Cryptanalysis of a system using matrices over group rings

Chris Monico, Mara D. Neusel

Department of Mathematics and Statistics
Texas Tech University
e-mail: c.monico@ttu.edu

Draft of July 9, 2015

Abstract

In several recent works of D. Kahrobaei, C. Koupparis, and V. Shpilrain, public-key protocols have been proposed which depend on the difficulty of computing discrete logarithms in matrix rings over group rings. In particular, the specific ring of 3×3 matrices over $\mathbb{F}_7 S_5$ has been proposed for use in some of these protocols. In this paper, we show that the discrete logarithm paper in this matrix ring can be solved on a modern PC in seconds, and we give a solution to the challenge problem over $\mathbb{F}_2 S_5$ proposed in one of the aforementioned works.

1 Introduction

In the recent works [10, 11, 12], several public-key protocols have been suggested whose security is dependent on the supposed difficulty of computing discrete logarithms in rings of matrices over group rings. The specific suggestion of 3×3 matrices over the group ring $\mathbb{F}_7 S_5$ has been made in all three of these references. The purpose of this article is to demonstrate that there is a practical algorithm for computing discrete logarithms in this matrix ring in seconds on a modern personal computer.

Throughout, let $R = \mathbb{F}_7 S_5$. It was shown in [15] that the regular representation of S_5 by 120×120 matrices over $\mathbb{F}_7$ can be used to embed the 3×3 matrix ring $M_3(R)$ into $M_{360}(\mathbb{F}_7)$, and the algorithm of Menezes and Wu [13] was adapted to singular matrices, which shows already that the Discrete Logarithm Problem (DLP) in $M_3(R)$ is at most as hard as the DLP in $\mathbb{F}_{7^{360}}$. Recent progress on the DLP in finite fields (i.e., Joux's algorithm [6, 2]) already makes this a tractable problem on digital computers. In [15], this embedding and the Menezes-Wu algorithm are used to show that the DLP in $M_3(R)$ can be solved by a probabilistic quantum algorithm in expected polynomial-time. In this paper, we show additionally that matrices resulting from this embedding do not give rise to maximally difficult DLPs. In fact, the matrices resulting from this embedding have minimal polynomials of degree at most 78, having irreducible factors of degree at most 18. As a result, the protocols proposed in [10, 11, 12] are broken by computing discrete logarithms in several finite rings of orders $7^{d_1}, \ldots, 7^{d_k}$ with $d_1 + \cdots + d_k \leq 78$ and $d_j \leq 18$ for $1 \leq j \leq k$. The relevant embeddings can be computed and these DLPs solved in seconds on a digital computer.

Although the ideas in this paper generalize to group rings $\mathbb{F}_q S_n$ with $\gcd(q, n!) = 1$, for clarity of exposition we will focus on the specific case $\mathbb{F}_7 S_5$ proposed in [10, 11, 12]. The challenge problem from the appendix of [10] is in $M_3(\mathbb{F}_2 S_5)$, whose structure is not described as easily as $M_3(R)$, but the method described herein was used to solve that challenge problem. The solution is given in Section 8.

2 Cryptosystems using $M_3(R)$

In [10] a Diffie-Hellman protocol is proposed over $M_3(R)$. In [11, 12], the following protocol is proposed which is similar in nature to the Cramer-Shoup system [4].

1. Alice chooses a hash function H on $M_3(R)^3$ which produces integers in some large range. She chooses integers x_1, x_2, y_1, y_2, z from some large interval $[0, n)$ and non-identity matrices $A_1, A_2 \in M_3(R)$ such that A_1 is invertible and $A_1 A_2 = A_2 A_1$. Finally, she computes

$$\begin{aligned} B &= A_1^z, \\ C &= A_1^{x_1} A_2^{x_2}, \\ D &= A_1^{y_1} A_2^{y_2}, \end{aligned}$$

   and publishes her public key (n, A_1, A_2, B, C, D).

2. Bob wishes to send Alice the message $N \in M_3(R)$. He chooses a random integer $r \in [0, n)$ and computes $U_1 = A_1^r$, $U_2 = A_2^r$, $V = B^r N$, and $W = C^r D^{r\alpha}$, where $\alpha = H(U_1, U_2, V)$. He sends (U_1, U_2, V, W) to Alice.

3. Alice first verifies that $W = U_1^{x_1 + \alpha y_1} U_2^{x_2 + \alpha y_2}$, rejecting the transmission if this is not satisfied. She then computes

$$(U_1^z)^{-1} V = (A_1^{rz})^{-1} B^r N = (A_1^{rz})^{-1} A_1^{rz} N = N.$$

If an attacker can find an integer r' for which $U_1 = A_1^{r'}$, then $B^{r'} = \left(A_1^{r'}\right)^z = (A_1^r)^z = B^r$ so that $N = \left(B^{r'}\right)^{-1} V$ is discovered. The algorithm described below for computing discrete logarithms in $M_3(R)$ will also produce the order of a matrix in $M_3(R)$; once the order of $B^{r'}$ is known then $(B^{r'})^{-1}$ may be computed via exponentiation.

3 The embedding

Consider the regular representation of S_5 over the field $\mathbb{F}_7$ of seven elements

$$\rho : S_5 \hookrightarrow \mathrm{GL}(120, \mathbb{F}_7).$$

This map can be linearly extended to

$$\psi : \mathbb{F}_7 S_5 \hookrightarrow M_{120}(\mathbb{F}_7),$$

which in turn induces a ring monomorphism

$$\Psi : M_3(\mathbb{F}_7 S_5) \hookrightarrow M_{360}(\mathbb{F}_7)$$

by applying ψ to each entry. It follows for $X, Y \in M_3(R)$ that $Y = X^k$ iff $\Psi(Y) = \Psi(X)^k$, translating a DLP in $M_3(R)$ into an equivalent DLP in $M_{360}(\mathbb{F}_7)$. In the next section, we'll show that the image of Ψ is not a simple ring and admits a decomposition (4.1) which can be exploited to expedite the calculation of discrete logarithms in $M_3(R)$.

4 Structure of matrices in $\operatorname{Im}\Psi$

The group ring $\mathbb{F}_7 S_5$ is semi-simple by Maschke's Theorem [9, Theorem 8.1], since the characteristic of the ground field does not divide the group order:

$$\operatorname{char}(\mathbb{F}_7) = 7 \not| \, 120 = |S_5|.$$

Thus, Wedderburn Theory tells us that there exists a decomposition into simple rings

$$\mathbb{F}_7 S_5 \cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_k}(\Delta_k),$$

for suitable division algebras $\Delta_1, \ldots, \Delta_k$ [5, Section 18.2]. Finally, since $\mathbb{F}_7$ is a splitting field for S_5 [7, Section 5.4], we obtain

$$\mathbb{F}_7 S_5 \cong M_{n_1}(F_7) \times \cdots \times M_{n_7}(\mathbb{F}_7)$$

where the n_i's are the degrees of the irreducible representations of S_5 which we can read off the character table for S_5 given in Table 1.

We note that this works in general: Whenever $\operatorname{char}(\mathbb{F}_q) \not| \, |S_n|$ we obtain

$$\mathbb{F}_q S_n \cong M_{n_1}(F_q) \times \cdots \times M_{n_k}(\mathbb{F}_q)$$

where the n_i's are the degrees of the irreducible representations of S_n which we can read off the character table. Without loss of generality we assume that the n_i's are ordered non-decreasingly. Then we have

$$n_1 = n_2 = 1, \quad \exists i \text{ such that } n_i = n - 1,$$

and furthermore

$$n_1^2 + \cdots + n_k^2 = n!$$

Finally note also that k is the number of conjugacy classes in S_n, i.e., set $k = k(n)$ then we have the following recursion formula [3, Chapter 13]

$$\sum_{n=0}^{\infty} k(n) t^n = \prod_{i=1}^{\infty} (1 - t^i)^{-1}.$$

classes:	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2 3 4 5)	(1 2)(3 4)	(1 2)(3 4 5)
sizes:	1	10	20	30	24	15	20
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	-1	1	1	-1
χ_3	4	2	1	0	-1	0	-1
χ_4	4	-2	1	0	-1	0	1
χ_5	5	-1	-1	1	0	1	-1
χ_6	5	1	-1	-1	0	1	1
χ_7	6	0	0	0	1	-2	0

Table 1: Character table of S_5 from [5].

Proposition 4.1 *Let $X \in \operatorname{Im}\Psi$. Then the minimal polynomial p_X of X has degree at most 78 and each irreducible factor of p_X has degree at most 18.*

Proof: From the character table of S_5 given in Table 1 [9, Chapter 19], it follows that the seven irreducible characters of S_5 have degrees 1,1,4,4,5,5, and 6. Thus we have

$$\mathbb{F}_7 S_5 \cong M_1(\mathbb{F}_7) \times M_1(\mathbb{F}_7) \times M_4(\mathbb{F}_7) \times M_4(\mathbb{F}_7) \times M_5(\mathbb{F}_7) \times M_5(\mathbb{F}_7) \times M_6(\mathbb{F}_7).$$

Therefore, we have that

$$\operatorname{Im}\Psi \cong M_3(\mathbb{F}_7 S_5) \cong M_3(\mathbb{F}_7)\times M_3(\mathbb{F}_7)\times M_{12}(\mathbb{F}_7)\times M_{12}(\mathbb{F}_7)\times M_{15}(\mathbb{F}_7)\times M_{15}(\mathbb{F}_7)\times M_{18}(\mathbb{F}_7). \quad (4.1)$$

Suppose

$$A = (A_1, \ldots, A_7) \in M_3(\mathbb{F}_7)\times M_3(\mathbb{F}_7)\times M_{12}(\mathbb{F}_7)\times M_{12}(\mathbb{F}_7)\times M_{15}(\mathbb{F}_7)\times M_{15}(\mathbb{F}_7)\times M_{18}(\mathbb{F}_7),$$

and let $p_j(t)$ be the minimal polynomial of A_j for $1 \leq j \leq 7$. With $f(t) = p_1(t)\ldots p_7(t)$ we have that $f(A) = 0$, so that f is divisible by the minimal polynomial p_A of A. Then $\deg p_A \leq \deg f \leq 3+3+12+12+15+15+18 = 78$. Furthermore, each irreducible factor $q(t)$ of p_A divides f, and hence divides some p_j, so that $\deg q \leq 18$. The isomorphism (4.1) implies the same result for all $X \in \operatorname{Im}\Psi$. □

5 DLP in $\operatorname{Im}\Psi$

As mentioned in the introduction, the algorithm of Menezes and Wu [13] can be adapted to compute discrete logarithms in $M_n(\mathbb{F}_q)$; i.e., it can be adapted to handle singular matrices. The idea of their algorithm is to compute (in polynomial-time) the Jordan decomposition of the base-matrix. Then for each irreducible factor $f(t)$ of the characteristic polynomial, they compute a discrete logarithm in the field extension $\mathbb{F}_{q^{\deg f}}$. In the present context, this reduces DLPs in $M_3(R)$ to computing a discrete logarithm in each field $\mathbb{F}_{7^{d_1}}, \ldots, \mathbb{F}_{7^{d_7}}$ for some $d_1, \ldots, d_7$ which satisfy $d_1, \ldots, d_7 \leq 18$ and $d_1 + \cdots + d_7 \leq 78$.

An alternate method for solving this discrete logarithm problem is described in a forthcoming paper by the first author. In the remainder of the paper, we assume that $\mathbb{F}_q$ is a prime field. Briefly, to solve $Y = X^k$ in $M_n(\mathbb{F}_q)$, let $\mu(t)$ be the minimal polynomial of X with factorization $\mu(t) = \pi_1(t)^{e_1} \cdots \pi_r(t)^{e_r}$. Write $Y = z(X)$ for a polynomial z with $\deg z < \deg \mu$. For each $1 \leq j \leq r$, use a Pohlig-Hellman strategy [17] to solve $t^{k_j} \equiv z(t) \pmod{\pi_j(t)^e}$ by successively computing discrete logarithms in multiplicative subgroups (of comparable orders) of

$$\mathbb{F}_q[t]/\langle \pi_j \rangle,\ \mathbb{F}_q[t]/\langle \pi_j^2 \rangle, \ldots,\ \mathbb{F}_q[t]/\langle \pi_j^{e_j} \rangle$$

A generalized Chinese Remainder Theorem is then used to find an integer k' for which $t^{k'} \equiv z(t) \pmod{\mu(t)}$, and it follows that $X^{k'} = Y$.

Specifically, we proceed as follows. To simplify notation, suppose j is fixed and let $e = e_j$, $\pi = \pi_j$. Let N_ℓ denote the multiplicative order of t in the ring $\mathbb{F}_q[t]/\langle \pi(t)^\ell \rangle$. Let k_ℓ be a nonnegative integer for which $t^{k_\ell} \equiv z(t) \pmod{\pi(t)^\ell}$.

First determine the multiplicative order N_1 of t in $\mathbb{F}_q[t]/\langle \pi \rangle$ in the usual way by factoring the order $q^{\deg \pi} - 1$ of the multiplicative group; if q and $\deg \pi$ are small, as in the present case, this can be done using tables of known factorizations for $p^m - 1$ with small p and m. The discrete logarithm problem

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

is solved using any algorithm for discrete logarithms in the finite field $\mathbb{F}_q$; our implementation simply uses Pohlig-Hellman with Pollard's rho.

Suppose now that N_ℓ and k_ℓ are known and $N_{\ell+1}$ and $k_{\ell+1}$ must be determined. If $t^{N_\ell} \equiv 1 \pmod{\pi(t)^{\ell+1}}$, then $N_{\ell+1} = N_\ell$ and so $k_{\ell+1} = k_\ell$. Otherwise, we first claim that $N_{\ell+1} = qN_\ell$. To see this, note that $t^{N_\ell} = 1 + h(t)\pi(t)^\ell$ for some polynomial h. Let $h(t) = h_0(t) + h_1(t)\pi(t)$ with $\deg h_0 < \deg \pi$, and it follows that

$$t^{N_\ell} \equiv 1 + h_0(t)\pi(t)^\ell \pmod{\pi(t)^{\ell+1}},$$

and $h_0(t) \neq 0$. Therefore,

$$t^{qN_\ell} \equiv (1 + h_0(t)\pi(t)^\ell)^q \equiv 1 \pmod{\pi(t)^{\ell+1}},$$

and so $N_{\ell+1} = qN_\ell$. Since $k_{\ell+1} \equiv k_\ell \pmod{N_\ell}$, it follows that $k_{\ell+1} = k_\ell + sN_\ell$ for some integer s, so that

$$(t^{N_\ell})^s \equiv z(t)t^{-k_\ell} \pmod{\pi(t)^{\ell+1}}.$$

Since the multiplicative order of t^{N_ℓ} in $\mathbb{F}_q[t]/\langle \pi(t)^{\ell+1} \rangle$ is q, it follows that there exists such an integer s with $0 \leq s < q$. Then $k_{\ell+1} = k_\ell + sN_\ell$ satisfies $t^{k_{\ell+1}} \equiv z(t) \pmod{\pi(t)^{\ell+1}}$.

Therefore, each DLP of the form $t^k \equiv z(t) \pmod{\pi(t)^e}$ can be solved by computing one DLP in the finite field $\mathbb{F}_q[t]/\langle \pi \rangle$ and at most $e - 1$ DLPs in groups of order q. The process is summarized below.

Algorithm 5.1 (DLP-local)
Input: *An irreducible polynomial* $\pi(t) \in \mathbb{F}_q[t]$*, a positive integer* e *and* $z(t)$ *in the cyclic subgroup* $\langle t \rangle$ *of* $\mathbb{F}_q[t]/\langle \pi(t)^e \rangle$*.*
Output: *The order* N *of* t *modulo* $\pi(t)^e$ *and an integer* k *such that* $t^k \equiv z(t) \pmod{\pi(t)^e}$*.*

1. *Use the factorization of* $q^{\deg \pi} - 1$ *to find the order of* t *modulo* $\pi(t)$*, and set* N *to be this order. Use Pohlig-Hellman and Pollard's rho method to find an integer* $0 \leq k < N$ *such that* $t^k \equiv z(t) \pmod{\pi(t)}$*.*

2. *For* j *from 2 to* e *do as follows: if* $t^N \not\equiv 1 \pmod{\pi(t)^j}$ *then find an integer* $0 \leq k_0 < q$ *such that* $(t^N)^{k_0} \equiv z(t)t^{-k} \pmod{\pi(t)^j}$ *and set* $k \leftarrow k + k_0 N$ *and* $N \leftarrow qN$*.*

The entire algorithm is then summarized as follows.

Algorithm 5.2 (DLP-global)
Input: *Matrices* $A, B \in M_N(\mathbb{F}_q S_n)$ *such that* A *is invertible and* $B \in \langle A \rangle$*.*
Output: *A nonnegative integer* k *such that* $B = A^k$*, and the order* N *of* A*.*

1. *Compute the embeddings* $X = \Psi(A) \in \mathrm{GL}_{n!N}(\mathbb{F}_q)$ *and* $Y = \Psi(B) \in \mathrm{GL}_{n!N}(\mathbb{F}_q)$ *as described in Section 6.*

2. *Compute the minimal polynomial* μ *of* X *and factor it over* $\mathbb{F}_q$ *as* $\mu(t) = \pi_1(t)^{e_1} \ldots \pi_r(t)^{e_t}$*.*

3. *Find* $z(t) \in \mathbb{F}_q[t]$ *with* $\deg z < \deg \mu$ *such that* $Y = z(X)$*. Set* $k \leftarrow 0, N \leftarrow 1$*.*

4. *For* j *from 1 to* r *do all of the following: use Algorithm 5.1 to find the order* N_j *of* t *modulo* $\pi_j(t)^{e_j}$ *and an integer* k_j *such that* $t^{k_j} \equiv z(t) \pmod{\pi_j(t)^{e_j}}$*. Use the Euclidean Algorithm to find integers* $u, v \in \mathbb{Z}$ *such that* $uN + vN_j = \gcd(N, N_j) = g$ *and set* $k \leftarrow k_j u(N/g) + kv(N_j/g)$*, and* $N \leftarrow NN_j/g$*, and* $k \leftarrow k \pmod{N}$*.*

5. *Output* k *and* N*.*

6 Complexity analysis

In this section we give a crude upper bound on the complexity of the attack. We suppose that the group ring under consideration is $\mathbb{F}_q S_n$ and the attacker will compute a discrete logarithm in the matrix ring $M_N(\mathbb{F}_q S_n)$. In this case, the keysize for the protocol is at least $k = n!N^2 \log_2 q$ bits.

The embedding $\psi : \mathbb{F}_q S_n \longrightarrow M_{n!}(\mathbb{F}_q)$ is computed as follows. Enumerate $S_n = \{\sigma_1, \ldots, \sigma_{n!}\}$, and let $\sum a_i \sigma_i \in \mathbb{F}_q S_n$. For each $1 \leq j \leq n!$, compute the product in the group-ring

$$\left(\sum_{i=1}^{n!} a_i \sigma_i \right) \sigma_j = \sum a_i^{(j)} \sigma_i,$$

and we have that $(a_1^{(j)}, \ldots, a_{n!}^{(j)})^T$ is the j-th column of $\psi\left(\sum a_i\sigma_i\right)$. With a precomputed lookup table for the operation in S_n, each column is computed using $\mathcal{O}(n!)$ $\mathbb{F}_q$-operations. We therefore use $\mathcal{O}((n!)^2)$ $\mathbb{F}_q$-operations to compute $\psi\left(\sum a_i\sigma_i\right)$, and $\mathcal{O}((n!N)^2) \leq \mathcal{O}(k^2)$ $\mathbb{F}_q$-operations to compute $\Psi\left(\sum a_i\sigma_i\right)$.

The minimal polynomial μ of the $(n!N) \times (n!N)$ matrix $\Psi\left(\sum a_i\sigma_i\right)$ can be computed in a straightforward way with $\mathcal{O}((n!N)^4) \leq \mathcal{O}(k^4)$ operations in $\mathbb{F}_q$.

One approach to factor μ is to first perform a squarefree factorization using $\mathcal{O}(\deg\mu(\deg\mu\log_2 q)^2)$ bit operations [1, Thm. 7.5.2]. The randomized Cantor-Zassenhaus Algorithm is used in a recursive fashion to find divisors; the probability of success is at least 1/2 at each stage, so we expect to use it no more than twice to find a divisor each time. Each application is accomplished with $\mathcal{O}((\deg\mu + \log_2 q)(\deg\mu\log_2 q)^2)$ bit operations [1, Thm. 7.4.6]. This is combined with an irreducibility test using the same number of operations [1, Thm. 7.6.2]. The number of times the Cantor-Zassenhaus Algorithm is expected to be used is not more than twice the total number of irreducible factors of μ, which itself is at most $\deg\mu$. Since $\deg\mu \leq n!N$, the entire process of factoring μ can be accomplished with $\mathcal{O}((n!)^3N^3\log_2^2 q(n!N + \log_2 q))$ bit operations, or $\mathcal{O}(k^4)$ $\mathbb{F}_q$-operations.

Therefore, Steps 1 and 2 in Algorithm 5.2 can be performed with $\mathcal{O}(k^4)$ operations. Since this is polynomial-time in the input size, we ignore it for the remainder of this section. But note that in this estimate we have not used the fact that $\deg\mu$ is known to be discernibly smaller than $n!N$. In particular, if $n = 5$ and $\text{char}(\mathbb{F}_q) \not| \, n!$, then $\deg\mu \leq 26N < 120N = n!N$. So in practice, this portion tends to be faster than this complexity bound would indicate.

In Step 3, we need to find $z_0, z_1, \ldots, z_{d-1} \in \mathbb{F}_q$ such that

$$Y = z_0 I + z_1 X + \cdots + z_{d-1}X^{d-1},$$

where $d = \deg\mu$. In the worst case, one may cast this as a system of $(n!N)^2$ equations in d unknowns and solve it using Gaussian Elimination. This would require $\mathcal{O}(d(n!N)^4)$ $\mathbb{F}_q$-operations. Since $d < n!N$, the number of $\mathbb{F}_q$-operations is bounded by $\mathcal{O}((n!N)^5) \leq \mathcal{O}(k^5)$, which is again polynomial-time in the input size. In practice, one may also use much faster probabilistic techniques.

In Step 4, each application of Algorithm 5.1 requires computing one DLP in the finite field $\mathbb{F}_q[t]/\langle\pi_j(t)\rangle$, and at most $e_j - 1$ more discrete logarithms in groups of order q. This is done using Pollard's rho method [18] and a total of $\mathcal{O}(q^{\deg\pi_j/2} + (e_j-1)q^{1/2}) = \mathcal{O}(e_j q^{\deg\pi_j/2})$ operations in subrings of $\mathbb{F}_q[t]/\langle\pi_j(t)^{e_j}\rangle$. This gives a bound of $\mathcal{O}((e_j\deg\pi_j)^2 e_j q^{\deg\pi_j/2}) = \mathcal{O}(e_j^3(\deg\pi_j)^2 q^{\deg\pi_j/2})$ $\mathbb{F}_q$-operations. Letting $\delta = \max\{\deg\pi_1, \ldots, \deg\pi_r\}$, this is $\mathcal{O}(e_j^3\delta^2 q^{\delta/2})$ $\mathbb{F}_q$-operations for each $1 \leq j \leq r$. So in total, Step 4 can be performed with $\mathcal{O}(\delta^2 q^{\delta/2}(e_1^3 + \cdots + e_r^3))$ $\mathbb{F}_q$-operations. Additionally, since $e_1 + \cdots + e_r \leq \deg\mu$, we can bound the number of operations by $\mathcal{O}(\delta^2 q^{\delta/2}(\deg\mu)^3) \leq \mathcal{O}((n!N\delta)^3 q^{\delta/2})$.

The results in the text generalize to show that if $n = 5$ and $\text{char}(\mathbb{F}_q) \not| \, 5!$ then $\delta \leq 6N$. So if $n = 5$ is fixed, the eavesdropper's problem is solved with $\mathcal{O}(N^6 q^{3N})$ $\mathbb{F}_q$-operations. If, in addition, $N = 3$ is fixed this yields a complexity bound of $\mathcal{O}(q^9)$ $\mathbb{F}_q$-operations to solve the DLP in this ring.

From the character table of S_6 [8], it can be similarly shown that if $n = 6$ and $\text{char}(\mathbb{F}_q) \not| \, 6!$, then $\delta \leq 16N$. In this case, Algorithm 5.2 solves the eavesdropper's problem with $\mathcal{O}(N^6 q^{8N})$

Ring	# DLPs	Avg. solve time	Max. solve time	Max. prime subgroup
$M_3(\mathbb{Z}_7 S_5)$	1000	2.5 sec.	6.2 sec.	16148168401
$M_3(\mathbb{Z}_{11} S_5)$	1000	157.8 sec.	6063.3 sec.	50544702849929377
$M_3(\mathbb{Z}_{13} S_5)$	1000	6.8 sec.	212.0 sec.	15798461357509
$M_3(\mathbb{Z}_{17} S_5)$	1000	8.1 sec.	58.7 sec.	2141993519227
$M_3(\mathbb{Z}_{19} S_5)$	1000	13.3 sec.	536.3 sec.	99995282631947

Table 2: Experimental results from computing discrete logarithms in various rings.

$\mathbb{F}_q$-operations. Similarly, if $n = 7$ and $\mathrm{char}(\mathbb{F}_q) \not| 7!$ then $\delta \le 35N$ and the eavesdropper's problem can be solved with $\mathcal{O}(N^6 q^{17.5N})$ operations. Note, however, that the keysize grows rapidly with n; if $n = 7$ the keysize would already be approximately $5040N^2 \log_2 q$ bits. For this reason, we have not attempted to carry out an asymptotic runtime estimate in terms of n. But in general, the eavesdropper's problem can be solved using $\mathcal{O}(N^6 q^{N\delta_n/2})$ $\mathbb{F}_q$-operations where δ_n is the maximum degree of an irreducible representation of S_n. The first few values of δ_n for $n = 2, 3, \ldots$ are $1, 2, 3, 6, 16, 35, 90, 216, 768, 2310, \ldots$ [16].

7 Experimental results

Table 2 summarizes experimental results obtained using our implementation in C of the attack given in this paper. We solved instances of discrete logarithms in rings of 3×3 matrices over $\mathbb{F}_q S_5$ for several prime values of q. In each experiment, matrices $X \in M_3(\mathbb{F}_q S_5)$ were chosen randomly until finding an invertible one. Then a random exponent k of 2048 bits was chosen, $Y = X^k$ computed, and k discarded. Note that since X has minimum polynomial with degree at most 78, the order of X is less than q^{78}, which is well below 2^{2048} for the primes used in these experiments. The indicated timings are for the times required to calculate the resulting discrete logarithms $\log_X Y$.

The experiments were performed on a single core of an Intel i7 processor at 1.6GHz and the number of times the experiment was repeated for each ring is indicated in the table. For each set of experiments, we also indicate the largest prime order subgroup encountered, as this has a large effect on the runtime of this Pohlig-Hellman type implementation, at Step 1 of Algorithm 5.1.

8 Example

In the appendix of [10] a Diffie-Hellman-like challenge problem is given consisting of matrices $M, M^a, M^b \in \mathbb{F}_2 S_5$. The structural results given in this paper do not directly generalize to this case, since $\mathrm{char}(\mathbb{F}_2)$ divides $|S_5|$. Nevertheless, a precise decomposition is not necessary. All that was necessary to solve the given challenge problem was to compute the images of M and M^a under the embedding $\Psi : M_3(\mathbb{F}_2 S_5) \longrightarrow M_{360}(\mathbb{F}_2)$, and proceed as described in Section 5.

Initial calculations showed that $\Psi(M^a)$ was not in the $\mathbb{F}_2$-span of $\Psi(M)^0, \ldots, \Psi(M)^{d-1}$, where d was the degree of the minimal polynomial of $\Psi(M)$ which would be a contradiction.

However, with the group operation of S_5 written in reverse, $(\sigma\tau)(j) = (\tau \circ \sigma)(j) = \tau(\sigma(j))$, the contradiction was resolved and a solution found. With this group operation, we found that $\Psi(M)$ has minimal polynomial

$$\mu(t) = t^{63} + t^{60} + t^{58} + t^{57} + t^{56} + t^{55} + t^{51} + t^{50} + t^{45} + t^{44} + t^{43} + t^{42} + t^{41} + t^{40} + t^{36} + t^{35} + t^{34} + t^{33} + t^{31} + t^{22} + t^{20} + t^{17} + t^{16} + t^{12}.$$

In light of this, there is a solution a with $a < 2^{63} \cdot 2^6 = 2^{69}$, and it could be found using Pollard's Rho method. However, the minimal polynomial μ factors over $\mathbb{F}_2$ as

$$\mu(t) = (t^8 + t^7 + t^5 + t + 1)^3 (t^7 + t^4 + t^3 + t^2 + 1)^2 (t^3 + t + 1)^4 t^{12} (t + 1).$$

By solving the obvious $360^2 \times 64$ linear system, we found that $M^a = z(M)$, where

$$\begin{aligned} z(t) &= t^{62} + t^{61} + t^{60} + t^{59} + t^{55} + t^{53} + t^{50} + t^{49} + t^{45} + t^{44} + \\ &\quad t^{42} + t^{41} + t^{40} + t^{37} + t^{35} + t^{31} + t^{30} + t^{28} + t^{27} + t^{26} + \\ &\quad t^{24} + t^{23} + t^{22} + t^{21} + t^{19} + t^{18} + t^{17} + t^{14} + t^{12} \end{aligned}$$

By solving $t^k \equiv z(t) \pmod{\pi(t)^e}$ for each irreducible $\pi(t) \neq t$ with $\pi(t)^e | \mu(t)$ and using the Chinese Remainder Theorem [1], we determined that $t^{217183} \equiv z(t) \pmod{\mu(t)}$, so that $\Psi(M)^{217183} = \Psi(M^a)$, and hence $M^{217183} = M^a$.

9 Acknowledgements

My colleague, good friend, and coauthor Mara Neusel passed away after the first draft of this paper was submitted and before the preparation of a revised draft. She will be dearly missed by many for years to come. Any inaccuracies or poor styling that may remain are strictly the fault of the first author.

We are grateful to the anonymous referee and editors for valuable feeback and suggestions on earlier drafts of this paper.

References

[1] E. Bach and J. Shallit. *Algorithmic Number Theory, Vol. 1.* The MIT Press, Cambridge 1996.

[2] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. *CoRR*, abs/1306.4244, 2013.

[3] P. J. Cameron. *Combinatorics.* Cambridge University Press, Cambridge 1994.

[1] In fact, upon computing the order of t modulo each factor of μ other than t^{12}, we determined that there was necessarily a solution with $a < 302260$ which could be determined by simple exhaustive search, but we wanted to test this method of solving the problem locally.

[4] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Advances in cryptology—CRYPTO '98 (Santa Barbara, CA, 1998)*, volume 1462 of *Lecture Notes in Comput. Sci.*, pages 13–25. Springer, Berlin, 1998.

[5] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[6] A. Joux. A new index calculus algorithm with complexity $L(1/4 + o(1))$ in very small characteristic. Cryptology ePrint Archive, Report 2013/095, 2013. `http://eprint.iacr.org/`.

[7] N. Jacobson. *Basic Algebra II*. Dover Publishing Inc., Mineola NY, 2009.

[8] G. James and A. Kerber. *The representation theory of the symmetric group*, volume 16 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Co., Reading, Mass., 1981. With a foreword by P. M. Cohn, With an introduction by Gilbert de B. Robinson.

[9] G. James and M. Liebeck. *Representations and Characters of Groups*. Cambridge University Press, Cambridge 1993.

[10] D. Kahrobaei, C. Koupparis, and V. Shpilrain. Public key exchange using matrices over group rings. *Groups Complex. Cryptol.*, 5(1):97–115, 2013.

[11] D. Kahrobaei, C. Koupparis, and V. Shpilrain. A CCA secure cryptosystem using matrices over group rings. *Contemp. Math., Amer. Math. Soc.*, 633:73–80, 2015.

[12] C. M. Koupparis. *Non-commutative cryptography: Diffie-Hellman and CCA secure cryptosystems using matrices over group rings and digital signatures*. ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–City University of New York.

[13] A. J. Menezes and Y. Wu. The discrete logarithm problem in $\mathrm{GL}(n, q)$. *Ars Combin.*, 47:23–32, 1997.

[14] C. Monico. Cryptanalysis of a matrix-based MOR system. *Comm. Algebra*, to appear.

[15] A. D. Myasnikov and A. Ushakov. Quantum algorithm for the discrete logarithm problem for matrices over finite group rings. *Groups, Complexity, Cryptology*, 6:31–36, 2014.

[16] The On-Line Encyclopedia of Integer Sequences. Published electronically at `http://oeis.org`, 2015, Sequence A003040.

[17] S.C. Pohlig and M.E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Trans. Inform. Theory*, 24:106–110, 1978.

[18] J. M. Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, 32:918–924, 1978.