Information Sciences 276 (2014) 319–331

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Cryptanalysis of a key exchange scheme based on block matrices

María Isabel González Vasco [a,1], Angel L. Pérez del Pozo [a,1,2], Pedro Taborda Duarte [a,*,3], Jorge L. Villar [b]

[a] Dpto. de Matemática Aplicada, Universidad Rey Juan Carlos, C/Tulipán s/n. 28933, Móstoles, Madrid, Spain
[b] Dpto. de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, C/Jordi Girona, 1-3, 08034 Barcelona, Spain

ARTICLE INFO

Article history:
Received 17 July 2010
Received in revised form 9 June 2013
Accepted 1 November 2013
Available online 21 November 2013

Keywords:
Key exchange scheme
Cryptanalysis
Finite field
Block matrix
Discrete logarithm problem

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, and its security is claimed to rely in the hardness of a discrete logarithm problem in a subgroup of $GL_n(\mathbb{Z}_p)$. However, the proposal's design allows for a clean attack strategy which exploits the fact that exponents are at some point added instead of multiplied as in a standard Diffie–Hellman construction. This strategy is moreover successful for a much more general choice of parameters than that put forward by Álvarez et al.

1. Introduction

The 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 [10] or the group of points of an elliptic curve [6,9].

Recently, Álvarez et al. [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 $M_1^v M_2^w$. 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).

* Corresponding author. Tel.: +34 645089547.
E-mail addresses: mariaisabel.vasco@urjc.es (M.I. González Vasco), angel.perez@urjc.es (A.L. Pérez del Pozo), pedro.duarte@urjc.es (P.T. Duarte), jvillar@ma4.upc.edu (J.L. Villar).
[1] Partially supported by research project CCG08-UCM/ESP-4394.
[2] Contact author.
[3] With support from Fundação para a Ciência e Tecnologia, Portugal ref: SFRH/BD/37869/2007.

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.11.009

Related work. The first attempt to use matrices over a finite field in a key exchange scheme was made by Odoni, Varadharajan and Sanders in 1984 [10]. 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 [7], the authors incorrectly use irreducible polynomials instead of primitive polynomials).

After that, Menezes and Vanstone proved in 1992 [7] 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 Wu [8] 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 Wu reduction, Climent et al. [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 et al. [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.

Our contribution. In this paper we exhibit a security weakness in (a generalization of) the key exchange protocol presented in [2,1]. This comes from the fact that the problem faced by a passive adversary is not that closely related to DLP, for the computation made on the secret exponents is actually addition (instead of multiplication). This simple observation allows us to describe a simple strategy to derive the shared key from the public information if the matrices M_1 and M_2 are both diagonalizable. Furthermore, if just one of them is diagonalizable, we also evidence the shared key can be computed by a passive adversary. Finally, we are able to point out different attack strategies that may also succeed even if none of the two matrices are diagonalizable. All in all, our discussion evidences it is not too realistic to hope for a secure construction of a key exchange protocol from the ideas exposed in [2,1].

Paper outline. We start by recalling some of the most relevant mathematical facts related to the scheme's parameter generation in Section 2 (underlying group structure, and how to generate high order elements from it), and we briefly recall the proposed scheme in Section 3. Section 4 contains our main result, i.e., the attack for the case $M_1,\ M_2$ diagonalizable, whereas Section 5 presents some extensions of the attack to the case when only one of the two matrices is non-diagonalizable, and some facts that render the scheme insecure even if both matrices are non-diagonalizable. For the shake of readability, quite a few technical results have been moved to two Appendices A and B.

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 $n, l \in \mathbb{N}$, consider the subgroup of $GL_{n+l}(\mathbb{Z}_p)$ under matrix multiplication defined 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 $h \geqslant 0$ then $M^h = \begin{pmatrix} A^h & X^{(h)} \\ 0 & B^h \end{pmatrix}$ with
$$X^{(h)} = \begin{cases} 0 & \text{if } h = 0 \\ \sum_{i=1}^{h} A^{h-i} X B^{i-1} & \text{if } h \geqslant 1 \end{cases}$$
2. If $a, b \geqslant 0$ 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 nonzero.