January 3, 2008

A SIMPLE GENERALIZATION OF THE ELGAMAL CRYPTOSYSTEM TO NON-ABELIAN GROUPS II

AYAN MAHALANOBIS

ABSTRACT. In this paper I study the MOR cryptosystem using the special linear group over finite fields. At our current state of knowledge, I show that the MOR cryptosystem is more secure than the ElGamal cryptosystem over finite fields.

1. INTRODUCTION

The MOR cryptosystem is a generalization of the ElGamal cryptosystem, where the discrete logarithm problem works in the automorphism group of a group G, instead of the group G itself. The framework for the MOR cryptosystem was first proposed in Crypto2001 by Paeng et al. [16]. Mahalanobis [13] used the group of unitriangular matrices for the MOR cryptosystem. That effort was successful, the MOR cryptosystem over the group of unitriangular matrices became as secure as the ElGamal over finite fields. That work was negatively criticized. Since there is more work involved in implementing matrix operations (matrix multiplication), the MOR cryptosystem over the group of unitriangular matrices has no future, and is thus unpublishable.

In this paper I offer another MOR cryptosystem, this time I use the group of unimodular matrices. More precisely I use $\mathrm{SL}(d,q)$, the *special linear group* over the finite field $\mathbb{F}_q$ of matrices of degree d. Since the automorphisms for the special linear group and the *projective special linear group* are the same and so is the structure of their automorphism groups, everything I say about the special linear group can be said about the projective special linear group too.

In the MOR cryptosystem thus produced, I am working with matrices of degree d over $\mathbb{F}_q$. To encrypt(decrypt) a plaintext(ciphertext) one works over the field $\mathbb{F}_q$. To break this cryptosystem one has to solve a discrete logarithm problem in finite extensions of $\mathbb{F}_{q^d}$. For a large enough d this provides a considerable security advantage. This is the central idea I am trying to "market" in this paper.

2000 *Mathematics Subject Classification.* 94A60, 20G40.

Key words and phrases. MOR cryptosystem, special linear groups.

There are significant challenges in implementation of this cryptosystem. Implementing matrix multiplication is hard. Though we have not reached the optimum speed for that [5], it might always stay harder than multiplication in a finite field. So one needs to find an optimum strategy to present the automorphisms and the underlying group for the MOR cryptosystem, see Section 8 for more details.

At the end I provide parameters for the proposed MOR cryptosystem. I suspect that the parameters are conservative and the degree of the matrix is unnecessarily big. I tried to show that for the chosen parameters, the MOR cryptosystem is almost as good as the ElGamal cryptosystem over elliptic curves (in terms of security); the golden standard in public key cryptography. I suspect that for most practical purposes, the degree of the matrix can be chosen even smaller.

I personally feel that the MOR cryptosystem is a gold mine for cryptography. There are definitely groups out there for which the cryptosystem is secure. There are two kinds of automorphisms for a group G, one that acts by conjugation and the other that does not. In this paper I refer to them as $\mathcal{A}$ and $\mathcal{B}$ respectively. For $\mathrm{SL}(d,q)$ the size of $\mathcal{B}$ became very small and so we had to rely on the the automorphisms from $\mathcal{A}$ only. However, if we can find groups where $\mathcal{B}$ is large, then those groups might provide us with a secure MOR cryptosystem; in which the security can not be reduced to the discrete logarithm problem in a finite field.

Acknowledgements. I learnt a lot from stimulating conversations with Colva Roney-Dougal, Steve Linton, Vladimir Shpilrain, Robert Gilman and William Kantor. A part of this paper was written when I was visiting the Center for Interdisciplinary Research in Computational Algebra, University of St Andrews.

2. The MOR cryptosystem

I shall give a bare-bone description of the MOR cryptosystem [16], see also [15]. A description and a critical analysis of the MOR cryptosystem is also in [13] and the references there.

2.1. 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:

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

Private Key: m.

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 from $\phi^{mr}(a)$ computes a.

Alice can compute ϕ^{-mr} two ways; if she has the information necessary to find out the order of the automorphism ϕ then she can use the identity $\phi^{t-1} = \phi^{-1}$ whenever $\phi^t = 1$. Also, she can find out the order of some subgroup in which ϕ belongs and use the same identity. However, smaller the subgroup, more efficient the decryption algorithm.

Let $G = \langle g \rangle$ be a finite cyclic group of order n written additively; then one can define $\phi : g \mapsto kg$ for some $k \in \mathbb{N}$. In this case $\phi^m : g \mapsto k^m g$; since g is a public information, the public information of ϕ and ϕ^m is identical to the public information of $k \mod n$ and $k^m \mod n$. So the discrete logarithm problem in the automorphism group of G, i.e., given ϕ and ϕ^m find m reduces to given $k \mod n$ and $k^m \mod n$ find m. This is the discrete logarithm problem [22, Chapter 6]. This clearly shows that the MOR cryptosystem as defined above is a straight forward generalization of the ElGamal cryptosystem [22, Cryptosystem 6.1] from a cyclic group to a non-abelian group.

3. The unimodular group of degree d over $\mathbb{F}_q$

The group $\mathrm{SL}(d, q)$ is the set of all matrices of degree d with determinant 1. It is well known that $\mathrm{SL}(d, q)$ is a normal subgroup of $\mathrm{GL}(d, q)$ the group of non-singular matrices of degree d over $\mathbb{F}_q$. In this article I consider $\mathbb{F}_q$ to be a finite extension of the ground field $\mathbb{Z}_p$ of degree γ where $\gamma \geq 1$.

Definition 1. For distinct ordered pair (i, j) I define a matrix unit $e_{i,j}$ as a matrix of degree d, such that, all entries in $e_{i,j}$ are 0, except the intersection of the i^{th} row and the j^{th} column; which is 1 (the identity in the field $\mathbb{F}_q$). Matrices of the form $1 + \lambda e_{i,j}$, $\lambda \in \mathbb{F}_q^{\times}$, are called the elementary matrices or elementary transvections. Here 1 is the identity matrix of degree d. I shall abuse the notation a little bit and use 1 for the identity of the field and the matrix group simultaneously.

It is known that the group $\mathrm{SL}(d, q)$ is generated by elementary transvections. The fundamental relations for the elementary transvections are the relations in the field and the ones stated below:

$$(1)\qquad [1+\lambda e_{i,j}, 1+\mu e_{k,l}] = \begin{cases} 1+\lambda\mu e_{i,l} & \text{if} \quad j=k,\ \ i\neq l \\ 1-\lambda\mu e_{k,j} & \text{if} \quad i=l,\ \ j\neq k \\ 1 & \text{otherwise} \end{cases}$$

$$(2)\qquad (1+\lambda e_{i,j})(1+\mu e_{i,j}) = 1+(\lambda+\mu)\, e_{i,j}$$

$$(3)\qquad (1+\lambda e_{i,j})^{-1} = (1-\lambda e_{i,j})$$

$$(4)\qquad (1+\lambda e_{i,j})^{k} = 1+k\lambda e_{i,j} \quad k\in\mathbb{N}$$

where $\lambda, \mu \in \mathbb{F}_q$.

4. Automorphisms of the unimodular group over $\mathbb{F}_q$

It is well known that the automorphisms of $\mathrm{SL}(d,q)$ are the following [4, 7, 21]:

Diagonal Automorphism: This is conjugation by a non-scalar diagonal matrix. Notice that: since diagonal matrices are not of determinant 1, the diagonal matrices are not in $\mathrm{SL}(d,q)$. So a diagonal automorphism is not an inner automorphism.

Inner Automorphism: This is the most well known automorphism of a non-abelian group G, defined by $x \mapsto g^{-1}xg$ for $g\in G$.

Graph Automorphism: The graph automorphism induces the map $A \mapsto \left(A^{-1}\right)^T$, $A \in \mathrm{SL}(d,q)$. Clearly, graph automorphisms are involutions, i.e., of order two and are not inner automorphisms.

Field Automorphism: This automorphisms is the action of a field automorphism of the underlying field to the individual entries of a matrix.

In this section I am interested in a special class of inner automorphisms, "permutation automorphisms". For a permutation automorphism the conjugator g in the inner automorphism is a permutation matrix. It is well known that for a permutation matrix P, $\det(P) = \pm 1$ and $P^{-1} = P^T$. The permutation matrix is constructed by taking the identity matrix 1 and then exchanging the row based on some permutation α. If the permutation α is even then the determinant of P is 1 otherwise it is -1. Note that if the determinant is -1 then conjugation by that permutation matrix is not an inner automorphism but it is close to being one and I will treat it like an inner automorphism in this paper.

4.0.1. *Effect of a permutation automorphism on an elementary transvections.* If A is an elementary transvection, i.e., $A = 1 + \lambda e_{i,j}$ and P be a permutation matrix, then $P^{-1}AP = 1 + \lambda e_{\alpha^{-1}(i),\alpha^{-1}(j)}$.

4.0.2. *Effect of a diagonal automorphism on an elementary transvection.* Let $D = [w_1, w_2, \ldots, w_n]$ be a diagonal matrix. If $A = 1 + \lambda e_{i,j}$ then $D^{-1}AD = 1 + (w_i^{-1}\lambda w_j)e_{i,j}$. Let us fix a (i, j) such that $1 \leq i, j \leq n$, then look at the *root subgroup* $\langle 1 + \lambda e_{i,j}\rangle$, $\lambda \in \mathbb{F}_q$. This subgroup is clearly isomorphic to $\mathbb{F}_q^+$.

Assume for a moment that I am using the MOR cryptosystem as described in Section 2.1 with G as the root subgroup defined above and ϕ as a diagonal automorphism. Then clearly for some $k \in \mathbb{F}_q^\times$.

$$\begin{aligned} \phi: &\quad 1 + e_{i,j} \mapsto \quad 1 + ke_{i,j} \\ \phi^m: &\quad 1 + e_{i,j} \mapsto \quad 1 + k^m e_{i,j}. \end{aligned}$$

Clearly we see that this MOR cryptosystem is identical to the ElGamal cryptosystem over finite fields. Since $\mathrm{SL}(d, q)$ is generated by elementary transvections, I claim that using the diagonal automorphisms of the special linear groups over finite fields, the MOR cryptosystem is identical to the ElGamal cryptosystem over finite fields. I will further assume that if we compose a diagonal automorphism with a different automorphism then the security of the MOR cryptosystem can not get any worse than that with the diagonal automorphism.

4.0.3. *The effect of the graph automorphism on an elementary transvection.* It is easy to see from the definition of the graph automorphism that if $A = 1 + \lambda e_{i,j}$ then $\left(A^{-1}\right)^T = 1 - \lambda e_{j,i}$.

4.0.4. *The effect of field automorphisms on an elementary transvections.* It is well known that the field automorphisms form a cyclic group generated by the Frobenius automorphism of the field $\mathbb{F}_q$, given by $\lambda \mapsto \lambda^p$, where p is the characteristic of the field $\mathbb{F}_q$. Then the action of field automorphism on an elementary transvection is $1 + \lambda e_{i,j} \mapsto 1 + \lambda^{p^i} e_{i,j}$ where $1 \leq i < \gamma$.

5. MOR with monomial automorphisms

Assume for a moment that I am only using the composition of a diagonal and a inner automorphism of $\mathrm{SL}(d, q)$, i.e., I am using MOR (Section 2.1) where $\phi = \phi_1 \circ \phi_2$ where ϕ_1 is a diagonal automorphism and ϕ_2 is a permutation automorphism. Then clearly ϕ is a monomial automorphism, conjugation by a monomial matrix. The diagonal automorphism ϕ_1 changes $1 + e_{i,j}$ to $1 + \lambda_{i,j}e_{i,j}$ for some $\lambda_{i,j} \in \mathbb{F}_q^\times$. Note that the $\lambda_{i,j}$ depends on the diagonal automorphism and once the diagonal automorphism is fixed $\lambda_{i,j}$ is also fixed for a particular (i,j). Then the permutation automorphism ϕ_2 changes $1+\lambda_{i,j}e_{i,j}$ to $1+\lambda_{i,j}e_{\beta(i),\beta(j)}$ where $\beta=\alpha^{-1}$. Here α is the permutation that gives rise to the permutation matrix P, used in the permutation automorphism.

I now look at the action of the exponentiation of the automorphism $\phi=\phi_1\circ\phi_2$ on the elementary transvection $1+e_{i,j}$. Notice that if

$$\phi : 1+e_{i,j} \xrightarrow{\text{diagonal}} 1+\lambda_{i,j}e_{i,j} \xrightarrow{\text{permutation}} 1+\lambda_{i,j}e_{\beta(i),\beta(j)}, \tag{5}$$

then

$$\phi^m : 1+e_{i,j} \longrightarrow 1+\prod_{l=0}^{m}\lambda_{\beta^l(i)\beta^l(j)}e_{\beta^m(i),\beta^m(j)} \tag{6}$$

Now let us assume that the order of β, $\circ(\beta)=\nu$ then

$$\phi^\nu : 1+e_{i,j} \mapsto 1+\prod_{l=0}^{\nu}\lambda_{\beta^l(i)\beta^l(j)}e_{i,j}.$$

This shows that there is clearly a cycle formed and if $\nu<m$, then this reduces the discrete logarithm problem in $\langle\phi\rangle$ to a discrete logarithm problem in the finite field $\mathbb{F}_q$. Though it is well known that in the symmetric group S_n, acting on n points, one can get elements with very high order. In our problem I am actually interested in the length of the orbit formed by the action of a cyclic subgroup of S_n, generated by β, on the set of distinct ordered pair of $\{1,2,\ldots,n\}$. It is known that these orbits are quite small.

Since the permutation β is easy to find from the public information ϕ and ϕ^m, unless the degree of the matrix d is astronomically big we do not have any chance for a MOR cryptosystem which is more secure than that of the ElGamal cryptosystem over finite fields.

Since the conjugacy problem is easy in $\mathrm{GL}(d,q)$, from the public information of ϕ_1 and ϕ_2 one can compute the conjugator monomial matrices for ϕ_1 and ϕ_2 modulo an element of the center of $\mathrm{GL}(d,q)$. I shall come back to this topic later (Section 7.2) in more details.

6. Structure of the automorphism group of $\mathrm{SL}(d,q)$

Let us start with a theorem describing the structure of the automorphism group of $\mathrm{SL}(d,q)$. Let $\mathcal{A}$ be the group of automorphisms generated by the diagonal and the inner automorphisms and $\mathcal{B}$ be the group generated by the graph and the field automorphisms. Recall that the center of the group $\mathrm{GL}(d,q)$ is the set of all scalar matrices $\lambda 1$ where $\lambda\in\mathbb{F}_q^\times$ and 1 is the identity matrix of degree d. I shall denote the center of $\mathrm{GL}(d,q)$ by Z and *the projective general linear group* $\dfrac{\mathrm{GL}(d,q)}{Z}$ by $\mathrm{PGL}(d,q)$.

A brief *warning* about the notation. To increase readability of the text, from now on, the image of a under f will be denoted either by a^f or by $f(a)$. Also, I might denote the conjugation of X by A as X^A.

Theorem 6.1. The group $\mathcal{A}$ is isomorphic to $\mathrm{PGL}(d,q)$ and $\mathrm{Aut}(\mathrm{SL}(d,q))$ is a semidirect product of $\mathcal{A}$ with $\mathcal{B}$.

Proof. From [2, Theorem 2.12] we know that any element in $\mathrm{GL}(d,q)$ is generated by the set consisting of all invertible diagonal matrices and all transvections. Note that Alperin and Bell [2] calls the invertible scalar matrices as diagonal matrices. Then we can define a map $\digamma : \mathrm{GL}(d,q) \to \mathcal{A}$ defined by $\digamma(A)$ maps $X \mapsto X^A$, clearly $\digamma$ is an epimorphism and $\mathrm{Ker}(\digamma) = Z$. From first isomorphism theorem we have that $\mathrm{PGL}(d,q) \cong \mathcal{A}$.

We are left to show that $\mathrm{Aut}(\mathrm{SL}(d,q))$ is a semidirect product of $\mathcal{A}$ with $\mathcal{B}$. To prove this we need to show that $\mathcal{A}$ is a normal subgroup of $\mathrm{Aut}\,(\mathrm{SL}(d,q))$ and $\mathrm{Aut}(\mathrm{SL}(d,q)) = \mathcal{AB}$. Notice that any $f \in \mathcal{B}$ is an automorphism of $\mathrm{GL}(d,q)$. With this in mind we see that for $A \in \mathrm{GL}(d,q)$ and $X \in \mathrm{SL}(d,q)$

$$X^{fAf^{-1}} = f\left(A^{-1}f^{-1}(X)A\right) = f(A)^{-1}Xf(A) = X^{f(A)}.$$

This proves that $\mathcal{A}$ is a normal subgroup of $\mathrm{Aut}(\mathrm{SL}(d,q))$. Now notice that for any $f \in \mathcal{B}$, $A^{-1}X^fA = \left((A^{-1})^{f^{-1}}XA^{f^{-1}}\right)^f$, where $A \in \mathrm{GL}(d,q)$. This proves that we can move elements of $\mathcal{B}$ to the right of the product of automorphisms. This proves our theorem. ●

Now notice that the order of $\mathcal{A}$ is actually big, it is $q^{\frac{n(n-1)}{2}}(q^n-1)\cdots(q-2)$ but the order of $\mathcal{B}$ is small. The group $\mathcal{B}$ is the direct product of the graph and field automorphisms. The order of $\mathcal{B}$ is 2γ where γ is the degree for the extension $\mathbb{F}_q$ over the ground field. Let $\gamma_1 = 2\gamma$.

Let ϕ and ϕ^m be as in Section 2.1, then from the previous theorem $\phi = A\psi_1$ and $\phi^m = A'\psi_2$, where $A, A' \in \mathcal{A}$ and $\psi_1, \psi_2 \in \mathcal{B}$. I shall consider $A \in \mathcal{A}$ as the conjugator as well, this is clearly the case because $\mathcal{A} \cong \mathrm{PGL}(d,q)$.

Now if $\phi = A\psi_1$, then $\phi^m = AA^{\psi_1}\cdots A^{\psi_1^{m-2}}A^{\psi_1^{m-1}}\psi_1^m$. In this case $AA^{\psi_1}\cdots A^{\psi_1^{m-2}}A^{\psi_1^{m-1}} \in \mathcal{A}$ and $\psi_1^m \in \mathcal{B}$.

Now if $\gamma_1 < m$ and since the order of ψ_1 divides γ_1, there are r_1 and r_2 such that $m-1 = k_1\gamma_1 + r_1$, where $0 \leq r_1 < \gamma_1$ and $r_2 = m \mod \gamma_1$. Then $AA^{\psi_1}\cdots A^{\psi_1^{m-1}}\psi_1^m = A_1^{k_1}AA^{\psi_1}\cdots A^{\psi_1^{r_1}}\psi_1^{r_2}$, where $A_1 = AA^{\psi_1}\cdots A^{\psi_1^{\gamma_1-1}}$. From the information of ϕ and ϕ^m we then have the information of ψ_1 and $\psi_1^{r_2}$. For all practical purposes of implementing this cryptosystem, the degree of the field extension cannot be too large, in this case one can do a exhaustive search on the cosets of $\mathcal{A}$ and find out ψ_1 and $\psi_1^{r_2}$ and do another exhaustive search to solve the discrete logarithm problem in ψ_1 and find the r_2. The information of r_2 gives us a vital information about the secret key m. This is clearly unacceptable. So the only way out of this situation is not to use automorphisms from $\mathcal{B}$.

Then for $X \in \mathrm{SL}(d,q)$ the automorphisms ϕ and ϕ^m as in Section 2.1 is given by

$$\phi = A^{-1}XA \quad \text{for some } A \in \mathcal{A} \tag{7}$$

$$\phi^m = A'^{-1}XA' \quad \text{for some } A' \in \mathcal{A} \tag{8}$$

Now notice that in the description of the MOR protocol we presented the automorphisms as action on generators and furthermore a set of generators for $\mathrm{SL}(d,q)$ are the elementary transvections.

In this case from the public information of ϕ and ϕ^m one can find A and A'. This problem is known to be easy in $\mathrm{GL}(d,q)$ and is often refereed to as *the special conjugacy problem* [15,16]. However, notice that A and A' are not unique. If A and A' satisfy the above equations then so will Az and $A'z'$ for any $z, z' \in Z$.

We just saw that the only way to build a secure MOR cryptosystem using $\mathrm{SL}(d,q)$ is using automorphisms from $\mathcal{A}$. Henceforth, whenever we are talking about the MOR cryptosystem in this paper we mean that we are using the group $\mathrm{SL}(d,q)$ and the automorphisms from $\mathcal{A}$.

7. Security of the proposed MOR cryptosystem

This paper is primarily focused with the discrete logarithm problem in the automorphism group of a non-abelian group. There are two kinds of attack on the discrete logarithm problem over finite fields. One is the generic attack, this attack uses a *black box* group algorithm and the other is an *index calculus* attack.

Since the black box group algorithms work in any group, they will work in the automorphism group too, see [11, Theorem 1]. We have no way to prevent that. On the other hand, these generic attacks are of exponential time complexity and so is of the least concern.

The biggest computational threat to any cryptosystem using the discrete logarithm problem is the subexponential attack like the index calculus attack [19]. It is often argued [10,20] that there is no index calculus algorithm for the elliptic curve cryptosystem that has subexponential time complexity. This fact is presented often to promote elliptic curve cryptosystem over a finite field cryptosystem [10]. So, the best we can hope from the present MOR cryptosystem is that the there is no index calculus attack or the index calculus attack becomes exponential. There are three issues with a MOR cryptosystem:

7.1. **Membership Problem.** I refer back to Equations 7 and 8. We know that solving conjugacy problem (special conjugacy problem) is easy in $\mathrm{GL}(d,q)$ but the solution is not unique. So, if I fix A then to solve the discrete logarithm problem, I need to find A^m. This means that I must find that A' for which $A' \in \langle A \rangle$. This means we have to perform a membership test for all elements of the form $\lambda A'$, $\lambda \in \mathbb{F}_q^\times$ in a cyclic subgroup generated by $\langle A \rangle$.

It is known [11, Theorem 1] that for generic attacks the membership problem does not add much to the complexity. This fact actually follows from the fact that we can get around the membership problem by moving to $\mathrm{PGL}(d,q)$. However, the characteristic polynomial is not invariant in the equivalence classes of $\mathrm{GL}(d,q)$ that are the elements of $\mathrm{PGL}(d,q)$. There is no obvious way (Menezes-Wu [14] algorithm does not work) to reduce the discrete logarithm problem in $\mathrm{PGL}(d,q)$ to some finite field and so there are no known index calculus algorithms.

7.2. **Inner automorphisms as matrices.** As it turns out the only way that a secure MOR cryptosystem might work for the unimodular group is through conjugation of matrices from $\mathcal{A}$. This MOR cryptosystem can be seen as working with inner automorphisms of $\mathrm{GL}(d,q)$. It is well known that the inner automorphisms work linearly on the d^2-dimensional algebra of matrices of degree d over $\mathbb{F}_q$. For a fixed basis, any linear operator on a vector space can be represented as a matrix. So, the discrete logarithm problem on $\langle \phi \rangle$ (Section 2.1) is now reduced to the discrete logarithm problem in $\mathrm{GL}(d^2,q)$[1]. The question is, how easy is it to solve this discrete logarithm problem?

The best algorithm for solving the discrete logarithm problem in $\mathrm{GL}(d,q)$ was given by Menezes et al. [14]. In this case the authors show that for $X, Y \in \mathrm{GL}(d,q)$, such that, $X^l = Y$, $l \in \mathbb{N}$; we can solve the discrete logarithm problem if $\chi(x)$ the characteristic polynomial of X factors into irreducible polynomials of small degree. If the characteristic polynomial is irreducible then the discrete logarithm problem in $\langle X \rangle$ reduces to the discrete logarithm problem in $\mathbb{F}_{q^d}$. However even if $\chi(x)$ is irreducible over

[1] I am making an optimistic assumption that the reduction can be actually carried out. The reason I say that is, the automorphisms are presented as action on generators of $\mathrm{SL}(d,q)$. However, I do not know any basis for the matrix algebra that belong to $\mathrm{SL}(d,q)$.

$\mathbb{F}_q$, it might be reducible over some extension of $\mathbb{F}_q$ of degree smaller than that of the d.

So now I want to maximize the degree of the extension, up to which the characteristic polynomial remains irreducible. For this a corollary comes in handy:

Corollary 7.1. An irreducible polynomial over $\mathbb{F}_q$ of degree n remains irreducible over $\mathbb{F}_{q^k}$ if and only if k and n are relatively prime.

Proof. See [17, Corollary 3.47]. •

In our case I am working in $\mathrm{GL}(d^2, q)$. So the characteristic polynomial has degree d^2. It is easy to see that if d is prime and the characteristic polynomial is irreducible then the extension of the lowest degree in which the characteristic polynomial will turn reducible is $\mathbb{F}_{q^d}$. Then the characteristic polynomial factors into d irreducible polynomials [17, Theorem 3.46]. Then we can create the splitting fields of these irreducible factors and work the Menezes-Wu algorithms in each of these splitting field.

The expected asymptotic complexity of the index calculus algorithm in $\mathbb{F}_{q^k}$ is $\exp\left((c+o(1))(\log q^k)^{\frac{1}{3}}(\log\log q^k)^{\frac{2}{3}}\right)$, where c is a constant, see [19] and [10, Section 4]. If the degree of the extension, k, is greater than $\log^2 q$ then the asymptotic time complexity of the index calculus algorithm is exponential. In our case that means if $d > \log^2 q$ then the asymptotic complexity of the index calculus algorithm becomes exponential.

However to use the Menezes-Wu algorithm there is a lot of work to be done. Principal ones are as follows:

z: Implement $\mathbb{F}_{q^d}$ and work in $\mathbb{F}_{q^d}$. This is a much larger field than $\mathbb{F}_q$.
y: Factor a polynomial of very large degree over $\mathbb{F}_{q^d}$.
x: Find the splitting field of d irreducible polynomials.

These steps are not counted in any index calculus algorithm, but one has to perform them to run the Menezes-Wu algorithm.

Taking all these steps together we conjecture that if $d \approx \log q$, then this cryptosystem should provide exponential security. There are two cryptosystems to compare with – the ElGamal cryptosystem over a finite field and the ElGamal cryptosystem over the elliptic curves. Both of these cryptosystems use the discrete logarithm problem, and the discrete logarithm problem in an automorphism group is our principal object of study.

If we choose that $d > \log^2 q$ then this MOR cryptosystems becomes as secure as the ElGamal over the elliptic curve groups because then the index calculus algorithm becomes exponential; otherwise we can not guarantee.

But on the other hand in the proposed MOR cryptosystem encryption and decryption works on $\mathbb{F}_q$ and breaking the cryptosystem depends on solving a discrete logarithm problem on finite extensions of $\mathbb{F}_{q^d}$. Since, implementing the index calculus attack becomes harder as the field gets bigger, it is clear that if we take d to be a prime and $d \approx \log q$, then the MOR cryptosystem is much more secure than the ElGamal cryptosystem over $\mathbb{F}_q$ and we conjecture it to be as secure as the ElGamal cryptosystem over the elliptic curve groups. I shall go in details about choice of parameters in Section 8.2.

7.3. **Central Attack.** The center Z of $\mathrm{GL}(d,q)$ is of the order $q-1$. Then from the public information of ϕ and ϕ^m (Section 2.1), where ϕ and ϕ^m are presented as action on some set of generators of $\mathrm{SL}(d,q)$; one can find the A and $A^m z$, where $A \in \mathcal{A}$ and $z \in Z$. Then we can compute A^{q-1} and $(A^m z)^{q-1} = \left(A^{q-1}\right)^m$. Then the discrete logarithm problem in $\langle\phi\rangle$ transforms into the discrete logarithm problem in A^{q-1}. However, we notice that the maximum order of an element in $\mathrm{GL}(d,q)$ is q^d-1. Also note that $q-1$ divides q^d-1. Then one can find an element $A \in \mathcal{A}$ such that the order of A in $\mathrm{GL}(d,q)$ is $q-1$, then the above attack is useless.

8. Implementation of this MOR cryptosystem

The cryptosystem we have in mind is the MOR cryptosystem (Section 2.1), the non-abelian group is $\mathrm{SL}(d,q)$ and the automorphisms are the automorphisms from $\mathcal{A}$. In this implementation the most important thing will be the presentation of ϕ and ϕ^m. We decided earlier that the presentation will be the action of the automorphisms on a set of generators $\{g_1, g_2, \ldots, g_\tau\}$. Now we can write $\phi(g_i)$ as a word in the generators $g_1, g_2, \ldots, g_\tau$ or we can write the product of the generators as a matrix. We choose the later, there are two reasons for that:

- **w:** This will contain the growth in the length of the word, especially while computing the powers of ϕ. That will stop any length based attack.
- **v:** This will add to the diffusion.

The set of generators for $\mathrm{SL}(d,q)$ that we have in mind is the elementary transvections. It is easy to go back and forth as words in elementary transvections and matrices.

A big question is how to compute large powers of ϕ efficiently? This is not the object of study for this paper and we will be brief on this topic. Since computing the power of an automorphism is in the heart of encryption and decryption for this and any MOR cryptosystem, I can not possibly over-emphasis the importance of this line of research.

Since a set of generators are elementary transvections, computing the power of ϕ can be done using only words in elementary transvections and the image of the automorphism on these elementary transvections. This can be done very efficiently. However, we have decided to write $\phi^m(g_i)$ as matrices. So, while computing the power of ϕ, one might have to go back and forth between words and matrices. The objective of this exercise is to reduce the amount of matrix multiplication in computing the power of ϕ. Also, one can use the relations among the elementary transvections to shorten the length of the word. There are quite a few options available.

We explore one of them in more details. Assume that we are computing the ϕ^m using the *square and multiply* algorithm [22, Algorithm 5.5]. In this algorithm one needs to multiply two group elements, in our case it is composing two automorphisms. So, I want to find out the worst-case complexity for multiplying two automorphisms. I further assume that the automorphism is given as the image of $(1 + e_{i,j})$, $i \neq j$, $i, j \in \{1, 2, \ldots, d\}$, the image is one $d \times d$ matrix. So for sake of notational convenience I assume that we are squaring ϕ, where ϕ is given by the action on elementary transvections. As is customary we assume that the field addition is free and we count the number of field multiplications necessary to do the computation.

Let's start with the matrix M such that $M = \phi\,(1 + e_{i,j})$, I shall use row operations to write M as product of elementary transvections. We count each row operation as d field multiplications and there are utmost d^2 row operation. So in the worst case after d^3 many field multiplication we have written M as a product of elementary transvection. At most there are d^2 many elementary transvections in the product[2].

Using the relation in Equation 2, we split each transvection into product of elementary transvection over the ground field. So now there are γd^2 elementary transvections over the ground field, for each of which the image under ϕ is known. Then the image under ϕ is computed and then and then there are $(p-1)\gamma d^4$ elementary transvection. The question is how to compute the matrix corresponding to that? I propose the following:

There are utmost $(p-1)\gamma d^4$ elementary transvections in the product of $\phi(M)$. Make d equally spaced partition of the product of $\phi(M)$. Then each one of these partitions can have utmost $(p-1)\gamma d^3$ elementary transvections. Now we multiply the $(p-1)\gamma d^3$ elementary transvections to get d many

[2] Some small examples computed by the author using GAP [9] suggests that in practice this number is much smaller.

matrices and them multiply these d many matrices to get the final matrix corresponding to $\phi^2\left(1+e_{i,j}\right)$. Now we multiply the $(p-1)\gamma d^3$ elementary transvections linearly, one after the other, and use the relations in Equations 1 and 2 . Notice that one of the components in this multiplication is an elementary transvection. So every multiplication can take utmost d many field multiplication. So the total complexity of multiplying $(p-1)\gamma d^3$ many elementary transvections is $(p-1)\gamma d^4$. Since different partitions can be multiplied in parallel we assume that the worst-case complexity is $(p-1)\gamma d^4$ field multiplications.

Now we have to multiply the d many matrices thus obtained. We assume that we use a straight line program to compute the product. Assuming that matrix multiplication can be done in d^3 field multiplication, we see that this also requires d^4 field multiplications. Since we can compute $\phi^2\left(1+e_{i,j}\right)$ in parallel for different i and j, we claim that we can multiply two automorphisms with worst-case complexity $(p-1)\gamma d^4+d^4$ field multiplications.

8.1. **Parameters for the cryptosystem.** We realized that if the conjugator A in ϕ (Equation 7) is a monomial matrix then that prevents the formation of a discrete logarithm problem in the λ of a elementary transvection $1+\lambda e_{i,j}$. We need the inner automorphism so that the attack due to small cycle size of the permutation in the monomial matrix can be avoided. So we have to take the automorphism as conjugation by $A \in \mathrm{GL}(d,q)$. Furthermore to avoid the central attack the A should be of order $q-1$ and the characteristic polynomial out of ϕ represented as a matrix in $\mathrm{GL}\big(d^2,q\big)$ should be irreducible.

The size of d and q is an open question. With the limited amount of knowledge we have about this cryptosystem we can only make a preliminary attempt to encourage further research. The current standard for security in the public key cryptography is 80-bit security. This means that the best known attack to the cryptosystem should take at least 2^{80} steps.

The best known attack on the discrete logarithm problem in the matrices A and A' (Equations 7 and 8) is the generic *square root* attack. So we have to ensure that to find m from A and A' one needs at least 2^{80} steps. For an attack algorithm we assume that computing in $\mathbb{F}_q$ and in $\mathrm{GL}(d,q)$ takes the same amount of time. Then from the central attack it follows that the field should be of size 2^{160}. So there are two choices for q, take q to be a prime of the order 2^{160}, i.e., a 160 bit prime; or take $\mathbb{F}_q=\mathbb{F}_{2^{160}}$. From our earlier analysis we know that the d should be a prime.

A similar situation arises with the discrete logarithm problem over the group of an elliptic curve over a finite field. The MOV attack reduces the discrete logarithm problem in the group of the elliptic curve over $\mathbb{F}_q$ to a discrete logarithm problem in $\mathbb{F}_{q^k}^{\times}$ for some integer k. This is of concern in the implementation of the elliptic curve cryptosystem, because if k is too small then there is an subexponential attack on the elliptic curve discrete logarithm problem. On the other hand the size of the group is almost as big as the field. To prevent the square root attack the size of the field has to be considerably higher. Once you assume that the field is of appropriate size (2^{160}), small k provides adequate security. Unfortunately, our case is quite similar. Though $\mathrm{GL}(d,q)$ can have elements of very high order, due to the central attack the only kind of element we can use are of order $q-1$. So we have to take the field $\mathbb{F}_q$ large to prevent generic attacks.

Koblitz et al. [10, Section 5.2] mentions that in practice $k \approx 20$ is enough for security. If we buy their argument, then it would seem that one can choose d to be a prime around 20. We suspect that one might be able to go even smaller, in our MOR cryptosystem, Menezes-Wu algorithm reduces the discrete logarithm problem in a finite extension of $\mathbb{F}_{q^d}$, not $\mathbb{F}_{q^d}$ itself.

So we propose $d = 13$, and q is as described earlier. Then we see that the if $q = 2^{160}$, then we are talking about a discrete logarithm problem in the extension of $\mathbb{F}_{2^{2080}}$. This clearly surpasses every standard for discrete logarithm problem over finite fields. At this size of the field, it does not matter if the index-calculus is exponential or sub-exponential. It is simply not doable.

8.2. **Generators for the cryptosystem.** The question we raise in this section is, are their better generators than the elementary transvections in $\mathrm{SL}(d,q)$? We saw that if we use the elementary transvections for a prime field then one needs (d^2-d) elementary transvections and $(d^2-d)\gamma$ elementary transvections for $\mathbb{F}_q$ where $q = p^{\gamma}$.

This is one of the major problems in the implementation of this cryptosystem. If d is 25 (say) and we are using a prime field then we need 2×600 matrices of size 25×25 for the public key. Similar will be the case for the ciphertext.

We now try to solve this problem. In this MOR cryptosystem (Section 2.1), generators play a major role. There are some properties of the generators that help; two of them are:

- **i:** There should be an efficient algorithm to solve the word problem in these generators.
- **ii:** Less the number of generators of the group, better is the cryptosystem.

Albert and Thompson [1] provides us with two generators for $\mathrm{SL}(d,q)$. They are

$$\mathrm{C} = 1 + \alpha e_{d-1,2} + e_{d,1}$$
$$\mathrm{D} = (-1)^d \left(e_{1,2} - e_{2,3} + \sum_{i=3}^{d} e_{i,i+1} \right)$$

where α is a primitive element of $\mathbb{F}_q$. It is clear from the proof of [1, Lemma 1] that to solve the word problem in these generators one has to solve the discrete logarithm problem in $\mathbb{F}_q$. This is clearly not useful for our cause. So we adapt the generators and extend it to show that for these generators one can compute the elementary transvections. Since the number of generators is 2γ, this gives us an advantage for the presentation of the public key and the ciphertext over elementary transvections. However, I know of no efficient algorithm to solve the word problem in these generators. If we can find one such algorithm then it can be argued that this cryptosystem would become more economical(efficient).

We now look at $\mathbb{F}_q$ as a γ-dimensional vector space over $\mathbb{F}_p$ and use the fact that $\mathbb{F}_q$ is an elementary abelian p-group of rank γ. We will generate $\mathrm{SL}(d,p)$ for the prime p and then use the relations in Equation 2 to generate $\mathrm{SL}(d,q)$. This is exactly the way one deals with the elementary transvections when working with a proper field extension.

We now prove a theorem which is an adaptation of [1, Lemma 1]. We use the convention used by Albert and Thomson,

$$e_{i,j} = e_{d+i,j} = e_{i,d+j}.$$

The proof of this lemma is practically identical with the proof of [1, Lemma 1]. We include a short proof for the convenience of the reader and some of the formulas we produce in the proof are useful for implementation.

Theorem 8.1. Let

$$C = 1 + e_{d-1,2} + e_{d,1} \quad \text{and} \quad D = (-1)^d \left(e_{1,2} - e_{2,3} + \sum_{i=3}^{d} e_{i,i+1} \right)$$

be elements of $\mathrm{SL}(d,p)$ where $d \geq 5$. Then C and D generates $\mathrm{SL}(d,p)$.

Proof. Let G_0 be the subgroup of $\mathrm{SL}(d,q)$ generated by C and D. We will now write down a few formulas, which follows from direct computation. For $2 \leq k \leq d-2$ we have

$$D^{-1} = (-1)^d \left(e_{2,1} - e_{3,2} + \sum_{i=3}^{d} e_{i+1,i} \right) \tag{9}$$

$$C_1 = D^{-1}CD = 1 - e_{d,3} + e_{1,2} \tag{10}$$

$$CC_1C^{-1}C_1^{-1} = \quad 1 + e_{d,2} \tag{11}$$

$$D^k = (-1)^{dk}\left(-e_{1,1+k} - e_{2,2+k} + \sum_{i=3}^{d} e_{i,i+k}\right) \tag{12}$$

$$D^{-k} = (-1)^{dk}\left(-e_{1+k,1} - e_{2+k,2} + \sum_{i=3}^{d} e_{i+k,i}\right) \tag{13}$$

$$C_k = D^{-k}CD^k = 1 - e_{k-1,k+2} - e_{k,k+1} \tag{14}$$

$$C_k^{-1} = 1 + e_{k-1,k+2} + e_{k,k+1} \tag{15}$$

$$\left(1 + e_{d,k}\right)C_k\left(1 - e_{d,k}\right)C_k^{-1} = 1 - e_{d,k+1} \tag{16}$$

From Equation (11) we see that $1 + e_{d,2}$ belongs to G_0 and then we use mathematical induction on k and Equation (16) proves that $1 + e_{d,k} \in G_0$ for $k = 2, \ldots, d-1$. Also $D^{-2}\left(1 + e_{d,d-1}\right)D^2 = 1 + e_{2,1} \in G_0$. Furthermore $[1 + e_{d,2}, 1 + e_{2,1}] = 1 + e_{d,1}$. This proves that $1 + e_{d,k} \in G_0$ for $k = 1, 2, \ldots, d-1$. Then we can use the relations in $\mathrm{SL}(d,p)$ to prove that $1 + e_{i,j} \in G_0$ for $i, j \in \{1, 2, \ldots, d\}$ and $i \neq j$. This proves the theorem. •

The proof of the theorem is constructive. It gives us a way to compute the elementary transvections from these generators of Albert and Thomson; one can use them effectively to publish the public key. There will be some precomputation involved to change the action of ϕ from these generators to elementary transvections.

9. Conclusions

In this paper I studied the MOR cryptosystem for the special linear group over finite fields. Cryptography is primarily driven by applicability. So it is natural to ask, how efficiently can one implement this MOR cryptosystem? How secure is the cryptosystem? I talked in details on both these issues in Sections 8 and 7 respectively. These are often hard questions to answer from a preliminary and often naive investigation. The worst case complexity is often far off from the actual cost of computation and security in itself is a very elusive concept. We now offer some realistic expectations on the computational cost of this MOR cryptosystem when $q = 2^\gamma$.

From the small experiments we did, it seems reasonable to assume that a randomly chosen element of $\mathrm{SL}(d,q)$ is generated by approximately d elementary transvections, not d^2 elementary transvections. This story is also corroborated by the proof of the previous theorem, where we show that $\mathrm{SL}(d,q)$ is generated by all transvections of the form $1+e_{d,k}$, $k = 1, 2, \ldots, d-1$. Then we need to compute the image of these d elementary transvections under the automorphism ϕ. For that we need to split each elementary transvections into product of elementary transvections over the ground field using Equation 2. Then in the worst case we now have γd elementary transvections. But since in any random binary string of length γ on average there are utmost $\frac{\gamma}{2}$ ones. So a more realistic expectation of the number of transvections is $\frac{\gamma}{2}d$. Using the same expectation as before the image of these transvections under ϕ will be a string of $\frac{\gamma}{2}d^2$ elementary transvections. Now if we use a straight line program, i.e., use the elementary transvections to multiply the one next to it to form the matrix, then the worst case complexity will be $\frac{\gamma}{2}d^3$ field multiplication. However, in reality that complexity will be something like $\frac{\gamma}{2}d^\lambda$ where $2 < \lambda \leq 3$. So it is safe to assume that in practice λ will be around 2.5.

With all this understanding we can say that if q is a field of characteristic 2 and degree γ, then composition of two automorphisms require around

$$d^2 + \frac{\gamma}{2}d^{2.5}$$

field multiplications.

Now notice that if I was working with a finite field $\mathbb{F}_{q^d}$ then the naive product of two non-zero field element costs around d^2 field multiplications. We are quite close to that. Moreover the security we get is discrete logarithm problem in a finite extension $\mathbb{F}_{q^d}$. This provides us with considerable security advantage than discrete logarithm problem in $\mathbb{F}_{q^d}^\times$.

Lastly, I recommend that the plaintext should be an elementary transvection. It is known that trace and determinant is invariant under matrix conjugation. So the trace or the determinant can give out information about the plaintext. However, if it is an elementary transvection then the trace is always d and the determinant 1.

References

[1] A.A. Albert and John Thompson, *Two-element genration of the projective unimodular group*, Illionois Journal of Mathematics **3** (1959), 421–439.

[2] J.L. Alperin and Rowen B. Bell, *Groups and Representations*, Springer, 1995.

[3] Daniel Andrén, Lars Hellström, and Klas Markström, *On the complexity of matrix reduction over finite fields*, Advances in applied mathematics **39** (2007), 428–452.

[4] Roger W. Carter, *Simple groups of Lie type*, John Willey & Sons, 1989.

[5] Don Coppersmith and Shmuel Winograd, *Matrix multiplication via arithmatic progression*, Proceedings of the nineteenth annual ACM conference on Theory of Computing, 1987, pp. 1–6.

[6] J.A. Dias da Silva, *Matrices with prescribed entries and characteristic polynomial*, Proceedings of the American Mathamtical Society **45** (1974), no. 1, 31–37.

[7] Jean Dieudonné and Loo-Keng Hua, *On the automorphisms of the classical groups*, Memoirs of the American Mathematical Society (1951), no. 2.

[8] John Dixon and Brian Mortimer, *Permutation groups*, Springer, 1996.

[9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.10*, 2007.

[10] Neal Koblitz, Alfred Menezes, and Scott Vanstone, *The state of elliptic curve cryptography*, Designs, Codes and Cryptogrpahy **19** (2000), 173–193.

[11] In-Sok Lee, Woo-Hwan Kim, Daesung Kwon, Sangil Nahm, Nam-Soek Kwak, and Yoo-Jin Baek, *On the security of MOR public key cryptosystem*, Asiacrypt 2004 (P.J.Lee, ed.), LNCS, no. 3329, Springer-Verlag, 2004, pp. 387–400.

[12] Ayan Mahalanobis, *A note on using finite non-abelian p-groups in the MOR cryptosystem*, http://arxiv.org/abs/cs.CR/0702095.

[13] ———, *A simple generalization of El-Gamal cryptosystem to non-abelian groups*, Tech. report, http://arxiv.org/abs/cs.CR/0607011, 2006, To appear, Communications in Algebra.

[14] Alfred Menezes and Yi-Hong Wu, *The discrete logarithm problem in $GL(n, q)$*, Ars Combinatorica **47** (1997), 23–32.

[15] Seong-Hun Paeng, *On the security of cryptosystem using the automorphism groups*, Information Processing Letters **88** (2003), 293–298.

[16] Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik Park, *New public key cryptosystem using finite non-abelian groups*, Crypto 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer-Verlag, 2001, pp. 470–485.

[17] Rudolf Ridl and Harald Niederreiter, *Finite fields*, second ed., Cambridge University Press, 2000.

[18] Joseph J. Rotman, *An introduction to the theory of groups*, 4 ed., Springer-Velag, 1994.

[19] Oliver Schirokauer, Damian Weber, and Thomas Denny, *Discrete logarithm: the effectiveness of the index calculus method*, Algorithmic number theory (Talence, 1996), LNCS, vol. 1122, 1996.

[20] Joseph Silverman and Joe Suzuki, *Elliptic curve discrete logarithms and the index calculus*, Asiacrypt'98 (K. Ohra and D. Pei, eds.), LNCS, vol. 1514, 1998, pp. 110–125.

[21] Robert Steinberg, *Automorphisms of finite linear groups*, Canadian Journal of Mathematics **12** (1960), 606–615.

[22] Douglas Stinson, *Cryptography theory and practice*, third ed., Chapman & Hall/CRC, 2006.

Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken, NJ 07030

E-mail address: Ayan.Mahalanobis@stevens.edu