Improved public key cryptosystem using finite non abelian groups

Seong-Hun Paeng, Daesung Kwon, Kil-Chan Ha, Jae Heon Kim

National Security Research Institute
161 Kajong-dong, Yusong-gu, Taejon, 305-350, KOREA
E-mail : shpaeng@etri.re.kr

Abstract

In [6], a new public key cryptosystem using finite non abelian groups was suggested. In this cryptosystem, the discrete logarithm problems in inner automorphism groups are used. In this paper, we generalize the system and give some examples of non abelian groups which is applicable to our system.

1 Introduction

In Crypto 2001, S.-H. Paeng et al. proposed a new public key cryptosystem in which the discrete logarithm problem (DLP) in inner automorphism groups is used [6]. It is known that the index calculus is the most efficient algorithm to solve the DLP in finite fields [1]. But it is not applicable to the DLP in many other groups (e.g. automorphism groups). So it will be an interesting research subject to study non abelian groups, their automorphism groups and the DLP in automorphism groups. In fact, we already have used homomorphisms and automorphisms in many cryptosystems. As a well known example, the DLP in $\mathbb{Z}_p$ is actually the DLP in the automorphism group $\mathbb{Z}_p^* \cong Aut(\mathbb{Z}_p)$. Another example is the ElGamal-type signature scheme. In this scheme, one makes a signature of a message by using the group operation on $\mathbb{Z}_p$ and verifies the homomorphic image of the signature (in $\mathbb{Z}_p^* = Aut(\mathbb{Z}_p)$).

We will generalize the cryptosystem suggested in [6] and name it **MOR** system. MOR system is based on the DLP in automorphism groups. In general, it is not easy to know the automorphism group $Aut(G)$ of G for a given G. But we can easily obtain the inner automorphism group $Inn(G)$ of G, where $Inn(G) = \{Inn(g) \mid g \in G\}$ and $Inn(g)(x) = gxg^{-1}$. Then $Inn : G \to Aut(G)$ can be considered as a homomorphism from G to $Aut(G)$. We call the problem to find an element of $Inn^{-1}(Inn(g))$ for a given g *the special conjugacy problem.* The advantages of MOR system suggested in [6] are as follows:

- It is possible to apply MOR system to G even if the DLP and the special conjugacy problem in G are not hard problems.
- When a non abelian group is used, the encryption scheme of MOR system is convertible to the scheme in which the fast encryption and decryption are possible. In this case, no message expansion is required.

- It is easy to make a signature scheme with MOR system: Note that in general, it is not easy to find a signature scheme using an infinite non abelian group such as a braid group [5].

In section 2, we review the basic MOR system suggested in [6] and suggest the generalized MOR scheme. In section 3, we study the DLP in some automorphism groups.

The author would like to express his gratitude to Dr. Bae Eun Jung and his colleagues in NSRI for their kind comments.

2 MOR cryptosystem

Let G be a non abelian group with non trivial center $Z(G) = \{x \in G \,|xy = yx \text{ for all } y \in G\}$. We assume that $Z(G)$ is not small. Let g be an element of G and $Inn(g)$ be an inner automorphism of g, i.e. $Inn(g)(x) = gxg^{-1}$.

2.1 Basic MOR scheme

The basic scheme is the following:

- public key : $Inn(g)$, $Inn(g^a)$
- secret key : a

A homomorphism $Inn(g)$ can be expressed as $\{Inn(g)(\gamma_i)\}$ for a generator set $\{\gamma_i\}$. If we know $\{Inn(g)(\gamma_i)\}$, then we can compute $Inn(g)(m)$ for any $m \in G$. Also we need an efficient algorithm to express m as a product of γ_i's.

Encryption

1. Alice chooses an arbitrary b and computes $(Inn(g^a))^b$.
2. Alice computes $E = Inn(g^{ab})(m) = (Inn(g^a))^b(m)$.
3. Alice computes $\varphi = Inn(g)^b$.
4. Alice sends (E, φ).

Decryption

1. Bob computes φ^{-a}.
2. Bob computes $\varphi^{-a}(E)$.

The security of the above system depends on the DH (or DLP)-problem on the inner automorphism group $Inn(G)$. In many cases, the index calculus algorithm cannot be applied to the DLP in $Inn(G)$. It is a well known fact that $Inn(G)$ is isomorphic to $G/Z(G)$.

2.2 Generalized MOR scheme

We consider the following sequence;

$$G \xrightarrow{q} G/N \xrightarrow{\phi} Aut(G'),$$

where N is a normal subgroup of G, q is a quotient map to G/N and ϕ is a homomorphism from G/N to $Aut(G')$, where G' may be different from G. Then the DLP in $Aut(G')$ is used in MOR system. Precisely, MOR system is described as follows:

- public key : $\phi(\bar{g})$, $\phi(\bar{g})^a$, where $\bar{g} = q(g)$
- secret key : a

Encryption

1. Alice chooses an arbitrary b and computes $(\phi(\bar{g}^a))^b$.
2. Alice computes $E = \phi(\bar{g})^{ab}(m) = (\phi(\bar{g})^a)^b(m)$ for $m \in G'$.
3. Alice computes $\varphi = \phi(\bar{g})^b$.
4. Alice sends (E, φ).

Decryption

1. Bob computes φ^{-a}.
2. Bob computes $\varphi^{-a}(E)$.

Also the index calculus algorithm cannot be applied to the DLP in $Aut(G')$ in many cases. Since we can use $\phi = Inn$ and $G' = G/N$, we can make many examples of MOR system.

Example 1. *(1) If $G = \mathbb{Z}_p$, $q = Id$ and $G' = G$, then $Aut(G) = \mathbb{Z}_p^*$. Then $\phi(x)(m) = mg^x$, where $\phi(1) = g$. Hence ElGamal encryption scheme is the special case of MOR system.*
(2) The case that $N = Z(G)$ and $\phi : G/Z(G) \to Inn(G)$ is an isomorphism is the basic MOR system suggested in [6]. (As an example in [6], if $G = SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$, then $\phi : G/Z(G) \to Inn(G)|_{SL(2,\mathbb{Z}_p)} \cong Inn(SL(2, \mathbb{Z}_p))$ and $G' = SL(2, \mathbb{Z}_p)$.)
(3) We can use the following sequence:

$$G \xrightarrow{q} G/Z(G) \xrightarrow{\iota} Inn(G) \xrightarrow{Inn} Inn(Inn(G)) \subset Aut(Inn(G)),$$

Then $N = Z(G)$, $\phi = Inn \circ \iota$ and the message space G' is $Inn(G)$.

If we use Example 1 (3) instead of the basic MOR scheme in [6], we can increase the security of the system as we see in section 3.

2.3 Fast encryption-decryption scheme

In ElGamal-type encryption schemes based on abelian groups (e.g. ECC), we must change b for each encryption. (If a fixed b is used, we can obtain $m_1^{-1}m_2 = (m_1 g^{ab})^{-1} m_2 g^{ab}$.) But in our scheme, it is impossible to obtain $m_1^{-1}m_2$ from $Inn(g^b)(m_1)$ and $Inn(g^b)(m_2)$. Thus we can use a fixed b for a long term. Note that if an adversary knows that $\phi(\bar{g}^{ab})(\gamma_i)$ for all elements of a generator set $\{\gamma_i\}$, then $\phi(\bar{g}^{ab})$ are known and the adversary decrypt any ciphertext. To prevent such an attack, one can use a padding method or restrict the message space.

2.4 Security of MOR

The first method to obtain the secret key from the public key is as follows. From $\phi(\bar{g})$ and $\phi(\bar{g})^a$, we obtain g and g^a if possible. Then we can obtain a by solving the DLP in G. But this method is not efficient. We denote the cardinality of N by $|N|$. Since $N \subset \mathrm{Ker}(\phi \circ q)$, if $|N|$ is sufficiently large, we cannot obtain precise g and g^a actually. Thus any algorithm to solve DLP is not applicable in G. Note that we can avoid this attack even if the special conjugacy problem and the DLP in G is not difficult.

Another method is to solve DLP in $Aut(G')$. As we mentioned in the introduction, the index calculus algorithm is not applicable to many cases. But there may be other algebraic methods to solve DLP in $Aut(G')$ as we see in the next section. So we must carefully check the security of MOR system for each G, G', ϕ, q.

3 Examples and Security

3.1 Linear groups

Most familiar non abelian groups are linear groups. The DLP on these groups can be reduced to the DLP in an extension field if we apply the Jordan decomposition theorem.

From now on, let p, q be prime numbers. Since $Z(\mathrm{SL}(2,\mathbb{Z}_p)) = \pm I$, the center is not large. So we cannot apply the basic MOR system to $\mathrm{SL}(2,\mathbb{Z}_p)$. Since $Z(\mathrm{GL}(2,\mathbb{Z}_p)) = \{cI \mid c \in \mathbb{Z}_p\}$, it seems possible to apply the basic MOR system to $\mathrm{GL}(2,\mathbb{Z}_p)$ at first glance. Assume that $Inn(g)$ and $Inn(g^k)$ are given. If $\det(g)$ is not a square of an element of $\mathbb{Z}_p$, then we solve the DLP for $Inn(g)^2$ and $Inn(g^{2k})$. So we may assume that $\det(g)$ is a square of some element in $\mathbb{Z}_p$. Let $g' = \sqrt{\det(g)}^{-1} g$. Then $g' \in \mathrm{SL}(2,\mathbb{Z}_p)$ and $Inn(g') = Inn(g)$. By the same reason, we can also obtain $h \in \mathrm{SL}(2,\mathbb{Z}_p)$ such that $Inn(g^k) = Inn(h)$. Since $Inn(g')^k = Inn(g^k) = Inn(h)$, $(g'^k)h^{-1} = \pm I$ and $g'^{2k} = h^2$. Then the DLP in $Inn(\mathrm{GL}(2,\mathbb{Z}_p))$ is reduced to the DLP in $\mathrm{GL}(2,\mathbb{Z}_p)$. For a linear group G, the DLP in $Inn(Inn(G))$ is also reduced to G.

Also note that linear group G is a subset of the matrix ring R. Thus the inner automorphism on G can be considered as a representation on the vector space R. If the determinant of the representation is not 1, then the DLP can be reduced to the DLP in $\mathbb{Z}_p$ and can be solved more easily.

3.2 Extension of linear groups

3.2.1 Extension of $\mathbf{SL}(2, \mathbb{Z}_p)$

In [6], the following extension of $G = \mathrm{SL}(2, \mathbb{Z}_p)$ was suggested. Let θ_1 be an injective homomorphism from $\mathbb{Z}_p$ to $\mathrm{SL}(2, \mathbb{Z}_p)$ and $\theta = Inn \circ \theta_1$. Then we can make an extension of $\mathrm{SL}(2, \mathbb{Z}_p)$, $\mathrm{SL}(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$. (See [3] or [6] for the precise definition of the semi-direct product.) Then we can easily verify that $|Z(G)| = 2p^2$, which is sufficiently large center. Moreover, it does not have a ring structure. Let $g = (a, b)$ for $a \in \mathrm{SL}(2, \mathbb{Z}_p)$ and $b \in \mathbb{Z}_p$. If $b = 0$, we have

$$(x, y)(a, 0)(x, y)^{-1} = (x\theta(y)(a)x^{-1}, 0) = ((x\theta_1(y))a(x\theta_1(y))^{-1}, 0). \tag{3.1}$$

In [6], we have the following equation:

$$(x, y)^n = ((x\theta_1(y))^n \theta_1(y)^{-n}, ny).$$

Combining these equations, we obtain that

$$(x, y)^n(a, 0)(x, y)^{-n} = ((x\theta_1(y))^n a(x\theta_1(y))^{-n}, 0). \tag{3.2}$$

Since the special conjugacy problem is easy in $\mathrm{SL}(2, \mathbb{Z}_p)$, we can obtain $\pm x\theta_1(y)$ and $\pm(x\theta_1(y))^n$ from $Inn(g)$ and $Inn(g^n)$. Then the DLP in $Inn(G)$ is reduced to the DLP in $\mathrm{SL}(2, \mathbb{Z}_p)$. We can find a similar weakness in $Inn(\mathrm{GL}(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p)$.

Generally, we can obtain the following theorem:

Theorem 1. *Let $\theta = Inn \circ \theta_1$ for a homomorphism $\theta_1 : G_2 \to G_1$. Then the DLP in $Inn(G_1 \times_\theta G_2)$ is reduced to the DLP's in $Inn(G_1)$ and $Inn(G_2)$.*

Proof. Let $g = (x, y) \in G_1 \times_\theta G_2$ and $\theta = Inn \circ \theta_1$ for a homomorphism $\theta_1 : G_2 \to G_1$. Then we have

$$(x, y)^k = ((x\theta_1(y))^k \theta_1(y)^{-k}, y^k)$$

and

$$(x, y)(a, b)(x, y)^{-1} = ((x\theta_1(y))a\theta_1(b)(x\theta_1(y))^{-1}(\theta_1(yb^{-1}y^{-1})), yby^{-1}). \tag{3.3}$$

From these equations, we have that

$$(x, y)^k(a, b)(x, y)^{-k} = ((x\theta_1(y))^k a\theta_1(b)(x\theta_1(y))^{-k}(\theta_1(y^k b^{-1} y^{-k})), y^k by^{-k}) = (A, B).$$

Then we have two conjugacy equations,

$$y^k by^{-k} = B$$

and

$$(x\theta_1(y))^k a\theta_1(b)(x\theta_1(y))^{-k} = A\theta_1(B).$$

Hence the DLP in $Inn(G_1 \times_\theta G_2)$ is reduced to the DLP's in $Inn(G_1)$ and $Inn(G_2)$. □

The reason of this reduction is that θ is induced from the inner automorphism. Considering

$$\begin{aligned} \psi : G_1 \times_\theta G_2 &\to G_1 \\ (x, y) &\mapsto x\theta_1(y), \end{aligned}$$

ψ is a quotient map from $G_1 \times_\theta G_2$ to G_1. So G_1 is both a normal subgroup by (3.1) and a quotient group of $G_1 \times_\theta G_2$. Thus the semi-direct product is similar to the direct product $G_1 \times G_2$. Consequently, we can find the same weakness in $Inn(\mathrm{SL}(2, \mathbb{Z}_p) \times_{Inn} \mathrm{SL}(2, \mathbb{Z}_p))$ and $Inn((\mathrm{SL}(2, \mathbb{Z}_p) \times_{\theta_1} \mathbb{Z}_p) \times_{\theta_2} \mathbb{Z}_q)$, etc. Thus if we use an extension of G by semi-direct product, it is important to find a homomorphism to $Aut(G)$ which is not induced from Inn.

Now we consider the generalized MOR scheme. The easiest way to obtain ϕ is to use Inn. But the DLP's in $Inn(Inn(G))$ for the above suggested G are not difficult. Precisely,

$$Inn(Inn(g^k))(Inn(m))(m') = Inn(g^k m g^{-k})(m') = g^k m g^{-k} m' g^k m^{-1} g^{-k}.$$

If we restrict m, m' to $\mathrm{SL}(2, \mathbb{Z}_p)$, we can obtain $g^k m g^{-k}$ by solving the special conjugacy problem in $\mathrm{SL}(2, \mathbb{Z}_p)$. Then the DLP in $Inn(Inn(G))$ is reduced to the DLP in $Inn(\mathrm{SL}(2, \mathbb{Z}_p))$.

3.2.2 $\mathbf{GL}(2, R) \times_\theta \mathbb{Z}_n$

Let R be a ring and $\phi : R \to R$ be a ring automorphism of R. Then we can find an automorphism of $\mathrm{GL}(2, R)$ by the following lemma:

Lemma 1. *Let $\tilde{\phi}$ be a map defined as follows:*

$$\begin{aligned} \tilde{\phi} : GL(2, R) &\to GL(2, R) \\ \begin{pmatrix} A & B \\ C & D \end{pmatrix} &\mapsto \begin{pmatrix} \phi(A) & \phi(B) \\ \phi(C) & \phi(D) \end{pmatrix}, \end{aligned} \tag{3.4}$$

where

$$GL(2, R) = \{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} | AD - BC \text{ is invertible} \}. \tag{3.5}$$

Then $\tilde{\phi}$ is an automorphism of $GL(2, R)$.

The proof is immediate from a direct computation.

Using the above automorphism, we can obtain automorphisms different from the inner automorphism. If we use R as a group ring $\mathbb{Z}_m(G)$ for some group G, then a ring automorphism $\sigma : \mathbb{Z}_m(G) \to \mathbb{Z}_m(G)$ is induced from a group automorphism $\sigma_0 : G \to G$, i.e.

$\sigma(\sum a_i g_i) = \sum a_i \sigma_0(g_i)$ for $a_i \in \mathbb{Z}_m$ and $g_i \in G$. Then the automorphism $\tilde{\sigma} : \mathrm{GL}(2, \mathbb{Z}_m(G)) \to \mathrm{GL}(2, \mathbb{Z}_m(G))$ is not induced from an inner automorphism.

Another example is as follows. For a ring R_0, let $R = R_0^{R_0}$ be the set of functions from R_0 to R_0. Then R is a ring with operations $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = f(x)g(x)$. For this ring, we can obtain an automorphism $\tilde{\sigma}$ as follows. Let σ be an injective map from R_0 to R_0. Note that σ is not necessarily an automorphism. Then we define

$$\tilde{\sigma}(f) := f \circ \sigma.$$

We can define σ such that the order of $\tilde{\sigma}$ is q for some prime q. Now we put

$$\theta(1)(\begin{pmatrix} A & B \\ C & D \end{pmatrix}) = \begin{pmatrix} \tilde{\sigma}(A) & \tilde{\sigma}(B) \\ \tilde{\sigma}(C) & \tilde{\sigma}(D) \end{pmatrix} \tag{3.6}$$

and construct $\mathrm{GL}(2, R) \times_\theta \mathbb{Z}_n$ for some n dividing q. Since θ is not induced from an inner automorphism, we can avoid the reduction in Theorem 1. We can use a function on R_0 which can be defined by recursion formula. Depending on the recursion formula, the DLP on $Inn(G)$ can be very difficult.

On the other hand, we can consider a quotient of some function ring for the simple expression of ring R. We replace the above R by a quotient ring of a polynomial ring as follows. Let R_0 be the polynomial ring $R_1[x]$ and $f(x)$ be a polynomial of degree k, where $R_1 = \mathbb{Z}_n$, $\mathrm{GF}(p^m)$, etc. We consider the ring $R_0/\langle f \rangle$.

The case of small k Let $\sigma(x) = \alpha x^2 + \beta x + \gamma$. (In fact, R_0 is not a subset of $R_1^{R_1}$.) Then we define a homomorphism $\tilde{\sigma}$ as follows:

$$\tilde{\sigma}(f) = f(\alpha x^2 + \beta x + \gamma).$$

Let J be an ideal $\langle x^3 + a_2 x^2 + a_1 x + a_0 \rangle$ of R_0 and $R = R_0/J$. Then every element of R can be represented by a polynomial of degree 2. If $\tilde{\sigma}(J) \subset J$, then the homomorphism $\bar{\sigma} : R_0/J \to R_0/J$ is induced from $\tilde{\sigma}$. We can find $\alpha, \beta, \gamma, a_0, a_1, a_2$ such that

$$\begin{aligned} 0 &= \bar{\sigma}(x^3 + a_2x^2 + a_1x + a_0)(\mathrm{mod}\ x^3 + a_2x^2 + a_1x + a_0) \\ &= (\alpha x^2 + \beta x + \gamma)^3 + a_2(\alpha x^2 + \beta x + \gamma)^2 \\ &\quad + a_1(\alpha x^2 + \beta x + \gamma) + a_0(\mathrm{mod}\ x^3 + a_2x^2 + a_1x + a_0), \end{aligned} \tag{3.7}$$

which implies that $\tilde{\sigma}(J) \subset J$. By explicit computations, we can find $\sigma' \in R$ such that $\sigma' \circ \sigma(x) = x$ so $\tilde{\sigma}$ is an automorphism.

Since R can be considered as a module with rank 3, a module homomorphism $\bar{\sigma}$ can be represented by a 3×3-matrix $\rho(\bar{\sigma})$. In fact, if $\rho(\bar{\sigma})$ is invertible, then $\bar{\sigma}$ is an automorphism. We want to choose σ such that $\rho(\bar{\sigma})$ is not diagonalizable. If $\rho(\bar{\sigma})$ is diagonalized, then we can express an element of $\mathrm{GL}(2, R)$ by $h = Av_2 + Bv_1 + Cv_0$ and $\rho(\bar{\sigma})(h) = aAv_2 + bBv_1 + cCv_0$, where A, B, C are 2×2-matrices and $a, b, c \in R_1$. Since $\bar{\sigma}(1) = 1$, the constant polynomial 1 is the eigenvector of $\rho(\bar{\sigma})$ with the eigenvalue 1.

We choose $\alpha, \beta, \gamma, a_0, a_1, a_2$ such that the minimal polynomial of $\rho(\bar{\sigma})$ has a factor $(x-a)^2$ for some a. Then $\rho(\bar{\sigma})$ is not diagonalizable. If we add a condition that the charateristic polynomial of $\rho(\bar{\sigma})$ is $(x-1)^2(x-a)$ or $(x-1)(x-a)^2$, we obtain additional 2 equations for 7 variables $\alpha, \beta, \gamma, a_0, a_1, a_2, a$. From (3.7), we already have 3 equations for $\alpha, \beta, \gamma, a_0, a_1, a_2$. Consequently, we have 5 equations for 7 variables $\alpha, \beta, \gamma, a_0, a_1, a_2, a$ so we can find solutions.

Remark 1. *For the simple computation, if we put $f(x) = (x-a_0)(x-a_1)(x-a_2)$, then we can determine α, β, γ by the Lagrange interpolating polynomial. (i.e. $f \circ \sigma = 0 \pmod{f}$ means that $\sigma(a_i) = a_j$.) Let*

$$\rho(\bar{\sigma}) = \begin{pmatrix} A & \alpha & 0 \\ B & \beta & 0 \\ C & \gamma & 1 \end{pmatrix}. \tag{3.8}$$

(The second column vector is (α, β, γ) by $\sigma(x) = \alpha x^2 + \beta x + \gamma$.) We can consider $A, B, C, \alpha, \beta, \gamma$ as functions of a_0, a_1, a_2. The charateristic polynomial is $(x-1)\{(x-\beta)(x-A) - \alpha B\}$. For the characteristic polynomial to have a factor $(x-a)^2$ for some a, $(x-\beta)(x-A) - \alpha B$ is $(x-1)(x-E)$ or $(x-E)^2$ for some E. If $(x-\beta)(x-A) - \alpha B = (x-1)(x-E)$, then

$$(\beta - 1)(A - 1) = \alpha B. \tag{3.9}$$

If $(x-\beta)(x-A) - \alpha B = (x-E)^2$, then

$$(\beta - A)^2 = -4\alpha B. \tag{3.10}$$

We only need to find a_0, a_1, a_2 satisfying one of the above equations (3.9) or (3.10).

The following example shows the existence of f and σ such that the minimal polynomial of $\rho(\bar{\sigma})$ has a factor $(x-a)^2$.

Example 2. (1) *Let $f(x) = x^3$ and $\sigma(x) = \alpha x^2 + \beta x$. It can be easily verified that $f \circ \sigma = 0 \pmod{f}$ and*

$$\rho(\bar{\sigma}) = \begin{pmatrix} \beta^2 & \alpha & 0 \\ 0 & \beta & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.11}$$

Let $\beta = 1$ and $\alpha \neq 0$. Then the minimal polynomial is $(x-1)^2$. If the minimal polynomial is $(x-1)^3$, then $\rho(\bar{\sigma})$ has more non commutativity. Precisely, $\rho(\bar{\sigma})$ is not splitted as follows: $R = V \oplus \langle v_0 \rangle$ and

$$\rho(\bar{\sigma}) = \rho(\bar{\sigma})|_V \oplus \rho(\bar{\sigma})|_{\langle v_0 \rangle},$$

i.e. $\rho(\bar{\sigma})(v + v_0) = \rho(\bar{\sigma})(v) + cv_0$ for $v, \rho(\bar{\sigma})(v) \in V$ and $c \in \mathbb{Z}_n$. Hence it would be better to take $f(x)$ and $\sigma(x)$ satisfying that the minimal polynomial of $\rho(\bar{\sigma})$ is $(x-1)^3$.

(2) Let $R_0 = GF(3^m)[x]$. We take $f(x) = x^3 - 1$ and $\sigma(x) = \alpha x^2 + \beta x + \gamma$. Then

$$\begin{aligned} f \circ \sigma &= 3(\alpha\gamma^2 + \alpha^2\beta + \beta^2\gamma)x^2 \\ &\quad + 3(\alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2)x \\ &\quad + \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma - 1 \\ &= \alpha^3 + \beta^3 + \gamma^3 - 1 = 0 \pmod{f}. \end{aligned} \tag{3.12}$$

We can easily find α, β, γ satisfying (3.12). Also we have

$$\rho(\bar{\sigma}) = \begin{pmatrix} 2\alpha\gamma + \beta^2 & \alpha & 0 \\ \alpha^2 + 2\beta\gamma & \beta & 0 \\ \gamma^2 + 2\alpha\beta & \gamma & 1 \end{pmatrix}. \tag{3.13}$$

The characteristic polynomial is $(x-1)(x^2 - (2\alpha\gamma + \beta^2 + \beta)x + \beta^3 - \alpha^3)$. If $(x-1)(x^2 - (2\alpha\gamma + \beta^2 + \beta)x + \beta^3 - \alpha^3)$ has double root,

$$4(\beta^3 - \alpha^3) = (2\alpha\gamma + \beta^2 + \beta)^2 \tag{3.14}$$

or

$$1 - (2\alpha\gamma + \beta^2 + \beta) + \beta^3 - \alpha^3 = 0 \tag{3.15}$$

should be satisfied. We choose α, β, γ such that the order of an eigenvalue of $\rho(\bar{\sigma})$ is sufficiently large in $GF(3^m)^*$ and (3.12) and (3.14) (or (3.15)) are satisfied.

If we take α such that $|\bar{\sigma}| = |\rho(\bar{\sigma})| = l$ and

$$Z(G) \supset \{(cI, kl) \mid c \in R_1,\ k = 0, 1, \cdots\}.$$

The following example shows why we do not use a polynomial with degree 2 for $f(x)$.

Example 3. *Let $f(x) = x^2 + a_1 x + a_0$ and $\sigma(x) = \alpha x + \beta$. Then $\rho(\bar{\sigma}) = \begin{pmatrix} \alpha & 0 \\ \beta & 1 \end{pmatrix}$ and $f \circ \sigma = 0 \pmod{f}$ implies that*

$$\begin{gathered} 2\alpha\beta + (\alpha - \alpha^2)a_1 = 0 \\ (\alpha^2 - 1)a_0 - \beta a_1 - \beta^2 = 0. \end{gathered} \tag{3.16}$$

In order that $\rho(\bar{\sigma})$ is not diagonalized, $\alpha = 1$. Then we have $2\beta = 0$. In this case, $|\bar{\sigma}| = 2$ so it is not useful for our cryptosystem.

Since the inner automorphism on the second component $\mathbb{Z}_n$ of G is the identity map, the message spaces must be restricted to $\mathrm{GL}(2, R)$. By explicit computations, we can verify that $Inn(g)$ is determined by $Inn(g)(\delta_{ij})$, $Inn(g)(x\delta_{ij})$ and $Inn(g)(x^2\delta_{ij})$ although G is not a ring, where δ_{ij} is the matrix in $\mathrm{GL}(2, R)$ such that (i, j)-entry is 1 and the others are all zero. Hence the public key $Inn(g^a)$ are expressed by $\{Inn(g^a)(\delta_{ij}), Inn(g^a)(x\delta_{ij}), Inn(g^a)(x^2\delta_{ij})\}$. In the fast encryption-decryption scheme in 2.3, $Inn(g^{ab})$ are precomputed and exchanged before the communication. In the encryption and decryption, $E = Inn(g^{ab})(m)$ and $Inn(g^{-ab})(E)$ are computed from a given $Inn(g^{ab})$, respectively. It takes 48-multiplications in R_1 for computing $Inn(g^{ab})(m)$ (or $Inn(g^{-ab})(E)$) in the encryption (or decryption), which is very fast comparing with other PKC's and does not depend on the size of n. To reduce the key size, we can express $Inn(g^a)$ by $\{Inn(g^a)(T), Inn(g^a)(S), Inn(g^a)(x\delta_{11})\}$, where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ which are generators of $\mathrm{SL}(2, \mathbb{Z}_n)$. Note that $x\delta_{ij} = A(x\delta_{11})B$ for some $A, B \in \mathrm{SL}(2, \mathbb{Z}_n)$ and δ_{ij} can be expressed as a sum of elements of $\mathrm{SL}(2, \mathbb{Z}_n)$. Furthermore, $Inn(g^a)(x^2\delta_{11}) = Inn(g^a)((x\delta_{11})^2) = (Inn(g^a)(x\delta_{11}))^2$. If the order of R_1 (e.g. $\mathbb{Z}_n$ or $\mathrm{GF}(p^n)$) is about 100 bits, then the public key size is about 3600 bits.

For the fast encryption-decryption scheme, it would be better to use a padding for a message, e.g. random polynomials in R are used in some entries of a message.

The case of large k Let $R_0 = \mathbb{Z}_2[x]$ and $f(x) = x^{k+1} + a_k x^k + \cdots + a_0$. We take $R = R_0/\langle f \rangle$ and $\sigma(x) = \alpha_k x^k + \cdots + \alpha_0$. Then we can find an automorphism $\bar{\sigma}$ on R by the same method as above. As Remark 1, if $f(x) = x^{k+1}$ and $\alpha_0 = 0$, then

$$\rho(\bar{\sigma}) = \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix}, \tag{3.17}$$

where A is $\mathrm{GL}(k, \mathbb{Z}_2)$. In the case of Example 2, it can be easily verified that $|\rho(\bar{\sigma})| = k - 1$, which is too small. But we can choose σ such that the characteristic polynomial is divided by $(x-1)^2$ and an irreducible polynomial of degree $k' \approx k$. Also σ is chosen so that the order of an eigenvalue of $\rho(\bar{\sigma})$ is sufficiently large in $\mathrm{GF}(2^k)^*$. Then $|\rho(\bar{\sigma})|$ is sufficiently large. If we take $k \approx 100$, then the public key size is about 1200 bit, which is smaller than the case of small k. The multiplication number is much larger than the case of large k but we only need multiplications in $\mathbb{Z}_2$, which is very easy.

References

[1] D. Coopersmith, A. M. Odlzyko, R. Schroeppel *Discrete logarithms in GF(p)* , Algorithmica, 1 (1986), 1–15

[2] T. ElGamal *A public key cryptosystem and a signature scheme based on discrete logarithms* , IEEE Transactions andInformation Theory, 31 (1985), 469–472

[3] T. W. Hungerford *Algebra*, Springer-Verlag

[4] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone *"Handbook of applied cryptography"*, CRC press, (1997)

[5] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. -S. Kang, C. Park *New public-key cryptosystem using braid groups*, Proc. Crypto 2000 (2000), 166–184

[6] S. -H. Paeng, K.- C. Ha, J. Kim, S. Chee, C. Park *"New public key cryptosystem using finite non abelian groups"*, to appear in Advances in Cryptology-Crypto 2001, (2001)

[7] S. C. Pohlig, M. E. Hellman *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Transactions on Information Theory, 23 (1978), 106–110

[8] J. M. Pollard *Monte Carlo methods for index computation (mod p)*, Mathematics of computation, 32 (1978), 918–924