Contemporary Mathematics
Volume **633**, 2015
http://dx.doi.org/10.1090/conm/633/12653

The MOR cryptosystem and finite p-groups

Ayan Mahalanobis

Abstract. The ElGamal cryptosystem is the most widely used public-key cryptosystem. It uses the discrete logarithm problem as the cryptographic primitive. The MOR cryptosystem is a similar cryptosystem. It uses the discrete logarithm problem in the automorphism group as the cryptographic primitive. In this paper, we study the MOR cryptosystem for finite p-groups. The study is complete for p'-automorphisms. For p-automorphisms there are some interesting open problems.

1. Introduction

This is a study of the MOR cryptosystem using finite p-groups. Similar studies were done by this author [**11**, **12**]. The MOR cryptosystem, that we are going to describe in details shortly, works with the automorphism group of a group. As a matter of fact, we do not even need a group. Any finitely presented structure on which automorphisms can be defined will do. We can define the MOR cryptosystem on that structure. However, a MOR cryptosystem might not be secure or implementation-friendly. So this paper can be seen as a search for favorable groups for the MOR cryptosystem in the class of finite p-groups.

Once we decide that we will look into the class of p-groups, an obvious question surfaces. Are there p-groups on which the cryptosystem is secure? Once the answer is yes, then is it any better than the existing one? So we have three questions in front of us:

1: Are there favorable p-groups?
2: Is the cryptosystem secure[1] on those groups?
3: Is the cryptosystem faster on those groups compared to a suitably defined ElGamal cryptosystem?

To answer these questions, we had to divide the automorphisms in two different classes. One, p-automorphisms and the other p'-automorphisms. For p'-automorphisms we show that there are secure MOR cryptosystems on a p-group. However, they offer no advantage than working with matrices over the finite field $\mathbb{F}_p$. So,

2010 *Mathematics Subject Classification.* Primary 94A60, 20D15.
Key words and phrases. MOR cryptosystem, finite p-groups, the discrete logarithm problem.
This research was supported by a NBHM research grant.

[1]There are many different definitions of security, we use the basic one – find m, from the automorphism ϕ and its power ϕ^m.

after reading this paper, one might argue and rightfully so: instead of using p'-automorphisms and p-group, why not just use matrices of the right size?

The case for p-automorphisms is little complicated and we say upfront that we have not been able to analyze it completely. The case of p-automorphisms break down into two sub-cases and we were able to deal with one easily. The other case is very interesting and we were able to shed some light into that with an example. However, a detailed analysis is missing and we leave it as ongoing research. The situation with p-automorphisms compared to p'-automorphisms is in many ways similar to the modular representation theory compared to the ordinary representation theory. The later is much easier to deal with than the former.

2. Definitions and notations

Most of the definitions used in this paper are standard and in Gorenstein [**3**]. However, we define a few of them for the convenience of the reader. All groups in this paper are finite. We use p for a prime and q for a prime-power.

DEFINITION 2.1 (p'-automorphisms and p-automorphisms). An automorphism ϕ of a p-group G is a p-automorphism if its order is power of p and p'-automorphism if its order is coprime to p.

In general, it is not true that an automorphism is either a p-automorphism or a p'-automorphism. However, for the purpose of understanding the security of a MOR cryptosystem, due to the Pohlig-Hellman algorithm [**5**, Section 2.9], an automorphism is either a p-automorphism or a p'-automorphism.

DEFINITION 2.2 (Special p-group). Usually, a special p-group is defined to be a p-group such that $\mathcal{Z}(G) = G' = \Phi(G)$ and is elementary-abelian. Here G', $\mathcal{Z}(G)$ and $\Phi(G)$ are the commutator subgroup, the center and the Frattini subgroup respectively. However, it is not very hard to show that the elemetary-abelian part is redundant.

DEFINITION 2.3 (Favorable p-group). A p-group G is called a favorable p-group, if there is a non-identity p'-automorphism ϕ of the group, such that, if the automorphism fixes a proper subgroup H of G, it is the identity on H.

A good example of a favorable p-group is the elementary-abelian p-group, denoted by G. Any automorphism of that can be realized as a matrix. If the characteristic polynomial of an automorphism ϕ is irreducible, then there are no ϕ-invariant proper subgroups of G. So the above condition is true vacuously.

A curious reader might find the requirement "p'-automorphism ϕ" unnecessary. The reason for the restriction is, for p'-automorphisms favorable p-groups is the right notion to look at. If there is a subgroup that is fixed by ϕ, one can study the discrete logarithm problem on the action of the automorphism on that subgroup, unless the automorphism is the identity on that subgroup. We will see, in the case of p'-automorphisms, the discrete logarithm problem in the automorphism group translates to the discrete logarithm problem in non-singular matrices. In the case of p-automorphisms, it is not clear if the notion of favorable p-group is the best way to go. We simply don't have enough examples of secure MOR cryptosystem using p-automorphisms of p-groups yet. So we refrain ourselves from defining favorable p-groups for p-automorphisms.

3. The MOR cryptosystem

In this section, we provide a somewhat detailed description of a small but important portion of *public-key cryptography*. We start with a cryptographic primitive – *the discrete logarithm problem*. The standard reference for public-key cryptography is Hoffstein et. al. [**5**].

DEFINITION 3.1 (The discrete logarithm problem). Let $G = \langle g \rangle$ be a finite cyclic group of prime order. We are given g and g^m for some $m \in \mathbb{N}$. The discrete logarithm problem is to find the smallest m.

The discrete logarithm problem is neither secure or insecure. It being secure or insecure is a property of the presentation of the group. The property of being secure or insecure is not a group theoretic property, it is not invariant under isomorphism.

The discrete logarithm problem is the easiest in prime subgroups of $(\mathbb{Z}_n, +)$ and is considered secure in prime subgroups of the multiplicative group of a finite field $\mathbb{F}_q^\times$ and is considered really secure in a prime order subgroup of the rational points of an elliptic curve. The difference in security between finite fields and points on elliptic curve is, there is no known sub-exponential attack against the elliptic curves.

A concept related to the discrete logarithm problem is the **Diffie-Hellman problem**. We have the same G as before, this problem is: given g, $g^{m'}$ and $g^{m''}$ compute $g^{m'm''}$. It is clear that if we know how to solve the discrete logarithm problem, i.e., we can find m' (or m''), we can then solve the Diffie-Hellman problem. The reverse direction is not known.

The most popular and prolific public-key cryptosystem is the *ElGamal cryptosystem*. It works in any cyclic subgroup of a group G. However, it might not be secure in any group.

3.1. Description of the ElGamal cryptosystem.

Private Key: m, $m \in \mathbb{N}$.
Public Key: g and g^m.

Encryption.

a: To send a message (plaintext) $a \in G$ Bob computes g^r and g^{mr} for a random $r \in \mathbb{N}$.
b: The ciphertext is $(g^r, g^{mr}a)$.

Decryption.

a: Alice knows m, so if she receives the ciphertext $(g^r, g^{mr}a)$, she computes g^{mr} from g^r and then g^{-mr} and then computes a from $g^{mr}a$.

It is known that the security of the ElGamal cryptosystem is equivalent to the Diffie-Hellman problem [**5**, Proposition 2.10]. A very similar idea is the MOR cryptosystem.

3.2. Description of the MOR cryptosystem. Let $G = \langle g_1, g_2, \ldots, g_\tau \rangle$, $\tau \in \mathbb{N}$ be a finite group and ϕ a non-trivial automorphism of G. Alice's keys are as follows:

Private Key: m, $m \in \mathbb{N}$.
Public Key: $\{\phi(g_i)\}_{i=1}^{\tau}$ and $\{\phi^m(g_i)\}_{i=1}^{\tau}$.

Encryption.

a: To send a message (plaintext) $a \in G$ Bob computes ϕ^r and ϕ^{mr} for a random $r \in \mathbb{N}$.

b: The ciphertext is $(\{\phi^r(g_i)\}_{i=1}^{\tau}, \phi^{mr}(a))$.

Decryption.

a: Alice knows m, so if she receives the ciphertext $(\phi^r, \phi^{mr}(a))$, she computes ϕ^{mr} from ϕ^r and then ϕ^{-mr} and then computes a from $\phi^{mr}(a)$.

Alice knows the order of the automorphism ϕ, she can use the identity $\phi^{t-1} = \phi^{-1}$ whenever $\phi^t = 1$ to compute ϕ^{-mr}.

It is easy to see the following: if one can solve the Diffie-Hellman problem in $\langle\phi\rangle$, he can break the MOR cryptosystem. This follows from the fact that ϕ^r and ϕ^m are public. If one can solve the Diffie-Hellman problem, one can compute ϕ^{mr} and get the plaintext. The next theorem proves the converse.

THEOREM 3.1. *If there is an oracle that can decrypt arbitrary ciphertext for the MOR cryptosystem, one can solve the Diffie-Hellman problem in* $\langle\phi\rangle$.

PROOF. Assume that there is an oracle that can decrypt arbitrary MOR ciphertext. Now recall that $a = \phi^{-mr}(\phi^{mr}(a))$. Now suppose we have $\phi^{m'}$ and $\phi^{m''}$ and we want to compute $\phi^{m'm''}$. Then tell the oracle that $\phi^{m'}$ is the public key and $\left(\phi^{m''}, g_i\right)$ is the ciphertext. The oracle will return $\phi^{-m'm''}(g_i)$ as the plaintext. Once this game is played for $i = 1, 2, \ldots, \tau$. We know $\phi^{-m'm''}(g_i)$ for $i = 1, 2, \ldots, \tau$ and hence $\phi^{m'm''}$. Thus solving the Diffie-Hellman problem in $\langle\phi\rangle$. •

In this paper we are primarily interested in exploring finite p-groups for the purpose of building a *secure* MOR cryptosystem. As is well known, security and computational efficiency goes hand in hand. So unless we explore the computational complexity of the MOR cryptosystem, a security analysis is useless. So there are two questions that we will explore in this paper:

a: Is it possible to build a secure MOR cryptosystem using finite p-groups?

b: Does this MOR cryptosystem has any advantage over existing cryptosystems?

Before we answer these questions, we need to explain one aspect of the security of the discrete logarithm problem. It is easy to see, using the Chinese remainder theorem, that the discrete logarithm problem in any cyclic group can be reduced to a discrete logarithm problem in its Sylow subgroups. Then a discrete logarithm problem in the Sylow subgroup can be further reduced to the discrete logarithm problem in a group of prime order [**5**, Section 2.9]. The end result is: the security of the discrete logarithm problem in a group is the security of the discrete logarithm problem in the largest prime-order subgroup in that group. In practice, the group considered for an efficient and secure implementation of the discrete logarithm problem is a group of prime order[2]. From the above argument, it is clear that we should only study **automorphisms of prime order** for the MOR cryptosystem.

One way to study automorphisms of a finite p-group for the MOR cryptosystem is using linear methods in nilpotent groups [**6**, Chapter VIII]. That is our principal

[2]The reader must have noticed that in the definition of the discrete logarithm problem we used groups of prime order.

objective in this paper. The idea is to find a series of subgroups such that automorphisms act linearly either on the subgroups or the quotients. We will soon assume, if a subgroup is fixed under an automorphism then it is the identity on that subgroup. With this assumption, we only have to look at the action of an automorphism on the sections of the series.

With these in mind, we look at the exponent-p central series of a finite p-group G. The series is defined as follows:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_k = 1$$

where $G_{i+1} = [G, G_i]\, G_i^p$. This series is well known to have elementary-abelian quotients and is used in many aspects of computations with finite p-groups [**14**].

There are two possible orders of an automorphism of a p-group for the MOR cryptosystem:

i: The automorphism ϕ is of order p.
ii: The order of ϕ is a prime different from p, i.e., a p'-automorphism.

This can again be subdivided into four different cases:

a: The automorphism is of order p and is identity on all the quotients of the exponent-p central series.
b: The automorphism is of order p and is not identity on at least one section of the exponent-p central series.
c: The automorphism is of order p' and is not identity on at least one section of the exponent-p central series.
d: The automorphism is of order p' and is identity on all sections of the exponent-p central series.

Recall that G_1 is the Frattini subgroup $\Phi(G)$. A well known theorem of Burnside says that:

THEOREM 3.2 (Burnside). *Let ϕ be an automorphism of a group G. If the greatest common divisor,* $\gcd(\mathrm{o}(\phi), |\Phi(G)|) = 1$ *and ϕ induces the identity automorphism on $G/\Phi(G)$, ϕ is the identity automorphism on G.*

PROOF. For a proof see [**1**, Theorem 1.15] or [**3**, Theorem 5.1.4]. •

This says, the case c above reduces to: the automorphism ϕ is of order p' and is not identity on $G/\Phi(G)$. In this case ϕ acts on $G/\Phi(G)$ linearly and the discrete logarithm problem in ϕ deduces to the discrete logarithm problem in matrices over $\mathbb{F}_p$. The size of the matrix is the same as the cardinality of a set of minimal generators of the p-group.

It is also well known, if d is the case then ϕ is the identity [**3**, Theorem 5.3.2]. So there is no point studying d.

So we have three cases to look at a, b and c above.

It is well known that usually, the exception being groups of prime order, p-groups come with lots of subgroups and normal subgroups. The most difficult issue that one faces in choosing a p-group and the automorphism ϕ for the MOR cryptosystem is the presence of subgroups of the p-group which is fixed by ϕ. If this happens, the discrete logarithm problem in the automorphism ϕ is reduced to the discrete logarithm problem in the restriction of ϕ to that subgroup. This reduction is most undesirable. On the other hand, working with non-abelian p-groups this reduction is bound to happen. For example, the commutator and the center are non-trivial characteristic subgroups. The way out of this situation is to

ensure, if ϕ fixes any subgroup then it is the identity on that subgroup. Once this condition is imposed, we will see that favorable groups with p'-automorphism are reduced to either the elementary abelian p-group or the class of p-groups G with $G' = \mathcal{Z}(G) = \Phi(G)$ and $\Phi(G)$ is elementary abelian. Here G' is the commutator subgroup, $\mathcal{Z}(G)$ is the center and $\Phi(G)$ is the Frattini subgroup of G. These two class of groups together are known as **special p-groups**.

4. MOR cryptosystems on finite p-groups using p'-automorphisms

In this section we look at the MOR cryptosystem over finite p-groups with p'-automorphisms. Our standard reference for group theory is Gorenstein [**3**] and for linear algebra is Roman [**15**]. We start with a generalization of a celebrated theorem from the odd-order paper.

THEOREM 4.1. *A solvable group G possesses a characteristic subgroup C with the following properties:*

- *Subgroup C is nilpotent with nilpotency class less than or equal 2.*
- *$\mathcal{Z}(C)$ is a maximal characteristic abelian subgroup of G.*
- *$\mathcal{C}_G(C) = \mathcal{Z}(C)$.*
- *Every nontrivial p'-automorphism of G induces a non-trivial automorphism on C.*

For a proof see [**1**, Theorem 14.1]. The subgroup C is called a *Thompson critical subgroup*. We will refer to it as a critical subgroup. There can be more than one critical subgroup in a group. It is clear from the theorem above, in our search for favorable p-groups, we should look at p-groups whose only critical subgroup is the whole group. We will call those groups **self-critical**. Since a self-critical group is of class at most 2, we should look at p-groups of class at most 2. Now if p is odd, in a p-group of class 2, $(xy)^p = x^p y^p$. This makes the subgroup $\Omega_1(G)$ of exponent p. Since $\Omega_1(G)$ is characteristic the following corollary follows immediately.

COROLLARY 4.2. *For an odd prime p, favorable p-groups are of class at most 2 with exponent p.*

Before we go any further we need to state a well known theorem due to Hall and Higman [**4**, Theorem C]. The proof is available in many standard textbooks [**3**, Theorem 5.3.7], so we won't reproduce it.

THEOREM 4.3. *Let G be a favorable p-group, then G/G' is elementary abelian.*

To summarize, favorable p-groups are of class at most 2 and G/G' is elementary-abelian. It follows that $G' \leq \mathcal{Z}(G)$. Then both G/G' and $G/\mathcal{Z}(G)$ are elementary abelian p-groups. We also have a p'-automorphism ϕ, such that, if ϕ fixes a subgroup of G, it is the identity on that subgroup. In particular, ϕ is the identity on G' and $\mathcal{Z}(G)$.

There are two different ways to look at this situation:

Ordinary representation theory. Let $A = \langle \phi \rangle$ be the subgroup generated by ϕ. Since ϕ is a p'-automorphism, the order of A is coprime to the order of the group G. We have a coprime action of A on G. In particular, we have a linear action of A on $V = G/G'$. Since this action is coprime we have the celebrated Maschke's theorem [**3**, Theorem 3.3.1] at our disposal. The theorem states, if we have an A-invariant proper subspace $W \subset V$, it has an A-invariant complement. In other words there is an A-invariant subspace W' of V such that $V = W \oplus W'$.

Linear algebra. Another way to look at the same situation is by linear algebra. Let $V = G/G'$. Clearly V is a finite dimensional vector-space over $\mathbb{F}_p$. Corresponding to a linear transformation ϕ of V, we can define scalar multiplication such that V is a finitely generated module over the principal ideal domain $\mathbb{F}_p[x]$ [**15**, Chapter 7]. We denote this module by V_ϕ. The reason we are interested in this module V_ϕ is that the submodules of V_ϕ are the ϕ-invariant subspaces of V. With this we have the full force of the theory of finitely generated modules over a principal ideal domain at our disposition; especially the decomposition theorem.

The minimal polynomial of ϕ is a generator of the annihilator ideal of V_ϕ in $\mathbb{F}_p[x]$. We denote it by $\mathfrak{m}_\phi$ and assume it to be monic. Let $\mathfrak{m}_\phi = f_1^{m_1}(x)f_2^{m_2}(x)\ldots - f_k^{m_k}(x)$ be the decomposition of $\mathfrak{m}_\phi$ as product of irreducible monic polynomials. One can write $V_\phi = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ where a generator of the annihilator ideal of each *primary component* V_i is $f_i^{m_i}$. Each V_i can either be cyclic or can be broken down as direct sum of cyclic modules. This theory is very well-known and successful, so we will omit the details and ask any interested reader to consult a textbook in linear algebra – Roman [**15**] being one of them.

LEMMA 4.4. *Let ϕ be a non-identity p'-automorphism on V, where V is a finite-dimensional vector space over $\mathbb{F}_p$; such that, if ϕ fixes a subspace of V then it is the identity on that subspace. The following is true:*

a. *The characteristic polynomial χ_ϕ of ϕ is irreducible.*
b. *The module V_ϕ is simple.*

PROOF. Recall that V_ϕ is a finitely generated module over a principal ideal domain $\mathbb{F}_p[x]$. Let $\mathfrak{m}_\phi$ be the minimal polynomial of V_ϕ. Assume that $\mathfrak{m}_\phi = f_1^{m_1}(x)f_2^{m_2}(x)\ldots f_k^{m_k}(x)$, where each $f_i(x)$ is monic irreducible over $\mathbb{F}_p$ and each m_i is a non-negative integer. Define the set

$$V_i = \{v \in V_\phi \ : \ f_i^{m_i}(\phi)v = 0\}.$$

Then the fundamental theorem of finitely generated module over a principal ideal domain says that $V_\phi = V_1 \oplus V_2 \oplus \ldots \oplus V_k$. Now assume for a moment that k is greater than 1. Then we have V_ϕ as direct sum of non-trivial submodules. Recall that submodules of V_ϕ are the ϕ-invariant subspaces of V. Then we have that V is a direct sum of two ϕ-invariant subspaces of V. So ϕ acts like identity on both these subspaces and hence is the identity on V. So this subspace decomposition is impossible, forcing k to be 1.

We have deduced that $\mathfrak{m}_\phi = f(x)^l$ where $f(x)$ is monic irreducible and l is a positive integer. If l is greater than 1, take the subspace $V' = \{v \in V_\phi \ : \ f^{l-1}(\phi)v = 0\}$. Also construct the subgroup $A = \langle\phi\rangle$. Since $\gcd(|A|, p) = 1$, from Maschke's theorem the subspace V' has a complement. This means that there is another A-invariant subspace V'' such that $V = V' \oplus V''$. Then using an argument similar to the one in last paragraph, we show that $l = 1$ and the minimal polynomial $\mathfrak{m}_\phi$ is irreducible.

From the above discussion it follows clearly that the module V_ϕ is cyclic with irreducible minimal polynomial. Since a cyclic module with irreducible minimal polynomial is non-derogatory [**15**, Theorem 7.11], we have the characteristic polynomial the same as the minimal polynomial.

The fact the module is simple, follows from the fact that the minimal polynomial of any submodule will divide the minimal polynomial of the module and the minimal polynomial of the module is irreducible. •

It is easy to prove a partial converse of the above lemma.

LEMMA 4.5. *Let ϕ be a linear transformation on the finite dimensional vector space over $\mathbb{F}_q$. If the characteristic polynomial χ_ϕ is irreducible, the only ϕ-invariant subspaces of V are 0 and V.*

PROOF. We will consider V_ϕ as a module over $\mathbb{F}_q[x]$. Since χ_ϕ is irreducible it is also the minimal polynomial. Now if S is a submodule of V_ϕ, then its minimal polynomial will divide χ_ϕ. Since χ_ϕ is irreducible, we have a proof. •

This lemma is the most useful lemma in this whole paper. This paper is in search of favorable p-groups and the corresponding automorphism. One way, and probably the easiest way, is to look at the characteristic polynomial corresponding to an automorphism. If that characteristic polynomial is irreducible, we have our favorable p-group and the necessary automorphism.

THEOREM 4.6. *A favorable p-group G is a special p-group.*

PROOF. We already know that G is of class at most 2 and $V = G/G'$ is an elementary-abelian p-group. Let ϕ be a p'-automorphism, such that, if it fixes a proper subgroup of G, then it is the identity on that subgroup. Since G' is characteristic, ϕ is the identity on G'. Consider the module V_ϕ over $\mathbb{F}_p[x]$ corresponding to ϕ. Then from the lemma above we know that the characteristic polynomial χ_ϕ is irreducible and V_ϕ is simple.

In any finite p-group, $G' \subseteq \Phi(G)$ and from above $G' \subseteq \mathcal{Z}(G)$. To show $G' = \mathcal{Z}(G)$, notice that V_ϕ is a simple module over $\mathbb{F}_p[x]$ and all submodules are ϕ-invariant subspaces. So $\mathcal{Z}(G)/G'$ cannot be a nontrivial submodule. Similar is the case with $\Phi(G)$.

So if we assume that G is not elementary-abelian, then $G' = \mathcal{Z}(G) = \Phi(G)$. •

At this point it is clear, to build a secure and optimal MOR cryptosystem with non-abelian p-groups one should look at special p-groups and an automorphism ϕ such that ϕ is identity on all subgroup it fixes. In particular ϕ must centralize $\Phi(G)$, so smaller the $\Phi(G)$ the better. So it is clear that we should look for groups with $\Phi(G)$ as small as possible. We conclude that for a non-abelian p-group (p odd) and p'-automorphisms the best group is an extra-special p-group of prime exponent. For abelian p-groups, we should look only at elementary-abelian p-groups. For p even, we still have the extra-special groups but we can use any exponent.

5. The MOR cryptosystem and elementary abelian p-group

As is well known, an elementary abelian p-group is a vector space over $\mathbb{F}_p$ the field of p elements. So one way to look at MOR cryptosystems over an elementary abelian group is MOR cryptosystems over a vector space. If we fix a basis for the vector space, any linear transformation gives rise to a matrix. So the discrete logarithm problem in invertible linear transformations turns out to be the discrete logarithm problem over non-singular matrices. So we need to say a few things about that. Before we do that, we also need to remind our reader that security and speed goes hand in hand. One reason, the discrete logarithm problem in matrices was avoided in cryptography was the belief that matrix exponentiation is much more expensive. The security advantage we gain from the discrete logarithm problem in matrices does not outweigh the cost of matrix exponentiation. This view was

put down by Menezes & Wu [**13**]. However with the recent advances in matrix exponentiation by Leedham-Green [**9**], the above argument is no longer valid. We get into the details of this argument in this section.

5.1. Solving the discrete logarithm problem in non-singular matrices. Let g and g^m belongs to $\mathrm{GL}(d, q)$, the discrete logarithm problem is to find m. This problem can be easy and hard. For uni-triangular matrices, i.e., matrices with one on the diagonal and arbitrary field element on the upper half and zero on the lower half, it is very easy. On the other hand, with matrices with irreducible characteristic polynomial, the discrete logarithm problem is hard.

Following is the work of Menezes & Wu [**13**], which is the best known algorithm to solve the discrete logarithm problem in matrices. This algorithm is basically a reduction of the discrete logarithm problem in $\mathrm{GL}(d, q)$ to a finite (possibly trivial) extension of $\mathbb{F}_q$.

5.2. The Menezes-Wu algorithm.

- Input: g and g^m.
- Output: m.
- From g, compute the characteristic polynomial χ_g of g.
- From g^m, compute the characteristic polynomial χ_{g^m} of g^m.

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ be the characteristic roots of g. This list might contain repeating entries. The characteristic roots lie in some finite (possibly trivial) extension of $\mathbb{F}_q$. Let $\{\beta_1, \beta_2, \ldots, \beta_d\}$ be the characteristic roots of g^m. This list might contain repeating entries. The roots lie in some finite (possibly trivial) extension of $\mathbb{F}_q$.

Then $\{\beta_1, \beta_2, \ldots, \beta_d\}$ is $\{\alpha_{i_1}^m, \alpha_{i_2}^m, \ldots, \alpha_{i_d}^m\}$, where $(i_1, i_2, \ldots, i_d)$ is $(1, 2, \ldots, d)$ permuted. Note that there is no obvious way to order characteristic roots, but following Menezes and Wu, we will assume that this permutation is not going to offer much resistance in computing m. In other words, we assume that we can find α_i and β_j such that $\alpha_i^m = \beta_j$. Once we have this, one can solve for $m \bmod \mathrm{o}(\alpha_i)$, where $\mathrm{o}(\alpha_i)$ is the multiplicative order of α_i. From, solving the required numbers of discrete logarithm problems in the suitable extensions and then applying the Chinese remainder theorem, one can solve the discrete logarithm problem in non-singular matrices. Note that the α_i and subsequently the β_j will be in some extension field (possibly trivial) of $\mathbb{F}_q$. The largest extension possible is $\mathbb{F}_{q^d}$ and this happens when the **characteristic polynomial is irreducible**.

The most serious attack on the discrete logarithm problem in a finite field is the sub-exponential attack like the index-calculus attack. In this attack, if we are solving the discrete logarithm problem in $\mathbb{F}_{q^d}$, the time-complexity of the attack is $\exp\left((c + o(1))(\log q^d)^{\frac{1}{3}}(\log\log q^d)^{\frac{2}{3}}\right)$, where c is a constant, see [**16**] and [**8**, Section 4]. It is clear, larger the d more secure is the discrete logarithm problem in matrices. So we can now safely conclude, to work with the discrete logarithm problem in matrices one should work with **matrices with irreducible characteristic polynomial**.

5.3. Exponentiation in non-singular matrices. This section is a brief introduction to an amazing algorithm by Leedham-Green [**9**, Section 10] to compute g^m for some $g \in \mathrm{GL}(d, q)$. We only deal with the case where the characteristic polynomial χ_g of g is irreducible.

ALGORITHM 5.1 (Leedham-Green).
Input: a matrix g of size d over a finite field $\mathbb{F}_q$ and a positive integer m.
Output: g^m

- *Find a matrix P such that $B = P^{-1}gP$ is in the Frobenius normal form.*
- *Determine the minimal polynomial $\mathfrak{m}(x)$ of B. Since the Smith normal form is sparse, it is easy to compute the minimal polynomial – it takes $O(d^2)$ field multiplications.*
- *Compute $t^m \bmod \mathfrak{m}(t)$ in $F[t]/\mathfrak{m}(t)$ as $\mathfrak{l}(t)$.*
- *Compute $C = \mathfrak{l}(B)$.*
- *Return PCP^{-1}.*

Notice that the objective of the above algorithm was to compute the power of an arbitrary matrix. In our case, for a MOR cryptosystem the matrix is not arbitrary, we can choose our matrix. So one can first choose an irreducible polynomial $\mathfrak{m}$ of degree d over $\mathbb{F}_q$. Then choose g to be the companion matrix for that polynomial $\mathfrak{m}$. Since the minimal polynomial divides the characteristic polynomial, the minimal polynomial is $\mathfrak{m}$ as well. So the first two steps and the last step in the above algorithm becomes redundant.

Once $\mathfrak{m}$ is irreducible in the above algorithm the quotient $\mathbb{F}[t]/\mathfrak{m}(t)$ is a field. So the third step is essentially an exponentiation in the field $\mathbb{F}_{q^d}$. So apart from computing the C in the above algorithm, exponentiation of a matrix with irreducible characteristic polynomial is the same as exponentiation in the finite field $\mathbb{F}_{q^d}$.

The following is now clear: the discrete logarithm problem in $\mathrm{GL}(d, q)$ is almost the same, both in terms of security and speed, to a discrete logarithm problem in $\mathbb{F}_{q^d}$. Note that this conclusion is remarkably different than that of Menezes & Wu [**13**], where they write-off completely the discrete logarithm problem in matrices.

Next we show that elementary-abelian p-groups are favorable p-groups.

LEMMA 5.2. *Let V be a vector space over $\mathbb{F}_p$. Let ϕ be a non-singular linear transformation on V. If $p|o(\phi)$, then V has a proper ϕ-invariant subspace.*

PROOF. Let $A = \langle\phi\rangle$. Then the given condition implies that $p||A|$. Considering the fact that any finite abelian group is the direct product of its Sylow subgroups, we see that one can write $\phi = \phi_p\phi_{p'}$. Where ϕ_p and $\phi_{p'}$ are p and p' non-trivial automorphism respectively. From the fact that $(x^q - 1) = (x - 1)^q$ for any p-power q, we see that all the eigenvalues of ϕ_p are $1 \in \mathbb{F}_p$. Let $\mathcal{E}$ be the eigenspace of 1 in V. Clearly $\mathcal{E}$ is a proper subspace of V. Let $v \in \mathcal{E}$. Then $\phi_p\phi_{p'}(v) = \phi_{p'}\phi_p(v)$, which implies $\phi_p\phi_{p'}(v) = \phi_{p'}(v)$. This proves that $\phi_{p'}(v) \in \mathcal{E}$. So $\mathcal{E}$ is a ϕ-invariant proper subspace of V. •

THEOREM 5.3. *An elementary-abelian p-group is a favorable p-group.*

PROOF. An elementary abelian p-group V is a vector space over $\mathbb{F}_p$. Then the automorphism group of V is $\mathrm{GL}(V)$. Let ϕ be an automorphism with irreducible characteristic polynomial. Then ϕ is a p'-automorphism. Then Lemma 4.5 proves the rest. •

6. The extra-special p-groups and its automorphism group

As we saw before, if we are dealing with p'-automorphisms, there are only two interesting class of finite p-groups. One is the elementary abelian p-group

and the other is extra-special p-groups. The case for extra special p-groups is interesting, because it provides us with non-abelian p-groups which is presented in the *power-commutator* form and provides us with a secure MOR cryptosystem; thus showing that abstract presentations can be useful. As we will see, the security with p'-automorphisms reduces to the discrete logarithm problem in non-singular matrices. This enables us to argue that working with p'-automorphisms of a p-group, one has no advantage from working with matrices. However, the case with p-automorphisms is not quite settled yet. We will see, as an example with the central automorphisms of the extra-special p-groups that there are some potential with p-groups. The potential is the impossibility of the reduction to matrices, which killed the p'-automorphisms.

6.1. Extra-special p-groups. It is well known that any special p-group is of exponent at most p^2. We saw earlier that for odd prime p we can concentrate on groups of exponent p. So for an odd prime p our principal interest is in the extra-special p-group of exponent p. Our principal reference is Gorenstein [**3**, Section 5.5]. We briefly summarize few facts about the extra-special p-group of exponent p denoted by G.

- The order of G is p^{2n+1} for some positive integer n. The cardinality of the minimal set of generators is $2n$ and let us denote that set by $\{x_1, y_1, x_2, y_2, \ldots, x_n, y_n\}$. There is a relation $[x_i, y_i] = z$, where $\mathcal{Z}(G) = \langle z \rangle$ and $z^p = 1$. Furthermore, $[x_i, x_j] = 1$ and $[x_i, y_j] = 1$ for $i \neq j$.
- The group G is the central product of n copies of the group of order p^3 given by

$$\langle x, y, z \mid x^p = y^p = z^p = 1, [x, z] = 1, [y, z] = 1, [x, y] = z \rangle.$$

- In the group G, $G = G' = \Phi(G)$ and is cyclic of order p.

In a p-group, finding all automorphisms is often a very hard job. However, for an extra-special p-groups it is not that hard. The automorphisms were studied extensively by Winter [**17**]. The study of automorphisms of an extra-special p-group is not that hard because of a bilinear map $B : G/G' \times G/G' \to \mathbb{F}_p$. The map is defined as follows, let $\bar{x}, \bar{y} \in G/G'$, then $[x, y] = z^a$ for some integer a. Then $B(\bar{x}, \bar{y}) = \bar{a}$, where $\bar{a} = a \bmod p$. It is known that B is an alternating, non-degenerate bilinear form on G/G'.

We will not do a detailed presentation of the automorphisms of the extra-special p-group of prime exponent. An interested reader can find that in Winter [**17**]. However, to facilitate further discussion we have to describe them briefly.

Since an extra-special p group is of class 2, we have that $[x^n, y] = [x, y]^n$. Recall that the center $\mathcal{Z}(G)$ is of prime order and any automorphism of $\mathcal{Z}(G)$ can be lifted to an automorphism of G. So we have a complete description of the automorphisms of G, that are not identity on $\mathcal{Z}(G)$.

So now we have to concentrate on the automorphisms that fix $\mathcal{Z}(G)$. It was shown by Winter that an automorphism ϕ of G is an automorphism of $G/\mathcal{Z}(G)$ if and only if it is the identity on $\mathcal{Z}(G)$.

It was further shown that for prime exponent, the automorphisms that fix $\mathcal{Z}(G)$ is the symplectic group $\mathrm{Sp}(2n, p)$. Winter denotes this subgroup of the automorphism group by H and has shown that it is a normal subgroup of the automorphism group.

To summarize, there are two kinds of automorphisms:

- **a:** Automorphisms that are not the identity on the center $\mathcal{Z}(G)$ of G. Since, any automorphism of the center can be extended to an automorphism of the whole group, and the center is cyclic. We have a complete understanding of these automorphisms. They are uninteresting to our cause.
- **b:** One that are identity on the center. These automorphisms form a normal subgroup of the automorphism group of G. We will call them H.

For obvious reasons we are interested in b above. Let ϕ be an automorphism that centralizes the center. Winter has shown that, $\bar{\phi} : G/\mathcal{Z}(G) \to G/\mathcal{Z}(G)$ is an automorphism of $G/\mathcal{Z}(G)$ preserving the bilinear form B. We will abuse the notation a little bit and call the automorphism on the central quotient ϕ as well.

An interesting normal subgroup of H is the group of inner automorphisms I. Using the fact that the commutator $G' \subseteq \mathcal{Z}(G)$ and the identity $ab = ba[a, b]$ for any $a, b \in G$, it is clear that an inner automorphism is of the form

$$\begin{aligned} x_i &\mapsto x_i z^{d_i} \\ y_i &\mapsto y_i z^{d_i'} \quad \text{where } 0 \leq d_i, d_i' < p. \end{aligned}$$

From the fact, the group of the inner automorphisms I is isomorphic to $G/\mathcal{Z}(G)$, it follows that there are p^{2n} inner automorphisms. It also follow from a simple counting argument on all possible choices of d_i and d_i'. From our understanding of the inner automorphisms, the following proposition is clear:

PROPOSITION 6.1. *An automorphism ϕ of G is an inner automorphism if and only if it is the identity on $\mathcal{Z}(G)$ and $G/\mathcal{Z}(G)$. The inner automorphisms commute and constitutes the group of central automorphisms.*

It is known [**17**, 3E], H/I is isomorphic to $\mathrm{Sp}(2n, p)$. Recall that $G/\mathcal{Z}(G)$ is a symplectic vector space over $\mathbb{F}_p$. We next show that the extra-special p-group of prime exponent is a favorable p-group.

THEOREM 6.2. *For an odd prime p, the extra-special p group of exponent p is a favorable p-group.*

PROOF. Let $\phi \in \mathrm{Sp}(2n, p)$, such that χ_ϕ is irreducible. From the above discussion, we can consider ϕ to be an automorphism of G that is the identity on G'. According to Lemma 4.5, there are no proper ϕ-invariant subspaces of G/G', and from Lemma 5.2 ϕ is a p'-automorphism. Now assume that H is a proper ϕ-invariant subspace of G. Then consider HG'. Notice that $G' = \Phi(G)$ and furthermore $\Phi(G)$ is the set of non-generators of G. Then it follows that HG' is a proper subgroup and so HG'/G' is a proper ϕ-invariant subspace of G/G'. Which implies that $HG' \subseteq G'$ and furthermore $H \subseteq G'$. •

COROLLARY 6.3. *For an odd prime p, the extra-special p-group of exponent p is self-critical.*

PROOF. Let G denote the extra-special p-group of exponent p and C be a critical subgroup of G. Then the condition $\mathrm{C}_G(C) = \mathcal{Z}(G)$ implies that C is not contained in $\mathcal{Z}(G)$. From the above theorem G is a favorable p-group. Then there is a corresponding automorphism ϕ. Let $V = G/G'$ and construct V_ϕ and it is known to be simple. Consider the subgroup CG'. Then CG' is either the whole group or the center $\mathcal{Z}(G)$. Since it can't be $\mathcal{Z}(G)$, it is the whole group. Now

notice that $G' = \Phi(G)$ and $\Phi(G)$ is the set of non-generators of G. It follows that if $CG' = G$, $C = G$. So G is self-critical. •

6.2. The case when $p = 2$. In this case a theorem of Winter [**17**, Theorem 1(c)] comes in handy.

THEOREM 6.4. *Let P be an extra-special group of order 2^{2n+1}. Subgroups H and I are as defined earlier. Then H/I is isomorphic to the orthogonal group $O_\varepsilon(2n, 2)$ of order $2^{n(n-1)+1}(2^n - \varepsilon)\prod_{i=1}^{n-1}\left(2^{2i} - 1\right)$. Here, $\varepsilon = 1$ if P is isomorphic to the central product of n dihedral groups of order 8 and $\varepsilon = -1$ if P is isomorphic to the central product of $n - 1$ dihedral group of order 8 and a quaternion group.*

From the above theorem, by selecting appropriate matrix with irreducible characteristic polynomial, it is easy to see that the case $p = 2$ follows the exact same pattern as that of $p \neq 2$. So we won't dwell with $p = 2$ any further.

7. MOR cryptosystems on finite p-groups using p-automorphisms

In the last section we looked at p'-automorphisms. In this section, we look at p-automorphisms. Our standard reference for p-automorphisms is Khukhro [**7**].

To recall, we looked at the exponent-p central series of a p-group. It is known that this series has elementary abelian sections. There are two cases with p-automorphisms.

a: The automorphism ϕ is not identity on at least one section of the series.
b: The automorphism ϕ is identity on all the sections.

In the case a above, one can not build a secure MOR cryptosystem. The reason is as follows:

THEOREM 7.1. *Let V be a vector space over $\mathbb{F}_q$, a field of characteristic $p > 0$. Let ϕ be a p-automorphism. Then ϕ can be written as a block-diagonal matrix with 1 in the diagonal. Phrased differently, all the eigenvalues of ϕ are 1.*

PROOF. The theorem is well-known, see [**7**, Theorem 2.5]. •

Once we have this theorem, the fact that the discrete logarithm problem in that matrix is easy follows from the following observation and the fact that the power of a block diagonal is the power of the respective blocks written as a block diagonal matrix maintaining the order of the block:

$$\begin{pmatrix} 1 & 1 & * & \dots & * \\ 0 & 1 & 1 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & m & * & \dots & * \\ 0 & 1 & m & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}.$$

This proves that the case a above is useless.

However, the case b above is of immense interest to us. We will give an example of this kind of automorphism. The reason for immense interest is as follows: anyone who is trying to build a new cryptosystem, will want to build a new cryptosystem. In the case of p'-automorphisms, in the MOR cryptosystem we saw, the security can be reduced to that of the discrete logarithm problem in matrices. The discrete logarithm problem in matrices is not a new cryptographic primitive. In this case (b above) we have a real good possibility of a new cryptographic primitive.

Let us look at the situation in some details. There are two subgroups of the automorphism group that we are interested in. One is the group of central automorphisms and the other is the group of inner automorphisms.

7.1. Central automorphisms. Most central automorphisms are p-automorphisms. To quote Curran and McCaughan [**2**], "So, roughly speaking, most of the central automorphisms are of p-power order".

Central automorphisms are the centralizer of the group of inner automorphisms in the automorphism group, they form a normal subgroup in the automorphism group. Let ϕ be a central automorphism, then $\phi(g) = gz_g$, $z_g \in \mathcal{Z}(G)$. It is clear from the definition that central automorphisms centralize the commutator subgroup. Now take an example of a finite p-group G, such that $\mathcal{Z}(G) \subseteq G'$. In this group, for a $g \in G$, we have $\phi(g) = gz_g$ and $\phi^m(g) = gz_g^m$. So from $g^{-1}\phi(g)$ and $g^{-1}\phi^m(g)$, the discrete logarithm problem in the automorphism ϕ reduces to the discrete logarithm problem in $z_g \in \mathcal{Z}(G)$. This is exactly the case with the extra-special p-group (see Proposition 6.1). In the case of the extra-special p-group of prime exponent, a central automorphisms acts as the identity in both $\mathcal{Z}(G)$ and $G/\mathcal{Z}(G)$. So the obvious way to reduce an automorphism to matrices over $\mathbb{F}_p$ do not work. However in this case, as demonstrated earlier, it reduces to the discrete logarithm problem in the center. The open question is, can there be other (secure) situations in which the discrete logarithm problem in the automorphism is not the discrete logarithm problem in the usual sense?

7.2. Inner automorphisms. The group of inner automorphisms of a p-group G is a p-group. Let $G = G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_k = 1$ be a sequence of subgroups in a p-group G. Let $g \in \mathrm{C}_G(G_2)$ be an element. Then consider the inner automorphism ϕ such that $\phi(x) = g^{-1}xg$. Then clearly, ϕ acts as the identity on G_i for $i \geq 2$ and G_i/G_{i+1} for $i \geq 1$. However, this is not enough. Recall that our target is, ϕ should act like the identity on all possible sections H/K where ϕ fixes K and H/K is elementary-abelian. The question is, are there p-groups, on which, using the inner automorphisms, one can build a secure MOR cryptosystem?

8. Conclusion

This paper is a study of finite p-groups for the MOR cryptosystem. The aim of this paper was not to provide with a secure MOR cryptosystem. For that, one can look into the arXiv preprint [**10**]. The purpose of this paper is to theoretically justify what can one expect out of finite p-groups. There are two classes of automorphisms one should look at. One is p-automorphisms and the other is p'-automorphisms. The case of p'-automorphism has been resolved in this paper as follows: for abelian groups, it is the elementary-abelian p-groups. For non-abelian groups, one should use the extra-special p-groups of exponent p. However there are very interesting questions that are open for p-automorphisms. We point those out in this paper.

References

[1] Yakov Berkovich, *Groups of prime power order. Vol. 1*, de Gruyter Expositions in Mathematics, vol. 46, Walter de Gruyter GmbH & Co. KG, Berlin, 2008. With a foreword by Zvonimir Janko. MR2464640 (2009m:20026a)

[2] M. J. Curran and D. J. McCaughan, *Central automorphisms of finite groups*, Bull. Austral. Math. Soc. **34** (1986), no. 2, 191–198, DOI 10.1017/S0004972700010054. MR854565 (87k:20042)

[3] Daniel Gorenstein, *Finite groups*, 2nd ed. Chelsea Publishing Co., New York, 1980. MR569209 (81b:20002)
[4] P. Hall and Graham Higman, *On the p-length of p-soluble groups and reduction theorems for Burnside's problem*, Proc. London Math. Soc. (3) **6** (1956), 1–42. MR0072872 (17,344b)
[5] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *An introduction to mathematical cryptography*, Undergraduate Texts in Mathematics, Springer, New York, 2008. MR2433856 (2009m:94051)
[6] B. Huppert and N. Blackburn, *Finite Groups II*, Springer-Verlag, 1982.
[7] E. I. Khukhro, *p-automorphisms of finite p-groups*, London Mathematical Society Lecture Note Series, vol. 246, Cambridge University Press, Cambridge, 1998. MR1615819 (99d:20029)
[8] Neal Koblitz, Alfred Menezes, and Scott Vanstone, *The state of elliptic curve cryptography*, Des. Codes Cryptogr. **19** (2000), no. 2-3, 173–193, DOI 10.1023/A:1008354106356. MR1759616 (2001i:94065)
[9] C. R. Leedham-Green and E. A. O'Brien, *Constructive recognition of classical groups in odd characteristic*, J. Algebra **322** (2009), no. 3, 833–881, DOI 10.1016/j.jalgebra.2009.04.028. MR2531225 (2010e:20075)
[10] Ayan Mahalanobis, *The MOR cryptosystem and extra-special p-groups*, http://arxiv.org/abs/1111.1043.
[11] ———, *A simple generalization of the ElGamal cryptosystem to non-abelian groups*, Communications in Algebra **36** (2008), no. 10, 3880–3891.
[12] Ayan Mahalanobis, *A simple generalization of the ElGamal cryptosystem to non-abelian groups II*, Comm. Algebra **40** (2012), no. 9, 3583–3596, DOI 10.1080/00927872.2011.602998. MR2981154
[13] Alfred J. Menezes and Yi-Hong Wu, *The discrete logarithm problem in* $\mathrm{GL}(n, q)$, Ars Combin. **47** (1997), 23–32. MR1487162 (98j:11122)
[14] M. F. Newman, Werner Nickel, and Alice C. Niemeyer, *Descriptions of groups of prime-power order*, J. Symbolic Comput. **25** (1998), no. 5, 665–682, DOI 10.1006/jsco.1997.0193. MR1617995 (99f:20054)
[15] Steven Roman, *Advanced linear algebra*, 3rd ed. Graduate Texts in Mathematics, vol. 135, Springer, New York, 2008. MR2344656 (2008f:15002)
[16] Oliver Schirokauer, Damian Weber, and Thomas Denny, *Discrete logarithms: the effectiveness of the index calculus method*, Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci. vol. 1122, Springer, Berlin, 1996, pp. 337–361, DOI 10.1007/3-540-61581-4_66. MR1446523 (98i:11109)
[17] David L. Winter, *The automorphism group of an extraspecial p-group*, Rocky Mountain J. Math. **2** (1972), no. 2, 159–168. MR0297859 (45 #6911)

IISER Pune, Dr. Homi Bhabha Road, Pashan Pune-411008, India
E-mail address: ayan.mahalanobis@gmail.com