Information Sciences 179 (2009) 2014–2021

Contents lists available at ScienceDirect

Information Sciences

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

Analysis and design of a secure key exchange scheme

Rafael Álvarez, Leandro Tortosa, José-Fco. Vicent *, Antonio Zamora

Departamento de Ciencia de la Computación e Inteligencia Artificial, Universidad de Alicante, Campus de San Vicente, Ap. Correos 99, E-03080 Alicante, Spain

ARTICLE INFO

Article history:
Received 23 February 2008
Accepted 15 February 2009

Keywords:
Cryptography
Security
Public key
Key exchange scheme
Block matrices
Quick exponentiation
Triangular matrices
Discrete logarithm problem

ABSTRACT

We propose a new key exchange scheme where the secret key is obtained by multiplying the powers of block upper triangular matrices. After studying the cryptographic properties of these block matrices, the theoretical aspects of this scheme are analyzed, concluding that common ciphertext attacks are not applicable to this cryptosystem. Moreover, our proposal is compared with the Diffie–Hellman scheme achieving satisfactory results.

1. Introduction

In large open networks, like the internet, an increasing demand for security can be observed. In order to establish a confidential channel (or session) between two users of such a network, classic single-key cryptography requires them to exchange a common secret key over a secure channel (see [1]). This may work if the network is small and local, but it is infeasible in non-local or large networks.

To simplify the key exchange problem, public-key cryptography provides a mechanism to allow secret session keys to be exchanged over an insecure channel. In such a framework, every user possesses a key pair consisting of a (non-secret) public key and a (secret) private key; only public keys are published.

A lot of popular public-key encryption systems are based on number theory problems such as factoring integers or finding discrete logarithms. The underlying algebraic structures are, very often, abelian groups; this is especially true in the case of the Diffie–Hellman method (DH), that was the first practical public-key technique and introduced in 1976 (see [8]). In such a system, when two parties want to communicate with each other, the sender encrypts the message with the recipient's public key and then transmits the cipher text to the recipient. Upon receiving the encrypted information, the recipient can decrypt the message with his private key (see [13]).

The discrete logarithm problem (DLP, see [9,16,18,23]) is, together with the Integer Factoring Problem (IFP, see [15,22]) and the Elliptic Curve DLP (ECDLP, see [3,7]), one of the main problems upon which public-key cryptosystems are built. Thus, efficiently computable groups where the DLP is hard to break (see [3,6,17]), are very important in cryptography.

* Corresponding author. Tel.: +34 96 590 3900; fax: +34 96 590 3902.
E-mail addresses: ralvarez@dccia.ua.es (R. Álvarez), tortosa@dccia.ua.es (L. Tortosa), jvicent@dccia.ua.es (J.-F. Vicent), zamora@dccia.ua.es (A. Zamora).

0020-0255/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2009.02.008

The purpose of this proposal is the analysis and implementation of a key exchange scheme based on a special group of block upper triangular matrices. The main idea of this paper is to study the cryptographic behavior of products of the type $M_1^v M_2^w$, with v, w integers and M_1, M_2 elements of the group of matrices previously mentioned.

In the first place we perform a study of the great cryptographic properties of this group of matrices. Secondly, we propose a key exchange scheme, perform a detailed security analysis and compare it with DH under MATLAB (see [11]).

2. Block upper triangular matrices

Given p a prime number and $r, s \in \mathbb{N}$, $\mathrm{Mat}_r(\mathbb{Z}_p)$, $\mathrm{Mat}_s(\mathbb{Z}_p)$, $\mathrm{Mat}_{r\times s}(\mathbb{Z}_p)$ are the matrices of sizes $r \times r, s \times s$ and $r \times s$, respectively, with elements in $\mathbb{Z}_p$ and by $\mathrm{GL}_r(\mathbb{Z}_p)$, $\mathrm{GL}_s(\mathbb{Z}_p)$, the invertible matrices of sizes $r \times r$ and $s \times s$, also with elements in $\mathbb{Z}_p$. Let us consider

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

and the subset

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

In order to obtain the cardinality of the subgroup generated by a matrix $M \in \Theta$ (order of M), we need to calculate powers of these block upper triangular matrices. So, we use the following theorem (see [4]).

Theorem 1. *Let* $M = \begin{bmatrix} A & X \\ O & B \end{bmatrix} \in \Theta$. *Taking* h *as a non-negative integer then*

$$M^h = \begin{bmatrix} A^h & X^{(h)} \\ O & B^h \end{bmatrix}, \quad \text{where } X^{(h)} = \begin{cases} O & \text{if } h = 0, \\ \sum_{i=1}^{h} A^{h-i} X B^{i-1} & \text{if } h \geqslant 1. \end{cases}$$

Also, if $0 \leqslant t \leqslant h$ *then*

$$X^{(h)} = A^t X^{(h-t)} + X^{(t)} B^{h-t} X^{(h)} = A^{(h-t)} X^{(h)} + X^{(h-t)} B^t.$$

When $t = 1$, we have

$$X^{(h)} = A X^{(h-1)} + X B^{h-1} \quad \text{or} \quad X^{(h)} = A^{h-1} X + X^{(h-1)} B.$$

Taking a, b integers such as $a + b \geqslant 0$, $X^{(a+b)} = A^a X^{(b)} + X^{(a)} B^b$.

3. Order of the elements

In our scheme, the space of keys is bounded by the order of the group generated by the following matrix:

$$M = \begin{bmatrix} A & X \\ \mathbf{0} & B \end{bmatrix} \in \Theta.$$

So, it is desirable to get orders as high as possible, and now, we describe the way to guarantee that this order is maximum (see [12,14]).

Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$ a monic polynomial in $\mathbb{Z}_p[x]$, whose companion $n \times n$ matrix is

$$\overline{A} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{bmatrix}.$$

If f is an irreducible polynomial in $\mathbb{Z}_p[x]$, then the order of the matrix $\overline{A}$ is equal to the order of any root of f in $\mathbb{F}_{p^n}$ and the order of $\overline{A}$ divides $p^n - 1$ (see [19]). Moreover, assuming that f is a primitive polynomial in $\mathbb{Z}_p[x]$, the order of $\overline{A}$ is exactly $p^n - 1$.