Security Analysis of the MOR Cryptosystem

Christian Tobias

Justus Liebig University Giessen, Department of Mathematics
Arndtstrasse 2, 35392 Giessen, Germany
christian.tobias@math.uni-giessen.de

Abstract. The paper cryptanalyses a new public key cryptosystem that has been recently proposed by Paeng, Ha, Kim, Chee and Park [5]. The scheme works on finite non-abelian groups. We focus on the group $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ which was discussed in [5] extensively.

Keywords: MOR Cryptosystem, Public Key Cryptosystem, Cryptanalysis, Conjugacy Problem, Finite Non Abelian Groups

1 Introduction

In [5] Paeng, Ha, Kim, Chee and Park presented a new public key encryption scheme based on the difficulty of the discrete log problem in the inner automorphism group of a non-abelian group G. This scheme was later called MOR cryptosystem [6]. As underlying group the authors propose the semi-direct product group $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ and discuss the resulting encryption scheme in detail. In [5] the authors do not give a formal proof of security for their system. They rather informally argue why an attacker should not be able to derive the secret key from the public key.
Our analysis of the MOR system comprises several attacks that enable an attacker to determine the plaintext message under certain conditions without compromising the secret key.

The security of the MOR system is closely related to the hardness of the conjugacy problem in the underlying group G. Given $x, y \in G$ the conjugacy problem is to find $w \in G$ such that $y = wxw^{-1}$. In MOR using $G = SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ the situation is slightly different. If $m \in G$ is the plaintext message, ciphertexts are of the form $C(m) = x^{ab} m x^{-ab}$. The special situation of MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$, that we use in our attacks, is that the value x can easily be calculated from the public information (an element from the centralizer of x is already sufficient). We will see that in this case an attacker can collect valuable information about m in a ciphertext-only attack.

To increase the efficiency of their scheme in $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ the authors further propose some modifications to the original scheme. The first proposal is to use $SL(2, \mathbb{Z}_p) \times_\theta \{0\} \cong SL(2, \mathbb{Z}_p)$ instead of $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$.
In its basic form the MOR system is a probabilistic encryption scheme: The sender has to choose a random encryption exponent for every message he wants

Y.G. Desmedt (Ed.): PKC 2003, LNCS 2567, pp. 175–186, 2003.

to encrypt. For $G = SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ the authors propose to fix the encryption exponent and use it for multiple encryptions. A randomised algorithm that maps plaintext messages in $\mathbb{Z}_p$ to matrices in $SL(2, \mathbb{Z}_p)$ is used to get a probabilistic encryption scheme. We will present and discuss the drawbacks of these modifications.

The rest of this paper is organised as follows. In section 2 we give a short summary of the MOR cryptosystem and its underlying constructions. For a more detailed description of the MOR system we refer to [5]. The sections 3 and 4 discuss the security of the MOR system. In section 3.1 we show that MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ is not harder than MOR using $SL(2, \mathbb{Z}_p)$. We further show that the parameter selection from [5] is not secure. In section 3.2 we present two ciphertext-only attacks for MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ that enable an attacker given one component of the plaintext to determine the whole plaintext message. In section 4 we investigate the security of the MOR cryptosystem when the encryption exponent is fixed. As we will see, MOR with fixed encryption exponent is vulnerable to known-plaintext attacks. Only one resp. two plaintext-ciphertext pairs are sufficient to decrypt all ciphertexts that were encrypted using the same exponent. In the appendix useful results about the matrix groups $SL(2, \mathbb{Z}_p)$ and $GL(2, \mathbb{Z}_p)$ are summarised.

Related Work: The conjugacy problem is considered a hard problem in braid groups. There is no known polynomial time algorithm which solves the decisional or the computational conjugacy problem in braid groups. For a detailed discussion of cryptography on braid groups we refer to [1, 3, 4].
Other cryptosystems using the conjugation map on matrix groups have been published by Yamamura [7, 8]. The systems later were broken by Blackburn and Galbraith [2].

2 Framework and Definitions

2.1 The MOR System

Definition 1 (Semi-direct Product Group). *Let G and H be given groups and $\theta : H \to Aut(G)$ be a homomorphism. Then the semi-direct product $G \times_\theta H$ is the set*

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

together with the multiplication map

$$(g_1, h_1)(g_2, h_2) = (g_1 \theta(h_1)(g_2), h_1 h_2)$$

The semi-direct product $G \times_\theta H$ is also a group.

Definition 2 (The Mapping Inn). *Let G be a group. Then the mapping*

$$\begin{aligned} Inn : G &\to Aut(G) \\ g &\mapsto Inn(g) \end{aligned}$$

is given by $Inn(g)(h) = ghg^{-1}$.

We call $Inn(g)$ an inner automorphism and $Inn(G) = \{Inn(g) \mid g \in G\}$ the inner automorphism group. If G is an abelian group then $Inn(g)$ is the identity map for all $g \in G$ and $Inn(G)$ is trivial. Let $\{\gamma_i\}$ be a set of generators of G. Since $Inn(g)$ is a homomorphism, $Inn(g)$ is totally specified for all $m \in G$ if the values $\{Inn(g)(\gamma_i)\}$ are given.

Definition 3 (Center, Centralizer). *Let G be a group. The center $Z(G)$ of G is defined as $Z(G) := \{g \in G \mid xg = gx \ \forall x \in G\}$.*
The centralizer $Z(g)$ of a group element $g \in G$ is defined as $Z(g) := \{h \in G \mid hg = gh\}$.
Note that $Z(G) = \bigcap_{g \in G} Z(g)$.

Definition 4 (Conjugacy Problem). *Let G be a group. For arbitrary $x, y \in G$ the conjugacy problem (CP) is to find $w \in G$ such that $wxw^{-1} = y$.*

Let $w \in G$ be a solution for the instance (x, y) of the CP, i.e. $wxw^{-1} = y$. Then $w \cdot Z(x)$ is the solution set for (x, y).

Definition 5 (Special Conjugacy Problem). *For a given $Inn(g)$ the special conjugacy problem is to find a group element $\bar{g} \in G$ satisfying $Inn(g) = Inn(\bar{g})$.*

The solution set for the special conjugacy problem is $g \cdot Z(G)$.

In $GL(2, \mathbb{Z}_p)$ the conjugacy problem is easy. To solve the special conjugacy problem in $GL(2, \mathbb{Z}_p)$ two pairs $(A_1, Inn(A_1))$ and $(A_2, Inn(A_2))$ with $A_1 \notin Z(A_2)$ are needed (see appendix A.2 for details).

The MOR cryptosystem: MOR is an asymmetric cryptosystem with a random value a as secret and the two mappings $Inn(g)$ and $Inn(g^a)$ (given as $\{Inn(g)(\gamma_i)\}$ and $\{Inn(g^a)(\gamma_i)\}$ for a generator set $\{\gamma_i\}$ of G) as corresponding public key.

The encryption process works as follows:

1. Alice expresses the plaintext $m \in G$ as a product of the γ_i.
2. Alice chooses an arbitrary b and computes $(Inn(g^a))^b$, i.e. $\{(Inn(g^a))^b(\gamma_i)\}$.
3. Alice computes $E = Inn(g^{ab})(m) = (Inn(g^a))^b(m)$.
4. Alice computes $\Phi = Inn(g)^b$, i.e. $\{Inn(g^b)(\gamma_i)\}$.
5. Alice sends (E, Φ).

Decryption Process:

1. Bob expresses E as a product of the γ_i.
2. Bob computes Φ^{-a}, i.e. $\{\Phi^{-a}(\gamma_i)\}$.
3. Bob computes $\Phi^{-a}(E)$.

In [5] no formal proof of security is given for the MOR cryptosystem. The authors state that the security of the MOR cryptosystem relies on the discrete

log problem in the inner automorphism group of G. They argue that even an adversary that is able to calculate discrete logs in G is not able to determine the secret exponent a since the conjugacy problem does not have a unique solution and if G has a center of appropriate size, the attacker gets a vast number of DLP instances and is not able to figure out the correct one.

2.2 MOR Using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$

In [5] the authors propose to use the group

$$G = SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$$

where

$$\theta = Inn \circ \theta_1 : \mathbb{Z}_p \to Aut(SL(2, \mathbb{Z}_p))$$

and θ_1 is an isomorphism from $\mathbb{Z}_p$ to $\langle \alpha \rangle$ with $\alpha \in SL(2, \mathbb{Z}_p)$ of order p. Thus we get $\theta(y)(x) = \theta_1(y)x\theta_1(y)^{-1}$.
Let $g = (x, y) \in G$. The conjugate of $(a, b) \in G$ is

$$\begin{aligned}(x, y)(a, b)(x, y)^{-1} &= (x\theta(y)(a)\theta(b)(x^{-1}), b) \\ &= (x\ \theta_1(y)a(\theta_1(y))^{-1}\ \theta_1(b)x^{-1}(\theta_1(b))^{-1}, b)\end{aligned}$$

Since $(x, y)^n = ((x\theta_1(y))^n\theta_1(y)^{-n}, ny)$ we get

$$(x, y)^n(a, b)(x, y)^{-n} = ((x\theta_1(y))^n a\ \theta_1(b)(x\theta_1(y))^{-n}\theta_1(-b), b)$$

The two matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ are generating $SL(2, \mathbb{Z}_p)$ and thus $\{(T, 0), (S, 0), (I, 1)\}$ is a generator set for $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$.
Given $g \in SL(2, \mathbb{Z}_p)$ with non-zero (2,1)-component a decomposition $g = T^{j_1}ST^{j_2}ST^{j_3}$ can be calculated efficiently (see [5]).

3 Attacking MOR Using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$

In this section we reveal several vulnerabilities of MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ and demonstrate how they can be exploited. In a first step we show that MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ is not more secure than MOR using $SL(2, \mathbb{Z}_p)$.

MOR using $SL(2, \mathbb{Z}_p)$ suffers from the big disadvantage that the ciphertext already reveals valuable information about the encrypted plaintext. If $\bar{M} = XMX^{-1}$ for $X, M \in SL(2, \mathbb{Z}_p)$ then $det(\bar{M}) = det(M)$ and $trace(\bar{M}) = trace(M)$. A MOR ciphertext is of the form $C(M) = g^{ab}Mg^{-ab}$. We present two simple but powerful attacks that can be carried out if g or any element of the centralizer of g is known to the attacker. Both attacks are ciphertext-only. The first attack uses the above mentioned properties of $G = SL(2, \mathbb{Z}_p)$, whereas the second may be used for arbitrary groups G where the conjugacy problem is easy.

3.1 MOR Using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ is not Harder than MOR Using $SL(2, \mathbb{Z}_p)$

We know that $Inn(g) = Inn(g \cdot z)$ if and only if $z \in Z(G)$. Let $G = SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$. Since $Z(G) = \{(x, y) \mid y \in \mathbb{Z}_q, x = \pm\theta_1(-y)\}$ we get $g \cdot Z(G) = \{(\pm x \cdot \theta_1(-z), y + z) \mid z \in \mathbb{Z}_q\}$ for $g = (x, y) \in G$.

Thus every $\hat{g} = (\hat{x}, \hat{y}) \in g \cdot Z(G)$ can be written as $\hat{g} = (\pm x\theta_1(-z), y + z)$ for a $z \in \mathbb{Z}_q$ and $\hat{x}\theta_1(\hat{y})$ is of the form

$$\begin{aligned} \hat{x}\theta_1(\hat{y}) &= \pm x\theta_1(-z)\theta_1(y + z) \\ &= \pm x\theta_1(y) \end{aligned}$$

It follows that the value $x\theta_1(y)$ is (apart from its sign) invariant for all elements of $g \cdot Z(G)$.

The encryption function of MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ is of the form

$$\begin{aligned} Inn(g^n)(m) &= (x, y)^n (m_1, m_2)(x, y)^{-n} \\ &= ((x\theta_1(y))^n m_1 \theta_1(m_2)(x\theta_1(y))^{-n} \theta_1(-m_2), m_2) \end{aligned}$$

where $g = (x, y), m = (m_1, m_2) \in SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$. By calculating $Inn(g^n)(m_i)$ for several messages $m_i \in SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ and solving the conjugacy problem in $SL(2, \mathbb{Z}_p)$ an attacker is able to extract $(\pm x\theta_1(y))^n$.
For MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ that means that an attacker is able to calculate $\pm x\theta_1(y)$ and $(\pm x\theta_1(y))^a$ from the receiver's public key and $(\pm x\theta_1(y))^b$ from the ciphertext.

Thus MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ is not harder than MOR using $SL(2, \mathbb{Z}_p)$. In particular, recovering the plaintext m in a ciphertext-only attack in MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ is not harder than the computational Diffie-Hellman problem in $SL(2, \mathbb{Z}_p)$.

In [5] the authors propose to choose $g = (x, y) \in SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ satisfying $x\theta_1(y) = A(I + c\delta_{12})A^{-1}$ for some $c \in \mathbb{Z}_p$ and $A \in SL(2, \mathbb{Z}_p)$ (where δ_{ij} is the matrix whose entries are all zero except the (i, j)-entry which is 1).
This is a really unfortunate choice since the authors themselves showed in [5], remark 1, that the discrete log problem is easy for matrices of this special form which means that the secret key a can be calculated easily in this case. In fact, the value $g = (x, y) \in G$ has to be chosen such that the discrete log problem is hard in the subgroup generated by $x\theta_1(y)$.

In the following sections we will concentrate on MOR using $SL(2, \mathbb{Z}_p)$, but with the techniques presented in this section the described attacks can easily be applied to attack MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ also.

3.2 Ciphertext-Only Attacks with Known Centralizer Elements

In this section we present two ciphertext-only attacks on MOR using $GL(2, \mathbb{Z}_p)$ and MOR using $SL(2, \mathbb{Z}_p)$.

Our attacker is given a ciphertext $\hat{M} = Inn(X^k)(M) = X^k M X^{-k}$. We assume that the attacker knows X or any element from the centralizer of X (Since the CP is easy in $SL(2, \mathbb{Z}_p)$, X can be computed given $Inn(X) = \{Inn(X)(\gamma_i)\}$ which is part of the receiver's public key.).

In our first attack we use the centralizer element $\hat{X} \in Z(X)$ to transform the given ciphertext $\hat{M}$ to a ciphertext $\hat{X} \cdot \hat{M} = X^k(\hat{X} \cdot M)X^{-k}$ of $\hat{X} \cdot M$. Using the invariance of the trace and the determinant under conjugation we get three equations in the components of M which enables us to derive the structure of the encrypted plaintext M. In particular, if one component of M is known, the whole plaintext matrix M can be reconstructed.

In the second attack the centralizer element $\hat{X} \in Z(X)$ is used to calculate $Inn(\hat{M})(\hat{X}) = (X^k \cdot M)\hat{X}(X^k \cdot M)^{-1}$. Since the conjugacy problem is easy in $GL(2, \mathbb{Z}_p)$ one gets information about the structure of $X^k \cdot M$.

This simple lemma will be very useful in the following sections:

Lemma 1. *Let* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, X = \begin{pmatrix} x & y \\ w & z \end{pmatrix}$ *and* $\hat{M} = XMX^{-1} = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$ *be in* $GL(2, \mathbb{Z}_p)$. *Then* $tr(M) = tr(\hat{M})$.

Proof. Since $X^{-1} = \begin{pmatrix} \frac{z}{detX} & \frac{-y}{detX} \\ \frac{-w}{detX} & \frac{x}{detX} \end{pmatrix} \in GL(2, \mathbb{Z}_p)$ we get $\hat{a} = \frac{1}{detX}(axz + cyz - bxw - dyw)$ and $\hat{d} = \frac{1}{detX}(bwx + dzx - awy - czy)$. It follows that $tr(\bar{M}) = \hat{a} + \hat{d} = \frac{1}{detX}((a+d)(xz - wy)) = \frac{1}{detX}((a+d)(detX)) = a + d = tr(M)$. □

Attack 1:
Using the notation of the lemma we know that $tr(\hat{M}) = tr(M) = a + d$. Let $\hat{X} = \begin{pmatrix} \hat{x} & \hat{y} \\ \hat{w} & \hat{z} \end{pmatrix} \in Z(X)$. We now compute $\bar{M} = \hat{X} \cdot \hat{M} = X^k(\hat{X} \cdot M)X^{-k}$ and get $tr(\bar{M}) = tr(\hat{X} \cdot M) = a\hat{x} + c\hat{y} + b\hat{w} + d\hat{z}$, i.e. a second linear equation for the desired values a, b, c, d.

Unfortunately, this trick only works once. If we do the same trick again with another centralizer element $\bar{X} = \begin{pmatrix} \bar{x} & \bar{y} \\ \bar{w} & \bar{z} \end{pmatrix} \in Z(X)$ and set $\widetilde{M} = \bar{X} \cdot \hat{M} = X^k(\bar{X} \cdot M)X^{-k}$, we get a system of three linear equations:

$$\begin{aligned} a \; + \qquad\qquad\qquad d \quad &= \quad tr(\hat{M}) \\ \hat{w} \cdot b + \hat{y} \cdot c + (\hat{z} - \hat{x}) \cdot d &= tr(\bar{M}) - \hat{x} \cdot tr(\hat{M}) \\ \bar{w} \cdot b + \bar{y} \cdot c + (\bar{z} - \bar{x}) \cdot d &= tr(\widetilde{M}) - \bar{x} \cdot tr(\hat{M}) \end{aligned}$$

We further know that $\hat{x} = \hat{z} + \frac{a-d}{c}\hat{w}$, $\hat{y} = \frac{b}{c}\hat{w}$, $\bar{x} = \bar{z} + \frac{a-d}{c}\bar{w}$ and $\bar{y} = \frac{b}{c}\bar{w}$ (see appendix A.1). Setting $k := \frac{\hat{w}}{\bar{w}}$ it follows that $k \cdot \bar{y} = \hat{y}$ and $k \cdot (\bar{z} - \bar{x}) = \hat{z} - \hat{x}$, i.e. our third equation differs from the second equation only by a constant factor.

The two linear equations allow us to express a and b in terms of c and d. If we further use that $det(\hat{M}) = det(M) = ad - bc$ we can also express c in terms of d and know that the searched plaintext has the structure $M = \begin{pmatrix} f_1(d) & f_2(d) \\ f_3(d) & d \end{pmatrix}$ where the functions f_1, f_2 and f_3 are known.

Attack 2:
Let again $\hat{M} = Inn(X^k)(M) = X^k M X^{-k}$. The aim of the second attack is to calculate the value $X^k \cdot M$.

Let $\hat{X} = \begin{pmatrix} \hat{x} & \hat{y} \\ \hat{c} & \hat{d} \end{pmatrix} \in Z(X)$ and $\bar{X} = \begin{pmatrix} \bar{x} & \bar{y} \\ \bar{c} & \bar{d} \end{pmatrix} = \hat{M}\hat{X}\hat{M}^{-1} = (X^k \cdot M)\hat{X}(X^k \cdot M)^{-1}$.
By solving the conjugacy problem for the instance $(\hat{X}, \bar{X})$ one gets that $X^k \cdot M = \begin{pmatrix} \frac{\hat{w}}{\bar{w}}t + \frac{\hat{x}-\bar{z}}{\bar{w}}s & \frac{\hat{y}}{\bar{w}}s + \frac{\hat{z}-\bar{z}}{\bar{w}}t \\ s & t \end{pmatrix}$ for some $s, t \in \mathbb{Z}_p$.

Unfortunately, performing this attack multiple times does not lead to more data about $X^k \cdot M$ (see appendix A.2).

If $X \in SL(2, \mathbb{Z}_p)$, we know that $det(X^k M) = det(M)$ and can further express s in terms of t.

4 Attacks when Exponents are Used Multiple Times

To make MOR using $SL(2, \mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ more efficient the authors propose to fix the encryption exponent b and use it for multiple encryptions.
The problem with that approach is that given one plaintext-ciphertext pair an attacker is able to calculate $(x\theta_1(y))^{ab}$ which can be used to decrypt all ciphertexts that were encrypted using the same b[1].

In [5] remark 4 the authors therefore propose to choose $\mathbb{Z}_p$ as message space and use some randomised padding technique:

Let $m \in \mathbb{Z}_p$ with $m \neq 0$ be the plaintext message. Choose random $r_1, r_2 \in_R \mathbb{Z}_p$ and encrypt $M = \begin{pmatrix} m & r_1 \\ r_2 & \frac{1+r_1 r_2}{m} \end{pmatrix} \in SL(2, \mathbb{Z}_p)$ with the MOR cryptosystem.

In this section we will present two attacks that show that this padding technique is highly insecure. Both attacks are known plaintext attacks, i.e. the attacker knows pairs of ciphertext and corresponding plaintext. We show that an attacker that knows one resp. two plaintext-ciphertext pairs is able to decrypt all ciphertexts that are encrypted using the same encryption exponent b.

Our attacks work in $SL(2, \mathbb{Z}_p)$ as well as in $GL(2, \mathbb{Z}_p)$. Since $GL(2, \mathbb{Z}_p)$ is the more general case, we concentrate on $GL(2, \mathbb{Z}_p)$ (though the MOR system was origionally presented using $SL(2, \mathbb{Z}_p)$). In our case, if a plaintext message $m \in \mathbb{Z}_p$ with $m \neq 0$ is given, we encrypt $M = \begin{pmatrix} m & r_1 \\ r_2 & r_3 \end{pmatrix} \in GL(2, \mathbb{Z}_p)$,

[1] If no element from the centralizer of $(x\theta_1(y))$ is known, two plaintext-ciphertext pairs are needed (see also appendix A.2).

where $r_1, r_2, r_3 \in_R \mathbb{Z}_p$ with the MOR cryptosystem. Since $det(M)$ is known, the value r_3 can be expressed as $r_3 = \frac{det(M)+r_1 r_2}{m}$.

Let $\bar{M} = XMX^{-1}$ be a MOR encryption of a message $m \in \mathbb{Z}_p$. This equation can also be written as $X^{-1}\bar{M}X = M$. If the plaintext m is known the attacker gets one equation over $\mathbb{Z}_p$ on the unknown entries of X per known plaintext-ciphertext-pair. In our attacks we further use the invariance of trace and determinant under conjugation and the homomorphic property of mapping $Inn(g)$, i.e. multiplying two ciphertexts $Inn(g)(m_1)$ and $Inn(g)(m_2)$ results in a ciphertext $Inn(g)(m_1 \cdot m_2)$ of $m_1 \cdot m_2$ (this property only holds if the exponent b is fixed for multiple encryption).

In the first attack we assume that the attacker knows an element $X \in Z(x\theta_1(y))$, i.e. we are in the situation of section 3.2. In fact our attack is very similar to section 3.2 attack 1 which enables an attacker to determine the whole plaintext message if only one component is known. We will see that one plaintext-ciphertext pair is sufficient to solve the special conjugacy problem in $GL(2, \mathbb{Z}_p)$, i.e. to find a value $\bar{X} \in GL(2, \mathbb{Z}_p)$ with $Inn(\bar{X}) = Inn((x\theta_1(y))^{ab})$.

In the second attack we assume that the attacker does not know any elements from the centralizer of $x\theta_1(y)$. This might be the case when the mapping $Inn(g)$ is represented in a different way. We show that in this case two plaintext-ciphertext pairs are sufficient to decrypt all future ciphertexts.
This attack also demonstrates that the special conjugacy problem might also be easy in $GL(2, \mathbb{Z}_p)$ if pairs $(A_i, Inn(A_i))$ are given, but only parts of the matrices A_i are known.

4.1 Attack with Known Centralizer

The attacker is given a message $m \in \mathbb{Z}_p$ and the corresponding ciphertext

$$C = (C_1, 0) = (x, y)^{ab}(M, 0)(x, y)^{-ab} = ((x\theta_1(y))^{ab} M (x\theta_1(y))^{-ab}, 0)$$

where $M = \begin{pmatrix} m & r \\ s & t \end{pmatrix} \in GL(2, \mathbb{Z}_p)$ with $r, s, t \in_R \mathbb{Z}_p$. We further assume that the attacker knows an element $X = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \in Z(x\theta_1(y))$ with $X \notin Z(M)$.

Since $tr(M) = tr(C_1)$ and $det(M) = det(C_1)$ the attacker can compute t and $r \cdot s$. We now use the trick of section 3.2 attack 1: $C_1 \cdot X = (x\theta_1(y))^{ab}(M \cdot X)(x\theta_1(y))^{-ab}$ and $tr(C_1 \cdot X) = tr(M \cdot X) = mx + rw + sy + tz$. This is sufficient to calculate r and s.[2]

With (M, C_1) and $(X \cdot M, X \cdot C_1)$ we get two instances of the conjugacy problem in $GL(2, \mathbb{Z}_p)$. From $X \notin Z(M)$ we get that $M \notin Z(X \cdot M)$. Thus,

[2] The matrix M can also be completely reconstructed if the semi-direct product group is used, i.e. if $C = (C_1, \bar{m}) = (x, y)^{ab}(M, \bar{m})(x, y)^{-ab} = ((x\theta_1(y))^{ab}(M\theta_1(\bar{m}))(x\theta_1(y))^{-ab}\theta_1(-\bar{m}), \bar{m})$. Since $\theta_1(\bar{m})$ and m are known, the evaluation of $tr(C_1\theta_1(\bar{m}))$ and $tr(XC_1\theta_1(\bar{m}))$ results in two linear equations in the variables r, s and t. We further know that $det(M) = det(C_1)$ which is sufficient to derive matrix M.

the two instances (M, C_1) and $(X \cdot M, X \cdot C_1)$ are sufficient to solve the special conjugacy problem in $GL(2, \mathbb{Z}_p)$, i.e. to find a matrix $\bar{X} \in GL(2, \mathbb{Z}_p)$ with $Inn(x\theta_1(y)) = Inn(\bar{X})$ (see appendix A.2).
This value $\bar{X}$ can be used to decrypt all following ciphertexts that where encrypted using the same encryption exponent b.

4.2 Attack without Centralizer Elements

We now assume that the attacker is given two plaintext messages $m_1, m_2 \in \mathbb{Z}_p$ and $\bar{A} = XAX^{-1} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$ and $\bar{B} = XBX^{-1} = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$ where $A = \begin{pmatrix} m_1 & r_1 \\ r_2 & r_3 \end{pmatrix}$ and $B = \begin{pmatrix} m_2 & s_1 \\ s_2 & s_3 \end{pmatrix}$ and $r_1, r_2, r_3, s_1, s_2, s_3 \in_R \mathbb{Z}_p$[3].

From the traces of $\bar{A}$ and $\bar{B}$ the attacker gets $tr(\bar{A}) = tr(A) = m_1 + r_3$ and $tr(\bar{B}) = tr(B) = m_2 + s_3$. Using the plaintexts m_1 and m_2 he is able to calculate r_3 and s_3. Evaluating the determinant $det(\bar{A}) = det(A) = m_1 \cdot r_3 - r_1 \cdot r_2$ the attacker is further able to compute $r_1 \cdot r_2$ resp. $s_1 \cdot s_2$.

We now use the homomorphic property of the conjugation map. Since $tr(\bar{A}\bar{B}) = tr(XABX^{-1}) = tr(AB) = m_1m_2 + r_1s_2 + r_2s_1 + r_3s_3$, we get $r_1s_2 + r_2s_1$.

By solving the quadratic equation

$$x^2 - (r_1s_2 + r_2s_1)x + s_1s_2r_1r_2 = 0$$

we get the two values $r_1 \cdot s_2$ and $r_2 \cdot s_1$ (we have to guess which of the two solutions equals $r_1 \cdot s_2$ and which equals $r_2 \cdot s_1$).

We now take a closer look at equation $\bar{A}X = XA$ which is equivalent to $\bar{A} = XAX^{-1}$ and describe it as a system of linear equations:

$$\begin{array}{rrrrrrrrr}
(m_1 - \bar{a})x & + & r_2y & - & \bar{b}w & & & = 0 \\
r_1x & + (r_3 - \bar{a})y & & & & - & \bar{b}z & = 0 \\
-\bar{c}x & & & + (m_1 - \bar{d})w & + & r_2z & & = 0 \\
& - & \bar{c}y & + & r_1w & + (r_3 - \bar{d})z & & = 0
\end{array}$$

By adding the linear equations resulting from $\bar{B}X = XB$ and simplifying the system by removing redundant equations we get:

$$\begin{array}{rrrrr}
x + & & \frac{s_2(\bar{d}-m_1)-r_2(\hat{d}-m_2)}{\bar{c}(\hat{d}-m_2)-\hat{c}(\bar{d}-m_1)}z & & = 0 \\
& y + & (\frac{\bar{d}-r_3}{\bar{c}} + \frac{\hat{c}r_1r_2-\bar{c}r_1s_2}{\bar{c}(\bar{c}(\hat{d}-m_2)-\hat{c}(\bar{d}-m_1))})z & & = 0 \\
& & w + & \frac{\hat{c}r_2-\bar{c}s_2}{\bar{c}(\hat{d}-m_2)-\hat{c}(\bar{d}-m_1)}z & = 0
\end{array}$$

[3] If the two MOR ciphertexts $C(m_1) = (\bar{A}, 0) = ((x\theta_1(y))^{ab}A(x\theta_1(y))^{-ab}, 0)$ and $C(m_2) = (\bar{B}, 0) = ((x\theta_1(y))^{ab}B(x\theta_1(y))^{-ab}, 0)$ are given, we get this form by setting $X = (x\theta_1(y))^{ab}$.

Since we know the values $r_1 \cdot r_2$ and $r_1 \cdot s_2$, we are able to express s_2 as $s_2 = k \cdot r_2$ for a $k \in \mathbb{Z}_p$. Thus we get $x = c_1 r_2 z$, $y = c_2 z$ and $w = c_3 r_2 z$ where $c_1 = \frac{(\hat{d}-m_2)-k(\bar{d}-m_1)}{\bar{c}(\hat{d}-m_2)-\hat{c}(\bar{d}-m_1)}$, $c_2 = \frac{r_3-\bar{d}}{\bar{c}} + \frac{\bar{c}r_1 s_2 - \hat{c}r_1 r_2}{\bar{c}(\bar{c}(\hat{d}-m_2)-\hat{c}(\bar{d}-m_1))}$ and $c_3 = \frac{k\bar{c}+\hat{c}}{\bar{c}(\hat{d}-m_2)-\hat{c}(\bar{d}-m_1)}$.

Since $\bar{a} = \frac{1}{detX}(m_1 xz + r_2 yz - r_1 xw - r_3 yw) = \frac{1}{detX} r_2 z^2 (m_1 c_1 + c_2 - r_1 r_2 c_1 c_3 - r_3 c_2 c_3)$ we get $r_2 z^2 = \frac{\bar{a} \cdot detX}{m_1 c_1 + c_2 - r_1 r_2 c_1 c_3 - r_3 c_2 c_3} =: c_4 \cdot detX$.

The values c_1, c_2, c_3 and c_4 are all that is necessary to decrypt arbitrary ciphertexts that are encrypted using the same matrix X. Assume that we are given a matrix $XCX^{-1} = \bar{C} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix}$ where $C = \begin{pmatrix} m_3 & t_1 \\ t_2 & t_3 \end{pmatrix}$ is completely unknown. We know that

$$\begin{aligned} m_3 &= \frac{1}{detX}(\tilde{a}xz - \tilde{c}xy + \tilde{b}wz - \tilde{d}xy) \\ &= \frac{1}{detX} r_2 z^2 (\tilde{a}c_1 - \tilde{c}c_1 c_2 + \tilde{b}c_3 - \tilde{d}c_2 c_3) \\ &= c_4(\tilde{a}c_1 - \tilde{c}c_1 c_2 + \tilde{b}c_3 - \tilde{d}c_2 c_3) \end{aligned}$$

and get the desired cleartext message by using the components of the ciphertext in combination with the precomputed constants c_1, c_2, c_3 and c_4. In a similar way all other components of C can be calculated.

5 Conclusion

In section 3.1 we showed that $x\theta_1(y)$ and $(x\theta_1(y))^a$ can be extracted from $Inn((x,y))$ and $Inn((x,y)^a)$. Hence, for the security of MOR using $G = SL(2,\mathbb{Z}_p) \times_\theta \mathbb{Z}_p$ it is necessary to choose $(x,y) \in G$ such that the discrete log problem is hard in the subgroup generated by $(x\theta_1(y))$. In particular, (x,y) must not be chosen such that $x\theta_1(y) = A(I + c\delta_{12})A^{-1}$ where $c \in \mathbb{Z}_p$ and $A \in SL(2,\mathbb{Z}_p)$ as proposed in [5].

With the ciphertext-only attacks from section 3.2 it is possible to determine the whole plaintext message if only one component is known. This attacks works in $SL(2,\mathbb{Z}_p)$ as well as in $SL(2,\mathbb{Z}_p) \times_\theta \mathbb{Z}_p$. To prevent this attack we recommend to use padding. Using the padding technique from [5] remark 4 (see section 4) and choosing the encryption exponent b randomly for every ciphertext is a good countermeasure against the presented attack.

The most critical point we discussed is fixing the encryption exponent b and using it for multiple encryptions. Without padding the resulting system is vulnerable to known plaintext attacks. If one plaintext-ciphertext pair is known all following ciphertexts can be decrypted. In section 4 we showed that the padding technique from [5] does not make the system more secure. It is an open question whether the MOR system (with fixed exponent) can be made secure by using an appropriate padding technique.

If MOR is used with $SL(2,\mathbb{Z}_p) \times_\theta \mathbb{Z}_p$, an appropriate padding technique and the encryption exponent is chosen uniformly and independently for every plaintext to be encrypted, the resulting system seems to offer a reasonable amount

of security (though there still is no formal proof). On the other hand calculating $Inn(g^b)$ and $Inn(g^{ab})$ from $Inn(g)$ and $Inn(g^a)$ which then is necessary for every single encryption process is computationally very expensive which makes the system less efficient than RSA and ElGamal.

References

[1] I. Anshel, M. Anshel, D. Goldfeld, "An Algebraic Method for Public-Key Cryptography", Mathematical Research Letters, 6 (1999), pp.287-291 176

[2] S. Blackburn, S. Galbraith, "Cryptanalysis of two cryptosystems based on group action", Advances in Cryptology - Asiacrypt 1999, LNCS 1716 176

[3] K. H. Koo, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park, "New Public-Key Cryptosystem Using Braid Groups", Advances in Cryptology - Crypto 2000, LNCS 1880, pp. 166-183 176

[4] E. Lee, S. J. Lee, S. G. Hahn, "Pseudorandomness from Braid Groups", Advances in Cryptology - Crypto 2001, LNCS 2139 176

[5] Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, Choonsik Park, "New Public Key Cryptosystem Using Finite Non Abelian Groups", Advances in Cryptology - Crypto 2001, LNCS 2139 175, 176, 177, 178, 179, 181, 184

[6] Seong-Hun Paeng, Daesung Kwon, Kil-Chan Ha, Jae Heon Kim "Improved public key cryptosystem using finite non abelian groups", IACR EPrint-Server, Report 2001/066, http://eprint.iacr.org/2001/066 175

[7] A. Yamamura, "Public key cryptosystems using the modular group", 1st International Public Key Cryptography Conference PKC 1998, LNCS 1431 176

[8] A. Yamamura, "A functional cryptosystem using a group action", 4th Australian Information Security and Privacy Conference ACISP 1999, LNCS 1587 176

A General Results for Matrix Groups

A.1 Computing Centralizers in $GL(2, \mathbb{Z}_p)$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z}_p)$ with $c \neq 0$. Then centralizer elements $C \in Z(A)$ are of the form

$$C = \begin{pmatrix} z + \frac{a-d}{c}w & \frac{b}{c}w \\ w & z \end{pmatrix} = \begin{pmatrix} \frac{a-d}{c}w & \frac{b}{c}w \\ w & 0 \end{pmatrix} + z \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

for arbitrary $w, z \in \mathbb{Z}_p$.

A.2 The Conjugacy Problem in $GL(2, \mathbb{Z}_p)$ and $SL(2, \mathbb{Z}_p)$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\hat{A} = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$ be a given instance of the conjugacy problem, i.e. a matrix $X = \begin{pmatrix} x & y \\ w & z \end{pmatrix}$ satisfying $\hat{A} = X \cdot A \cdot X^{-1}$ has to be found.

If we write $\hat{A} = X \cdot A \cdot X^{-1}$ as $\hat{A} \cdot X = X \cdot A$, we get the following system of linear equations:

$$\begin{array}{rrrrrrrrr}
(a-\hat{a})\cdot x & + & c\cdot y & - & \hat{b}\cdot w & & & = 0\\
b\cdot x & + & (d-\hat{a})\cdot y & & & - & \hat{b}\cdot z & = 0\\
-\hat{c}\cdot x & & & + & (a-\hat{d})\cdot w & + & c\cdot z & = 0\\
& - & \hat{c}\cdot y & + & b\cdot w & + & (d-\hat{d})\cdot z & = 0
\end{array}$$

By removing redundant equations one gets:

$$\begin{array}{rrrrr}
x & + (\frac{\hat{d}-a}{\hat{c}})\cdot w - & \frac{c}{\hat{c}}\cdot z & = 0\\
y - & \frac{b}{\hat{c}}\cdot w & + \frac{\hat{d}-d}{\hat{c}}\cdot z & = 0
\end{array}$$

(Note that we only considered the case that $\hat{c} \neq 0$. The case $\hat{c} = 0$ is analogue.)

That means that the matrices that solve the conjugacy problem are of the form $\bar{X} = \begin{pmatrix} \frac{c}{\hat{c}}\cdot z + \frac{a-\hat{d}}{\hat{c}}\cdot w & \frac{b}{\hat{c}}\cdot w + \frac{d-\hat{d}}{\hat{c}}\cdot z \\ w & z \end{pmatrix}$ where $w, z \in \mathbb{Z}_p$.

In $SL(2, \mathbb{Z}_p)$ we further know that $det(\bar{X}) = 1$ and can replace w by a term depending only on z.

Let $G \in \{GL(2, \mathbb{Z}_p), SL(2, \mathbb{Z}_p)\}$. Given only one instance of the conjugacy problem in G, i.e. $M, \bar{M} = XMX^{-1} \in G$, the solution set for the CP is $L = X \cdot Z(M)$.

If more than one instance is given, i.e. $M_1, M_2, \bar{M_1} = XM_1X^{-1}, \bar{M_2} = XM_2X^{-1} \in G$ that does not necessarily imply that the solution set can further be narrowed. If $M_1 \in Z(M_2)$ the solution set is still $L = X \cdot Z(M)$. If $M_1 \notin Z(M_2)$ the solution set is $L = X \cdot Z(G)$.

Since $Inn(g) = Inn(g \cdot z)$ for $z \in Z(G)$ and for all $g \in G$ we are able to solve the special conjugacy problem in the latter case.

Remark: If $(M_1, \bar{M_1} = XM_1X^{-1})$ with $M_1 \notin Z(X)$ is an instance of the conjugacy problem and an element $\hat{X} \in Z(X)$ with $\hat{X} \notin Z(M_1)$ is known, we can easily construct a second instance $(M_2, \bar{M_2})$ with $M_1 \notin Z(M_2)$ of the conjugacy problem by setting $M_2 = \hat{X}M_1$ and $\bar{M_2} = \hat{X}\bar{M_1} = X(\hat{X}M_1)X^{-1}$.