Taylor & Francis
Taylor & Francis Group

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

**Ayan Mahalanobis**

*Indian Institute of Science Education and Research Pune,
Pashan, Pune, India*

*This is a study of the MOR cryptosystem using the special linear group over finite fields. The automorphism group of the special linear group is analyzed for this purpose. At our current state of knowledge, I show that this MOR cryptosystem has better security 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 by Paeng et al. [13]. Mahalanobis [10] used the group of unitriangular matrices for the MOR cryptosystem. That effort was successful: the MOR cryptosystem over the group of unitriangular matrices over $\mathbb{F}_q$ is as secure as the ElGamal cryptosystem over the finite field $\mathbb{F}_q$.

In this article we study the MOR cryptosystem over $\mathrm{SL}(d, q)$. If we assume that the only way to break the proposed MOR cryptosystem is to solve the discrete logarithm problem in the automorphism group, then it follows that the proposed MOR cryptosystem is *as secure as* the ElGamal cryptosystem over $\mathbb{F}_{q^d}$.

This is a major improvement. This MOR cryptosystem works 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 $\mathbb{F}_{q^d}$. Even for a small positive integer $d$, this provides us with a *considerable security* advantage.

There are some challenges in the implementation of this cryptosystem. Implementing matrix multiplication is hard. Though we have not reached the optimum speed for that [4], 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. The key-size for this MOR cryptosystem is big, compared with the conventional ElGamal cryptosystem.

At the end, I provide parameters for the proposed MOR cryptosystem. I suspect that the parameters are too conservative and the degree of the matrix is unnecessarily big. The overly conservative estimates are to show that, for chosen parameters, the MOR cryptosystem is almost as secure as the ElGamal cryptosystem over elliptic curves using fields of the same size, the golden standard in public key cryptography. For most practical purposes, the degree of the matrix can be chosen smaller. However the key-size for this MOR cryptosystem is larger than that of the ElGamal cryptosystem over the rational points of elliptic curves.

## 2. THE MOR CRYPTOSYSTEM

This section contains a bare-bone description of the MOR cryptosystem [13], see also [12]. A description and a critical analysis of the MOR cryptosystem is also in [10] and the references therein.

### 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 $\phi$ a nontrivial (public) 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 $\phi^r$ and $\phi^{mr}$ 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 $\phi^{mr}$ from $\phi^r$, and then $\phi^{-mr}$, and then computes $a$ from $\phi^{mr}(a)$.

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

## 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 nonsingular matrices of degree $d$ over $\mathbb{F}_q$. In this article, $\mathbb{F}_q$ is a finite extension of the prime field $\mathbb{Z}_p$ of degree $\gamma$ where $\gamma \geq 1$.

**Definition 1.** For distinct ordered pair $(i, j)$, 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 $1 + \lambda e_{i,j}$, $\lambda \in \mathbb{F}_q^\times$ where $i \neq j$ 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 [14, Theorem 8.8]. The fundamental relations between the elementary transvections are the relations in the field and the ones stated below:

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

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

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

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

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 generated by the following [3, 5, 17]:

**Diagonal Automorphism:** This is conjugation by a nonscalar diagonal matrix. Notice that, since all diagonal matrices are not of determinant 1, the diagonal matrices are often not in $\mathrm{SL}(d, q)$. So a diagonal automorphism is not always 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 $A \mapsto (A^{-1})^T$, $A \in \mathrm{SL}(d, q)$. 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, "the 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 rows based on some permutation $\alpha$. If the permutation $\alpha$ is even then the determinant of $P$ is 1, and otherwise it is $-1$. Note that, if the determinant is $-1$, then the 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 article.

### 4.1. 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 $P^{-1}AP = 1 + \lambda e_{\alpha^{-1}(i), \alpha^{-1}(j)}$.

### 4.2. Effect of a Diagonal Automorphism on an Elementary Transvection

Let $D = [w_1, w_2, \ldots, w_d]$ 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 $1 \leq i, j \leq d$, and look at the *root subgroup* $\langle 1 + \lambda e_{i,j}\rangle$, $\lambda \in \mathbb{F}_q$ where $i \neq j$. This subgroup is 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 $\phi$ as a diagonal automorphism. Then for some $\kappa \in \mathbb{F}_q^\times$,

$$\phi : 1 + e_{i,j} \mapsto 1 + \kappa e_{i,j}$$
$$\phi^m : 1 + e_{i,j} \mapsto 1 + \kappa^m e_{i,j}.$$

We see that this MOR cryptosystem is equivalent 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. It is reasonable to assume that there are other automorphisms, composition of which with the diagonal automorphisms will provide us with better security.

### 4.3. The Effect of the Graph Automorphism on an Elementary Transvection

From the definition of the graph automorphism, it is clear that if $A = 1 + \lambda e_{i,j}$, then $(A^{-1})^T = 1 - \lambda e_{j,i}$.

### 4.4. 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 $1 + \lambda e_{i,j} \mapsto 1 + \lambda^{p^s} e_{i,j}$ where $1 \leq s < \gamma$.

## 5. MOR WITH MONOMIAL AUTOMORPHISMS

Assume for a moment that I am only using the composition of a diagonal and an inner automorphism of $\mathrm{SL}(d, q)$, i.e., I am using MOR (Section 2.1) where $\phi = \phi_1 \circ \phi_2$, where $\phi_1$ is a diagonal automorphism and $\phi_2$ is a permutation automorphism. Then clearly, $\phi$ is a monomial automorphism, conjugation by a monomial matrix. The diagonal automorphism $\phi_1$ 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 $(i, j)$. The permutation automorphism $\phi_2$ changes $1 + \lambda_{i,j} e_{i,j}$ to $1 + \lambda_{i,j} e_{\beta(i),\beta(j)}$ where $\beta = \alpha^{-1}$. Here $\alpha$ is the permutation that gives rise to the permutation matrix $P$, used in the permutation automorphism.

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

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

then

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

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

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

This shows that a cycle is formed and if $v < m$, 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, the interest is in the length of the orbit formed by the action of a cyclic subgroup of $S_n$, generated by $\beta$, on the set of the distinct ordered pair of $\{1, 2, \ldots, n\}$. It is known that these orbits are quite small.

Since the permutation $\beta$ is easy to find from the public information $\phi$ and $\phi^m$, 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 $\text{GL}(d, q)$, from the public information of $\phi_1$ and $\phi_2$, one can compute the conjugator monomial matrices for $\phi_1$ and $\phi_2$ modulo an element of the center of $\text{GL}(d, q)$. I shall come back to this topic later (Section 7.2) in more detail.

## 6. STRUCTURE OF THE AUTOMORPHISM GROUP OF $\text{SL}(d, q)$

Let us start with a well-known theorem describing the structure of the automorphism group of $\text{SL}(d, q)$. Let $\mathscr{A}$ be the group of automorphisms generated by the diagonal and the inner automorphisms and $\mathscr{B}$ be the group generated by the graph and the field automorphisms. Recall that the center of the group $\text{GL}(d, q)$ 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 $\text{GL}(d, q)$ by $Z$ and *the projective general linear group* $\text{GL}(d, q)/Z$ by $\text{PGL}(d, q)$.

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 denote the conjugation of $X$ by $A$ as $X^A$.

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

*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. Then we can define a map $F : \mathrm{GL}(d, q) \to \mathscr{A}$ defined by $F(A)$ maps $X \mapsto X^A$; clearly, $F$ is an epimorphism and $\mathrm{Ker}(F) = Z$. From the first isomorphism theorem, we have that $\mathrm{PGL}(d, q) \cong \mathscr{A}$.

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

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

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

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

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

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, $AA^{\psi_1}\cdots A^{\psi_1^{m-2}}A^{\psi_1^{m-1}} \in \mathscr{A}$ and $\psi_1^m \in \mathscr{B}$.

Now if $\gamma_1 < m$ and since the order of $\psi_1$ divides $\gamma_1$, there is $r_1$ such that $m - 1 = r\gamma_1 + r_1$, where $0 \leq r_1 < \gamma_1$, and let $r_2 = r_1 + 1$. Then $AA^{\psi_1}\cdots A^{\psi_1^{m-1}}\psi_1^m = A_1^r AA^{\psi_1}\cdots A^{\psi_1^{r_1}}\psi_1^{r_2}$, where $A_1 = AA^{\psi_1}\cdots A^{\psi_1^{\gamma_1-1}}$. From the information of $\phi$ and $\phi^m$, we then have the information of $\psi_1$ 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 an exhaustive search on the cosets of $\mathscr{A}$ and find out $\psi_1$ and $\psi_1^{r_2}$ and do another exhaustive search to solve the discrete logarithm problem in $\psi_1$ and find the $r_2$. The information of $r_2$ gives us a vital information about the secret key $m$, since $r_2 = m \mod \gamma_1$. This is clearly unacceptable. So the only way out of this situation is not to use automorphisms from $\mathscr{B}$.

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

$$\phi(X) = A^{-1}XA \quad \text{for some } A \in \mathrm{GL}(d, q) \tag{7}$$

$$\phi^m(X) = A'^{-1}XA' \quad \text{for some } A' \in \mathrm{GL}(d, q). \tag{8}$$

Now notice, 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 $\phi$ and $\phi^m$ one can find a candidate for $A$ and $A'$. This problem is known to be easy in $GL(d, q)$ and is often refereed to as *the special conjugacy problem* [12, 13]. However, notice that $A$ and $A'$ are not unique. For example, if $A$ and $A'$ satisfy the above equations then so will $Az$ and $A'z'$ for any $z, z' \in Z$, see Section 7.1.1.

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

## 7. SECURITY OF THE PROPOSED MOR CRYPTOSYSTEM

This article is primarily focused on 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 a black box group algorithm works in any group, they will work in the automorphism group too, see [9, 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 a subexponential attack like the index calculus attack [15]. It is often argued [8, 16] that there is no index calculus algorithm for most elliptic curve cryptosystems that has subexponential time complexity. This fact is often presented to promote elliptic curve cryptosystem over a finite field cryptosystem [8]. So, the best we can hope from the present MOR cryptosystem is that there is no index calculus attack or the index calculus attack becomes exponential.

### 7.1. 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, i.e., automorphisms from $\mathscr{A}$. This MOR cryptosystem can be seen as working with inner automorphisms of $GL(d, q)$. 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 $GL(d^2, q)$. The question is, how easy is it to solve this discrete logarithm problem?

The best algorithm for solving the discrete logarithm problem in $GL(n, q)$ was given by Menezes and Wu [11]. In this case, for $X, Y \in GL(n, q)$, such that, $X^l = Y$, $l \in \mathbb{N}$ one has to compute $l$. The method is as follows: Factorize the characteristic polynomial $\chi(x)$ of $X$ into its irreducible factors over $\mathbb{F}_q$. Then go to the splitting field of each irreducible factor. Then the discrete logarithm problem in $GL(n, q)$ can be reduced to the discrete logarithm problem in the splitting fields $\mathbb{F}_{q^t}$, where $1 \leq t \leq n$. If the characteristic polynomial is irreducible, then the discrete logarithm problem in $\langle X \rangle$ reduces to the discrete logarithm problem in $\mathbb{F}_{q^n}$.

In our case, we are working in $GL(d^2, q)$. So the characteristic polynomial has degree $d^2$. It is easy to see that if the characteristic polynomial is irreducible, then

the extension of the lowest degree in which the characteristic polynomial will split is $\mathbb{F}_{q^{d^2}}$. However this is not the case, since $\phi(1) = 1$, 1 is an eigenvalue of $\phi$, and so the best we can hope for is $\mathbb{F}_{q^{d^2-1}}$.

**7.1.1. Recovering the conjugator up to a scalar multiple.** Let $\phi(X) = A^{-1}XA$, where $A \in \mathrm{GL}(d, q)$. Since $\phi$ is linear, if we take $X = 1 + e_{ij}$, $i \neq j$; then $\phi(X) = A^{-1}XA = 1 + A^{-1}e_{ij}A$. Now if we look at $e_{ij}A$ closely, then $e_{ij}A$ is a matrix where the $j$th row of $A$ is the $i$th row of $e_{ij}A$, and the rest all zeros. Since $A$ is nonsingular, all the contents of any row can not be all zeros. From this it follows that the matrix $A^{-1}e_{ij}A$ consists of $d$ columns, each of which is a constant multiple of the $i$th column of $A^{-1}$. One of these columns must be nonzero. Now consider $A^{-1}(1 + e_{i,i+1})A - 1$ for $i = 1, 2, \ldots, d-1$, and let each $I_i$ be a corresponding nonzero column. Then construct a $d \times d$ matrix, whose first $d - 1$ columns are the columns $I_1, I_2, \ldots, I_{d-1}$ and the $d$th column being a nonzero column of $A^{-1}(1 + e_{d1})A - 1$. Then we end up with a matrix $N = A^{-1}D$, where $D = [w_1, w_2, \ldots, w_d]$ is a diagonal matrix. Since $N$ is known, we have found $A^{-1}$ up to a diagonal matrix.

It is obvious that $N^{-1}\phi(X)N = D^{-1}XD$ and hence $N^{-1}(1 + e_{ij})N - 1 = w_i^{-1}w_j e_{ij}$. Then by taking $j = 1, 2, \ldots, d$ and $i = 1$, we can find $w_2^{-1}w_1, w_3^{-1}w_1, \ldots,$ $w_d^{-1}w_1$, and form the diagonal matrix $D' = [1, w_1 w_2^{-1}, w_1 w_3^{-1}, \ldots, w_1 w_d^{-1}]$. It is easy to see now that $ND'$ is $A^{-1}w_1$ and we have found $A$ up to a scalar multiple.

It is not hard to convince oneself that once $A$ is found up to a scalar multiple from $\phi$, in most cases the discrete logarithm problem in $\phi$ turns out to be a discrete logarithm problem in $A$. If one recovers $Ac_1$ and $A^m c_2$ from $\phi$ and $\phi^m$, where $c_1, c_2 \in \mathbb{F}_q^\times$, then compute $(Ac_1)^{q-1} = A^{q-1}$ and $(A^m c_2)^{q-1} = A^{m(q-1)}$ and solve the corresponding discrete logarithm problem. From Menezes and Wu [11], it is clear that this discrete logarithm problem can have a complexity that of the discrete logarithm problem in $\mathbb{F}_{q^d}$.

We can stop this attack by taking $A$ to be of order $q - 1$. But, if the eigenvalues of $A$ are $\mu_1, \mu_2, \ldots, \mu_d$, then $\mu_1^m, \mu_2^m, \ldots, \mu_d^m$ are eigenvalues of $A^m$. On the other hand, the eigenvalues of $cA$ are $c\mu_1, c\mu_2, \ldots, c\mu_d$, $c \in \mathbb{F}_q$. When one recovers $c_1 A$ and $c_2 A^m$, $c_1, c_2 \in \mathbb{F}_q$, one recovers eigenvalues $c_1\mu_1, c_1\mu_2, \ldots, c_1\mu_d$ and $c_2\mu_1^m, c_2\mu_2^m, \ldots, c_2\mu_d^m$. Then one can compute $\frac{\mu_i}{\mu_j}$ and $\left(\frac{\mu_i}{\mu_j}\right)^m$, by taking quotients. Notice that these quotients belong to $\mathbb{F}_{q^d}$. However, since there is no unique way to order the eigenvalues, one might not be able to match a quotient with its power. Then we might have to deal with several quotients to get to the right $m$. However, for all practical applications, the size of the matrix $d$ is small and so this search is not going to cost much; on top of that one can do this in parallel. So it is reasonable to claim at this stage that the discrete logarithm problem in $\phi$ is reduced to a discrete logarithm problem in $\mathbb{F}_{q^d}$.

The expected asymptotic complexity of the index calculus algorithm in $\mathbb{F}_{q^n}$ is $\exp\left((c + o(1))(\log q^n)^{\frac{1}{3}}(\log \log q^n)^{\frac{2}{3}}\right)$, where $c$ is a constant, see [15] and [8, Section 4]. If the degree of the extension, $n$, 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.

If we choose $d \geq \log^2 q$, then this MOR cryptosystems becomes as secure as the ElGamal over the elliptic curve groups, because the index calculus algorithm

is exponential; otherwise, we cannot 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 $\mathbb{F}_{q^d}$. Since, implementing the index calculus attack becomes harder as the field gets bigger, it is clear that if we take $d \ll \log^2 q$, then the MOR cryptosystem is much more secure than the ElGamal cryptosystem over $\mathbb{F}_q$.

## 8.  IMPLEMENTATION OF THIS MOR CRYPTOSYSTEM

The cryptosystem we have in mind is the MOR cryptosystem (Section 2.1), the nonabelian group is $\mathrm{SL}(d, q)$, and the automorphisms are the automorphisms from $\mathscr{A}$. In this implementation, the most important thing will be the presentation of $\phi$ and $\phi^m$. 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 latter, and there are two reasons for that:

1) This will contain the growth in the length of the word, especially while computing the powers of $\phi$. That will stop any length-based attack.
2) 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 using row reduction.

A big question is how to compute large powers of $\phi$ efficiently. This is not the principal object of study for this article, and we will be brief on this topic.

Since a set of generators are elementary transvections, computing the power of $\phi$ 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 $\phi$, 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 $\phi$. 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 such option in more detail. Assume that we are computing the $\phi^m$ using the *square and multiply* algorithm [18, Algorithm 5.5]. In this algorithm, one needs to multiply two group elements in our case; it is composing two automorphisms. So, we need 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 $\phi$, where $\phi$ 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 us start with the matrix $M$ such that $M = \phi(1 + e_{i,j})$. I shall use row operations to write $M$ as a 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.[1]

Using the relation in Eq. (2), we split each transvection into product of elementary transvections over the prime subfield. So now there are $\gamma d^2$ elementary transvections over the prime subfield, for each of which the image under $\phi$ is known. Then the image under $\phi$ is computed, 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 solution.

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 matrices and them multiply these $d$ many matrices to get the final matrix corresponding to $\phi^2(1+e_{i,j})$. Now we multiply the $(p-1)\gamma d^3$ elementary transvections linearly, one after the other, and use the relations in Eqs. (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 $\phi^2(1+e_{i,j})$ 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 $\phi$ (Eq. (7)) is a monomial matrix, then that prevents the formation of a discrete logarithm problem in the $\lambda$ of an 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 $A \in \mathrm{GL}(d,q)$.

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 $A'$ (Eqs. (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. If we

---

[1]Some small examples computed by the author using GAP [6] suggest that in practice this number is much smaller.

assume that the order of the matrix $A$ is the same as the order of the field,[2] then the order of the field should be around $2^{160}$. 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 $\mathbb{F}_q = \mathbb{F}_{2^{160}}$.

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 $\mathbb{F}_{q^n}^{\times}$ for some positive integer $n$. This is of concern in the implementation of the elliptic curve cryptosystem, because if the $n$ is too small, then there is an subexponential attack on the elliptic curve discrete logarithm problem. On the other hand, the size of the elliptic curve 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 $n$ provides adequate security. Our case is quite similar.

Koblitz et al. [8, Section 5.2] mentions that in practice $n \approx 20$ is enough for security. If we buy their argument, then it would seem that one can choose $d$ to be around 20. We suspect that one might be able to go even smaller. In our MOR cryptosystem, the Menezes–Wu algorithm reduces the discrete logarithm problem in $\mathbb{F}_{q^d}$.

So we propose $d = 19$, and $q$ is as described earlier. Then we see that if $q = 2^{160}$, then we are talking about a discrete logarithm problem in $\mathbb{F}_{2^{3040}}$. This 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 subexponential. It is simply not doable.

## 8.2. Generators for the Cryptosystem

The question I raise in this section is. Are there 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. We now try to solve this problem for $\mathrm{SL}(d, p)$, where $p$ is a prime. 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 the following ones:

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

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

$$\mathrm{C} = 1 + \alpha e_{d-1,2} + e_{d,1}$$

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

[2]The size of the field is motivated by the use of similar field in elliptic curve cryptography. For elliptic curves, the choice depends on the fact that the size of the group of rational points on an elliptic curve is roughly the size of the field. In our case, there are matrices of high order in $\mathrm{GL}(d, q)$. So the field can be chosen smaller, depending on the matrix we choose to use.

where $\alpha$ 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 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 in $\mathrm{SL}(d, p)$. Since the number of generators is 2, 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).

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

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

The proof of this lemma is practically identical with the proof of [1, Lemma 1]. I 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*

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

*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 $\mathrm{SL}(d, p)$ generated by $C$ and $D$. I will now provide a few formulas that follow from direct computation. For $2 \leq k \leq d - 2$, we have

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

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

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

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

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

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

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

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

From Eq. (11) we see that $1 + e_{d,2}$ belongs to $G_0$, and then we use mathematical induction on $k$. Equation (16) proves that $1 + e_{d,k} \in G_0$ for $k = 2, \ldots, d - 1$. Also,

$D^{-2}(1 + e_{d,d-1})D^2 = 1 + e_{2,1} \in G_0$. 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. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

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 $\phi$ from these generators to elementary transvections.

## 9. CONCLUSIONS

This article studies the MOR cryptosystem for the special linear group over finite fields. Cryptography is primarily driven by applicability. So it is natural to ask, "How can one efficiently 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 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 $\mathrm{SL}(d, p)$ is generated by all transvections of the form $1 + e_{d,k}$, $k = 1, 2, \ldots, d - 1$ and by Humphries [7].

Then we need to compute the image of these $d$ elementary transvections under the automorphism $\phi$. For that, we need to split each elementary transvections into product of elementary transvections over the ground field using Eq. (2). Then in the worst case we now have $\gamma d$ elementary transvections. But in any random binary string of length $\gamma$ on average there are about $\frac{\gamma}{2}$ 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 $\phi$ will be a string of $\frac{\gamma}{2}d^2$ elementary transvections. Now if we use a straight line program, i.e., if we 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 $\lambda$ will be around 2.5.

With all this understanding, we can say that if $q$ is a field of characteristic 2 and degree $\gamma$, then the composition of two automorphisms requires around

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

field multiplications. If we were working with a finite field $\mathbb{F}_{q^d}$, then the naive product of two nonzero field elements cost around $d^2$ field multiplications. We are quite close to that.

I recommend that the plaintext should be an elementary transvection. It is known that trace and determinant are 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 is 1.

## ACKNOWLEDGEMENTS

## REFERENCES

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

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

[3] Carter, R. W. (1989). *Simple Groups of Lie Type*. John Willey & Sons.

[4] Coppersmith, D., Winograd, S. (1987). Matrix multiplication via arithmatic progression. *Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing*, pp. 1–6.

[5] Dieudonné, J., Hua, L.-K. (1951). On the automorphisms of the classical groups. *Memoirs of the American Mathematical Society* 2.

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

[7] Humphries, S. P. (1986). Generation of special linear groups by transvections. *Journal of Algebra* 99:480–495.

[8] Koblitz, N., Menezes, A., Vanstone, S. (2000). The state of elliptic curve cryptography. *Designs, Codes and Cryptogrpahy* 19:173–193.

[9] Lee, I.-S., Kim, W.-H., Kwon, D., Nahm, S., Kwak, N.-S., Baek, Y.-J. (2004). On the security of MOR public key cryptosystem. In: Lee, P. J., ed. *Asiacrypt 2004*. LNCS, No. 3329, Springer-Verlag, pp. 387–400.

[10] Mahalanobis, A. (2008). A simple generalization of ElGamal cryptosystem to non-abelian groups. *Communication in Algebra* 36(10):3878–3889.

[11] Menezes, A., Wu, Y.-H. (1997). The discrete logarithm problem in GL($n$, $q$). *Ars Combinatoria* 47:23–32.

[12] Paeng, S.-H. (2003). On the security of cryptosystem using the automorphism groups. *Information Processing Letters* 88:293–298.

[13] Paeng, S.-H., Ha, K.-C., Kim, J. H., Chee, S., Park, C. (2001). New public key cryptosystem using finite non-abelian groups. In: Kilian, J., ed. *Crypto 2001*. LNCS, Vol. 2139. Springer-Verlag, pp. 470–485.

[14] Rotman, J. J. (1994). *An Introduction to the Theory of Groups*. 4 ed. Springer-Velag.

[15] Schirokauer, O., Weber, D., Denny, T. (1996). Discrete logarithm: the effectiveness of the index calculus method. *Algorithmic Number Theory (Talence, 1996)*. LNCS 1122:337–361.

[16] Silverman, J., Suzuki, J. (1998). Elliptic curve discrete logarithms and the index calculus. In: Ohra, K., Pei, D., eds. *Asiacrypt'98*. LNCS, Vol. 1514, pp. 110–125.

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

[18] Stinson, D. (2006). *Cryptography Theory and Practice*. 3rd ed. Chapman & Hall/CRC.