Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp163-168)

A Public Key Cryptosystem Based on Block Upper Triangular Matrices[*]

RAFAEL ALVAREZ[1], LEANDRO TORTOSA[3], JOSE-FRANCISCO VICENT[3], and ANTONIO ZAMORA[4]
Departamento de Ciencia de la Computación e Inteligencia Artificial
Universidad de Alicante
Campus de Sant Vicent del Raspeig, Ap. Correos 99, E-03080, Alicante
SPAIN

Abstract: - We propose a public key cryptosystem based on block upper triangular matrices. This system is a variant of the Discrete Logarithm Problem with elements in a finite group, capable of increasing the difficulty of the problem while maintaining the key size. We also propose a key exchange protocol that guarantees that both parties share a secret element of this group and a digital signature scheme that provides data authenticity and integrity.

Keywords: - cryptography, security, public-key, DLP, finite fields, Diffie-Hellman key agreement, polynomial matrices, digital signature.

1 Introduction

In large open networks like the internet an increasing demand for security is observed. In order to establish a confidential channel between two users of such a network, classical single-key cryptography requires them to exchange a common secret key over a secure channel. 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, modern public-key cryptography provides a mechanism in which the keys to be exchanged do not need to be secret. 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. They are used to encrypt the messages to be sent to the owner of the key or to verify digital signatures issued by the owner of the key. Before using someone else's public key to encrypt a message or verify a signature, one should make sure that the key really belongs to the intended recipient or the indicated issuer of the signature. Achieving authenticity of public keys can be done in several ways. Public key cryptosystems are essential for electronic commerce or electronic banking transactions; they assure privacy as well as integrity of the transactions between two parties. Digital signatures are used to sign electronic documents and they are also mostly based on public-key techniques.

A lot of popular public-key encryption systems are based on number-theoretic 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, see [1]), that was the first practical public key technique and introduced in 1976. 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.

The Discrete Logarithm Problem (DLP, see [4, 6, 8]) is, together with the Integer Factoring Problem (IFP, see [14]) and the Elliptic Curve DLP (ECDLP, see [11]), one of the main problems upon which public-key cryptosystems are built. Thus, efficiently computable groups where the DLP is hard to break, are very important in cryptography. In recent years, cryptographic research has become more and more important due to the increasing number of application areas related to the field, requiring data confidentiality, authentication and integrity.

[*] This work was partially supported by Generalitat Valenciana grant number GV04B-462.

The method presented in this paper, generalises the DH approach to a group based on the powers of a block upper triangular matrix, which is a very flexible technique.

The usual sizes for the keys in the IFP or DLP are around 1024 binary digits, existing well known algorithms of sub-exponential order that solve these problems (see [5, 12, 13]).

Our system is capable of increasing the computational cost required for a successful attack on the generated DLP for equivalent key sizes.

The rest of the paper is divided as follows: section 2 shows some properties necessary for the proposed cryptosystem. Section 3 is divided in several subsections: a key exchange protocol, an encryption scheme and a digital signature scheme. Finally, several conclusions about the system are given in section 4.

2 Preliminaries

Some basic linear algebra properties, necessary for the purpose of the paper, are presented in this section.

Given p a prime number and $r,\ s \in \mathbb{N}$, we denote by $Mat_{r\times s}(\mathbb{Z}_p)$ the matrices of size $r \times s$, with elements in $\mathbb{Z}_p$, and by $GL_r(\mathbb{Z}_p)$ and $GL_s(\mathbb{Z}_p)$ the invertible matrices of size $r \times r$ and $s \times s$.

We define

$$\theta = \left\{ \begin{bmatrix} A & X \\ \mathbf{0} & B \end{bmatrix}, A \in GL_r(\mathbb{Z}_p), B \in GL_s(\mathbb{Z}_p), X \in Mat_{r\times s}(\mathbb{Z}_p) \right\}.$$

Theorem 1 *The set θ has a structure of non-abelian group for the product of matrices.*

Proof: Given the definition of θ, it is obvious that the product operation is closed.

The identity element is

$$I = \begin{bmatrix} I_r & \mathbf{0} \\ \mathbf{0} & I_s \end{bmatrix},$$

where I_r and I_s, are respectively the identity matrices $r \times r$ and $s \times s$.

The inverse of any element $M = \begin{bmatrix} A & X \\ \mathbf{0} & B \end{bmatrix}$, is

$$M^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}XB^{-1} \\ \mathbf{0} & B^{-1} \end{bmatrix}.$$

The associative property is obvious since they are square matrices.

□

Theorem 2 Let $M = \begin{bmatrix} A & X \\ \mathbf{0} & B \end{bmatrix} \in \theta$, we *consider the subgroup generated by the different powers of M.*

Taking h as a non negative integer then

$$M^h = \begin{bmatrix} A^h & X^{(h)} \\ \mathbf{0} & B^h \end{bmatrix}, \qquad (1)$$

where

$$X^{(h)} = \begin{cases} \mathbf{0} & if \quad h = 0, \\ \sum_{i=1}^{h} A^{h-i} X B^{i-1} & if \quad h \geq 1. \end{cases} \qquad (2)$$

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

$$X^{(h)} = A^t X^{(h-t)} + X^{(t)} B^{h-t}, \qquad (3)$$
$$X^{(h)} = A^{h-t} X^{(h)} + X^{(h-t)} B^t. \qquad (4)$$

Proof: The equation (1) is proven using induction on *h*. For $h-0$ and $h-1$, the result is obvious. It is supposed to be true for $h-1$ and will be demonstrated true for *h*.

We have

$$\begin{aligned} M^h &= MM^{h-1} \\ &= \begin{bmatrix} A^{h-1} & X^{(h-1)} \\ \mathbf{0} & B^{h-1} \end{bmatrix} \begin{bmatrix} A^h & X^{(h)} \\ \mathbf{0} & B^h \end{bmatrix} \\ &= \begin{bmatrix} A^h & AX^{(h-1)} + XB^{h-1} \\ \mathbf{0} & B^h \end{bmatrix}, \end{aligned}$$

from the induction hypothesis, applying (2) we have that

$$\begin{aligned} X^{(h)} &= AX^{(h-1)} + XB^{h-1} \\ &= A\sum_{i=1}^{h-1} A^{h-1-i} XB^{i-1} + XB^{h-1} \\ &= \sum_{i=1}^{h-1} A^{h-i} XB^{i-1} + XB^{h-1} \\ &= \sum_{i=1}^{h} A^{h-i} XB^{i-1}, \end{aligned}$$

obtaining the same expression as in (2).

Also, if $0 \le t \le h$, we have

$$\begin{aligned} M^h &= M^t M^{h-t} \\ &= \begin{bmatrix} A^t & X^{(t)} \\ \mathbf{0} & B^t \end{bmatrix} \begin{bmatrix} A^{h-t} & X^{(h-t)} \\ \mathbf{0} & B^{h-t} \end{bmatrix} \\ &= \begin{bmatrix} A^h & A^t X^{(h-t)} + X^{(t)} B^{h-t} \\ \mathbf{0} & B^h \end{bmatrix}. \end{aligned}$$

Comparing this result to (1) we obtain (3). Expression (4) is proven in the same way.

□

As a consequence, in the case $t = 1$ we have

$$X^{(h)} = AX^{(h-1)} + XB^{h-1},$$
$$X^{(h)} = A^{h-1}X + X^{(h-1)}B,$$

and, taking *a, b* integers such as $a + b \ge 0$, we have

$$X^{(a+b)} = A^a X^{(b)} + X^{(a)} B^b. \qquad (5)$$

Given $M \in \theta$, it is known (see [9]) that *o(M) = lcm(o(A), o(B)),* on the other hand, the way to obtain a maximum *o(M)* is shown in [3, 7]. Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{r-1} x^{r-1} + x^r,$$
$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{s-1} x^{s-1} + x^s,$$

be two primitive polynomials in $\mathbb{Z}_{p[x]}$, and $\overline{A}, \overline{B}$ the corresponding associated matrices; let *P, Q* be two invertible matrices, $A = P\overline{A}P^{-1}$ and $B = Q\overline{B}Q^{-1}$.

With this construction, the order of *M* is

$$o(M) = lcm(p^r - 1,\ p^s - 1),$$

this number will be maximum if we take *r* and *s* prime (see [10]).

In table 1, where the value that appears in the column *o(M)* represents the number of decimal digits (the integer 2^{128} has 39 digits), it can be observed that the values of *r* and *s* do not need to be very big to optimise the order.

Table 1. Order of M, for different values of p, r and s

p	*r*	*s*	Digits	*p*	*r*	*s*	Digits
3	32	31	30	19	16	19	39
	48	47	39		32	31	57
	64	63	47		64	63	98
5	32	31	38	31	16	15	40
	30	33	39		32	31	64
	64	63	61		64	63	111
7	24	27	39	251	12	13	46
	32	31	43		32	31	76
	64	63	70		64	63	168
11	22	21	39	257	9	10	40
	32	31	50		32	31	93
	64	63	67		64	63	169

It is easy to reduce a general DLP in a cyclic group (with order $o(M)$) whose factorization is known. It is very important in the election of the group that the order is prime or at least with very big prime factors. So if $o(M)$ is a prime number, it will require on the order of $\sqrt{o(M)}$ operations to compute the discrete logarithm in group θ.

Theorem 3 *Given* $M \in \theta$*, with order m, we have that* $X^{(h+m+1)} = X^{(h+1)}$*, with* $0 \le h \le m-1$.

Proof: *We have that* $M^m = I$*, as a consequence*

$$M^{m+1} = \begin{bmatrix} A^{m+1} & X^{(m+1)} \\ \mathbf{0} & B^{m+1} \end{bmatrix} = M, \qquad (6)$$

then

$$X^{(m)} = X^{(0)} = \mathbf{0},$$
$$X^{(m+1)} = X^{(1)} = X,$$
$$A^{m+1} = A,$$
$$B^{m+1} = B.$$

It is proven using induction on *n*.

For $n = 0$ we have

$$X^{(m+1)} = X^{(1)}.$$

We suppose that it is true for $h-1$, that is

$$X^{(h-1+m+1)} = X^{(h)},$$

and we have

$$\begin{aligned} X^{(h+m+1)} &= X^{(1+h-1+m+1)} \\ &= X^{[1+(h-1+m+1)]} \\ &= AX^{(h-1+m+1)} + X^{(1)}B^{h-1+m+1} \\ &= AX^{(h)} + X^{(1)}B^{h-1}B^{m+1} \\ &= AX^{(h)} + X^{(1)}B^{h-1}B \\ &= AX^{(h)} + X^{(1)}B^{h} \\ &= X^{(h+1)}. \end{aligned}$$

□

Given $M \in \theta$, and the set

$$G = \left\{ X^{(0)}, X^{(1)}, X^{(2)}, \ldots\ldots, X^{(m-1)} \right\},$$

we define the operator $\otimes$, for a pair $X^{(a)},\ X^{(b)} \in G,$ as

$$X^{(a)} \otimes X^{(b)} = X^{(j)},$$

with $j = a + b (\operatorname{mod} m)$.

Theorem 4 *The set G is an abelian group for the operator* $\otimes$.

Proof: Given the definition of G and the operator $\otimes$, it is evident that it is an internal operation.

Taking a a non negative integer, the identity element is $X^{(0)}$ as

$$X^{(a)} \otimes X^{(0)} = A^{a}\mathbf{0} + X^{(a)}B^{0} = A^{a}\mathbf{0} + X^{(a)} = X^{(a)},$$

and

$$X^{(0)} \otimes X^{(a)} = A^{a}X^{(a)} + \mathbf{0}B^{0} = X^{(a)}.$$

Note that

$$X^{(0)} = \mathbf{0}$$

and that

$$B^{0} = A^{0} = I.$$

The inverse of any element $X^{(a)}$ is $X^{(m-a)}$ as, by definition,

$$X^{(a)} \otimes X^{(m-a)} = X^{(0)},$$

$$X^{(m-a)} \otimes X^{(a)} = X^{(0)},^{,}$$

$$X^{(m-a)} \otimes X^{(a)} = X^{(0)} = A^{m-a}X^{(a)} + X^{(m-a)}B^{a},$$

and the inverse of $X^{(0)}$ is the same matrix.

It validates the associative property as

$$\begin{aligned} (X^{(a)} \otimes X^{(b)}) \otimes X^{(c)} &= X^{(j_1)} \otimes X^{(c)} \\ &= X^{(j_2)} \\ &= X^{(a)} \otimes X^{(j_3)} \\ &= X^{(a)} \otimes (X^{(b)} \otimes X^{(c)}), \end{aligned}$$

with

$$j_1 = (a+b) \bmod m,$$

$$j_2 = (j_1 + c) \bmod m = (a+b+c) \bmod m,$$

$$j_3 = (b+c) \bmod m.$$

□

3 The algorithms.

3.1 Key exchange protocol

We will see now the proposed system of block matrices applied to the DH key exchange protocol.

Let *U* and *V* be two interlocutors who wish to exchange a key, then

1. *U* and *V* agree on *p, M*
2. *U* randomly generates a private key *k₁*, with $1 \le k_1 \le m$, and computes
$$M^{k_1} = \begin{bmatrix} A^{k_1} & X^{(k_1)} \\ \mathbf{0} & B^{k_1} \end{bmatrix}.$$
3. *V* randomly generates a private key *k₂*, with $1 \le k_2 \le m$, and computes
$$M^{k_2} = \begin{bmatrix} A^{k_2} & X^{(k_2)} \\ \mathbf{0} & B^{k_2} \end{bmatrix}.$$
4. The public key of *U* and *V* are respectively $(X^{(k_1)}, B^{k_1})$ and $(X^{(k_2)}, B^{k_2})$.
5. *U* computes $X^{(k_1+k_2)} = A^{k_1}X^{(k_2)} + X^{(k_1)}B^{k_2}$.
6. *V* computes $X^{(k_2+k_1)} = A^{k_2}X^{(k_1)} + X^{(k_2)}B^{k_1}$.

In this way, the key shared by *U* and *V* is

$$P = X^{(k_1+k_2)} = X^{(k_2+k_1)},$$

now both interlocutors, share a common and secret element.

An attacker could know *p* and *M*, but to obtain the shared secret would have to face a problem with a complexity similar to that of the DLP (see [6]).

3.2 Data encryption

We have to start from the same public and private elements seen previously in the key exchange protocol (which we suppose already done).

The interlocutor *U* wishes to, privately, send a message to *V*. The message must be coded as a matrix $\Delta = X^{(h)} \in G$.

Encryption:

1. U builds the matrices
$$T_1 = \begin{bmatrix} A & \Delta \\ \mathbf{0} & B \end{bmatrix},$$
$$T_2 = \begin{bmatrix} A & P \\ \mathbf{0} & B \end{bmatrix},$$
that are invertible since *A* and *B* are invertible too.
2. *U* computes matrix $C = T_1 T_2$ and sends this matrix to *V*.

Decryption:

1. *V* generates the matrix
$$T_2 = \begin{bmatrix} A & P \\ \mathbf{0} & B \end{bmatrix}$$
and computes its inverse.
2. *V obtains* T_1 carrying out the product CT_2^{-1}.
3. *V* recovers the message Δ selecting, the respective block of T_1.

With this, the functions of encryption and decryption of the interlocutor *V* would be respectively

1. $E_{k_2}(\Delta) = T_1 T_2$.
2. $D_{k_2}(C) = CT_2^{-1} = T_1$.

With the appropriate quick exponentiation algorithms (see [2]), the elements of *G* and the powers of *A* and *B* can be computed efficiently.

The complexity of the problem that an attacker would face is in the order of that of the DLP, acting, in effect, as a deterrent for a possible attack.

3.3 Signature scheme

We propose a digital signature scheme that requires the original message in order to verify the signature.

The scheme, that follows, is based on the ElGamal (see [15]) digital signature scheme.

We suppose that the users *U* and *V* have exchanged the key *P*, and *U* has sent the message Δ to *V*, according to the previous protocol. If the transmitter *U* wishes to sign digitally the message Δ proceeds in the following way

1. *U* generates a random number *w*.
2. *U* computes $H = B^w$ and $X^{(w)}$.
3. *U* computes
$$J = X^{(k_1+w)} = A^{k_1} X^{(w)} + X^{(k_1)} B^w.$$
4. *U* computes $T = \Delta - X^{((k_1+w)+k_2)}$ where
$$X^{((k_1+w)+k_2)} = A^{k_1+w} X^{(k_2)} + X^{(k_1+w)} B^{k_2}$$
$$= A^{k_1} A^w X^{(k_2)} + X^{(k_1+w)} B^{k_2}$$
That is to say, in order to compute *T* it is necessary to obtain A^{k_1} and A^w, which are private keys of the sender *U*, it is also necessary $X^{(k_2)}$ and $B^{(k_2)}$, which are public keys of the receiver *V* and $X^{(k_1+w)}$, which can be obtained from the data accessible to *U*.
5. The digital signature is (H, J, T).

If the receiver wishes to verify the digital signature of *U*, he proceeds in the following way

1. V computes
$$X^{((k_1+w)+k_2)} = X^{(k_2+(k_1+w))}$$
$$= A^{k_2} X^{(k_1+w)} + X^{(k_2)} B^{k_1+w}$$
$$= A^{k_2} X^{(k_1+w)} + X^{(k_2)} B^{k_1} B^w$$
Note that all the necessary elements for this calculation are public keys, elements of the digital signature or private keys of *V*
2. *V* computes $Y = \Delta - X^{(k_2+(k_1+w))}$.
3. *V* compares Δ and *Y*, turning out to be an authentic signature if $\Delta = Y$ and false if $\Delta \neq Y$.

4. Conclusions

With the aim of creating systems that allow to increase the computational cost required to break certain well known problems, we have presented a public key cryptosystem based on a generalization of the DLP for block upper triangular matrices, which provides an efficient protection against common attacks without the need of bigger key sizes.

For the development of this cryptosystem we have defined a set of matrices G that with an operator $\otimes$ form an abelian group, necessary for the definition of the key exchange protocol, public key cryptosystem and digital signature scheme.

Given two parties *U* and *V*, the key exchange protocol guarantees that both parties share a secret element of G; the public key cryptosystem defined assures data confidentiality and the digital signature scheme guarantees authentication and integrity.

References:

[1] Diffie, W., Hellman, M. New directions In Cryptography. *IEEE Trans. Information Theory*. **22**: 644-654. 1976.

[2] Gordon, D. M. A Survey of Fast Exponentiation Methods. Journal of Algorithms. **27**: 129–146. 1998.

[3] Hoffman, K., Kunze, R. Linear Algebra. Prentice-Hall. New Jersey. 1971.

[4] McCurley K. The discret logarithm problem. Crytology and Computational Number Theory, Proceedings of Symposia in Applied Mathematics. **42:** 49–74. 1990.

[5] Menezes, A., van Oorschot, P., Vanstone, S. Handbook of Applied Cryptography. *CRC Press*. Florida. 2001.

[6] Menezes, A., Wu, Y-H. The Discrete Logarithm Problem in GL(n,q). *Ars Combinatoria*. **47:** 22-32. 1997.

[7] Odoni, R. W. K., Varadharajan, V., Sanders, P. W. Public Key Distribution in Matrix Rings. *Electronic Letters*. **20**: 386-387. 1984.

[8] Stallings, W. Cryptography and Network Security. Principles and Practice. Third Edition. *Prentice Hall.* New Jersey. 2003

[9] Koblitz, N. A Course in Number Theory and Cryptography. Springer-Verlag. 1987.

[10] Lidl, R., Niederreiter, H. Introduction to Finite Fields and Their Applications. Cambridge University Press. 1994.

[11] Blake, I., Seroussi, G. Smart, N. Elliptic Curves in Cryptography. London Mathematical Society Lecture Notes Series 265. Cambridge University Press. 1999.

[12] Pohlig. S, Hellman, M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Trans. **24**: 106-110. 1979.

[13] Coppersmith, D., Odlyzko, A., and Schroeppel, R. Discrete logarithms in GF(p). Algorithmica 1-15. 1986.

[14] Rivest, R., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *ACM Communications*. **21**: 120-126. 1978.

[15] Elgamal, T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Trans. Inform. Theory*. **31**: 469-472. 1985.