Information Sciences 223 (2013) 317–321

Contents lists available at SciVerse ScienceDirect

Information Sciences

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

Cryptanalysis of Álvarez et al. key exchange scheme

Abdel Alim Kamal, Amr M. Youssef *

Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada H3G 1M8

ARTICLE INFO

Article history:
Received 27 May 2011
Received in revised form 30 May 2012
Accepted 14 October 2012
Available online 23 October 2012

Keywords:
Key exchange
Cryptanalysis
Block upper triangular matrices
Non-abelian groups

ABSTRACT

Álvarez et al. (Information sciences 179 (12) (2009)) proposed a new key exchange scheme where the secret key is obtained by multiplying powers of block upper triangular matrices whose elements are defined over $\mathbb{Z}_p$. In this note, we show that breaking this system with security parameters (r,s,p) is equivalent to solving a set of $3(r+s)^2$ linear equations with $2(r+s)^2$ unknowns in $\mathbb{Z}_p$, which renders this system insecure for all the suggested practical choices of the security parameters.

1. Introduction

Public-key cryptography [7] provides key exchange mechanisms in which secret keys can be exchanged between users over insecure communication channels. These key exchange mechanisms are usually based on number theory problems such as the discrete logarithm problem (DLP) [6], integer factorization [13] and elliptic curve DLP [5]. However, such systems require a large number of arithmetic operations, which makes them hard to implement in most resource constrained applications. To overcome this problem, key exchange protocols based on efficient matrix algebra have been proposed (e.g., see [17]). Odoni et al. [11] introduced the discrete logarithm problem for matrices over $\mathbb{F}_q$ and proposed a Diffie-Hellman key exchange protocol based on matrices. Menezes and Wu [8] reduced the discrete logarithm problem for matrices to some discrete logarithm problems over small extensions of $\mathbb{F}_q$.

Recently, Álvarez et al. [3] proposed a key exchange scheme utilizing the non-abelian group of block upper triangular matrices (see also [1,4,2]). Álvarez et al. claimed that one of the main advantages of their scheme (hereafter referred to as the ATVZ scheme) is the absence of big prime numbers, which yields faster arithmetic operations and avoids the need for primality testing. Moreover, they also claimed that the proposed scheme is very efficient since it employs fast exponentiation algorithms for this type of matrices. In particular, by analyzing the order of the non-abelian group generated by these matrices as a function of the security parameters (r,s,p), as well as the implementation efficiency of these schemes, Álvarez et al. concluded that their system with security parameters $(r=2,s=89,p=2903)$ has better performance than the Diffie–Hellman scheme with a similar level of security (key size of approximately 1024 bits).

In [16], Vasco et al. showed that breaking the ATVZ scheme can be reduced to solving a small set of discrete logarithm problems in an extension of the base field. Consequently, Vasco et al. concluded that the ATVZ scheme does not offer any computational advantage over the original Diffe–Hellman key exchange scheme. While the results presented in [16] challenge the efficiency claims made by Álvarez et al. [3] by showing that working with the proposed non-abelian group of block upper triangular matrices does not offer a computational advantage over working in the base field, these results do not

* Corresponding author. Tel.: +1 514 848 2424.
E-mail addresses: a_kamala@ciise.concordia.ca (A.A. Kamal), youssef@ciise.concordia.ca (A.M. Youssef).

0020-0255/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2012.10.010

present a practical attack on the ATVZ scheme for the recommended sizes of the security parameters. In particular, the main result in [16] is that breaking the ATVZ scheme can be reduced to solving a set of discrete logarithm problems (DLPs) in an extension of the base field Z_p. However, it is well known that solving the DLP is a hard problem and this kind of reduction does not present a practical threat to the algorithm. More precisely, if we apply the conclusion of the above technical report to the algorithm parameters suggested by Álvarez et al., then, in order to break this scheme following the suggested technique, one needs to solve a set of DLPs over the extension fields $GF(5167^{83}), GF(2903^{89})$ or $GF(2437^{97})$ (see Table 3 in [3]). This is roughly equivalent to the prohibitive task of solving several DLPs with a prime of size 1024 bits (for $GF(5167^{83}), GF(2903^{89})$) and 1091 bits (for $GF(2437^{97})$).

In this note, we show that breaking this scheme is equivalent to solving a set of $3(r+s)^2$ consistent linear equations with $2(r+s)^2$ unknowns in $\mathbb{Z}_p$, which renders this system insecure for the suggested practical choices of the above security parameters. The rest of this note is organized as follows. In the next section, we briefly describe some details of the ATVZ key exchange scheme. The proposed attack is described in Section 3. Finally, Section 4 presents our conclusions.

2. Description of the ATVZ key exchange scheme

For completeness, in this section we briefly review the relevant definitions and details of the ATVZ key exchange scheme. For further details, the reader is referred to [3].

Let $\mathrm{Mat}_{r\times s}(\mathbb{Z}_p)$ denote the set of matrices of size $r\times s$ with elements in $\mathbb{Z}_p$ where p is a prime number. Let $\mathrm{Gl}_r(\mathbb{Z}_p)$ denote the general linear group of invertible matrices of sizes $r\times r$, also with elements in $\mathbb{Z}_p$.

Let $\Theta = \left\{ \begin{bmatrix} A & X \\ \mathbf{0} & B \end{bmatrix} : A \in \mathrm{Gl}_r(\mathbb{Z}_p), B \in \mathrm{Gl}_s(\mathbb{Z}_p), X \in \mathrm{Mat}_{r\times s}(\mathbb{Z}_p) \right\}$.

If $M \in \Theta$ and $h \geqslant 0$ then $M^h = \begin{bmatrix} A^h & X^{(h)} \\ \mathbf{0} & B^h \end{bmatrix}$ where

$$X^{(h)} = \begin{cases} \mathbf{0} & \text{if } h = 0 \\ \sum_{i=1}^{h} A^{h-i} X B^{i-1} & \text{if } h \geqslant 1 \end{cases}.$$

Let $M_1 = \begin{bmatrix} A_1 & X_1 \\ \mathbf{0} & B_1 \end{bmatrix}$ and $M_2 = \begin{bmatrix} A_2 & X_2 \\ \mathbf{0} & B_2 \end{bmatrix}$ be two elements of the set Θ with order m_1 and m_2, respectively.

For $x, y \in \mathbb{N}$, we define

$$A_{xy} = A_1^x A_2^y$$
$$B_{xy} = B_1^x B_2^y$$
$$C_{xy} = A_1^x X_2^{(y)} + X_1^{(x)} B_2^y$$

The ATVZ key exchange scheme can be summarized as follows [3]:

1. Alice and Bob agree on a prime p and two matrices $M_1, M_2 \in \Theta$ with large orders m_1 and m_2, respectively.
2. Alice generates two random private keys[1] $l, m \in \mathbb{N}$ such that $1 \leqslant l \leqslant m_1 - 1, 1 \leqslant m \leqslant m_2 - 1$, and computes A_{lm}, B_{lm}, C_{lm} constructing
$$C = \begin{bmatrix} A_{lm} & C_{lm} \\ \mathbf{0} & B_{lm} \end{bmatrix}$$
3. Alice sends C to Bob.
4. Bob generates two random private keys $v, w \in \mathbb{N}$ such that $1 \leqslant v \leqslant m_1 - 1, 1 \leqslant w \leqslant m_2 - 1$, and computes A_{vw}, B_{vw}, C_{vw} constructing
$$D = \begin{bmatrix} A_{vw} & C_{vw} \\ \mathbf{0} & B_{vw} \end{bmatrix}$$
5. Bob sends D to Alice.
6. The public keys of Alice and Bob are respectively the matrices C and D.
7. Alice computes $K_a = A_1^l A_{vw} X_2^{(m)} + A_1^l C_{vw} B_2^m + X_1^{(l)} B_{vw} B_2^m$. It should be noted that K_a is the upper right $r\times s$ matrix in
$$M_a = M_1^l D M_2^m = \begin{bmatrix} A_a & K_a \\ \mathbf{0} & B_a \end{bmatrix}. \quad (1)$$

[1] In [3], the symbols r, s were mistakenly used to simultaneously refer to both the security parameters and the secret exponents chosen by Alice, in step 2 of the key exchange algorithm. In this submission, to avoid any possible confusion, we use r, s to refer to the system parameters and l, m to refer to the secret exponents chosen by Alice.

8. Bob computes $K_b = A_1^v A_{lm} X_2^{(w)} + A_1^v C_{lm} B_2^w + X_1^{(v)} B_{lm} B_2^w$. Similarly, we have

$$M_b = M_1^v C M_2^w = \begin{bmatrix} A_b & K_b \\ \mathbf{0} & B_b \end{bmatrix}. \tag{2}$$

Finally, Alice and Bob share the key $K = K_a = K_b$.

3. The proposed attack

The above construction for M_1 and M_2 is used to guarantee a large order of the non-abelian group generated by these matrices and to attain a fast exponentiation algorithm for this type of matrices. On the other hand, our attack does not depend on the particular method by which the matrices M_1 and M_2 are constructed. From the analysis provided in [3], we have

$$C = M_1^l M_2^m,$$
$$D = M_1^v M_2^w.$$

Thus, despite the apparent complexity of the above key exchange scheme, when analyzing its security, one can simply view it as follows:

1. Alice and Bob agree on a prime p and two matrices $M_1, M_2 \in \Theta$.
2. Alice sends $C = M_1^l M_2^m$ to Bob.
3. Bob sends $D = M_1^v M_2^w$ to Alice.
4. Both Alice and Bob calculate $M_1^{l+v} M_2^{w+m}$ and extract the secret key from it (see Eqs. (1) and (2)).

In what follows, we show that, given the public matrices C and D, the attacker can easily recover the secret key.

Lemma 1. *Let W_1 and W_2 be two invertible matrices of dimension $(r+s) \times (r+s)$ that satisfy*

$$W_1 M_1 = M_1 W_1 \tag{3}$$

$$W_2 M_2 = M_2 W_2 \tag{4}$$

$$D = W_1 W_2 \tag{5}$$

Then we have

$$M_1^{l+v} M_2^{w+m} = W_1 C W_2.$$

Proof. Using mathematical induction, it is easy to show that $W_1 M_1 = M_1 W_1$ and $W_2 M_2 = M_2 W_2$ implies that $W_1 M_1^l = M_1^l W_1$ and $W_2 M_2^m = M_2^m W_2$, respectively. The rest of the proof follows by noting that

$$W_1 C W_2 = W_1 M_1^l M_2^m W_2 = M_1^l W_1 W_2 M_2^m = M_1^l D M_2^m. \qquad \square$$

The above lemma shows that while the attacker may not be able to recover the secrets chosen by Alice and Bob, i.e., l, v, w, m, or the associated matrices $M_1^l, M_1^v, M_2^w, M_2^m$, the attacker can still recover the overall secret key agreed upon between Alice and Bob if she is able to find any W_1 and W_2 that satisfy the above set of equations. This seemingly nonlinear system of equations can be easily linearized as follows:

From Eq. (3), we have

$$W_1 M_1 = M_1 W_1 \iff W_1 M_1 W_1^{-1} = M_1 \iff M_1 W_1^{-1} = W_1^{-1} M_1$$

The attacker can easily solve a linear system of equations for W_1^{-1} and W_2 by replacing Eq. (3) by $M_1 W_1^{-1} = W_1^{-1} M_1$ and Eq. (5) by $W_1^{-1} D = W_2$. In other words, the attacker solves the system of equations given by

$$\begin{aligned} W_1^{-1} M_1 &= M_1 W_1^{-1} \\ W_2 M_2 &= M_2 W_2 \\ W_1^{-1} D &= W_2, \end{aligned} \tag{6}$$

which corresponds to solving a set of $3(r+s)^2$ linear equations with $2(r+s)^2$ unknowns, corresponding to the elements of W_1^{-1} and W_2 over $\mathbb{Z}_p$.

The following lemma shows that the attacker is always able to find a valid solution for (6).

Lemma 2. *The linear system of equations defined in (6) is consistent.*

Proof. The proof follows directly by noting that $W_1 = M_1^v$ and $W_2 = M_2^w$ is a valid solution for this system of equations. □

The following toy example illustrates the idea of the attack.

Example 1. Let $p = 37, r = 2, s = 3, l = 11, m = 32, v = 17, w = 39$,

$$M_1 = \begin{bmatrix} 3 & 31 & 24 & 12 & 13 \\ 9 & 24 & 28 & 20 & 26 \\ 0 & 0 & 9 & 16 & 14 \\ 0 & 0 & 25 & 17 & 2 \\ 0 & 0 & 23 & 12 & 30 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 7 & 14 & 18 & 12 & 4 \\ 22 & 16 & 15 & 12 & 6 \\ 0 & 0 & 29 & 36 & 8 \\ 0 & 0 & 33 & 15 & 35 \\ 0 & 0 & 5 & 24 & 5 \end{bmatrix}$$

Alice calculates $C = M_1^l M_2^m = \begin{bmatrix} 31 & 14 & 31 & 19 & 31 \\ 35 & 10 & 10 & 32 & 21 \\ 0 & 0 & 36 & 8 & 30 \\ 0 & 0 & 9 & 18 & 10 \\ 0 & 0 & 27 & 5 & 11 \end{bmatrix}$ and sends it to Bob.

Bob calculates $D = M_1^v M_2^w = \begin{bmatrix} 7 & 25 & 32 & 23 & 21 \\ 16 & 28 & 18 & 15 & 32 \\ 0 & 0 & 33 & 12 & 17 \\ 0 & 0 & 16 & 25 & 20 \\ 0 & 0 & 33 & 18 & 14 \end{bmatrix}$ and sends it to Alice.

Thus we have

$$M_a = M_b = M_1^{l+v} M_2^{m+w} = \begin{bmatrix} 2 & 15 & 33 & 18 & 26 \\ 14 & 2 & 3 & 27 & 16 \\ 0 & 0 & 28 & 1 & 5 \\ 0 & 0 & 17 & 18 & 14 \\ 0 & 0 & 11 & 13 & 5 \end{bmatrix}$$

and the secret calculated by Alice and Bob is given by $\begin{bmatrix} 33 & 18 & 26 \\ 3 & 27 & 16 \end{bmatrix}$.

It is easy to verify that

$$W_2 = \begin{bmatrix} 5 & 14 & 24 & 21 & 19 \\ 22 & 14 & 32 & 29 & 12 \\ 0 & 0 & 4 & 20 & 21 \\ 0 & 0 & 26 & 8 & 0 \\ 0 & 0 & 11 & 10 & 10 \end{bmatrix} \quad \text{and} \quad W_1^{-1} = \begin{bmatrix} 20 & 17 & 2 & 20 & 31 \\ 30 & 16 & 34 & 31 & 24 \\ 0 & 0 & 9 & 4 & 6 \\ 0 & 0 & 36 & 10 & 16 \\ 0 & 0 & 34 & 1 & 32 \end{bmatrix} \Rightarrow W_1 = \begin{bmatrix} 19 & 33 & 31 & 31 & 13 \\ 6 & 33 & 18 & 21 & 18 \\ 0 & 0 & 22 & 16 & 11 \\ 0 & 0 & 30 & 9 & 13 \\ 0 & 0 & 15 & 7 & 18 \end{bmatrix}$$

is one valid solution to the systems of equations given by (6), from which the attacker calculates

$$W_1 C W_2 = \begin{bmatrix} 2 & 15 & 33 & 18 & 26 \\ 14 & 2 & 3 & 27 & 16 \\ 0 & 0 & 28 & 1 & 5 \\ 0 & 0 & 17 & 18 & 14 \\ 0 & 0 & 11 & 13 & 5 \end{bmatrix} = M_a = M_b.$$

It is obvious that the secret key is given by the upper right $r \times s = 2 \times 3$ matrix of $W_1 C W_2$.

4. Discussion and conclusions

The ATVZ key exchange scheme is insecure for all suggested practical choices of the security parameters (r, s, p). Our attack is also directly applicable to the new system recently proposed by Álvarez et al. in [2]. As mentioned above, our attack does not depend on the particular method by which the involved matrices are generated, and hence the idea of linearization used in this paper can be applied to a wider class of similar key exchange schemes.

Several key exchange algorithms based on matrices have been proposed. However, to the authors' knowledge, almost all practical proposals have been broken (e.g., see [12,18]) due to the inherent linearity of the underlying matrices' operations. Designing a secure key exchange algorithm based on matrices or other non-commutative finite groups/rings with efficient operations remains a very interesting and challenging research problem.

Finally, it should be noted that the ATVZ scheme can be seen as a variant of the key agreement scheme proposed by Stickel [15]. In [14], Shpilrain cryptanalyzed Stickel's scheme and proposed some alternatives to make it more secure. Later, Mullan [9] [10] attacked the Shpilrain's alternatives and illustrated the insecurity of schemes based on Stickel's original proposal. Thus, our attack can be seen as a direct application of the linearization idea presented in [9,10,14] to the ATVZ system.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that helped improve the quality of the paper.

References

[1] R. Álvarez, F. Ferrández, J. Vicent, A. Zamora, Applying quick exponentiation for block upper triangular matrices, Applied Mathematics and Computation 183 (2006) 729–737.
[2] R. Álvarez, F. Martínez, J. Vicent, A. Zamora, Cryptographic applications of 3×3 block upper triangular matrices, in: Proceedings of Hybrid Artificial Intelligent Systems – 7th International Conference, HAIS 2012, Part II, LNCS, vol. 7249, Springer, 2012, pp. 97–104.
[3] R. Álvarez, L. Tortosa, J. Vicent, A. Zamora, Analysis and design of a secure key exchange scheme, Information Sciences 179 (2009) 2014–2021.
[4] R. Álvarez, L. Tortosa, J. Vicent, A. Zamora, A non-abelian group based on block upper triangular matrices with cryptographic applications, in: M. Bras-Amorós, T. Hholdt (Eds.), Proceedings of 18th Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes, AAECC'09, Catalonia, Spain, 2009, pp. 117–126.
[5] I. Blake, G. Seroussi, N. Smart, Elliptic curves in cryptography, London Mathematical Society, Lecture Notes Series, vol. 256, Cambridge University Press, 1999.
[6] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (1985) 469–472.
[7] A. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptographic Research, CRC Press, 1996.
[8] A. Menezes, Y. Wu, The discrete logarithm problem in Gl(n,q), Ars Combinatoria 47 (1997) 23–32.
[9] C. Mullan, Cryptanalysing variants of Stickel's key agreement protocol, Journal of Mathematical Cryptology 4 (2011) 365–373.
[10] C. Mullan, Some Results in Group-Based Cryptography, PhD Thesis, Royal Holloway University of London, 2011.
[11] R. Odoni, V. Varadharajan, P. Sanders, Public key distribution in matrix rings, IEE Electronics Letters 20 (1984) 386–387.
[12] M. Rasslan, A. Youssef, Cryptanalysis of a public key encryption scheme using ergodic matrices, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E94.A (2011) 853–854.
[13] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (1978) 120–126.
[14] V. Shpilrain, Cryptanalysis of Stickel's key exchange scheme, in: Proceedings of Computer Science in Russia, LNCS, vol. 5010, Springer, 2008, pp. 283–288.
[15] E. Stickel, A new public-key cryptosystem in non abelian groups, in: Proceedings of the 13th International Conference on Information Systems Development. Vilnius Technika, Vilnius 2004, 70–80.
[16] M. Vasco, A. del Pozo, P. Duarte, Cryptanalysis of a key exchange scheme based on block matrices, IACR Archive report <http://eprint.iacr.org/2009/553.pdf>.
[17] C. Wu, E. Dawson, Generalized inverses in public key cryptosystem design, IEE Proceedings – Computers and Digital Techniques 145 (1998) 321–326.
[18] A. Youssef, S. Tavares, Cryptanalysis of key agreement scheme based on generalised inverses of matrices, IEE Electronics Letters 33 (1997) 1777–1778.