Cryptanalysis of a key exchange scheme based on block matrices

María Isabel González Vasco*, Angel L. Pérez del Pozo*† and Pedro Taborda Duarte‡

Dpto. de Matemática Aplicada, Universidad Rey Juan Carlos
C/ Tulipán s/n. 28933, Móstoles, Madrid, Spain
{mariaisabel.vasco, angel.perez, pedro.duarte}@urjc.es

November 11, 2009

Abstract

In this paper we describe a cryptanalysis of a key exchange scheme recently proposed by Álvarez, Tortosa, Vicent and Zamora. The scheme is based on exponentiation of block matrices over a finite field of prime order. We present an efficient reduction of the problem of disclosing the shared key to the discrete logarithm problem (DLP) in an extension of the base field.

Keywords: key exchange scheme, cryptanalysis, finite field, block matrix, discrete logarithm problem

1 Introduction

The very well known Diffie-Hellman key exchange scheme [5] was the first published public key cryptographic protocol, allowing two users communicating over a public insecure channel to agree on a common shared secret key. One of the most common platform groups candidates to implement this protocol is the multiplicative group of a finite field. In this case, the problem of obtaining the shared key from the exchanged data is trivially solved if one can solve the discrete logarithm problem (DLP) in the finite field, but this is considered to be a computationally hard problem for appropriately chosen parameters. Some other groups have been proposed as platform groups for Diffie-Hellman-like protocols, such as the group of non-singular matrices over a finite field [12] or the group of points of an elliptic curve [7] and [11].

Recently, Álvarez, Tortosa, Vicent and Zamora [1, 2] proposed a key exchange protocol where the platform group is the 2×2 block upper triangular invertible matrices over a finite field. Essentially, two *high order* public matrices M_1 and M_2 are generated in this group (the authors in [1, 2] suggest using companion matrices of primitive polynomials in blocks $(1, 1)$ and $(2, 2)$ to maximize the order). Then the two users choose secret exponents (r, s) and (v, w) respectively, and exchange the matrices $M_1^r M_2^s$ and $M_1^u M_2^v$. The shared key is the $(1, 2)$ block of the matrix $M_1^{r+v} M_2^{s+w}$. This is done mainly in order to avoid a reduction from the DLP in the matrix group to the DLP in the base field (see the *Related work* paragraph). The computational problem of recovering the private keys from the public information can thus be stated as (2EXP problem in 4.2): from the exchanged data $M_1^r M_2^s$ and $M_1^v M_2^w$, compute the secret exponents r, s (or v, w).

* partially supported by research project CCG08-UCM/ESP-4394
† contact author
‡ with support from *Fundação para a Ciência e Tecnologia, Portugal ref: SFRH/BD/37869/2007*

This immediately allows one to recover the shared matrix $M_1^{r+v} M_2^{s+w}$.

Our contribution. The main result in this paper is an efficient reduction from the 2EXP problem to the DLP in a finite extension of the base field in case companion matrices of primitive polynomials are used. This is done in three steps: first, we show how the 2EXP problem can be solved separately in the $(1,1)$ and $(2,2)$ blocks to obtain a solution for the whole problem. Second, we study the 2EXP problem when the matrices are arbitrary invertible matrices. In this case we reduce the 2EXP problem to a computational problem (2EXP* in 4.2.1) in an extension of the base field. Third, we focus on the case where the involved matrices are generated using companion matrices of primitive polynomials, as proposed in [1, 2]. In this situation we are able to reduce the 2EXP problem to solving the DLP in a finite extension of the base field. Thus we conclude that the use of this scheme offers no advantage over the original Diffie-Hellman key exchange scheme. We also provide an observation about the public parameters generation (specifically, the matrices M_1 and M_2 must be chosen in a way that they do not commute) and some remarks about the order of these matrices.

Related work. As far as we now, the first attempt to using matrices over a finite field in a key exchange scheme was made by Odoni, Varadharajan and Sanders in 1984 [12]. They use an invertible matrix as a group generator and then proceed as in the usual Diffie-Hellman key exchange protocol. In order to get a high enough order for the generating matrix, they define a block diagonal matrix, where the blocks are similar to companion matrices of primitive polynomials (in fact, as pointed out in [9], the authors incorrectly use irreducible polynomials instead of primitive polynomials).

After that, Menezes and Vanstone proved in 1992 [9] that the DLP in the cyclic group generated by one of these block matrices can be efficiently reduced to the DLP in an extension of the base field, thus showing that this kind of groups offers no advantage over finite fields. In a subsequent paper of 1997, Menezes and Yi-Hong Wu [10] extended this reduction to the general case, that is, they showed that the DLP in the general linear group $GL_n(\mathbb{Z}_p)$ can be efficiently reduced to the DLP in certain "small" extension of the base field.

In order to avoid the Menezes and Yi-Hong Wu reduction, Climent, Ferrández, Vicent and Zamora [3] proposed in 2006 another matrix based key exchange protocol (CFVZ protocol). They use 2×2 block upper triangular matrices, where the diagonal blocks have integer entries while the (1,2) block has entries in the set of rational points of an elliptic curve. In this case the two parties of the protocol interchange the (1,2) block of a randomly chosen power of one of these matrices. The shared key is the (1,2) block of another matrix which they can compute with their secret data.

In 2007, Climent, Gorla and Rosenthal [4] published a cryptanalysis of this last protocol. They showed how the problem of computing the shared key can be efficiently reduced to solving several DLP's in the group associated to the elliptic curve. They also proved how solving simultaneously these DLP's problems is essentially as hard as solving one single DLP. Therefore they conclude that the CFVZ protocol offers no advantage over working in the elliptic curve group.

Paper outline. In Section 2 we introduce the subgroup of the general linear group $GL_n(\mathbb{Z}_p)$ which is used in the proposed key exchange scheme. We recall how the public data is generated by using companion matrices of primitive polynomials and provide some remarks about the orders of these matrices. In Section 3 the key exchange protocol is described. Section 4 is devoted to the cryptanalysis of the scheme. First we study the general case, when the public matrices are arbitrary and then we focus on the case when they are generated by using companion matrices of primitive polynomials. In the former we reduce the problem of disclosing the secret keys to a computational problem in an extension of the base field, while in the later we show that this problem can be solved by computing discrete logarithms in that extension. Finally we summarize our conclusions in Section 5. The proofs of the claims in Section 2 are included in the Appendix.

2 Preliminaries

The following is a description of the underlying group structure. We describe some properties and simple consequences of the definitions, and recall the method proposed in [1, 2] for generating high order elements.

2.1 Underlying group structure

Given a prime number p and $n, l \in \mathbb{N}$, define the subgroup of $GL_{n+l}(\mathbb{Z}_p)$ under matrix multiplication by

$$\Theta(p,n,l) = \left\{ \begin{pmatrix} A & X \\ 0 & B \end{pmatrix} : \quad A \in GL_n(\mathbb{Z}_p), B \in GL_l(\mathbb{Z}_p),\ X \in Mat_{n\times l}(\mathbb{Z}_p) \right\}$$

We simply write Θ when p, n and l are fixed. The following are some simple consequences of the definition:

1. If $M \in \Theta$ and $h \geq 0$ then $M^h = \begin{pmatrix} A^h & X^{(h)} \\ 0 & B^h \end{pmatrix}$ with
$$X^{(h)} = \begin{cases} 0 & if\ h = 0 \\ \sum_{i=1}^{h} A^{h-i} X B^{i-1} & if\ h \geq 1 \end{cases}$$
2. If $a, b \geq 0$ then $X^{(a+b)} = A^a X^{(b)} + X^{(a)} B^b$
3. If $M = \begin{pmatrix} A & X \\ 0 & B \end{pmatrix} \in \Theta$ then the characteristic polynomials $p_M,\ p_A$ and p_B of $M,\ A$ and B respectively, are related by $p_M(\lambda) = p_A(\lambda) \cdot p_B(\lambda)$. Hence, λ is an eigenvalue of M if and only if it is an eigenvalue of A or B and moreover, since A and B are invertible λ is always non zero.

2.2 High order elements M from Θ:

As described in section 3, the key exchange protocol presented in [1, 2] is based on products of certain powers (the private keys) of elements $M_1, M_2 \in \Theta$. Therefore, it is important that these elements achieve a high order so that exhaustive search attacks are prevented. In [1, 2] the following method is proposed:

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^{n-1} + x^n$ and $g(x) = b_0 + b_1 x + \ldots + b_{l-1} x^{l-1} + x^l$ be two primitive polynomials in $\mathbb{Z}_p[x]$ and A_f, B_g the corresponding companion matrices i.e.

$$A_f = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

$$B_g = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -b_0 & -b_1 & -b_2 & \cdots & -b_{l-2} & -b_{l-1} \end{pmatrix}$$

Then, let $P \in GL_n(\mathbb{Z}_p)$ and $Q \in GL_l(\mathbb{Z}_p)$ and set

$$A = PA_fP^{-1} \in GL_n(\mathbb{Z}_p)$$

and

$$B = QB_gQ^{-1} \in GL_l(\mathbb{Z}_p)$$

Choose $X \in Mat_{n\times l}(\mathbb{Z}_p)$ and set $M = \begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$.

As described, in this construction any "X-matrix" is valid, so that we assume that X *may* be chosen at random.

In the original papers [1, 2], it is claimed that, with this construction, the order of M is such that $ord(M) = lcm(p^n - 1, p^l - 1)$ and if n and l are chosen to be relatively prime then $ord(M)$ is maximum. Next we provide a couple of remarks about these claims:

Remark 2.1. *Note that it is not true that $ord(M) = lcm(ord(A), ord(B))$ for an arbitrary matrix $M \in \Theta$, as the following example shows:*
In $\mathbb{Z}_5$ set $A = \begin{pmatrix} 1 & 3 \\ 0 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 0 & 2 \\ 0 & 2 & 1 \\ 1 & 2 & 2 \end{pmatrix}$ and $X = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix}$. It can be computed that $ord(A) = 4$, $ord(B) = 12$. Then $lcm(ord(A), ord(B)) = 12$ but $ord(M) = 60$.

However, if M is chosen as in 2.2 then it is true that $ord(M) = lcm(ord(A), ord(B)) = lcm(p^n - 1, p^l - 1)$. We have not been able to find a demonstration of this fact in the literature therefore we include a proof of the following lemma in the Appendix.

Lemma 2.1. *Take M as in 2.2. Let $a = ord(A)$, $b = ord(B)$ and $k = lcm(a, b)$. Then*

1. *$a = p^n - 1$ and $b = p^l - 1$*
2. *$X^{(k)} = 0$*
3. *$ord(M) = k$*

Remark 2.2. *Suppose that the overall dimension m of M is fixed, and consider n and l such that $n + l = m$. It is true, as stated by the authors, that if n and l are relatively prime, then the number of common divisors of $p^n - 1$ and $p^l - 1$ is diminished (in fact $gcd(p^n - 1, p^l - 1) = p - 1$). However, one may wonder how to choose n and l among the possible options such that $n + l = m$ and the order of M is maximized. The behavior of the function $lcm(p^x - 1, p^{m-x} - 1)$ for coprime*

x and $m-x$ depends only on the product $(p^x-1)(p^{m-x}-1)$, a function which is symmetric around $m/2$ and increasing from 1 to $m/2$. To find the maximum of $lcm(p^x-1, p^{m-x}-1)$ when x and $m-x$ are coprime, one only has to find the x_0 closest to $m/2$ such that $gcd(x_0, m-x_0)=1$. Therefore, by choosing n and l coprime such that $n+l=m$, $ord(M)$ varies from $p^{m-1}-1$ to $lcm(p^{x_0}-1, p^{m-x_0}-1)$ and the maximum order for M is attained when $n=x_0$ and $l=m-x_0$. All the details and proofs can be found in the Appendix.

3 The key exchange protocol

Next we describe the key exchange protocol as proposed in [1, 2].

1. Alice and Bob agree on a prime p and on n, l. Then they choose $M_1, M_2 \in \Theta(p, n, l)$ of high order. Let $| < M_1 > | = m_1$ and $| < M_2 > | = m_2$ and write $M_1 = \begin{pmatrix} A_1 & X_1 \\ 0 & B_1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} A_2 & X_2 \\ 0 & B_2 \end{pmatrix}$
2. Alice generates random $r, s \in \mathbb{N}$ such that
$$1 \leq r \leq m_1 - 1 \quad and \quad 1 \leq s \leq m_2 - 1$$
3. Alice computes $C = M_1^r M_2^s = \begin{pmatrix} A_C & X_C \\ 0 & B_C \end{pmatrix}$ and sends C to Bob
4. Bob generates random $v, w \in \mathbb{N}$ such that
$$1 \leq v \leq m_1 - 1 \quad and \quad 1 \leq w \leq m_2 - 1$$
5. Bob computes $D = M_1^v M_2^w = \begin{pmatrix} A_D & X_D \\ 0 & B_D \end{pmatrix}$ and sends D to Alice
6. Alice computes $K_a = A_1^r A_D X_2^{(s)} + A_1^r X_D B_2^s + X_1^{(r)} B_D B_2^s$.
7. Bob computes $K_b = A_1^v A_C X_2^{(w)} + A_1^v X_C B_2^w + X_1^{(v)} B_C B_2^w$.
8. According to the next lemma, the shared key K is $K = K_a = K_b$.

Proposition 3.1 (Shared key)**.** *Following the protocol, $K_a = K_b$ and moreover K_a (and K_b) is the $(1,2)$ entry of $M_1^{r+v} M_2^{s+w}$.*

Proof. It is easy to see that
$$M_1^r D M_2^s = \begin{pmatrix} A_1^{r+v} A_2^{s+w} & K_a \\ 0 & B_1^{r+v} B_2^{s+w} \end{pmatrix}$$
and
$$M_1^v C M_2^w = \begin{pmatrix} A_1^{r+v} A_2^{s+w} & K_b \\ 0 & B_1^{r+v} B_2^{s+w} \end{pmatrix}$$
and also
$$M_1^r D M_2^s = M_1^{r+v} M_2^{s+w} = M_1^v C M_2^w$$
Therefore $K_a = K_b$ □

1. The public data:
   - $\star$ p prime
   - $\star$ n, l
   - $\star$ M_1, $M_2 \in \Theta(p, n, l)$
2. The private data:
   - $\star$ Alice: (r, s)
   - $\star$ Bob: (v, w)
3. Data exchanged:
   - $\star$ $C = M_1^r M_2^s$
   - $\star$ $D = M_1^v M_2^w$

The shared key is the entry $(1,2)$ of $M_1^{r+v} M_2^{s+w}$

Figure 1: Public and private data of the protocol

Alice		Bob
$1 \leq r \leq m_1 - 1$ and $1 \leq s \leq m_2 - 1$	$\longrightarrow$	$C = M_1^r M_2^s$
$D = M_1^v M_2^w$	$\longleftarrow$	$1 \leq v \leq m_1 - 1$ and $1 \leq w \leq m_2 - 1$
$K_a = (M_1^r D M_2^s)_{(1,2)}$		$K_b = (M_1^v C M_2^w)_{(1,2)}$
	$K = K_a = K_b$	

Figure 2: Key exchange protocol

4 Security Analysis

In this section we present the security analysis and an attack on the scheme of section 3. The first subsection consists on a remark on the key generation procedure. The second subsection provides a reduction of the cryptographic problem to a related problem in an extension of the base field. The third section presents an attack on the protocol in case the entries are generated using companion matrices of primitive polynomials as is suggested by the authors of [1, 2]. We show that in this case it is possible to reduce the problem to that of computing discrete logarithms in an extension of the base field. This shows that the protocol does not offer an advantage over computation in $\mathbb{Z}_p$, since the computational cost of operations in $GL_n(\mathbb{Z}_p)$ is higher than in $\mathbb{Z}_p$.

4.1 Key generation

If M_1 and M_2 commute then the shared key can be computed by

$$K = M_1^{r+v} M_2^{s+w} = M_1^r M_1^v M_2^s M_2^w = M_1^r M_2^s M_1^v M_2^w = CD$$

Although the probability that this happens (at least for u.a.r chosen matrices) is very small, it is obvious that the protocol should not accept this kind of keys.

$M_1 \in \Theta$ and $M_2 \in \Theta$ should be such that $M_1 M_2 \neq M_2 M_1$

4.2 Reduction to the DLP in a finite field

We will show here that, with the proposed key generation, it is possible to reduce the problem of finding the secret keys r and s, to solving a certain problem in an extension of the base field. The problem of recovering the secret key in the proposed key exchange protocol can be stated in the following way:

2EXP problem: Suppose $M_1, M_2 \in \Theta(p, n, l)$ have orders m_1 and m_2 respectively. Let also $1 \leq r \leq m_1 - 1$ and $1 \leq s \leq m_2 - 1$. Given M_1, M_2 and $C = M_1^r M_2^s$, find r, s.

Proposition 4.1. *Recovering the private keys in the proposed key exchange protocol can be reduced to solving the 2EXP problem for matrices in $GL_n(\mathbb{Z}_p)$ and in $GL_l(\mathbb{Z}_p)$.*

Proof. Suppose that the orders of the matrices A_i, B_i and M_i are a_i, b_i and $m_i = lcm(a_i, b_i)$ respectively. An adversary $\mathcal{A}$ able to get the matrix $C = M_1^r M_2^s$ can easily compute $A_1^r A_2^s$ and $B_1^r B_2^s$. Then, by solving the 2EXP problem in $GL_n(\mathbb{Z}_p)$ and in $GL_l(\mathbb{Z}_p)$, $\mathcal{A}$ gets the values $r \bmod a_1$, $s \bmod a_2$, $r \bmod b_1$ and $s \bmod b_2$. From these values, $\mathcal{A}$ can easily compute $r \pmod{m_1}$, $s \pmod{m_2}$ and the private keys are disclosed. *A priori* it is necessary to solve both instances of the 2EXP problem, for $A_1^r A_2^s$ and $B_1^r B_2^s$. □

Therefore it is enough to solve the 2EXP problem for each of the pairs (A_1, A_2) and (B_1, B_2) given M_1 and M_2. The next sections will first describe the general case and then proceed to the case when these pairs of matrices are generated as in section 2.2. Note that in this case each matrix from each pair is generated using primitive polynomials of the same degree. In this last case we are able to further reduce the 2EXP problem in $GL_n(\mathbb{Z}_p)$ to the DLP problem in the extension field $\mathbb{F}_{p^n}$.

4.2.1 The general case

We consider the Jordan normal form of $A_1, A_2 \in GL_n(\mathbb{Z}_p)$. More precisely, suppose the characteristic polynomial of A_1 is given by $p_1 = f_1^{e_1} \cdots f_k^{e_k}$ where the f_i are distinct irreducible polynomials of degree d_i in $\mathbb{Z}_p[x]$. Then the smallest extension field containing all the eigenvalues of A_1 is the field $E_1 = \mathbb{F}_{p^{\bar{d_1}}}$ with $\bar{d_1} = lcm(d_1, d_2, \ldots, d_k)$. Similarly for A_2, the smallest extension field containing all the eigenvalues of A_2 is the field $E_2 = \mathbb{F}_{p^{\bar{d_2}}}$ with a similar $\bar{d_2}$.

Let $E = \mathbb{F}_{p^{lcm(\bar{d_1}, \bar{d_2})}}$. Then it is well known that there exist $P_1 \in GL_n(E_1)$ and $P_2 \in GL_n(E_2)$

such that $A_1 = P_1^{-1} J P_1$ and $A_2 = P_2^{-1} H P_2$ where J and H are the Jordan matrices of each i.e.

$$J = \begin{pmatrix} J_{k_1}(\lambda_1) & 0 & \cdots & 0 \\ 0 & J_{k_2}(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{k_t}(\lambda_t) \end{pmatrix}$$

and

$$H = \begin{pmatrix} H_{l_1}(\alpha_1) & 0 & \cdots & 0 \\ 0 & H_{l_2}(\alpha_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & H_{l_u}(\alpha_u) \end{pmatrix}$$

The $J_{k_i}(\lambda_i),\ i = 1, \dots, t$ (resp. $H_{l_i}(\alpha_i),\ i = 1, \dots, u$) are the Jordan blocks of A_1 of size k_i associated to the eigenvalue λ_i (resp. Jordan blocks of A_2 of size l_i associated to the eigenvalue α_i) such that $\sum_{i=1}^{t} k_i = \sum_{i=1}^{u} l_i = n$. i.e. they are the $k_i \times k_i$ size matrices

$$J_{k_i}(\lambda_i) = \begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_i & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{pmatrix}$$

and the $l_i \times l_i$ size matrices

$$H_{l_i}(\alpha_i) = \begin{pmatrix} \alpha_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & \alpha_i & 1 & \cdots & 0 & 0 \\ 0 & 0 & \alpha_i & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_i & 1 \\ 0 & 0 & 0 & \cdots & 0 & \alpha_i \end{pmatrix}$$

Note that $\lambda_1, \dots, \lambda_t$ (resp. $\alpha_1, \dots, \alpha_u$) need not be necessarily distinct. In [10] the authors describe an algorithm for computing the Jordan canonical form in $GL_n(\mathbb{Z}_p)$ that runs in expected polynomial time.

Then $C = A_1^r A_2^s = P_1^{-1} J^r P_1 \cdot P_2^{-1} H^s P_2$ which means $J^r (P_1 P_2^{-1}) H^s = P_1 C P_2^{-1}$ i.e.

$$J^r Z H^s = W \tag{4.2.1}$$

with known $Z = P_1 P_2^{-1} = [z_{ij}]$ and $W = P_1 C P_2^{-1} = [w_{ij}]$. This equation is in the field E.

Since $J^r = \bigoplus_{i=1}^{t} (J_{k_i}(\lambda_i))^r$ and $H^s = \bigoplus_{i=1}^{u} (H_{l_i}(\alpha_i))^s$, and it can be shown that entries (a,b) are given by

$$((J_{k_i}(\lambda_i))^r)_{ab} = \binom{r}{b-a} \lambda_i^{r-b+a}, \quad 1 \le a \le b \le k_i \tag{4.2.2}$$

$$((H_{l_i}(\alpha_i))^s)_{ab} = \binom{s}{b-a} \alpha_i^{s-b+a}, \quad 1 \le a \le b \le l_i \tag{4.2.3}$$

we get $(J^r Z H^s)_{ab} = \sum_{i,j=1}^{n} (J^r)_{aj} \cdot z_{ji} \cdot (H^s)_{ib}$.

So for example, for $1 \le a \le k_1$ and $l_1 + 1 \le b \le l_1 + l_2$ (i.e. "choosing" $J_{k_1}(\lambda_1)$ and $H_{l_2}(\alpha_2)$), we get

$$\begin{aligned} (J^r Z H^s)_{ab} &= \sum_{i=l_1+1}^{l_1+l_2} \sum_{j=1}^{k_1} ((J_{k_1}(\lambda_1))^r)_{aj} \cdot z_{ji} \cdot ((H_{l_2}(\alpha_2))^s)_{ib} \\ &= \sum_{i=l_1+1}^{l_1+l_2} \sum_{j=1}^{k_1} \binom{r}{j-a} \binom{s}{b-i} z_{ji}\, \lambda_1^{r-j+a} \alpha_2^{s-b+i} \end{aligned}$$

Choosing $a = k_1$ and $b = l_1 + 1$, equations 4.2.2 and 4.2.3 imply that $j = k_1$ and $i = l_1 + 1$ so that

$$(J^r Z H^s)_{k_1\,(l_1+1)} = z_{k_1\,(l_1+1)} \cdot \lambda_1^r \alpha_2^s$$

In general, for $a(j_1) = \sum_{i=1}^{j_1+1} k_i$ and $b(j_2) = 1 + \sum_{i=1}^{j_2} l_i$ with $j_1 = 0, \ldots, t-1$ and $j_2 = 0, \ldots, u-1$ we have

$$(J^r Z H^s)_{a(j_1)\,b(j_2)} = z_{a(j_1) b(j_2)} \cdot \lambda_{j_1+1}^r \alpha_{j_2+1}^s$$

Equation 4.2.1 then becomes

$$z_{a(j_1)b(j_2)} \cdot \lambda_{j_1+1}^r \alpha_{j_2+1}^s = w_{a(j_1)b(j_2)} \quad j_1 = 0, \ldots, t-1 \text{ and } j_2 = 0, \ldots, u-1 \tag{4.2.4}$$

Note that in equation 4.2.4, appear all the possible products of eigenvalues of A_1 by those of A_2. This shows that, if we can solve for at least one pair (j_1, j_2), the problem of given $\lambda_{j_1+1}^r \alpha_{j_2+1}^s$ computing r, s, we can also break the protocol. Therefore we reduced the original 2EXP problem to the following 2EXP* problem:

2EXP* problem: Suppose $A_1, A_2 \in GL_n(\mathbb{Z}_p)$ have orders a_1 and a_2 respectively, and let (λ_{k_1}) and (α_{k_2}) $(1 \le k_1, k_2 \le n)$ denote the eigenvalues of A_1 and A_2 respectively. Let also $1 \le r \le a_1 - 1$ and $1 \le s \le a_2 - 1$.
Given a set of elements $\{u_{ij} = \lambda_j^r \alpha_j^s\}$ (in a certain extension field of $\mathbb{Z}_p$) of size less or equal to n^2, find r, s.

Thus we have reduced the key recovering problem to a computational problem in a finite field. Moreover, if the next two conditions (I) and (II) hold, we are able to reduce the 2EXP* problem to the DLP problem. Observing equation 4.2.4 we conclude that:

I. If A_1 and A_2 share a common eigenvalue $\gamma = \lambda_{j_1+1} = \alpha_{j_2+1} \neq 1$ and $z_{a(j_1)b(j_2)} \neq 0$ then $\gamma^{r+s} = w_{a(j_1)b(j_2)} \cdot z^{-1}_{a(j_1)b(j_2)}$

II. If $\alpha_{k_2} = 1 \wedge \lambda_{k_1} \neq 1$ and $z_{a(k_1)b(k_2)} \neq 0$ then $\lambda^r_{k_1} = w_{a(k_1)b(k_2)} \cdot z^{-1}_{a(k_1)b(k_2)}$

We have thus reduced the problem of retrieving the private keys to solving the DLP in a finite field if the following happens to be true: A_1 and A_2 share a common eigenvalue, and A_1 (or A_2) has eigenvalue 1. In general, both conditions are necessary to retrieve the private keys r, s by solving the DLP's (I) and (II). Therefore matrices satisfying (I) and (II) simultaneously should be avoided in the parameter generation procedure.

4.2.2 A_1 and A_2 chosen as in section 2.2

Note that now we have $ord(A_1) = ord(A_2) = p^n - 1$. Suppose that A_1 and A_2 are matrices similar to companion matrices of some primitive polynomials f_1 and f_2 of degree n. Then

Lemma 4.1.

1. *$f_1 = p_{A_1}$ and $f_2 = p_{A_2}$*
2. *The eigenvalues of A_1 are s.t. $\{\lambda_1, \dots, \lambda_n\} \subseteq F_1 \simeq \mathbb{F}_{p^n}$ and $\forall_i\ \lambda_i$ generates F_1^**
3. *The eigenvalues of A_2 are s.t. $\{\alpha_1, \dots, \alpha_n\} \subseteq F_2 \simeq \mathbb{F}_{p^n}$ and $\forall_i\ \alpha_i$ generates F_2^**
4. *A_1 and A_2 are diagonalizable in the extensions F_1 and F_2.*

Proof. See for example [6]. □

In particular this means that 1 is not an eigenvalue of neither A_1 nor of A_2 and therefore the method for solving for r, s described at the end of section 4.2.1 may not necessarily apply since condition (I) is also necessary in general for solving equation 4.2.4. We will see in the following that nevertheless, in this case, retrieving the private keys r, s is no harder than solving a discrete logarithm in $\mathbb{F}_{p^n}$.

Since the Jordan matrices of A_1 and A_2 are diagonal, equation 4.2.4 becomes

$$z_{ij} \lambda_i^r \alpha_j^s = w_{ij} \quad \forall_{i,j} \tag{4.2.5}$$

Write $\lambda = \lambda_i$ and $\alpha = \alpha_j$. At this we have the following situation:

1. We are considering extension fields of $\mathbb{F}_p$ for each root λ and α of f_1 and f_2. Therefore, $\lambda^r \in \mathbb{F}_p(\lambda)$ and $\alpha^s \in \mathbb{F}_p(\alpha)$. Moreover, $\mathbb{F}_p(\lambda) \simeq \mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^n}$.
2. If $z_{ij} \neq 0$ then $u_{ij} = z_{ij}^{-1} w_{ij} = \lambda^r \alpha^s$ belongs to a finite extension of $\mathbb{F}_p$ by adjoining the roots λ and α i.e $u_{ij} \in \mathbb{F}_p(\lambda)(\alpha)$.

By the *subfield criterion* (see [8] pag. 49 for example) there exists exactly one subfield of $\mathbb{F}_p(\lambda)(\alpha)$ with p^n elements. Therefore $\mathbb{F}_p(\lambda) = \mathbb{F}_p(\alpha)$ and hence

$$\mathbb{F}_p(\lambda)(\alpha) = \mathbb{F}_p(\lambda) = \mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^n}$$

We then conclude that if $z_{ij} \neq 0$ then $\{\alpha_j, u_{ij}\} \subseteq \mathbb{F}_p(\lambda_i)^*$, and therefore, by 2 of lemma 4.1 there exists $0 \leq x_j \leq p^n - 1$ such that

$$\alpha_j = \lambda_i^{x_j}$$

Equation 4.2.5 then becomes

$$\lambda_i^{r+x_j s} = u_{ij}$$

in $\mathbb{F}_{p^n}$.

Generating a new equation 4.2.5 with the same i but a different k such that $f_2(\alpha_k) = 0$ and $z_{ik} \neq 0$ (i.e. by considering a different eigenvalue of A_2) we also have $\alpha_k = \lambda_i^{x_k}$ for $0 \leq x_k \leq p^n - 1$. Note that $Z = P_1 P_2^{-1}$ must have many entries different from 0. Therefore, solving the DLP system in $\mathbb{F}_{p^n}$ for x_j and x_k, gives us another system of DLP's in $\mathbb{F}_{p^n}$:

$$\begin{cases} \lambda_i^{r+x_j s} & = u_{ij} \\ \\ \lambda_i^{r+x_k s} & = u_{ik} \end{cases} \tag{4.2.6}$$

We now need to solve this system to retrieve the private keys r and s.

4.2.3 Solving system 4.2.6

We suppose we were able to compute x_j and x_k. Suppose also without loss of generality that $i = j = 1$ and $k = 2$ (i.e. we are considering λ_1, α_1, α_2) and that $u_{11} = \lambda_1^{y_1}$ and $u_{12} = \lambda_1^{y_2}$. Then we are looking for (one of) the solutions of the system

$$\begin{cases} \bar{r} + x_1 \bar{s} & = & y_1 \bmod (p^n - 1) \\ \\ \bar{r} + x_2 \bar{s} & = & y_2 \bmod (p^n - 1) \end{cases} \tag{4.2.7}$$

Applying reduction, we find that $(x_2 - x_1)\bar{s} = y_2 - y_1 \bmod (p^n - 1)$, and since the original s is a solution, we conclude that $d = gcd(x_2 - x_1, p^n - 1)$ divides $(y_2 - y_1)$. There are therefore exactly d solutions to system 4.2.7. If $(\bar{x}, \bar{y})$ is such that $d = (x_2 - x_1)\bar{x} + (p^n - 1)\bar{y}$ then the solutions to system 4.2.7 are given by

$$\begin{aligned} s_i &= \bar{x}(y_2 - y_1)/d + i(p^n - 1)/d \quad \bmod (p^n - 1) \\ r_i &= y_1 - x_1 s_i \quad \bmod (p^n - 1) \end{aligned}$$

where $i = 0, \ldots, d-1$. Of these d pairs (r_i, s_i), one will be the original (r, s).

Depending on the chosen λ_1, α_1 and α_2, the number of solutions can be high, so it is clear that this choice is important for solving the system. We will show that it is always possible to choose "well" i.e. choosing λ_1, α_1 and α_2 such that $d = gcd(x_2 - x_1, p^n - 1)$ is small.

Choose one root λ_1 of f_1 and one root α_1 of f_2. Because f_2 is primitive, there exists j such that $\alpha_j = \alpha_1^p$ (in fact all the other roots of f_2 are of the form $\alpha_1^{p^j}$, $j = 1, \ldots, n-1$) and moreover, if $\alpha_1 = \lambda_1^{x_1}$ and $\alpha_j = \lambda_1^{x_2}$ then

$$\lambda_1^{p\,x_1} = \alpha_1^p = \alpha_j = \lambda_1^{x_2}$$

Therefore $x_2 = p\,x_1 \bmod (p^n - 1)$ and consequently

$$d = gcd(x_2 - x_1, p^n - 1) = gcd(x_1(p-1), p^n - 1)$$

Now, if $d|x_1(p-1)$ then it must be that $d = d_1 d_2$, with $d_1|x_1$ and $d_2|(p-1)$. On the other hand $d\,|(p^n-1)$ implies that $d_1|(p^n-1)$ and $d_2|(p^n-1)$. Since all roots are primitive x_1 must be invertible mod(p^n-1) (by 3 of lemma 4.1 $\lambda_1 = \alpha_1^{y_1}$ for some $1 \leq y_1 < p^n - 1$, which means that $x_1\,y_1 = 1 \mod (p^n-1)$). Hence $gcd(x_1, p^n-1) = 1$ and therefore $d_1 = 1$ (since d_1 is a common divisor of x_1 and $p^n - 1$) i.e. d must be the *greatest common divisor* of $p-1$ and p^n-1. Therefore $d = p-1$. If $z_{11} = 0$ or $z_{1j} = 0$ we choose other roots.

We have thus shown that, by choosing a root λ_1 of A_1 and two "successive" roots α_1 and $\alpha_j = \alpha_1^p$ of A_2, such that the corresponding z_{11} and z_{1j} are non zero, then the number of solutions of the system 4.2.7 is $p-1$. Of these, one solution is the original (r, s).

5 Conclusions

We have presented a cryptanalysis and an attack on the key exchange scheme proposed in [1, 2]. More precisely, we have shown that breaking the scheme can be reduced to solving a computational problem in an extension of the base field. Moreover, if the parameters M_1 and M_2 are generated using companion matrices of primitive polynomials, then this computational problem can be further reduced to a small set of discrete logarithm problems in an extension of the base field. We have also commented on the need for the protocol to make sure the parameters do not commute. We thus conclude that the scheme offers no advantage over working in the base field.

References

[1] R. Álvarez, L. Tortosa, J. Vicent, and A. Zamora, *Analysis and design of a secure key exchange scheme*, Information Sciences, 179 (2009), pp. 2014–2021.

[2] ——, *A non-abelian group based on block upper triangular matrices with cryptographic applications*, in AAECC-18 '09: Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Berlin, Heidelberg, 2009, Springer-Verlag, pp. 117–126.

[3] J. Climent, F. Ferrández, J. Vicent, and A. Zamora, *A nonlinear elliptic curve cryptosystem based on matrices*, Applied Mathematics and Computation, 174 (2006), pp. 150–164.

[4] J. Climent, E. Gorla, and J. Rosenthal, *Cryptanalysis of the cfvz cryptosystem*, Advances in Mathematics of Communications, 1 (2007), pp. 1–11.

[5] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inf. Theory, 22 (1976), pp. 644–654.

[6] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 1990.

[7] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comput., 48 (1987), pp. 203–209.

[8] R. Lidl and H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and its Applications)*, Cambridge University Press, October 1996.

[9] A. Menezes and S. Vanstone, *A note on cyclic groups, finite fields, and the discrete logarithm problem*, Applicable Algebra in Engineering, Communication and Computing, 3 (1992), pp. 67–74.

[10] A. Menezes and Y.-H. Wu, *The discrete logarithm problem in gl(n, q)*, Ars Comb., 47 (1997).

[11] V. Miller, *Uses of elliptic curves in cryptography*, in Advances in Cryptology - Proceedings of Crypto'85. Lecture Notes in Computes Science, vol. 218, Berlin, Heidelberg, 1986, Springer-Verlag, pp. 417–426.

[12] R. Odoni, V. Varadharajan, and P. Sanders, *Public key distribution in matrix rings*, Electronic Letters, 20 (1984), pp. 386–387.

A Appendix

We first include here the proof of lemma 2.1:

Lemma A.1. *Take M as in 2.2. Let $a = ord(A)$, $b = ord(B)$ and $k = lcm(a, b)$. Then*

1. $a = p^n - 1$ *and* $b = p^l - 1$
2. $X^{(k)} = 0$
3. $ord(M) = k$

Proof.

1. See, for example, [9].
2. Suppose that $b < a$ with $a = qb + r$ and $1 \leq r \leq b-1$ (note that $b \nmid a$ since $gcd(a, b) = p-1$) and suppose also that $k = q_1 a = q_2 b$. Then $I = B^{bq_2} = B^{aq_1} = B^{rq_1}$ and the following holds:

$$
\begin{aligned}
X^{(k)} &= \sum_{i=1}^{k} A^{k-i} X B^{i-1} \\
&= \sum_{i=1}^{k} A^{-i} X B^{i-1} \\
&= \sum_{i=1}^{q_1} \sum_{j=(i-1)a+1}^{ia} A^{-j} X B^{j-1} \\
&= \sum_{i=1}^{q_1} \sum_{j=1}^{a} A^{-j} X B^{j+(i-1)a-1} \\
&= \sum_{i=1}^{a} A^{-i} X B^{i} \cdot \sum_{j=1}^{q_1} B^{(j-1)a-1} \\
&= X^{(a)} B \cdot \sum_{j=1}^{q_1} B^{(j-1)a-1}
\end{aligned}
$$

$$= X^{(a)} \sum_{j=1}^{q_1} B^{(j-1)a}$$
$$= X^{(a)} \sum_{j=1}^{q_1} B^{(j-1)r}$$

Now note that $0 = B^{q_1 r} - I = \left(\sum_{j=1}^{q_1} B^{(j-1)r}\right)(B^r - I)$. Because 1 is not an eigenvalue of B (see discussion following lemma 4.1 in 4.2.2) it follows that 1 is also not an eigenvalue of B^r (because the eigenvalues of B are roots of f_2 and therefore have order b) and therefore $B^r - I$ is invertible. Hence $\sum_{j=1}^{q_1} B^{(j-1)r} = 0$ from which it follows that $X^{(k)} = 0$.

3. $M^{k_1} = I$ if and only if $a|k_1$ and $b|k_1$ and $X^{(k_1)} = 0$. Obviously $k = lcm(a, b)$ is the least positive integer satisfying these conditions and hence

$$ord(M) = lcm(a, b)$$

□

The next results justify all the claims made in Remark 2.2:

Lemma A.2. *$gcd(a, b) = 1$ if and only if $gcd(p^a - 1, p^b - 1) = p - 1$*

Proof. Suppose $a > b$ and $gcd(a, b) = 1$. Then

$$\begin{aligned} gcd(p^b - 1, p^a - 1) &= gcd(p^b - 1, p^a - p^b) \\ &= gcd(p^b - 1, p^b(p^{a-b} - 1)) \\ &= gcd(p^b - 1, p^b)gcd(p^b - 1, p^{a-b} - 1) \\ &= gcd(p^b - 1, p^{a-b} - 1) \end{aligned}$$

because $gcd(p^b - 1, p^b) = gcd(p^b, p^{a-b} - 1) = 1$. Iterating this process one concludes that

$$gcd(p^b - 1, p^a - 1) = gcd(p^b - 1, p^{a-b} - 1) = gcd(p^b - 1, p^{a-k\cdot b} - 1)$$

where $k = max\{i : \ a - kb \geq 0\} \equiv \lfloor a/b \rfloor$ and the remainder $r_1 = a - k \cdot b$ is such that $0 \leq r_1 \leq b - 1$. Therefore

$$gcd(p^b - 1, p^a - 1) = gcd(p^b - 1, p^{r_1} - 1)$$

Consider the following:

If $gcd(a, b) = 1$ then $r_1 \neq 0$. If $r_1 \geq 2$ then one computes the division of b and r_1 and obtains

$$gcd(p^b - 1, p^{r_1} - 1) = gcd(p^{r_1} - 1, p^b - 1) = gcd(p^{r_1} - 1, p^{b - \lfloor b/r_1 \rfloor r_1} - 1) = gcd(p^{r_1} - 1, p^{r_2} - 1)$$

with r_2 the remainder $b = \lfloor b/r_1 \rfloor \cdot r_1 + r_2$ and $0 \leq r_2 \leq r_1 - 1$. Again, if $gcd(a, b) = 1$ then $gcd(b, r_1) = 1$ and therefore $r_2 \neq 0$.

We can repeat this process until the first remainder $r_i = 1$, which we know will happen if $gcd(a, b) = 1$. We then get

$$gcd(p^b - 1, p^a - 1) = gcd(p^{r_{i-1}} - 1, p - 1) = p - 1$$

On the other hand, if $d > 1$ is a common divisor of a and b then $p^d - 1 > p - 1$ is a common divisor of $p^a - 1$ and $p^b - 1$. □

In the following, we suppose that the overall dimension m of M is fixed and set

$$N = \{x \in \{1, \dots, m-1\} : gcd(x, m-x) = 1\}$$

Corollary A.2.1.
$\forall x \in N$ $gcd(p^x - 1, p^{m-x} - 1) = p - 1$ and $lcm(p^x - 1, p^{m-x} - 1) = (p^x - 1)(p^{m-x} - 1)/(p - 1)$

Next lemma is easy to prove:

Lemma A.3. *Let $\hbar(x) = lcm(p^x - 1, p^{m-x} - 1)$. Then*

1. *If m even and $m/2$ even then maximum of $\hbar$ in N is attained at $x_0 = m/2 - 1$*
2. *If m even and $m/2$ odd then maximum of $\hbar$ in N is attained at $x_0 = m/2 - 2$*
3. *If m odd then maximum of $\hbar$ in N is attained at $x_0 = \lfloor m/2 \rfloor$*

Proposition A.1.

1. *$Min_{x\in N}\ lcm(p^x - 1, p^{m-x} - 1) = p^{m-1} - 1$*
2. *Let $1 \le y \le m-1$ such that $y \notin N$. Then*
$$lcm(p^y - 1, p^{m-y} - 1) \le Min_{x\in N}\ lcm(p^x - 1, p^{m-x} - 1)$$
3. *$Max_{x\in N}\ lcm(p^x - 1, p^{m-x} - 1) =$*

$$\begin{cases} (p^{m/2-1} - 1)(1 + p + \ldots + p^{m/2}) & , m \text{ even and } m/2 \text{ even} \\ \\ (p^{m/2-2} - 1)(1 + p + \ldots + p^{m/2+1}) & , m \text{ even and } m/2 \text{ odd} \\ \\ (p^{\lfloor m/2 \rfloor} - 1)(1 + p + \ldots + p^{\lfloor m/2 \rfloor}) & , m \text{ odd} \end{cases}$$

Proof.

1. As observed, the minimum is attained at $x_0 = 1$ (1 is always in N). The result follows.
2. It is enough to consider the case $y \le \lfloor m/2 \rfloor$ such that $d = gcd(y, m-y) \ge 2$. Let $d_y = gcd(p^y - 1, p^{m-y} - 1)$ and suppose that $y = k_1 d$ and $m - y = k_2 d$. Then $p^d - 1$ is a common divisor of $p^y - 1$ and $p^{m-y} - 1$, from which it follows that $d_y \ge p^d - 1$ and hence

$$\begin{aligned} lcm(p^y - 1, p^{m-y} - 1) &\le (p^y - 1)(p^{m-y} - 1)/(p^d - 1) \\ &= (p^{m-y} - 1) \sum_{i=0}^{k_1 - 1} p^{id} \\ &= \sum_{i=0}^{k_1 - 1} p^{id+m-y} - \sum_{i=0}^{k_1 - 1} p^{id} \\ &\le \sum_{i=0}^{m-d} p^i \\ &\le p^{m-d+1} - 1 \\ &\le p^{m-1} - 1 \end{aligned}$$

3. $lcm(p^x - 1, p^{m-x} - 1) = (p^x - 1)(p^{m-x} - 1)/(p-1)$ for $x \in N$ by corollary A.2.1, and lemma A.3 provides the maximizing points x_0. The result follows by computing

$$lcm(p^{x_0} - 1, p^{m-x_0} - 1) = (p^{x_0} - 1)(p^{m-x_0} - 1)/(p-1)$$

$\square$