Journal of Applied Mathematics & Bioinformatics, vol.5, no.3, 2015, 37-48
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2015

Handling problems in cryptography with matrix factorization

G.C. Meletiou[1], D.S. Triantafyllou[2] and M.N. Vrahatis[3]

Abstract

Matrix manipulations of cryptographic functions are revisited. The Discrete logarithm function and the Diffie Hellman mapping can be expressed as products of Vandermonde matrices. First we consider orbits of repeated applications of the cryptographic transformations. The difficulty to compute the cryptographic function (in other terms the robustness of the cryptosystem) is related to the length of the orbit. We determine it either by computational experiments or with theoretical tools. We investigate the behaviour of powers of matrices constructed from the generators α of the multiplicative group for several primes p in $\mathbb{Z}_p$. We study how the sequence of powers of these matrices leads to the identity matrix in respect to the generator α, the prime numbers p and the elements of the main diagonal of the matrices. Finally, the matrix factorization approach (LU factorization) is revisited.

[1] A.T.E.I. of Epirus, P.O. Box 110, GR-47100, Arta, Greece. E-mail: gmelet@teiep.gr
[2] University of Military Education, Hellenic Army Academy, GR-16673, Vari, Greece. E-mail: dtriant@math.uoa.gr
[3] Computational Intelligence Laboratory (CILab), Department of Mathematics, University of Patras, GR-26110 Patras, Greece. E-mail: vrahatis@math.upatras.gr

Article Info: *Received* : November 3, 2014. *Revised* : February 5, 2015.
Published online : September 15, 2015.

Mathematics Subject Classification: 94A60; 11T71; 68P25; 11T55; 65T50; 41A05; 41A10; 92B20; 82C32
Keywords: LU factorization; matrix triangularization; encryption; decryption; orbit

1 Introduction

In recent cryptographic research the approach of matrix transformations has been used. The LU factorization (also called LU decomposition) has been applied in various cryptographic schemes. Factorizing the matrix A as $A = L \cdot U$ is computationally feasible, however reconstructing the initial matrix A knowing only the matrix U or only the matrix L is an NP-hard problem [3]. The matrix A can be used for the representation of an image, a diagram, or a data table, etc. The main idea is to factorize A in order to achieve availability, persistence, integrity, and confidentiality of the information [16]. The LU decomposition has been used in key pre-distribution schemes [1]. Users are represented as nodes since applications of Distributed Sensor Networks are concerned. Each node corresponds to the i-th row and the i-th column of a symmetric matrix $A = (A_{ij})_{1 \leqslant i,j \leqslant n}$ and the entry $A_{ij} = A_{ji}$ is the symmetric (session) key between the i-th and the j-th user. The matrix A is factorized as $A = L \cdot U$. The i-th row of L is kept secret by the i-th user, a kind of private key, while the i-th column of U plays the role of the public key. Users i and j exchange their columns and compute A_{ij} and A_{ji} respectively which coincide since A is symmetric. Of course the aforementioned scheme requires the participation of a dealer (central authority). In some similar schemes LU decomposition is replaced by $L \cdot D \cdot U^{'}$ decomposition [2, 8].

In [14, 15] Bilateral Remote User Authentication Schemes have been proposed based on LU decomposition. A user is authenticated from a central authentication server. The central authority generates a symmetric square matrix A and assigns an entry of the form $A_{ij} = A_{ji}$ for each user and matrix A is factorized as $A = L \cdot U$ and a smart card is issued to each user. The information which is contained on the card includes the i-th column of U, key A_{ij}, j in encrypted form and the identity of the user. The main idea is to derive authentication by comparing A_{ij} and A_{ji} since A is symmetric. In improved

versions of the aforementioned schemes anonymity of the users is guaranteed [9, 17].

In the paper at hand we investigate the powers of matrices related to cryptographic transformations. The matrices represent the discrete logarithm function and they are derived from the interpolation formula. The powers of matrices represent the multiple discrete logarithm. The paper is organized as follows. In Section 2, the required definitions and mathematical tools as well as the LU factorization scheme are presented. In Section 3, the proposed algorithms are numerically implemented and the results are summarized in tables and figures. Finally, in Section 4, a synopsis and concluding remarks are presented.

2 The Discrete Logarithm function and matrix factorizations

In this section, we present formulas for the polynomial interpolation of the discrete logarithm and the multiple discrete logarithm function. The LU factorization algorithm is also developed.

Definition 2.1. *Let*

$$A = (A_{ij})_{1 \leqslant i,j \leqslant p-1} = \left(\frac{-1}{a^{i \cdot j}} \right)_{1 \leqslant i,j \leqslant p-1},$$

be a $(p-1) \times (p-1)$ *matrix with* p *prime and* $a \in \mathbb{Z}_p$*, where* a *is a generator of the multiplicative group.*

Remark 2.2. *The matrix* A *is invertible.*

Proposition 2.3. [10, 11] The product

$$\begin{bmatrix} 1 & 2 & \dots & p-1 \end{bmatrix} \cdot A \cdot \begin{bmatrix} x \\ x^2 \\ \vdots \\ x^{p-1} \end{bmatrix}$$

is the Lagrange interpolation polynomial for the Discrete Logarithm function, thus

$$\log_a x = \begin{bmatrix} 1 & 2 & \dots & p-1 \end{bmatrix} \cdot A \cdot \begin{bmatrix} x \\ x^2 \\ \vdots \\ x^{p-1} \end{bmatrix} = \sum_{j=1}^{p-2} \frac{x^j}{1-a^j},\ x \neq 0.$$

Definition 2.4. *Let N be a $(p-1) \times (p-1)$ matrix with p prime of the following form*

$$N = \begin{bmatrix} 1 & 2 & \dots & p-1 \\ 1^2 & 2^2 & \dots & (p-1)^2 \\ \vdots & \vdots & \ddots & \vdots \\ 1^{p-1} & 2^{p-1} & \dots & (p-1)^{p-1} \end{bmatrix} \in \mathbb{Z}_p^{(p-1)\times(p-1)}.$$

Remark 2.5. *The matrix N is invertible.*

Proposition 2.6. [12] Suppose that $\log_a x = c$, then it holds that

$$\begin{bmatrix} c & c^2 & \dots & c^{p-1} \end{bmatrix}^\top = N \cdot A \cdot \begin{bmatrix} x & x^2 & \dots & x^{p-1} \end{bmatrix}^\top.$$

If d is the multiple discrete logarithm of x with multiplicity k, then it holds that

$$\begin{bmatrix} d & d^2 & \dots & d^{p-1} \end{bmatrix}^\top = (N \cdot A)^k \cdot \begin{bmatrix} x & x^2 & \dots & x^{p-1} \end{bmatrix}^\top$$

and

$$d = \begin{bmatrix} 1 & 2 & \dots & p-1 \end{bmatrix} \cdot (N \cdot A)^k \cdot \begin{bmatrix} x & x^2 & \dots & x^{p-1} \end{bmatrix}^\top.$$

The set $\{(N \cdot A),\ (N \cdot A)^2, \dots, (N \cdot A)^j, \dots\}$ determines the orbit of the element $(N \cdot A)$. The length of the orbit is the minimum positive integer k for which $(N \cdot A)^k = I$, where I is the identity matrix. In other terms k is the order of the element $(N \cdot A)$. According to [5] the value of k has to be very large. Our computational experiments with small primes verify it. It is profound that $(N \cdot A)^{-1}$ is the transformation of the discrete exponential function; exponentiation modulo a prime is computable (square and multiply algorithm). Therefore the order of $(N \cdot A)$ has to be high since computing discrete logarithms and multiple discrete logarithms is infeasible.

The aim of the paper at hand is the extraction of conclusions concerning the orbit of $(N \cdot A)$ for various values of the prime p and the generator a. The

highest the order the hardest is to compute the discrete logarithm function, therefore the safer the encoding.

Another scope of the paper is the factorization of $(N \cdot A)^i,\ i = 1, 2, \ldots, k$ through the LU decomposition in order to compare the diagonal elements of U with the diagonal elements of I (the ones).

We elaborate two real valued functions for the matrix:

1. the *quasideterminant* which is obtained by the product of all diagonal elements of U considered as nonnegative integers less than p,

2. the *quasinorm* which is the Euclidean norm of the diagonal elements.

Then we investigate possible "convergence" of these functions to 1.

In our approach we apply the LU factorization of a matrix A which is briefly presented in the following paragraphs.

The given matrix A is factorized to a lower triangular matrix L with ones in its main diagonal and the multipliers in the entries below the diagonal and to an upper triangular matrix U, such that $A = L \cdot U$. Since the computations are performed in $\mathbb{Z}_p$, there are no floating point errors and thus there is no need of using pivoting.

The LU Factorization algorithm can be given as follows [6, 7]:

Algorithm of the LU Factorization:
for $k = 1 : p - 1$
$m_{ik} = A_{ik}/A_{kk},\ i = k + 1 : m$
$A_{ij} = A_{ij} - m_{ik}A_{kj},\ i = k + 1 : m,\ j = k + 1 : n$

Numerical Complexity: The required floating point operations of the LU factorization of a $(p-1) \times (p-1)$ matrix is $O\big((p-1)^3/3\big)$.

3 Numerical implementation

In this section we calculate numerically the orbit and the order of the element $(N \cdot A)$. In the following tables we present the results of the computed

orders for various values of the prime p and the generator a of the multiplicative group of the field.

Table 1: k (minimum power k: $(N \cdot A)^k = I$), α (generator), p=47

α	5	11	13	19	23	29	31	41	43
k	96	378	3036	136	546	144	150	3003	1170

Table 2: k (minimum power k: $(N \cdot A)^k = I$), α (generator), p=73

α	5	11	13	29	31	47	53	59
k	1326	2720	1830	210	70	918	9020	3570

Table 3: k (minimum power k: $(N \cdot A)^k = I$), α (generator), p=101

α	2	3	7	11	29	53	59	61	67	73	83	89
k	46200	7110	2156	33726	440572	460	4830	4950	1020	1998	90	1104

As it is shown in Tables 1, 2 and 3, the order of the element $(N \cdot A)$ is at least of order of p, thus the encoding is safe. More precisely, in Table 3, for $p = 101$ and generator $\alpha = 29$ the order is 440572 which is significant greater than $p = 101$ enforcing the safety.

Next, we perform LU factorizations to $(N \cdot A)^i$, $i = 1, 2, \ldots, k$. We obtain two sequences, the sequence of the quasideterminants and the sequence of the quasinorms. If there was any kind of convergence of the sequence of $((N \cdot A)^i)$, $i = 1, 2, \ldots, (\text{order} - 1)$ to $I = (N \cdot A)^{\text{order}}$, then every element of the main diagonal of $(N \cdot A)^i$ should converge to 1. Thus, the quasinorm of these elements and the quasideterminant of $(N \cdot A)^i$ computed in $\mathbb{R}$ should converge to 1.

Implementing several examples for various primes p and all of their generators α we lead to the result that there is no relationship between them. Actually, there is a significant difference of the order of the computed quasideterminants and quasinorms of all the powers $(N \cdot A)^i$, $i = 1, 2, \ldots, (\text{order} - 1)$ with the quasideterminant and the quasinorm of $I = (N \cdot A)^{\text{order}}$ which is equal to 1.

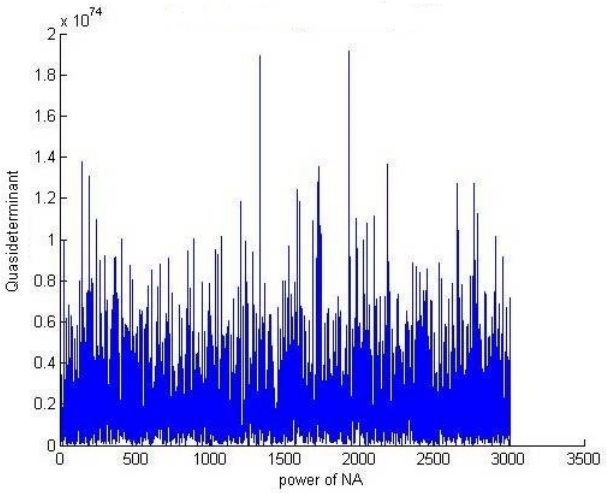

Figure 1: Quasideterminants of $(N \cdot A)^i,\ i = 1, 2, \ldots, \text{order},\ p = 47,\ \alpha = 41$

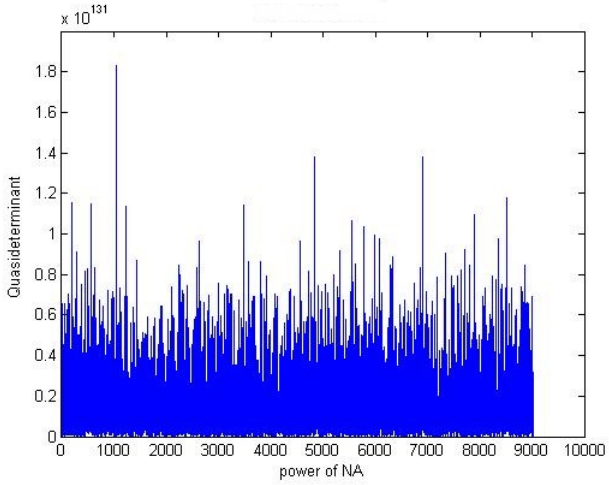

Figure 2: Quasideterminants of $(N \cdot A)^i,\ i = 1, 2, \ldots, \text{order},\ p = 71,\ \alpha = 53$

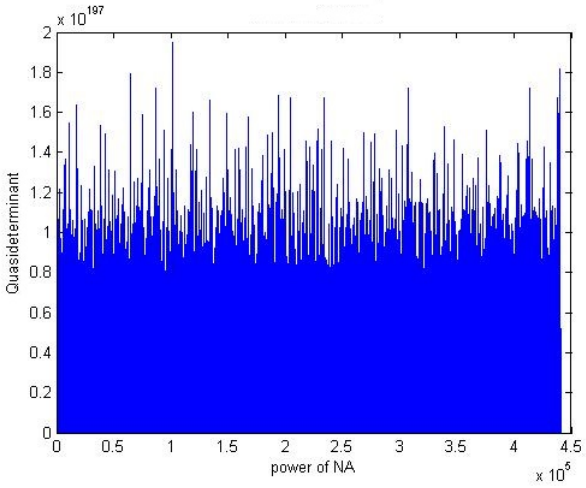

Figure 3: Quasideterminants of $(N \cdot A)^i,\ i = 1, 2, \ldots, \text{order},\ p = 101,\ \alpha = 29$

In Figures 1, 2 and 3, the quasideterminants of $(N \cdot A)^i,\ i = 1, 2, \ldots, \text{order}$ are presented graphically. We used various values of p and α. Specifically in Figure 1 we used the values $p = 47$ and $\alpha = 41$, in Figure 2 the values $p = 73$ and $\alpha = 53$ while in Figure 3 we used the values $p = 101$ and $\alpha = 29$. The minimum quasideterminants are of high order ($10^{74} \gg 1$ (Figure 1), 10^{119} (Figure 2) and ($10^{193} \gg 1$ (Figure 3)). Only the last one (the one that corresponds to $(N \cdot A)^{\text{order}} = I$ is equal to 1. Thus, there is not any convergence to 1 for the quasideterminants of the powers of $(N \cdot A)$ proving experimentally that the encoding is safe. The orbits are of order of $3 \cdot 10^3 \gg 1$, $9 \cdot 10^3 \gg 1$ and $4.4 \cdot 10^5 \gg 1$ respectively.

Finally, we investigate the relationship between the quasinorm of the diagonal entries of $(N \cdot A)^i$, for $i = 1, 2, \ldots, k$ with the quasinorm of the diagonal entries of $(N \cdot A)^k = I$. Again, experimentally is shown that there is not any relation between them (Figures 4,5 and 6).

4 Synopsis and concluding remarks

Initially in the paper at hand, we made a brief survey of earlier schemes based on matrix factorization (decomposition). The LU factorization has been applied to many schemes since reconstructing the original matrix from one

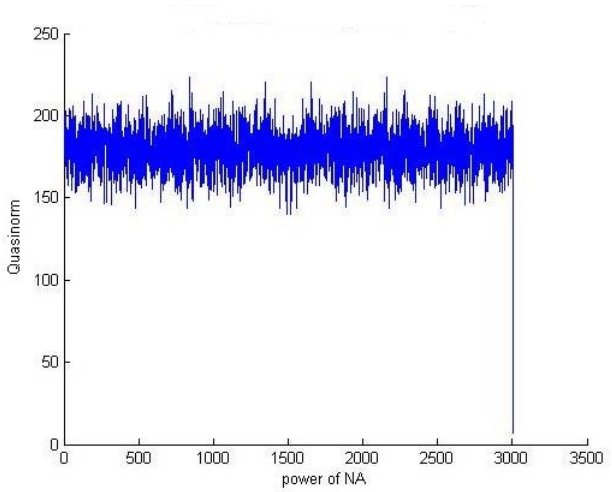

Figure 4: Quasinorms of $(N \cdot A)^i,\ i = 1, 2, \ldots, \text{order},\ p = 47,\ \alpha = 41$

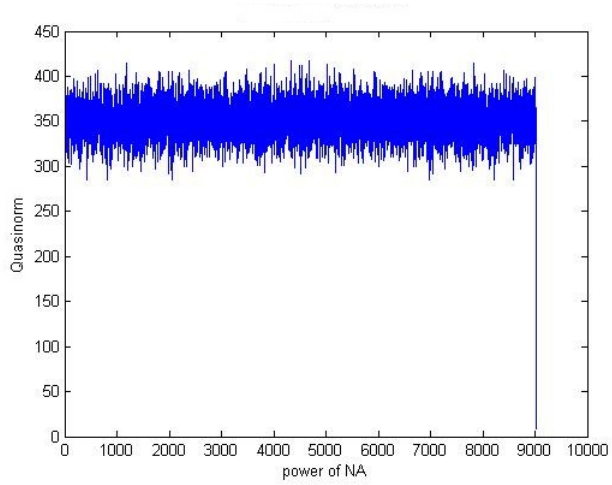

Figure 5: Quasinorms of $(N \cdot A)^i,\ i = 1, 2, \ldots, \text{order},\ p = 73,\ \alpha = 53$

of the factors is a NP hard problem. We studied repeated applications of cryptographic functions extending the employment of matrices. We elaborated powers of matrices in order to compute the length of the orbits and to relate it to the robustness of a scheme. A number of computational experiments verified previous theoretical results related to the Multiple Discrete Logarithm function. The orbits of the matrices were of the same order of there size, thus, the encryption is safe. The quasideterminants and the entries of the main

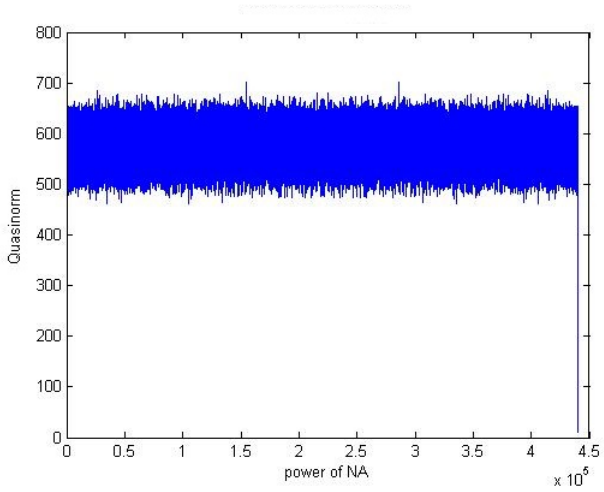

Figure 6: Quasinorms of $(N \cdot A)^i,\ i = 1, 2, \ldots,$ order, $p = 101,\ \alpha = 29$

diagonal of the powers of the matrices do not converge smoothly to those of I (which is the initial matrix powered to its order), enforcing the encoding since there is no relationship between them.

The study of other factorizations in order to achieve better representations of cryptographic functions and facing the computational equivalence of the discrete logarithm and the Diffie Hellman problem are open topics for future work.

References

[1] Sung Jin Choi and Hee Yong Youn, An Efficient Key Pre-distribution Scheme for Secure Distributed Sensor Networks, EUC *Workshops* 2005, LNCS 3823, (2005), 1088–1097.

[2] Sung Jin Choi and Hee Yong Youn, MKPS, A Multi-level Key Pre-distribution Scheme for Secure Wireless Sensor Networks, *Human-Computer Interaction*, Part II, HCII 2007, LNCS 4551, (2007), 808–817.

[3] Sung Jin Choi and Hee Yong Youn, A Novel Data Encryption and Distribution Approach for High Security and Availability Using LU Decompo-

sition, LNCS, 3046, (2004), 637–646.

[4] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inf. Th.*, **22**(6), (1976), 644–654.

[5] L. Glebsky and I. Shparlinski, Short Cycles in Repeated Exponentiation Modulo a Prime, *Des. Cod. Crypt.*, **56**(1), (2009), 35–42.

[6] B.N. Datta, *Numerical Linear Algebra and Applications*, Second Edition, SIAM, United States of America, 2010.

[7] G.H. Golub and C.F. van Loan, *Matrix Computations*, Third Edition, The John Hopkins Univercity Press, Baltimore, 1996.

[8] S. Kumar and D. Dohare, Efficient Key Distribution Schemes for Wireless Sensor Networks Using LDU Composition of Symmetric Matrices, *Communications in Computer and Information Science*, **197**, (2011), 343–357.

[9] Xiong Li, Jianwei Niu, Muhammad Khurram Khan and Zhibo Wang, Applying LU Decomposition of Matrices to Design Anonymity Bilateral Remote User Authentication Scheme, *Mathematical Problems in Engineering*, **2013**, (2013), 1–10, Article ID 910409.

[10] G.C. Meletiou, Explicit form for the discrete logarithm over the field GF(p,k), *Archivum Mathematicum*, **29**, (1993), 25–28.

[11] G.C. Meletiou and G. Mullen, A note on Discrete Logarithms in finite fields, A.A.E.C.C., **3**, (1992), 75–79.

[12] G.C. Meletiou, E.C. Laskari, D.K. Tasoulis and M.N. Vrahatis, Matrix representations of Cryptographic Functions, *Journal of Applied Mathematics and Bioinformatics*, **3**(1), (2013), 205–213.

[13] G.C. Meletiou and A. Winterhof, Interpolation of the Double Discrete Logarithm, LNCS, **5130**, (2008), 1–10.

[14] A.S.K. Pathan and C.S. Hong, An efficient bilateral remote user authentication scheme with smart cards, *Proceedings of the 33rd Korea Information Science Society Fall Conference*, **33**(2)(D), (October, 2006), 132–134.

[15] A.S.K. Pathan, C.S. Hong and T. Suda, A novel and efficient bilateral remote user authentication scheme using smart cards, *Proceedings of the IEEE International Conference on Consumer Electronics*, (January, 2007), 1–2.

[16] D.S. Triantafyllou, Numerical Linear Algebra methods in Data Encoding and Decoding, *Journal of Applied Mathematics and Bioinformatics*, **3**(1), (2013), 193–203.

[17] H.R. Tseng, R.H. Jan and W. Yang, A bilateral remote user authentication scheme that preserves user anonymity, *Security and Communication Networks*, **1**(4), (2008), 301–308.

[18] A. Winterhof, A note on the interpolation of the Diffie-Hellman mapping, *Bull. Austral. Math. Soc.*, **64**(3), (2001), 475–477.