Cryptanalysis of a matrix-based MOR system

Chris Monico
Department of Mathematics and Statistics
Texas Tech University
e-mail: c.monicottu.edu
Draft of April 1, 2014

Abstract
We cryptanalyze a recently proposed matrix-based MOR cryptosystem. We first show that the keysize of the proposed system can be substantially reduced with no loss of security. Subsequently, we show that there is a subexponential attack on the system and that, with its suggested parameters, it requires a (reduced) keysize of at least 115,520 bits to achieve the same level of security as a 6080-bit traditional ElGamal key.

1 Introduction
In [1], the author proposes an implementation of the MOR cryptosystem [3] using automorphisms of the special linear group \( \text{SL}(d, \mathbb{F}_q) \) over a finite field \( \mathbb{F}_q \). This system is a generalization of the ElGamal cryptosystem, and the proposed system may be summarized as follows.

Fix a positive integer \( d \) and finite field \( \mathbb{F}_q \). For each \( i, j \in \{1, 2, \ldots, d\} \) let \( e_{ij} \) denote the \( d \times d \) matrix over \( \mathbb{F}_q \) having a one in the \( (i, j) \)-th position and zeros elsewhere, and set \( E_{ij} = I + e_{ij} \).

1. Alice chooses \( A \in \text{GL}(d, \mathbb{F}_q) \) and a positive integer \( a \). She uses \( A \) to determine an automorphism \( \phi \) of \( \text{SL}(d, \mathbb{F}_q) \) by \( \phi(X) = A^{-1}XA \). She computes \( \{\phi(E_{ij})\}_{i \neq j} \), and \( \{\phi_1(E_{ij})\}_{i \neq j} \), where \( \phi_1 = \phi^a \).
2. Alice publishes her public key: \( d, \mathbb{F}_q, \{\phi(E_{ij})\}_{i \neq j}, \{\phi_1(E_{ij})\}_{i \neq j} \).
3. Bob wishes to send Alice the message \( P \in \text{SL}(d, \mathbb{F}_q) \). He chooses a random positive integer \( b \) and computes and sends to Alice \( \{\phi_2(E_{ij})\}_{i \neq j} \) and \( \phi_3(P) \), where \( \phi_2 = \phi^b \) and \( \phi_3 = \phi_1^b \).
4. Alice computes \( \phi_3^{-1} = \phi_2^{-a} \) and recovers \( P = \phi_3^{-1}(\phi_3(P)) \).
Note, in particular, that Alice’s matrix $A$ is not part of the public key. Instead, the automorphism $\phi$ of $\text{SL}(d, \mathbb{F}_q)$ is given implicitly by its action on a set of generators. This introduces some additional computational requirements on using the system, since Alice and Bob must be able to efficiently compute the action of large powers of $\phi$, $\phi_1$, and $\phi_2$ on the generators using such a description. This can done in a straightforward way using the $E_{ij}$ matrices, since e.g.,

$$\phi(I + \lambda e_{ij}) = I + \lambda A^{-1} e_{ij} A = I + \lambda(-I + \phi(I + e_{ij})) = (1 - \lambda)I + \lambda \phi(E_{ij}),$$

and writing an arbitrary matrix in $\text{SL}(d, \mathbb{F}_q)$ as a product of matrices of the form $I + \lambda e_{ij}$ is easily done using Gaussian elimination.

In this paper, we first show that the keysize of this system can be substantially reduced with no loss of security. We then show that there is an attack on this system whose runtime is a subexponential function of the reduced keysize, and therefore, a subexponential function of the original keysize as well.

## 2 Recovering a scalar multiple of $A$

Suppose $\phi$ is an automorphism of $\text{SL}(d, \mathbb{F}_q)$ of the form $\phi(X) = U^{-1} X U$ for some unknown $U \in \text{GL}(d, \mathbb{F}_q)$ and we have ‘black-box access’ to $\phi$. It was already observed in [1] that one may efficiently find a matrix $\tilde{U}$ such that $\tilde{U} = \alpha U$ for some unknown scalar $\alpha$. For completeness, we describe the procedure here.

For all $i \neq j$ we have that

$$\phi(I + e_{ij}) - I = U^{-1} e_{ij} U = (u_{j1} v_i, u_{j2} v_i, \ldots, u_{jd} v_i),$$

where $v_i$ is the $i$-th column of $U^{-1}$. Since $v_i \neq 0$ for all $1 \leq i \leq d$, it follows that $u_{j1} = 0$ iff the first column of $\phi(I + e_{ij}) - I$ is zero. Since $U$ is invertible, there is a $k$ for which $u_{k1} \neq 0$, and we may find such a $k$ by computing $\phi(I + e_{11}) - I, \phi(I + e_{12}) - I, \ldots$ until one is found for which the first column is not $0$. Note that $u_{k1}$ is itself unknown - all that is known is that it is nonzero.

For each $1 \leq i \leq n$, we find $u_{k1} v_i$ as the first column of the matrix $\phi(I + e_{ik}) - I$, and construct the matrix

$$W = (u_{k1} v_1, \ldots, u_{k1} v_d).$$

It follows that $W = u_{k1} U^{-1}$, and so $W^{-1} = u_{k1}^{-1} U$, a scalar multiple of $U$.

This process requires at most $2d$ calls to the black-box function $\phi$ and the inversion of a single $d \times d$ matrix, and is therefore polynomial-time, assuming the black-box function $\phi$ is such. In particular, the key for this system is unnecessarily large. Instead of issuing as part of the public key $\{\phi(E_{ij})\}_{i \neq j}$ and $\{\phi_1(E_{ij})\}_{i \neq j}$, which have combined size $2d^2(d - 1) \log_2 q$, Alice could simply give out a random scalar multiple of $A$ and a random scalar multiple of $A^a$, substantially reducing this portion of the key size to $2d^2 \log_2 q$ with no loss of security at all. With the value $d = 19$ proposed in [1], this reduces the keysize by a factor of $1/342$. 

2
3 Reduction to DL-like problem in $GL(d, \mathbb{F}_q)$

Suppose that $\phi, \phi_1, \phi_2, \phi_3$ are automorphisms of $SL(d, \mathbb{F}_q)$ of the form

$$\phi(X) = A^{-1}XA,$$
$$\phi_1(X) = A^{-a}XA^a,$$
$$\phi_2(X) = A^{-b}XA^b,$$
$$\phi_3(X) = A^{-ab}XA^{ab},$$

for some unknown $A \in GL(d, \mathbb{F}_q)$, $a, b \in \mathbb{Z}$, and that we have black-box access to $\phi, \phi_1, \phi_2$.

If $T, D \in GL(d, \mathbb{F}_q)$ and $k \in \mathbb{Z}$ satisfy $\phi(X) = T^{-1}XT$, $\phi_1(X) = T^{-k}XT^k$, and $\phi_2(X) = D^{-1}XD$, then for all $X \in SL(d, \mathbb{F}_q)$ we have that

$$D^{-k}XDT^k = \phi_2^k(X) = A^{-kb}XA^{kb} = \phi^{kb}(X) = T^{-kb}XT^{kb} = \phi_1^h(X) = A^{-ab}XA^{ab} = \phi_3(X),$$

so that $X = D^k\phi_3(X)D^{-k}$. Therefore, given such $T, D$ and $k$, we may easily invert $\phi_3$.

Using the technique of Section 2, we may efficiently find matrices $S, T, D \in GL(d, \mathbb{F}_q)$ so that $\phi(X) = T^{-1}XT$, $\phi_1(X) = S^{-1}XS$, and $\phi_2(X) = D^{-1}XD$ for all $X \in SL(d, \mathbb{F}_q)$. Furthermore, if $\alpha \in \mathbb{F}_q^*$ is a scalar and $k \in \mathbb{Z}$ and $S = \alpha T^k$, then for all $X \in SL(d, \mathbb{F}_q)$ we have that

$$T^{-k}XT^k = \alpha S^{-1}X(\alpha^{-1}S) = S^{-1}XS = \phi_1(X),$$

as needed. So the cryptanalyst’s problem is reduced to the following: given $S, T \in GL(d, \mathbb{F}_q)$, find an integer $k$ so that $S = \alpha T^k$ for some scalar $\alpha \in \mathbb{F}_q$. In the present context, this problem necessarily has a solution since $T = \alpha_1 A$ and $S = \alpha_2 A^a$ for some $a \in \mathbb{Z}$ and $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$.

4 Translating to a polynomial ring problem

Throughout, suppose we are given two matrices $S, T$ such that $S = \alpha T^k$ for some unknown $\alpha \in \mathbb{F}_q$ and unknown $k \in \mathbb{Z}$. Let $\mu(t) \in \mathbb{F}_q[t]$ denote the minimal polynomial of $T$ and set $n = \deg \mu$. Then $\alpha t^k = \gamma(t) + w(t)\mu(t)$ for some $\gamma, w \in \mathbb{F}_q[t]$ with $\deg \gamma < n \leq d$, and it follows that $\alpha t^k = \gamma(T)$, and so $S = \gamma(T)$. On the other hand, since $T^0, T^1, \ldots, T^{n-1}$ are linearly independent over $\mathbb{F}_q$, $S$ is uniquely represented as a linear combination of these matrices. Therefore, if we solve a system of $d^2$ linear equations in $n$ unknowns to write

$$S = c_0 I + c_1 T + \cdots + c_{n-1} T^{n-1},$$

we have that $\gamma(t) = c_0 + c_1 t + \cdots + c_{n-1} t^{n-1}$ and $\alpha t^k \equiv \gamma(t) \pmod{\mu(t)}$. Furthermore, if $\alpha \in \mathbb{F}_q$ and $k \in \mathbb{Z}$ can be found which satisfy $\alpha t^k \equiv \gamma(t) \pmod{\mu(t)}$, it follows that $\alpha t^k = \gamma(T) = S$. The problem at hand is therefore reduced to finding such $\alpha$ and $k$. Suppose that $\mu(t) = \pi_1(t)^{e_1} \cdots \pi_m(t)^{e_m}$ with each $\pi_j \in \mathbb{F}_q[t]$ irreducible and $e_j \geq 1$. We will first solve the problem modulo each ideal $\langle \pi_j(t)^{e_j} \rangle$ and then lift these to a global solution
Suppose that \( \pi(t) \in \mathbb{F}_q[t] \) is irreducible, \( \pi(t) \neq t \), and \( e \geq 1 \) is the largest integer for which \( \pi^e \mid \mu \). Let \( N \) denote the order of \( t \) in the multiplicative group \((\mathbb{F}_q[t]/\langle \pi^e \rangle)^\ast\). Let \( N_1 \) denote the order of \( t \) in \((\mathbb{F}_q[t]/\langle \pi^e \rangle)^\ast\). In the worst case, \( N_1 \) can be determined in the standard way, by factoring the order \( q^{\deg \pi} - 1 \) of this group. This factorization can be done using the number field sieve in time which is a subexponential function of \( \log(q^{\deg \pi}) \), and therefore a subexponential function of the keysize \( 2d^2 \log_2 q \) since \( \deg \pi \leq d \). Specifically, given the factorization \( q^{\deg \pi} - 1 = p_1^{f_1} \cdots p_r^{f_r} \), the order of \( t \) in \((\mathbb{F}_q[t]/\langle \pi \rangle)^\ast\) can be determined by the following algorithm.

1. Set \( N_1 \leftarrow q^{\deg \pi} - 1 \), and \( j \leftarrow 1 \).

2. Find the largest nonnegative integer \( f \in [0, f_j] \) for which \( t^{N_1/p_j^f} \equiv 1 \pmod{\pi(t)} \) then set \( N_1 \leftarrow N_1/p_j^f \). Set \( j \leftarrow j + 1 \).

3. If \( j \leq r \), goto Step 2. Otherwise, output \( N_1 \) as the order of \( t \).

However, a complete factorization of \( q^{\deg \pi} - 1 \) seems not to be generally necessary. Each element \( \beta \) of the group \((\mathbb{F}_q[t]/\langle \pi \rangle)^\ast\) has order \( (q^{\deg \pi} - 1)/a_\beta \) for some divisor \( a_\beta \) of \((q^{\deg \pi} - 1)\). Since this group is cyclic, if \( p \) is a prime divisor of \( q^{\deg \pi} - 1 \), then for randomly chosen \( \beta \), it follows that \( p \mid a_\beta \) with probability \( 1/p \). Therefore, to find the order of a randomly chosen element, with high probability it would suffice to find the small prime divisors of \( q^{\deg \pi} - 1 \), say those with at most 20 digits, and apply the algorithm above with the incomplete factorization.

For the problem at hand, we need to determine the order of the specific element \( t \), which is certainly not a randomly chosen element. Although we are not offering any theoretical basis for this, experimental evidence suggests that the order of \( t \) still behaves in roughly the same way as a randomly chosen element. In each performed experiment, we chose a prime \( q \), a degree \( \delta \), and 10000 randomly chosen irreducible polynomials in \( \mathbb{F}_q[t] \) of degree \( \delta \). For each irreducible polynomial \( \pi(t) \), we computed the order of \( t \) modulo \( \pi(t) \) and examined the frequency of occurrences of each prime divisor of \( q^\delta - 1 \) as a cofactor of the order of \( t \) (that is, how often each such prime did not divide the order of \( t \)). The results of one typical such experiment are summarized in Table 1.

This suggests that we need not completely factor \( q^{\deg \pi} - 1 \) to find the order of \( t \) modulo \( \pi \); it should most often suffice to find the small prime factors. In the event that we do this and make an error, it either will not affect the rest of our attack, or the failure will present itself as an inconsistent system of congruences later.

Once the order of \( t \) modulo \( \pi \) is known, it is a straightforward matter to determine the order of \( t \) modulo \( \pi^e \). Suppose that \( N_1 \) is the order of \( t \) modulo \( \pi \), so that \( t^{N_1} = 1 + h(t)\pi(t) \).
<table>
<thead>
<tr>
<th>$p$</th>
<th>freq. of $p \mid \text{ord}(t)$</th>
<th>rel. freq.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>9766</td>
<td>1/1.02396</td>
</tr>
<tr>
<td>3</td>
<td>4733</td>
<td>1/2.11282</td>
</tr>
<tr>
<td>5</td>
<td>2001</td>
<td>1/4.99750</td>
</tr>
<tr>
<td>7</td>
<td>1376</td>
<td>1/7.26744</td>
</tr>
<tr>
<td>13</td>
<td>776</td>
<td>1/12.8866</td>
</tr>
<tr>
<td>31</td>
<td>342</td>
<td>1/29.2398</td>
</tr>
<tr>
<td>113</td>
<td>104</td>
<td>1/96.1539</td>
</tr>
<tr>
<td>1847</td>
<td>9</td>
<td>1/1111.11</td>
</tr>
<tr>
<td>1871</td>
<td>8</td>
<td>1/1250.00</td>
</tr>
<tr>
<td>17683</td>
<td>1</td>
<td>1/10000.0</td>
</tr>
</tbody>
</table>

Table 1: Results of an experiment with $q = 786945682360241$, $\delta = 6$. 10000 irreducible polynomials in $\mathbb{F}_q$ of degree $\delta$ were chosen and the order of $t$ modulo each of them was computed. The table summarizes how often each prime $p$ did not divide the order of $t$. The remaining possible primes 218963, 227579167, 827073991, 2351403673, 386895615713, 3290126882059, 22878386160649 divided the order of $t$ in every case.

for some $h(t) \in \mathbb{F}_q[t]$. Letting $p = \text{char}(\mathbb{F}_q)$, we have that $t^{pN_1} = 1 + h(t)^p \pi(t)^p$, and by induction, $t^{p^kN_1} = 1 + h(t)^{p^k} \pi(t)^{p^k}$. It follows that the order of $t$ modulo $\pi(t)^e$ is one of $N_1, pN_1, p^2N_1, \ldots, p^fN_1$, where $f$ is the least positive integer for which $p^f \geq e$.

### 4.2 Discrete logarithms in $\mathbb{F}_q[t]/\langle \pi^e \rangle$

Suppose we have that $t^k \equiv z(t) \pmod{\pi(t)^e}$ for some unknown $k \in \mathbb{Z}$. Since $\pi(t)$ is irreducible, $\mathbb{F}_q[t]/\langle \pi(t) \rangle$ is a finite field and we may solve the DLP

$$t^{k_1} \equiv z(t) \pmod{\pi(t)},$$

for $k_1$ using any of the standard DLP algorithms for this finite field.

We show now how to easily lift this to a solution modulo $\pi(t)^{e'}$, one degree at a time. Suppose $e' \geq 1$ and we’ve found a positive integer $k'$ for which $t^{k'} \equiv z(t) \pmod{\pi(t)^{e'}}$. Then $t^{k'} = z(t) + r(t)\pi(t)^{e'}$ for some $r(t)$ with $\deg r < \deg \pi$. Note that we may easily determine $r(t)$ modulo $\pi(t)$ via

$$r(t) \mod \pi(t) = \frac{t^{k'} - z(t) \mod \pi(t)^{e'+1}}{\pi(t)^{e'}}.$$

We wish to find an integer $k''$ for which $t^{k''} \equiv z(t) \pmod{\pi(t)^{e'+1}}$. Let $N$ denote the order of $t$ modulo $\pi(t)^{e'}$ so that

$$t^N = 1 + g(t)\pi(t)^{e'}, \quad \text{for some } g(t) \in \mathbb{F}_q[t].$$

Note that we may easily determine $g(t)$ modulo $\pi(t)$ via

$$g(t) \mod \pi(t) = \frac{t^N - 1 \mod \pi(t)^{e'+1}}{\pi(t)^{e'}}.$$
Since \( k'' \equiv k \pmod{N} \), we have that \( k'' = k' + sN \) for some \( s \in \mathbb{Z} \). Then
\[
    z(t) \equiv t^{k''} \equiv t^{k'} t^{sN} \equiv (z(t) + r(t)\pi(t)^e)\left(1 + g(t)\pi(t)^e\right)^s \pmod{\pi(t)^{e' + 1}} \\
    \equiv (z(t) + r(t)\pi(t)^e)\left(1 + sg(t)\pi(t)^e\right) \pmod{\pi(t)^{e' + 1}} \\
    \equiv z(t) + \pi(t)^e\left(sg(t)z(t) + r(t)\right) \pmod{\pi(t)^{e' + 1}},
\]
from which we have that \( sg(t)z(t) + r(t) \equiv 0 \pmod{\pi(t)} \). Since each of \( g(t) \), \( z(t) \), \( r(t) \) are known modulo \( \pi(t) \), it is a trivial matter to find such an \( s \).

Therefore, discrete logarithms in \( \mathbb{F}_q[t]/\langle \pi(t)^e \rangle \) are no harder than discrete logarithms in \( \mathbb{F}_q[t]/\langle \pi(t) \rangle \), and may be computed using an appropriate \( L_{q^{\log_q[1/3,c]}} \) algorithm.

### 4.3 Solving locally

We first require a straightforward lemma.

**Lemma 4.1** Suppose \( \pi(t) \in \mathbb{F}_q[t] \) is irreducible and \( e \) is a positive integer. Then \( x \in \mathbb{F}_q[t] \) satisfies \( x^{q-1} \equiv 1 \pmod{\pi(t)^e} \) if and only if \( x = \alpha + h(t)\pi(t)^e \) for some \( \alpha \in \mathbb{F}_q \) and \( h(t) \in \mathbb{F}_q[t] \).

**Proof:** The “if” is clear, so we prove only the converse. Since \( \mathbb{F}_q[t]/\pi(t) \) is a field extension of \( \mathbb{F}_q \), the result clearly holds when \( e = 1 \).

Proceeding by induction on \( e \), suppose the result holds for \( e = e' \), and \( x \in \mathbb{F}_q[t] \) satisfies \( x^{q-1} \equiv 1 \pmod{\pi(t)^{e' + 1}} \). Then \( x^{q-1} \equiv 1 \pmod{\pi(t)^e} \), so by the induction hypothesis,
\[
    x = \alpha + h(t)\pi(t)^e, \text{ for some } \alpha \in \mathbb{F}_q \text{ and } h(t) \in \mathbb{F}_q[t].
\]
It follows that
\[
    1 \equiv x^{q-1} \equiv \left(\alpha + h(t)\pi(t)^e\right)^{q-1} \pmod{\pi(t)^{e' + 1}} \\
    \equiv \sum_{j=0}^{q-1} \binom{q-1}{j} \alpha^{q-1-j} h(t)^{j} \pi(t)^{e'j} \pmod{\pi(t)^{e' + 1}} \\
    \equiv \alpha^{q-1} + (q-1)\alpha^{q-2}h(t)\pi(t)^e \pmod{\pi(t)^{e' + 1}} \\
    \equiv 1 - \alpha^{q-2} h(t) \pi(t)^e \pmod{\pi(t)^{e' + 1}}.
\]
Therefore \( \alpha^{q-2} h(t) \pi(t)^e \equiv 0 \pmod{\pi(t)^{e' + 1}} \), so that \( h(t) = \pi(t)h_1(t) \) for some \( h_1 \) and we have \( x = \alpha + h_1(t)\pi(t)^e \).

Suppose that \( \pi(t) \) is irreducible over \( \mathbb{F}_q \), \( e \) is a positive integer and \( \gamma(t) \equiv \alpha t^k \pmod{\pi(t)^e} \) for some unknown \( \alpha \in \mathbb{F}_q \) and unknown \( k \in \mathbb{Z} \).

As described in Section 4.2, find an integer \( k_0 \) for which
\[
    \gamma(t)^{q-1} \equiv (t^{q-1})^{k_0} \pmod{\pi(t)^e}.
\]
Set \( \alpha_0 = t^{-k_0} \gamma(t) \) and note that \( \alpha_0^{q-1} \equiv 1 \pmod{\pi(t)^e} \), so \( \alpha_0 \in \mathbb{F}_q \) by Lemma 4.1. Then \( \gamma(t) \equiv \alpha_0 t^{k_0} \pmod{\pi(t)^e} \).
4.4 Solving globally

Suppose that \(\pi(t)\) is irreducible over \(\mathbb{F}_q\) and \(\pi(t)^e|\mu(t)\). Let \(\ell\) denote the least positive integer for which \(t^\ell\) is constant modulo \(\pi(t)^e\). Let \(N\) denote the order of \(t\) in the ring \(\mathbb{F}_q[t]/\langle \pi^e \rangle\). Let \(u, v \in \mathbb{Z}\) so that \(u\ell + vN = \gcd(\ell, N) = g\). Since \(t^g = t^{u\ell + vN} \equiv (t^\ell)^u\) is constant modulo \(\pi(t)^e\), it follows that \(g \geq \ell\), so that \(g = \ell\). Therefore \(\ell|N\). It follows immediately that \(\ell = N/w\) for some \(w\) dividing \(q - 1\). In [1], it is proposed to take \(q\) around \(2^{160}\), and for such \(q\) it is a trivial matter to factor \(q - 1\) completely. Therefore, \(\ell\) may be easily determined from \(N\) in an obvious way.

Suppose that \(\mu(t) = \pi_1(t)^{e_1} \cdots \pi_m(t)^{e_m}\), with the \(\pi_j\) irreducible and \(e_j \geq 1\). For each \(1 \leq j \leq r\), let \(\ell_j\) be the least positive integer such that \(t^{\ell_j}\) is constant modulo \(\pi_j(t)^{e_j}\). Then solutions \(a_j\) to each of

\[
\gamma(t) \equiv \alpha_j t^{\ell_j} \pmod{\pi_j(t)^{e_j}}, \quad \text{for some } \alpha_j \in \mathbb{F}_q,
\]

are unique modulo \(\ell_j\), and may be found using the technique described in Section 4.3.

We then want to find a solution to the system of congruences

\[
\begin{cases}
  a \equiv a_1 \pmod{\ell_1} \\
  \vdots \\
  a \equiv a_m \pmod{\ell_m}.
\end{cases}
\]

Note that a solution necessarily exists, so this system is consistent; in practice, the system obtained may be inconsistent if we obtained incorrect values for some \(\ell_j\) resulting from having used an incomplete factorization in computing the order of \(t\) modulo some \(\pi_j(t)^e\). This situation is a low-probability event but is easily rectified by computing the complete factorization of each \(q^{\deg \pi_j} - 1\) and recomputing the orders rigorously.

5 A small example

For the example in this section, we take \(\mathbb{F}_q = \mathbb{F}_{173}\) and \(d = 3\). Suppose we’ve used the technique described in Section 2 to obtain matrices

\[
T = \begin{pmatrix}
27 & 19 & 23 \\
106 & 8 & 3 \\
43 & 149 & 111
\end{pmatrix}, \quad S = \begin{pmatrix}
124 & 85 & 143 \\
35 & 112 & 74 \\
51 & 144 & 2
\end{pmatrix},
\]

for which \(\phi(X) = T^{-1}XT\) and \(\phi_1(X) = S^{-1}XS\) for all \(X \in \text{SL}(3, \mathbb{F}_{173})\). The minimal polynomial \(\mu\) of \(T\) is \(\mu(t) = t^3 + 27t^2 + 132t + 31\), which is irreducible. We solve a system of 9 equations in 3 unknowns to write \(S\) as a linear combination of \(T^0, T^1, T^2\):

\[
S = 160I + 161T + 113T^2.
\]

The polynomial \(\gamma(t) = 160 + 161t + 113t^2\) therefore satisfies \(\alpha t^k \equiv \gamma(t) \pmod{\mu(t)}\), for some unknown \(k \in \mathbb{Z}\) and \(\alpha \in \mathbb{F}_{173}\).
We compute
\[
\begin{align*}
x & := t^{q-1} \mod \pi(t) = 18 + 144t + 46t^2, \\
y & := \gamma(t)^{q-1} \mod \pi(t) = 42 + 104t + 170t^2,
\end{align*}
\]
and solve the discrete log problem \( y = x^{a_0} \) in \( \mathbb{F}_q[t]/\langle \mu(t) \rangle \). We obtain the solution \( a_0 = 19982 \), and set \( \alpha_0 := \left( t^{-a_0} \gamma(t) \mod \pi(t) \right) = 89 \). It follows that \( \gamma(t) \equiv 89t^{19982} \mod \pi(t) \), and so \( S = 89T^{19982} \). Thus, \( \phi_1(X) = T^{-19982}XT^{19982} \), as desired.

6 Runtime

The techniques of Sections 2 and 3 to reduce the problem to solving \( S = \alpha T^k \) are clearly polynomial-time in the keysize. The minimal polynomial \( \mu \) of \( T \) is computed and factored in probabilistic polynomial-time as \( \mu(t) = \pi_1(t)^{e_1} \cdot \pi_m(t)^{e_m} \). Using the number field sieve to factor each integer \( q^{\deg \pi_j} - 1 \), we determine \( \ell_1, \ell_2, \ldots, \ell_m \) with \( \sum_j L_{q^{\deg \pi_j}}[1/3, c_1] \) operations for some \( c_1 > 0 \). Using the techniques in Sections 4.2 and 4.3, we find \( a_1, \ldots, a_m \) such that
\[
\gamma(t) \equiv \alpha_j t^{a_j} \mod \pi_j(t)^{c_j}, \quad \text{for some } \alpha_j \in \mathbb{F}_q,
\]
by computing a discrete logarithm in each field \( \mathbb{F}_q[t]/\langle \pi_j(t) \rangle \). This can be done with a total of \( \sum_j L_{q^{\deg \pi_j}}[1/3, c_2] \) operations for some \( c_2 > 0 \). All other calculations require polynomial-time, so the total runtime for this attack is
\[
\sum_j L_{q^{\deg \pi_j}}[1/3, c],
\]
where \( c = \max\{c_1, c_2\} \). Since \( \sum_j \deg \pi_j \leq d \), this runtime is maximized when \( \mu(t) = \pi(t) \) is irreducible of degree \( d \), and the worst-case runtime is \( L_{q^d}[1/3, c] \). Since this is a subexponential function of \( \log(q^d) \), it is also a subexponential function of the (reduced) keysize \( 2d \log_2(q^d) \).

7 Conclusions

The system proposed in [1] with its suggested parameters of \( q \approx 2^{160}, d = 19 \) offers no more security than the traditional ElGamal system in a finite field whose size is around \( 2^{160-19} = 2^{3040} \). While the keysize for such an ElGamal system would be about 6080 bits, the system proposed in [1] requires a keysize of about \( 2 \cdot 19^3 \cdot 18 \cdot 160 = 39,507,840 \) bits. As mentioned in Section 2, this keysize can be reduced to \( 2 \cdot 19^2 \cdot 160 = 115,520 \) bits with no loss of security. However, there seems to be no particular advantage over traditional ElGamal to offset this larger keysize; the MOR system here requires a keysize 19 times larger than ElGamal to offer (at most) the same level of security and is computationally more expensive to implement. On the other hand, if a 115,520-bit key were acceptable in a particular application, then the security afforded by an ElGamal system with this keysize would be far greater than the proposed MOR variant and it would be computationally comparable to implement.
References

