interactive key sharing

User A can generate the shared key K_{AB} as follows:

$$e_B = h(ID_B),$$

Table 2. Small example of residue class decomposition of $\mathbb{Z}_n^\sharp$ when $n = 3 \cdot 5 \cdot 11$, ($g = 112$).

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
g^i	1	112	4	118	16	142	64	73	91	127	34	13	136	52	49	43	31	7	124	28
$-g^i$	164	53	161	47	149	23	101	92	74	38	131	152	29	113	116	122	134	158	41	137

$$e'_B = \begin{cases} e_B & \text{if } \left(\frac{e_B}{n}\right) = 1, \\ \alpha e_B & \text{if } \left(\frac{e_B}{n}\right) = -1, \end{cases}$$

$$K_{AB} \equiv e'^{2s_A}_B \equiv g^{2s_A s_B} \pmod{n}.$$

4.4 Theorems for particular cases

In the following theorems, prime numbers $(p, q, r) \equiv (3, 3, 1) \pmod 4$ are assumed to be used in the proposed scheme without loss of generality.

The maximum generator g is assumed to satisfy the following congruences:

$$g \equiv \begin{cases} g_p^2 \pmod p, \\ g_q \pmod q, \\ g_r \pmod r, \end{cases}$$

where $g_p \in S_p$, $g_q \in S_q$ and $g_r \in S_r$.

Theorem 15 *Let $e \in \mathbb{Z}_n^\sharp$. Then we have $e \in \langle g \rangle_n$ if and only if $(e/p) = 1$.*

Proof From Theorem 14, e belongs to either $\langle g \rangle_n$ or $-\langle g \rangle_n$. If $e \in \langle g \rangle_n$, e can be uniquely represented as $e \equiv g^i \pmod n$ where $i \in \mathbb{Z}_{\lambda(n)}$. Thus,

$$\left(\frac{e}{p}\right) = \left(\frac{g^i}{p}\right) = \left(\frac{g_p^i}{p}\right)^2 = 1.$$

If $e \notin \langle g \rangle_n$, e can be uniquely represented as $e \equiv -g^i \pmod n$ where $i \in \mathbb{Z}_{\lambda(n)}$. Thus,

$$\left(\frac{e}{p}\right) = \left(\frac{-g^i}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{g^i}{p}\right) = -1.$$

Consequently, if $(e/p) = 1$ then $e \in \langle g \rangle_n$, which is the converse.

(QED)

From Theorem 15, it is evident that TC can determine whether $e'_k \in \langle g \rangle_n$ or not without computing the discrete logarithm of e'_k.

Theorem 16 *If p, q and r satisfy one of the following congruences, the relation $(2/n) = -1$ holds.*

$$(p, q, r) \equiv (3, 3, 5), (7, 7, 5), (7, 3, 1) \pmod 8.$$

Proof From Lemma 9,

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{q}\right)\left(\frac{2}{r}\right) = -1.$$

(QED)

Theorem 16 yields the condition that $\alpha = 2$ can be used.

5. Conclusions

We have discussed in detail the discrete logarithm problem over n where n is a product of three prime numbers. We have shown the theorem that either e or $-e$ has the discrete logarithm over n for an arbitrary element e such that $(e/n) = 1$. We then have proposed a new ID-NIKS using the discrete logarithm problem over a product of three prime numbers based on this theorem. It should be noted that the proposed scheme can circumvent the square-root attack.

References

[1] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Infom. Theory, **22** (1976), 644–654.

[2] Y. Murakami and M. Kasahara, An ID-based key distribution system (in Japanese), IEICE Tech. Rep. ISEC, **90** (1990), 29–36.

[3] Y. Murakami and M. Kasahara, The discrete logarithm problem under a composite modulus (in Japanese), IEICE Tech. Rep. ISEC, **90** (1990), 33–40.

[4] 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.

[5] 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.

[6] U. M. Maurer and Y. Yacobi, A non-interactive public-key distribution system, Designs, Codes and Cryptography, **9** (1996), 305–316.

[7] Y. Murakami, M. Kasahara, Murakami-Kasahara ID-based key sharing scheme revisited, – in comparison with Maurer-Yacobi scheme –, IEICE Tech. Rep. ISEC, **105** (2005), 9–16.

[8] W. Abe, N. Kunihiro and K. Ohta, Maurer-Yacobi ID-based encryption scheme revisited (in Japanese), Proc. of the 2005 Symposium on Cryptography and Information Security (2005), 2011–2016.

[9] A. J. Menezes, P. C. Oorschot and S. A. Vanstone, Handbook of applied cryptography, USA, CRC Press, 1996.