On the Security of MOR Public Key Cryptosystem

In-Sok Lee[1⋆†], Woo-Hwan Kim[1⋆†], Daesung Kwon[2], Sangil Nahm[3†], Nam-Seok Kwak[1⋆†], and Yoo-Jin Baek[4†]

[1] ISaC, Department of Mathematics, Seoul National Univ., Seoul, 151-747, Korea
{islee,whkim,kwarc}@math.snu.ac.kr
[2] National Security Research Institute (NSRI), Taejon, 305-350, Korea
ds_kwon@etri.re.kr
[3] Department of Mathematics, Purdue University, West Lafayette, IN 47907, USA
snahm@purdue.edu
[4] Multimedia Lab., Samsung Electronics Co., Suwon, 442-742, Korea
yoojin.baek@samsung.com

Abstract. For a finite group G to be used in the MOR public key cryptosystem, it is necessary that the discrete logarithm problem(DLP) over the inner automorphism group $\mathrm{Inn}(G)$ of G must be computationally hard to solve. In this paper, under the assumption that the special conjugacy problem of G is easy, we show that the complexity of the MOR system over G is about $\log |G|$ times larger than that of DLP over G in a generic sense. We also introduce a group-theoretic method, called the group extension, to analyze the MOR cryptosystem. When G is considered as a group extension of H by a simple abelian group, we show that DLP over $\mathrm{Inn}(G)$ can be 'reduced' to DLP over $\mathrm{Inn}(H)$. On the other hand, we show that the reduction from DLP over $\mathrm{Inn}(G)$ to DLP over G is also possible for some groups. For example, when G is a nilpotent group, we obtain such a reduction by the *central commutator attack*.
Key words: MOR cryptosystem, discrete logarithm problem, group extension, central commutator attack

1 Introduction

At Crypto 2001, Paeng et al. [8] proposed the MOR public key cryptosystem using finite non-abelian groups. For a group G to be used in the MOR public key cryptosystem, it is necessary that the discrete logarithm problem(DLP) over the inner automorphism group $\mathrm{Inn}(G)$ of G must be computationally hard to solve, and there must be an efficient way to represent group elements as products of the specified generators of G. Furthermore, we expect the security of the MOR system to be something

⋆ Supported in part by KRF grant #2004-070-C00001 and BK21 Project in 2004.
† Partially supported by NSRI.

'mor(e)' than that of DLP over G. Also it should be noted that the difficulty of DLP depends not only on the algebraic structure of the group, but also on how elements of the group are represented.

Despite of many cryptographic advantages(see [8]) of the MOR cryptosystem, the groups proposed so far have turned out to be unsatisfactory(see [7, 9, 14]).

In this paper, we are not trying to suggest new candidates for the groups G to be used in the MOR cryptosystem. We would rather intend to reveal the reasons why it is not easy to find *good* candidates for G. Thus, we hope that this paper helps searching for suitable groups for the MOR system.

First, in Section 2, we compute the complexity of finding the secret keys of MOR system in a generic sense. Under the assumption that the special conjugacy problem of G is easy, we show that the complexity of MOR system over G is about $\log |G|$ times larger than that of DLP over G in a generic sense. This result is somewhat unexpected, since our *intuitive* expectation for the generic complexity of MOR system is about $|Z(G)|$ times larger than that of DLP over G.

Next, in Section 3, using the well-known theory of group extensions, we show that it is possible to 'reduce' the problem of finding the secret keys of MOR system over G to that of the MOR system over (smaller) subgroups H of G. Our method is a generalization of various attacks given in [7, 9, 14].

In Section 4, we intend to find a reduction algorithm, which reduces MOR system over G to DLP over G. (If this reduction were efficient enough, MOR system would have less advantage in security than other public key cryptosystem based on DLP over G.) We show that this reduction is possible for the groups which are nilpotent or 'nearly' nilpotent. We call our reduction the *central commutator attack* and we note that this attack is generic.

In this paper, we use the following standard notations: If N is a normal subgroup of G and $g \in G$, the order of g is denoted by $|g|$ and the image of g in G/N is denoted by $\overline{g}$. We let $\mathrm{Inn}(g)$ be the inner automorphism of G induced by g, that is,

$$\mathrm{Inn}(g)(x) = g^{-1}xg, \qquad (x \in G)$$

and we let $\mathrm{Inn}(G) = \{\mathrm{Inn}(g) \mid g \in G\}$ be the subgroup of inner automorphisms in $\mathrm{Aut}(G)$. We note that $\mathrm{Inn}(G) \approx G/Z(G)$, where

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$$

is the center of G.

2 MOR Cryptosystem

2.1 Description of MOR Cryptosystem

The MOR cryptosystem [8] is described as follows.

– Bob's Public key : $(\mathrm{Inn}(g),\ \mathrm{Inn}(g^s))$
– Bob's Secret key : An integer $s(\mathrm{mod}\,|\overline{g}|)$, where $\overline{g} \in G/Z(G)$

It should be noted that for a fixed generating set $\{\gamma_i \mid i \in I\}$ of G, a public key $(\mathrm{Inn}(g),\ \mathrm{Inn}(g^s)) = (\varphi, \varphi^s)$ is described by the data $\{\varphi(\gamma_i)\}$ and $\{\varphi^s(\gamma_i)\}$.

Encryption

1. Alice chooses a random integer r and computes $(\mathrm{Inn}(g^s))^r = \mathrm{Inn}(g^{sr})$.
2. Alice computes $E = \mathrm{Inn}(g^{sr})(M)$.
3. Alice computes $\mu = (\mathrm{Inn}(g))^r = \mathrm{Inn}(g^r)$.
4. Alice sends (E, μ) to Bob.

Decryption

1. Bob computes $\mu^{-s} = \mathrm{Inn}(g^{-sr})$.
2. Bob recovers $M = \mu^{-s}(E)$.

2.2 MOR Cryptosystem and Related Problems

For simplicity, let us write DLP(G) for DLP over G. Thus DLP(Inn(G)) stands for DLP over the inner automorphism group Inn(G) of G.

The security of MOR system is related with the following problems :

– [Special Conjugacy Problem] : For a given $\varphi \in \mathrm{Inn}(G)$, find $h \in G$ such that $\mathrm{Inn}(h) = \varphi$.

– [DLP(Inn(G))] : Given $\varphi, \varphi^s \in \mathrm{Inn}(G)$ for some $s \in \mathbb{Z}$, find $s(\mathrm{mod}\,|\varphi|)$.

Throughout this paper, let us assume(agree(?)) that the special conjugacy problems over G are not hard to solve. (Otherwise, one can exploit the cryptosystem using the hardness of the special conjugacy problem over G.) Therefore, for given $\mathrm{Inn}(g)$, we may find $g' \in G$ satisfying $\mathrm{Inn}(g) = \mathrm{Inn}(g')$. It means that $g' = gz$ for some $z \in Z(G)$. In this case, DLP(Inn(G)) can be restated as follows :

$$\text{Find an integer } s(\mathrm{mod}\,|\overline{g}|) \text{ for given } g,\ g^s z \in G, \text{ where } z \in Z(G),$$

or

$$\text{Find an integer } s(\mathrm{mod}\,|\overline{g}|) \text{ for given } \overline{g},\ \overline{g}^{\,s} \in G/Z(G).$$

It means that DLP(Inn(G)) is equivalent to DLP($G/Z(G)$).

In particular, if $|Z(G)|$ is sufficiently large, there is little possibility that $g^s z$ is contained in the cyclic subgroup $\langle g \rangle$ for a randomly chosen $z \in Z(G)$. Hence, existing algorithms for solving DLP(G) do not seem to be directly applied to DLP(Inn(G)). On the contrary, if $|Z(G)|$ is too large, then Inn(G) becomes too small to be used for MOR system. Therefore, we conclude that the appropriate size of $Z(G)$ is crucial in MOR system.

2.3 Central Attack

The crucial role of $Z(G)$ gives rise to the following *intrinsic* attack against MOR system.

Assume that $|Z(G)| = m$ is known. For given g and $g^s z$ for some $s \in \mathbb{Z}$ and $z \in Z(G)$, we get $h_1 = g^m$ and $h_2 = (g^s z)^m = (g^m)^s$. Now, solving DLP($\langle g^m \rangle$) or DLP($G$), we get $s(\bmod |g^m|)$, which gives a partial information of the secret key s. Of course, g^m may be the identity of G in the extreme case(for example, see [8, p. 477]).

2.4 Complexity of Generic Algorithm on MOR System

Since middle of 90's, a lot of works [11, 4–6] have been done on generic algorithms for DLP and their lower bounds of complexity. Algorithms which do not exploit any particular property of representations of the group are called generic, and the baby-step giant-step algorithm is one of the generic algorithms for DLP. In generic algorithms for DLP, only group operations and equality tests are used.

Let $\{\gamma_i \mid i \in I\}$ be a given generating set of G for MOR system, and a public key (φ, φ^s) be given by $\{\varphi(\gamma_i)\}$ and $\{\varphi^s(\gamma_i)\}$. Assuming that the special conjugacy problem over G is not difficult as before, we get g and $g^s z$ for some unknown $z \in Z(G)$.

Let $Mul_G(\cdot,\cdot)$, $Inv_G(\cdot)$ and $Equ_G(\cdot,\cdot)$ denote the group operation (multiplication and inversion) oracles and the equality test oracle of G, respectively. Now, consider the factor group $G/Z(G)$. The generic operations of $G/Z(G)$ can be *realized* using those of G as follows.

- Group operation oracle of $G/Z(G)$:

$$Mul_{G/Z(G)}(g_1, g_2) = Mul_G(g_1, g_2),$$
$$Inv_{G/Z(G)}(g) = Inv_G(g).$$

- Equality test oracle of $G/Z(G)$:

$$Equ_{G/Z(G)}(g_1, g_2) = \begin{cases} \texttt{True} & (\text{if } g_1 g_2^{-1} \gamma_i = \gamma_i g_1 g_2^{-1} \text{ for all } i \in I), \\ \texttt{False} & (\text{otherwise}). \end{cases}$$

One equality test in $G/Z(G)$ requires at most $(2|I|+1)$ calls of Mul_G, 1 call of Inv_G and $|I|$ calls of Equ_G. Under the assumption that $|I| = O(\log|G|)$, we have the following result as a direct application of the Pohlig-Hellman algorithm in [10].

Theorem 1. *Let a public key of MOR system* $(\mathrm{Inn}(g),\ \mathrm{Inn}(g^s))$ *be given, and let* $|\overline{g}| = \prod_{i=1}^{k} p_i^{e_i}$*, where* p_i *are distinct primes. Under the assumption that* $|I| = O(\log|G|)$ *and that the special conjugacy problem over G is easy, the secret key s can be computed by* $O(\sum e_i(\log|\overline{g}| + p_i)\log|G|)$ *group operations and equality tests of group elements. If a memory space for storing* $\lceil\sqrt{p}\rceil$ *group elements(where p is the largest prime factor of* $|\overline{g}|$*) is available, the running time can be reduced to* $O(\sum e_i(\log|\overline{g}| + \sqrt{p_i}\log p_i)\log|G|)$*.*

Proof. By the above discussion, one equality test between two elements of $G/Z(G)$ requires $O(\log|G|)$ group operations and equality tests of elements of G. The second assertion follows directly from [10]. □

Thus, in a generic sense, the complexity of computing the secret key of MOR system is about $\log|G|$ times larger than that of solving DLP(G).

This result is somewhat unexpected, since our *intuitive* expectation for the generic complexity of MOR system is about $|Z(G)|$ times larger than that of DLP over G. (If the equality test oracle of $G/Z(G)$ were; "check if $g_1 = g_2 z$ for each $z \in Z(G)$", then we would obtain the result matching our *intuition*. So, the point is that one equality test between two elements of $G/Z(G)$ requires *only* $O(\log|G|)$ group operations and equality tests of elements of G.)

3 Group Extensions and MOR Cryptosystem

Since it does not seem easy to find a *good* candidate for MOR cryptosystem from the list of well-known finite groups, we consider an *inductive argument* as follows. Suppose that the group G is *good* for MOR system, and suppose that G has the smallest order among *good* candidates. Then we think of G as a group extension of a maximal normal subgroup H of G, which is *not suitable* for MOR system by the hypothesis.

In this section, generalizing the various ideas of [7, 9, 14], we show that it is possible to w-reduce(see the definition below) DLP(Inn(G)) to DLP(Inn(H)), where H is a maximal normal subgroup of G.

Definition 2 Given $\varphi, \varphi^s \in \mathrm{Inn}(G)$ with a secret key $s (\mathrm{mod}\, |\varphi|)$, if we can compute ψ, ψ^s for some $\psi \in \mathrm{Inn}(H)$, we say DLP(Inn(G)) can be *w-reduced* (weakly-reduced) to DLP(Inn(H)). In this case, note that we can recover $s(\mathrm{mod}\,|\psi|)$, provided DLP(Inn(H)) is not hard to solve. (Of course, $|\psi|$ may be 1 in the extreme case.)

Although the theory of group extension(see, for example, [2, § 15.1] or [13, § 2.7]) is quite standard and well-known, we briefly sketch the proofs for some results of group extensions to prepare for our proof of Theorem 10.

3.1 Group Extensions

Definition 3 For given two groups H and F, if $H \triangleleft G$ and $G/H \cong F$, then we call G *a group extension of* H *by* F.

Theorem 4. *(See [2, 13].) If G is a group extension of H by F, there exist functions $T : F \to \mathrm{Aut}(H)$ and $f : F \times F \to H$ satisfying the following conditions:*
(1) $T(\tau) \circ T(\sigma) = \mathrm{Inn}(f(\sigma,\tau)) \circ T(\sigma\tau),$ *for* $\sigma, \tau \in F$,
(2) $f(\sigma,\tau\rho)\,f(\tau,\rho) = f(\sigma\tau,\rho)\,T(\rho)(f(\sigma,\tau)),$ *for* $\sigma,\tau,\rho \in F$,
(3) $f(1,1) = 1$.

Proof. Let $t : F \to G$ give rise to a bijection between F and a complete set of coset representatives of H in G such that $t(1) = 1$ (t is called a transversal). Next, we define two functions $T : F \to \mathrm{Aut}(H)$ and $f : F \times F \to H$ by
(a) $T(\sigma)(h) = t(\sigma)^{-1} h\, t(\sigma)$, for $\sigma \in F,\ h \in H$,
(b) $f(\sigma,\tau) = t(\sigma\tau)^{-1}\, t(\sigma)\, t(\tau)$, for $\sigma,\tau \in F$.
Then, T and f satisfy the conditions (1)–(3). □

Remark 5 If T and f satisfy the conditions (1)–(3) of Theorem 4, then we call f *a factor set belonging to* T. If a factor set f is obtained from G as (a) and (b) in the proof of Theorem 4, then we call f *a factor set associated with the extension* G.

Theorem 6. *(See [2, 13].) Let $f : F \times F \to H$ be a factor set belonging to $T : F \to \mathrm{Aut}(H)$. Then there exists a group G which is a group extension of H by F such that f is a factor set associated with G.*

Proof. Put $G = \{\, t(\sigma)a \mid \sigma \in F,\ a \in H\}$ and define a binary operation $*$ on G by

$$[t(\sigma)a] * [t(\tau)b] = t(\sigma\tau)\, f(\sigma,\tau)\, T(\tau)(a)\, b, \qquad (\sigma,\tau \in F,\ a,b \in H).$$

Then, G becomes a group extension of H by F. Moreover, $t(\sigma)1$ is actually a transversal and (T, f) satisfies the conditions (a) and (b) in the proof of Theorem 4. $\square$

Corollary 7 *(See [2, 13].) The group extension G is uniquely determined by T and f. In this case, we denote $G = [H, F, T, f]$.*

We note that semi-direct products are group extensions with the trivial factor sets. In [7, 9], it is shown that DLP over inner automorphism groups of semi-direct products can be reduced to DLP over inner automorphism groups of individual groups. For group extensions, a similar result can be derived.

Theorem 8. *Assume the group extension data $G = [H, F, T, f]$ is known. If F is non-abelian, then $\mathrm{DLP}(\mathrm{Inn}(G))$ can be w-reduced to $\mathrm{DLP}(\mathrm{Inn}(F))$.*

Proof. Let $\varphi = \mathrm{Inn}(g)$ and $g = t(\sigma)a$, where $\sigma \in F,\ a \in H$. For any $x = t(\tau)b \in G$, we have

$$\begin{aligned}\varphi(x) &= [(t(\sigma)a)^{-1}] * [t(\tau)b] * [t(\sigma)a] \\ &= [t(\sigma^{-1})d] * [t(\tau)b] * [t(\sigma)a], \quad (\text{where } T(\sigma)(d) = f(\sigma^{-1}, \sigma)^{-1}a^{-1}) \\ &= [t(\sigma^{-1}\tau)\, f(\sigma^{-1}, \tau)\, T(\tau)(d)\, b] * [t(\sigma)a] \\ &= t(\sigma^{-1}\tau\sigma)\, f(\sigma^{-1}\tau, \sigma) \cdot T(\sigma)(f(\sigma^{-1}, \tau)\, T(\tau)(d)\, b) \cdot a.\end{aligned}$$

Similarly there exists $A \in H$ such that $\varphi^s(x) = t(\sigma^{-s}\tau\sigma^s)A$. Let $\Psi = \mathrm{Inn}(\sigma)$. Then, the problem of finding s from given $\varphi, \varphi^s \in \mathrm{Inn}(G)$ can be w-reduced to that of finding s from $\Psi, \Psi^s \in \mathrm{Inn}(F)$. $\square$

Theorem 8 implies that the smaller order $\overline{\sigma} \in F/Z(F)$ has, the less information about s is exposed. Therefore, it is reasonable to take F to be abelian. The next theorem is useful when we investigate group extensions by finite cyclic groups.

Theorem 9. *(See [2, § 15.3].) If G is a group extension of H by $\mathbb{Z}_n$, then G is uniquely determined by $\chi \in \mathrm{Aut}(H)$ and $\alpha \in H$ satisfying the following conditions:*
(1) $\chi^n = \mathrm{Inn}(\alpha) \in \mathrm{Inn}(H)$,
(2) $\chi(\alpha) = \alpha$.

Proof. Write $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. We choose a coset representative $\overline{1}$ of 1, and define a transversal $t : \mathbb{Z}_n \to G$ by $t(i) = \overline{1}^i$ for $0 \le i \le n-1$. Then, $\overline{1}^n = \alpha$ for some $\alpha \in H$. Therefore $\chi := \mathrm{Inn}(\overline{1})|_H \in \mathrm{Aut}(H)$. Then

χ and α satisfy conditions (1) and (2). Conversely, if χ and α are given, we define $T : \mathbb{Z}_n \to \mathrm{Aut}(H)$ and $f : \mathbb{Z}_n \times \mathbb{Z}_n \to H$ by

$$T(i) = \chi^i, \qquad (0 \le i \le n-1)$$
$$f(i,j) = \begin{cases} 1 & \text{if } i+j < n, \\ \alpha & \text{if } i+j \ge n. \end{cases}$$

Then T and f satisfy the conditions (1)–(3) of Theorem 4. □

3.2 MOR System and Group Extensions

Let G be given by a group extension of H by F. The case, for which F is non-abelian, is not desirable since DLP(Inn(G)) can be w-reduced to DLP(Inn(F)) by Theorem 8.

Furthermore, since every finite group has a composition series, we may regard G as a group extended by finite simple groups for finitely many times. Therefore, in this section, we analyze the case when $F = \mathbb{Z}_p$ for some prime p. Now we have the main result of the present section.

Theorem 10. *If the group extension data $G = [H, \mathbb{Z}_p, T, f]$ is known, then* DLP(Inn(G)) *can be w-reduced to* DLP(Inn(H)).

Proof. Let $G = [H, \mathbb{Z}_p, T, f]$. Then, by Theorem 9, there exist $\chi \in \mathrm{Aut}(H)$ and $\alpha \in H$ satisfying the following conditions:

$$T(i) = \chi^i, \qquad (0 \le i < p),$$
$$f(i,j) = \begin{cases} 1 & \text{if } i+j < p, \\ \alpha & \text{if } i+j \ge p, \end{cases}$$
$$\chi^p = \mathrm{Inn}(\alpha) \in \mathrm{Inn}(H).$$

Now, we compute $Z(G)$. If $t(i)a \in Z(G)$, then for all $j \in \mathbb{Z}_p$ and $b \in H$, we have

$$[t(i)a] * [t(j)b] = [t(j)b] * [t(i)a].$$

Therefore,

$$t(i+j)\, f(i,j)\, \chi^j(a)\, b = t(j+i)\, f(j,i)\, \chi^i(b)\, a$$

and hence this implies $\chi^j(a) = a$ and $b = a^{-1}\, \chi^i(b)\, a$. Note that this is equivalent to $\chi(a) = a$ and $\chi^i = \mathrm{Inn}(a^{-1})$. Hence we conclude that

$$Z(G) = \{\, t(i)a \mid \chi(a) = a,\ \chi^i = \mathrm{Inn}(a^{-1})\}.$$

Since $\chi^p = \mathrm{Inn}(\alpha) \in \mathrm{Inn}(H)$ and p is prime, we note that the order of $\overline{\chi}$ in $\mathrm{Out}(H) = \mathrm{Aut}(H)/\mathrm{Inn}(H)$ is 1 or p.

Case 1. $|\overline{\chi}| = 1$.

We prove this case by showing that there is a *computable* isomorphism between $G/Z(G)$ and $H/Z(H)$. If $|\overline{\chi}| = 1$, then $\chi = \mathrm{Inn}(h)$ for some $h \in H$. Since $\chi^i = \mathrm{Inn}(h^i) = \mathrm{Inn}(a^{-1})$, there exists $z_i \in Z(H)$ such that $h^i = a^{-1}z_i$ (i.e., $h^i a \in Z(H)$). Then h commutes with a and thus $\chi(a) = \mathrm{Inn}(h)(a) = a$. Therefore,

$$Z(G) = \{\, t(i)a \mid h^i a \in Z(H)\}$$

and we have

$$|Z(G)| \geq |Z(H)|.$$

Next, we find an isomorphism between $G/Z(G)$ and $H/Z(H)$. Since $\chi^p = \mathrm{Inn}(h^p) = \mathrm{Inn}(\alpha)$, we have $\alpha = h^p z$ for some $z \in Z(H)$. We define $\Psi : G \to H/Z(H)$ by

$$\Psi(t(i)a) = \overline{h^i a}, \qquad (a \in H,\ i \in \mathbb{Z}_p).$$

Then we can show the followings.

1. Ψ is a group homomorphism:

$$\begin{aligned}
&\Psi([t(i)a] * [t(j)b]) = \Psi\left(t(i+j)\, f(i,j)\, \chi^j(a)\, b\right) \\
&= \begin{cases} \overline{h^{i+j}\, \chi^j(a)\, b} = \overline{h^{i+j}\, h^{-j}\, a\, h^j\, b} = \overline{h^i a}\ \overline{h^j b}, & \text{if } i+j < p \\ \overline{h^{i+j-p}\, h^p\, z\, \chi^j(a)\, b} = \overline{z\, h^i\, a\, h^j\, b} = \overline{h^i a}\ \overline{h^j b}, & \text{if } i+j \geq p \end{cases} \\
&= \Psi(t(i)a)\, \Psi(t(j)b).
\end{aligned}$$

2. Ψ is surjective: For $\overline{g} \in H/Z(H)$, where $g \in H$, we have

$$\Psi(t(i)h^{-i}g) = \overline{h^i h^{-i} g} = \overline{g}.$$

3. $\mathrm{Ker}\ \Psi = Z(G)$: $t(i)a \in \mathrm{Ker}\ \Psi \ \Leftrightarrow\ h^i a \in Z(H) \Leftrightarrow\ t(i)a \in Z(G)$.

Hence, by the first isomorphism theorem, we have

$$\overline{\Psi} : G/Z(G) \xrightarrow{\approx} H/Z(H).$$

Note that $\overline{\Psi}$ is *computable* since h can be derived from $\chi = \mathrm{Inn}(h)$.

Case 2. $|\overline{\chi}| = p$.

If $|\overline{\chi}| = p$, i should be 0 in order that the equation $\chi^i = \mathrm{Inn}(a^{-1})$ holds. Moreover, since $\chi^0(b) = b = aba^{-1}$ for all $b \in H$, a must be contained in $Z(H)$. Therefore, we have

$$Z(G) = \{\, t(0)a \mid \chi(a) = a,\ a \in Z(H)\} \leq Z(H).$$

For given $\mathrm{Inn}(t(i)a)$ and $\mathrm{Inn}\left((t(i)a)^s\right)$, under the assumption that the special conjugacy problem of G is easy, we can find $t(j)c$ and $t(l)d$ such that $\mathrm{Inn}(t(i)a) = \mathrm{Inn}(t(j)c)$ and $\mathrm{Inn}\left((t(i)a)^s\right) = \mathrm{Inn}(t(l)d)$. Then we must have $i \equiv j \pmod p$ and $c = az$ for some $z \in Z(H)$ with $\chi(z) = z$. Similarly, we get $is \equiv l \pmod p$. Consequently, we obtain $s \equiv r' \pmod p$ and thus we may put $s = pr + r'$ for some integer r. Since

$$\begin{aligned}
(t(i)a)^p =& \overbrace{[t(i)a] * [t(i)a] * \cdots * [t(i)a]}^{p\text{-times}} \\
=& \overbrace{[t(i)a] * [t(i)a] * \cdots * [t(i)a]}^{(p-1)\text{-times}} * [t(2i)\, f(i,i)\, T(i)(a)\, a] \\
=& \overbrace{[t(i)a] * \cdots * [t(i)a]}^{(p-2)\text{-times}} * [t(3i)\, f(i,2i)\, T(2i)(a)\, f(i,i)\, T(i)(a)\, a] \\
=& \; t(0) \prod_{j=0}^{p-1} f(i,ij)\, T(ij)(a) \\
=& \; t(0)\, \Phi,
\end{aligned}$$

where $\Phi = \displaystyle\prod_{j=0}^{p-1} f(i,ij)\, T(ij)(a)$, we have

$$\mathrm{Inn}\left((t(i)a)^p\right) = \mathrm{Inn}(t(0)\, \Phi)$$

and

$$\mathrm{Inn}\left((t(i)a)^s\right) \circ \mathrm{Inn}\left((t(i)a)^{-r'}\right) = \mathrm{Inn}\left((t(i)a)^{pr}\right) = \mathrm{Inn}\left(t(0)\, \Phi^r\right).$$

We may consider $\mathrm{Inn}(t(0)\,\Phi)|_H$ and $\mathrm{Inn}\left(t(0)\,\Phi^r\right)|_H$ as elements of $\mathrm{Inn}(H)$, and we conclude that DLP(Inn(G)) is w-reduced to DLP(Inn(H)). $\square$

Example 11 Let Λ be the graph automorphism of order 2 of $\mathrm{SL}_n(q)$(see [12, § 10]). The group extension $G = [\mathrm{SL}_n(q), \mathbb{Z}_2, \Lambda, 1]$ belongs to Case 2. In this case, the order of $Z(G)$ is the same as that of $\mathrm{SL}_n(q)$.

Example 12 A metacyclic group(for example, see [3, p. 99]) is a semi-direct product and belongs to Case 2. In this case, the order of the center of the group decreases.

In Case 1, since we can find a *computable* isomorphism

$$\overline{\Psi} : G/Z(G) \xrightarrow{\approx} H/Z(H),$$

we see that DLP(Inn(G)) can be *completely* reduced to DLP(Inn(H)) in this case.

Example 13 (See [8].) Let $G = \mathrm{SL}_2(p) \times_\theta \mathbb{Z}_p$, where

$$\theta = \mathrm{Inn} \circ \theta_1 : \mathbb{Z}_p \to \mathrm{Aut}(\mathrm{SL}_2(p)),$$

and θ_1 is an isomorphism from Z_p to $\langle \alpha \rangle$, $\alpha \in \mathrm{SL}_2(p)$. Then

$$Z(G) = \{\, t(i)a \mid h^i a = \pm I,\ a \in \mathrm{SL}_2(p)\}.$$

Note that $|Z(G)| > |Z(H)|$ and hence this example belongs to Case 1. Therefore, we have

$$G/Z(G) \cong \mathrm{SL}_2(p)/Z(\mathrm{SL}_2(p)) \cong \mathrm{PSL}_2(p).$$

Remark 14 Moreover, all semi-direct products using inner automorphisms are of Case 1. This is the reason why the authors of [7, 9] search for outer automorphisms.

Remark 15 As in [8, 9], even when the message space is restricted to $\{\, t(0)h \mid h \in H\}$, a similar reduction is possible and we omit the proof.

Remark 16 Since we can only w-reduce DLP(Inn(G)) to DLP(Inn(H)), we may not succeed in recovering full information about the secret keys. However, we note that there are many choices of maximal normal subgroups H in G. Thus, we may conclude that the group extension data $G = [H, \mathbb{Z}_p, T, f]$ should not be easily obtained in order to have a secure MOR system. This should be kept in mind when we search for suitable groups for MOR system.

4 Central Commutator Attack

As we have mentioned in Section 2, DLP(Inn(G)), which is the underlying problem of MOR system, depends a lot on the center $Z(G)$ of G. We are thus naturally led to consider the lower central series of G. Especially, we are interested in the nilpotent groups of which the length of lower central series are finite.

In this section, we show that there is a reduction algorithm for MOR system on a nilpotent group.

4.1 Central Commutator Attack

As before, for $g \in G$, we assume a public key $(\mathrm{Inn}(g),\ \mathrm{Inn}(g^s)) = (\varphi, \varphi^s)$ is given.

Lemma 17 *Suppose we can find $h, z \in G$ such that $z = \varphi(h^{-1})h = g^{-1}h^{-1}gh \neq 1$ and $\varphi(z^{-1})z = g^{-1}z^{-1}gz = 1$, then z^s can be computed from φ^s.*

Proof. Observe the following computation:

$$\varphi^s(h^{-1})h = g^{-s}h^{-1}g^s h = g^{-s}(h^{-1}gh)^s = g^{-s}(gz)^s = z^s. \quad \square$$

Thus, if we can find such h and z and can solve DLP($\langle z \rangle$) from z and z^s, we get $s(\bmod |z|)$. To find such h and z, assume G is nilpotent and consider the lower central series of G;

$$G = G^0 > G^1 > \cdots > G^{k-1} > G^k = \langle 1 \rangle,$$

where $G^i = [G, G^{i-1}]$. We have $k \geq 2$ because we are assuming G is non-abelian. Since $G^{k-2} \nleq Z(G)$ and $G^{k-1} \leq Z(G)$, there exists $h \in G^{k-2} \backslash Z(G)$. Letting $z = g^{-1}h^{-1}gh \in G^{k-1}$, z is contained in $G^{k-1} \leq Z(G)$ and thus z commutes with g. This technique is called the *central commutator attack*, since z and $z^s \in Z(G)$ are central commutators.

However, when z is the identity of G, we do not get any information about s, and the condition $z \neq 1$ is not guaranteed here. The next algorithm settles this problem and it can be applied to any nilpotent group.

Lemma 18 *Let G be a nilpotent group of nilpotency $(k-1)$ with $k \geq 2$. Then the Algorithm-1 below outputs z and z^s with $z \neq 1$(and n in the Algorithm-1 satisfies $n \leq k$).*

Algorithm-1	
Input:	$\varphi = \mathrm{Inn}(g)$ and $\varphi^s = \mathrm{Inn}(g^s)$ such that $\varphi \neq 1$.
Step 1:	Define $\sigma(x) := \varphi(x^{-1})x = g^{-1}x^{-1}gx$ and choose x_0 such that $\sigma(x_0) \neq 1$.
Step 2:	For $m \in \mathbb{N}$, define $x_m := \sigma(x_{m-1})$ and let n be the smallest integer such that $x_n = 1$.
Step 3:	Put $h = x_{n-2},\ z = x_{n-1}$ and compute $z^s = \varphi^s(h^{-1})h$.
Output:	z and z^s with $z \neq 1$.

Proof. For $\mathrm{Inn}(g)$ to be used for an encryption, there should exist x_0 which is not trivially encrypted, i.e., $\varphi(x_0) \neq x_0$ and $g^{-1}x_0\, g\, x_0{}^{-1} \neq 1$. Since G is a nilpotent group of nilpotency $(k-1)$, we have the following lower central series of G;

$$G = G^0 > G^1 > \cdots > G^{k-1} > G^k = \langle 1 \rangle,$$

where $G^i = [G, G^{i-1}]$. Define σ and x_m as in the Algorithm-1. We note that $x_m \in G^m$ for $m = 1, \dots, k$ and thus $x_k = 1$. Therefore we see that $n \leq k$. Since n is the smallest integer such that $x_n = 1$, we have $z = x_{n-1} \neq 1$. Now, if we put $h = x_{n-2}$, then h and z satisfy the conditions of Lemma 17 and thus we get $\varphi^s(h^{-1})h = z^s$. □

Thus by solving DLP($\langle z\rangle$), one can compute some partial information of the secret, i.e., $s(\bmod |z|)$. Moreover, we will show that one can recover s completely, if DLP over prime order subgroups of G are easy.

Let $m = |\overline{g}| = \prod_{i=1}^{k} p_i^{e_i}$ be the order of $\overline{g}$ in $G/Z(G)$, where p_i are distinct primes. Then the following algorithm is nothing but an application of the Pohlig-Hellman algorithm [10] to MOR system.

- Step A : For a fixed i, compute $s(\bmod p_i^j)$ for $j = 1, \dots, e_i$, inductively.
- Step B : Compute $s(\bmod {p_i}^{e_i})$ for each $i = 1, \dots, k$.
- Step C : Using the Chinese remainder theorem, compute $s(\bmod m)$.

We note that only the Step A is essential here : Fix a prime factor p of m, and let e be the exponent of p in m. Let

$$s(\bmod p^e) = \sum_{j=0}^{e-1} s_j p^j, \qquad (0 \leq s_j \leq p-1).$$

First, compute

$$\psi := (\mathrm{Inn}(g))^{m/p} = \mathrm{Inn}(g^{m/p})$$

and

$$\psi_0 := (\mathrm{Inn}(g^s))^{m/p} = \mathrm{Inn}(g^{m/p})^s = \mathrm{Inn}(g^{m/p})^{s_0} = \psi^{s_0}.$$

Since $g^{m/p}$ is not contained in $Z(G)$, we have $\psi(\gamma_i^{-1})\gamma_i \neq 1$ for some i, where $\{\gamma_i \mid i \in I\}$ is a given generating set of G. Applying the Algorithm-1 to ψ and ψ_0, we get h, z and z^{s_0} such that

$$z = (g^{-m/p})h^{-1}(g^{m/p})h \quad \text{and} \quad (g^{-m/p})z^{-1}(g^{m/p})z = 1.$$

Observe that $|z| = p$. Solving DLP($\langle z\rangle$), we obtain s_0. Now, assume that we have obtained $s_0, \dots, s_{\ell-1}$ for some $\ell < e$. Next, we compute

$$\begin{aligned}\psi_\ell :=& (\mathrm{Inn}(g^s) \circ \mathrm{Inn}(g)^{-\sum_{j=0}^{\ell-1} s_j p^j})^{m/p^{\ell+1}} \\ =& (\mathrm{Inn}(g^{s-\sum_{j=0}^{\ell-1} s_j p^j}))^{m/p^{\ell+1}} \\ =& \mathrm{Inn}(g^{m/p})^{s_\ell}.\end{aligned}$$

Again applying the Algorithm-1 to ψ and ψ_ℓ, and solving DLP($\langle z\rangle$), we obtain s_ℓ. By induction we can compute $s(\bmod p^e)$. In summary, we have the following result.

Theorem 19. *Let G be a finite nilpotent group. For given* $\mathrm{Inn}(g)$ *and* $\mathrm{Inn}(g^s)$*, by solving DLP over prime order subgroups of G, one can recover $s(mod\,|\overline{g}|)$ completely. In other words,* $\mathrm{DLP}(\mathrm{Inn}(G))$ *can be completely reduced to DLP over prime order subgroups of G.*

We mention here that the central commutator attack is generic in the sense that the algorithm does not use particular property of representations of the group but uses only group operations and equality tests of group elements.

Even when G is not nilpotent, the Algorithm-1 can be applied. First, observe the following.

Lemma 20 *For $x \in G$ define $\tau_x : G \to G$ by*

$$\tau_x(y) = x^{-1}y^{-1}xy, \qquad (y \in G).$$

Then $G/Z(G)$ has nontrivial center if and only if there exists $x \in G\backslash Z(G)$ such that $\tau_x(G) \subseteq Z(G)$.

Proof. Elementary(see, for example, [1, p. 70]).

When the center of $G/Z(G)$ is non-trivial, there exists $x \in G$ such that $[x, G] \subseteq Z(G)$. Thus, given $\varphi = \mathrm{Inn}(g)$, we have $\tau_x(g) = x^{-1}\varphi(x) \in Z(G)$ and $\varphi(x^{-1})\, x \in Z(G)$. Now we see that Algorithm-1 works. Therefore, we might say that Algorithm-1 is valid if G is 'nearly' nilpotent.

When the center of $G/Z(G)$ is trivial, G has the *trivial upper central series* and perhaps is secure against the central commutator attack. But we expect this kind of groups would be 'similar' to simple groups or semi-simple linear groups which are usually not suitable for MOR system.

5 Conclusion

The security of the MOR cryptosystem using a group G is based on the hardness of $\mathrm{DLP}(\mathrm{Inn}(G))$ and is related with the size of $Z(G)$. In a generic sense, the complexity of $\mathrm{DLP}(\mathrm{Inn}(G))$ is about $\log|G|$ times larger than that of $\mathrm{DLP}(G)$, since Pohlig-Hellman or the baby-step giant-step algorithm can be applied to MOR system, provided the special conjugacy problem of G is easy.

Since every finite group G has a composition series, we may regard G as a group extended by finite simple groups for finitely many times. This leads us to analyze a group extension G of H by $\mathbb{Z}_p$ for some prime p, and it is shown that $\mathrm{DLP}(\mathrm{Inn}(G))$ can be w-reduced to $\mathrm{DLP}(\mathrm{Inn}(H))$.

We note that there are many choices of maximal normal subgroups H in G. Thus, we may conclude that the group extension data $G = [H, \mathbb{Z}_p, T, f]$ should not be easily obtained in order to have a secure MOR system. This should be kept in mind when we search for suitable groups for MOR system.

We also analyzed MOR systems on finite nilpotent groups. If G is nilpotent, or $Z(G/Z(G)) \neq 1$, using central commutator attacks, it is shown that DLP(Inn(G)) can be completely reduced to DLP(G).

Finally, it should be noted again that MOR system and DLP highly depend on the representations (or presentations) of groups.

References

1. M. L. Curtis, *Matrix groups*, Springer-Verlag, New York, 1979.
2. M. Hall, *The theory of groups*, The Macmillan company, 1959.
3. T. Hungerford, *Algebra*, Springer-Verlag, 1974.
4. U. Maurer, Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms, in *Advances in Cryptology - Crypto 1994*, *Lecture Notes in Comput. Sci.*, 839, Springer-Verlag, New York, 1994, pp. 271–281.
5. U. Maurer and S. Wolf, The Diffie-Hellman protocol, in *Des. Codes Cryptography*, 19(2), 2000, pp. 147–171.
6. U. Maurer and S. Wolf, Lower bounds on generic algorithms in groups, in *Advances in Cryptology - Eurocrypt 1998*, *Lecture Notes in Comput. Sci.*, 1403, Springer-Verlag, New York, 1998, pp. 72–84.
7. S. Paeng, On the security of cryptosystem using automorphism groups, in *Inf. Process. Lett.*, 88(6), 2003, pp. 293–298.
8. S. Paeng, K. Ha, J. Kim, S. Chee and C. Park, New public key cryptosystem using finite nonabelian groups, in *Advances in Cryptology - Crypto 2001*, *Lecture Notes in Comput. Sci.*, 2139, pp. 470–485.
9. S. Paeng, D. Kwon, K. Ha and J. Kim, Improved public key cryptosystem using finite nonabelian groups, Cryptology ePrint Archive, Report 2001/066, `http://eprint.iacr.org/2001/066/`.
10. S. Pohlig and M. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, *IEEE Trans. Inform. Theory*, 24, 1978, pp. 106–110.
11. V. Shoup, Lower bounds for discrete logarithms and related problems, in *Advances in Cryptology - Eurocrypt 1995*, *Lecture Notes in Comput. Sci.*, 1233, Springer-Verlag, New York, 1997, pp. 256–266.
12. R. Steinberg, *Lectures on Chevalley groups*, Yale University, 1967.
13. M. Suzuki, *Group theory I*, Springer-Verlag, 1977.
14. C. Tobias, Security analysis of the MOR cryptosystem, in *Proceedings of PKC 2003, Lecture Notes in Comput. Sci.*, 2567, Springer-Verlag, 2003, pp. 175–186.