Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 205-213
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

Matrix representation of cryptographic functions

G.C. Meletiou[1], E.C. Laskari[2], D.K. Tasoulis[3] and M.N. Vrahatis[4]

Abstract

The Discrete Logarithm and the Diffie-Hellman are two hard computational problems, closely related to cryptography and its applications. The computational equivalence of these problems has been proved only for some special cases. In this study, using LU-decomposition to Vandermonde matrices, we are able to transform the two problems in terms of matrices, thus giving a new perspective to their equivalence. A first study on matrix expressions for the Double and Multiple Discrete Logarithms is also presented.

[1] A.T.E.I. of Epirus, P.O.110, GR-47100 Arta, Greece,
University of Patras Artificial Intelligence Research Center, University of Patras, GR-26110 Patras, Greece, e-mail: gmelet@teiep.gr

[2] Computational Intelligence Laboratory, Department of Mathematics, Univeristy of Patras, GR-26110 Patras, Greece, e-mail: elena@math.upatras.gr

[3] Computational Intelligence Laboratory, Department of Mathematics, Univeristy of Patras, GR-26110 Patras, Greece, e-mail: dtas@math.upatras.gr

[4] Computational Intelligence Laboratory, Department of Mathematics, Univeristy of Patras, GR-26110 Patras, Greece, Computational Intelligence Laboratory, Department of Mathematics, Univeristy of Patras, GR-26110 Patras, Greece, e-mail: vrahatis@math.upatras.gr

Article Info: *Received* : November 1, 2012. *Revised* : January 30, 2013
Published online : March 30, 2013

Mathematics Subject Classification: 94A60, 11T71, 12Y05, 15A24
Keywords: Cryptography; Discrete Logarithm; matrix representations

1 Introduction

Public key cryptography [5, 14] motivated a number of hard and complex computational problems [12, 14]. We state the well known Discrete Logarithm problem and the Diffie-Hellman problem.

(a) **The Discrete Logarithm Problem (DLP)** [1, 4, 12]. Let G be a finite cyclic group generated by g and $h \in G$. Given g and h, compute an integer z in $[0, |G| - 1]$, such that $g^z = h$. The integer z is called the discrete logarithm of h to the base g.

(b) **The Diffie-Hellman Problem (DHP)** [5]. Let G be a finite cyclic group generated by g and $f, h \in G$. Suppose further that $f = g^z, h = g^w$, for some integers z, w in $[0, |G| - 1]$. Given g, h and f, compute g^{zw}.

The corresponding cryptographic functions are the discrete logarithm function and the Diffie-Hellman key function.

Since many contemporary cryptosystems rely on the assumption that these two problems are computationally intractable in polynomial time, various attempts to address these problems have been performed. These attempts include both interpolation and approximation techniques, since functions from a finite field to itself can always be represented by polynomials (Lagrangian interpolation) [4, 7]. Also, studies for the reformulation of these cryptographic problems have been presented. One of these studies exploits matrices to formulate the DLP and DHP [8].

The paper is organized as follows. In section 2 recent matrix formulations of the DLP and the DHP are reported and matrix transformations using LU-decomposition through Newton polynomials are presented. Section 3 exhibits a first study on matrix transformations for the Double and Multiple Discrete Logarithms. The epilogue of the paper is given in section 4.

2 Transformations in Terms of Matrices

The Discrete Logarithm function can be written as

$$\log_a(x) = \sum_{i=1}^{p-2}(x^i(1-\alpha^i)^{-1}),$$

or equivalently

$$\log_a(x) = (1, 2, \ldots, p-1)A(x, x^2, \ldots, x^{p-1})^\top, \tag{1}$$

where $x \neq 0$, $A = \{A_{ij}\}$, $1 \leqslant i, j \leqslant p-1$, with $A_{ij} = -\alpha^{-ij}$, and α is a generator of the multiplicative group of $\mathbb{Z}_p$ [8, 11]. Matrix A represents a Discrete Fourier Transform [13].

The Diffie-Hellman key function, $K : (\alpha^u, \alpha^v) \mapsto \alpha^{uv}$, can be written as the two variable polynomial, $K(x, y) = -\sum_{i,j=1}^{p-1} \alpha^{-ij} x^i y^j$, or equivalently as

$$K(x, y) = (y, y^2, \ldots, y^{p-1})A(x, x^2, \ldots, x^{p-1})^\top, \tag{2}$$

where $y \neq 0$ [18]. The question of computational equivalence of the DLP and DHP can be formulated by matrix computations of Equations (1) and (2).

Consider the $(p-1) \times (p-1)$ symmetric Vandermonde matrix

$$W = \{W_{ij}\},\ 1 \leqslant i, j \leqslant p-1, \text{ with } W_{ij} = w^{(i-1)(j-1)},$$

where $w = \alpha^{-1}$. Matrix W is a Discrete Fourier Transform, like matrix A in Eq.(1). Matrix W can be obtained by applying an elementary permutation (shifting) to the columns and rows of $-A$. Thus, Eqs. (1) and (2) can be written as

$$\log_a(x) = -(p-1, 1, 2, \ldots, p-2)W(x^{p-1}, x, \ldots, x^{p-2})^\top, \tag{3}$$

and

$$K(x, y) = -(x^{p-1}, x, x^2, \ldots, x^{p-2})W(y^{p-1}, y, \ldots, y^{p-2})^\top, \tag{4}$$

respectively. Next, following the approach of Newton polynomials described in [15], we have $t_i(x) = \prod_{j=0}^{p-3}(x - w^j)$, for $i = 1, \ldots, p-2$, and $t_0(x) = 1$. Then, using LU-decomposition, matrix W can be factorized to $W = LU$, where L is a lower triangular matrix defined by $L^{-1} = (\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{p-2})^\top$, with $\mathbf{t}_i$ the vector of the coefficients for the polynomial t_i, and U is the upper triangular matrix, $U = \{U_{ij}\}$, $1 \leqslant i, j \leqslant p-1$, with $U_{ij} = t_{i-1}(w^{j-1})$, which equals to

$$U = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & w-1 & w^2-1 & w^3-1 & \dots & w^{p-2}-1 \\ 0 & 0 & (w^2-1)(w^2-w) & (w^3-1)(w^3-w) & \dots & (w^{p-2}-1)(w^{p-2}-w) \\ 0 & 0 & 0 & \prod_{j=0}^{2}(w^3-w^j) & \dots & \vdots \\ \vdots & \vdots & \vdots & \dots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & \prod_{j=0}^{p-3}(w^{p-2}-w^j) \end{pmatrix}.$$

Since matrix W is symmetric, the upper triangular matrix U can also be factorized to $U = DL^\top$, where $D = \mathrm{diag}(U)$. So matrix L does not have to be computed by its inverse matrix, as it can be obtained directly by matrix U. Thus, matrix L assumes the form

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & (w^2-1)(w-1)^{-1} & 1 & 0 & \dots & 0 \\ 1 & (w^3-1)(w-1)^{-1} & (w^3-1)(w^3-w)(w^2-1)^{-1}(w^2-w)^{-1} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (w^{p-2}-1)(w-1)^{-1} & \dots & \dots & \dots & 1 \end{pmatrix}.$$

Set $F(x) = L^\top \mathbf{x}$, with $\mathbf{x}^\top = (x^{p-1}, x, \dots, x^{p-2})$. Using the previous factorization of matrix W and taking under consideration Eqs. (3) and (4), the Discrete Logarithm function can be written as

$$-\mathbf{n}^\top LDL^\top \mathbf{x} = -\mathbf{n}^\top LDF(x),$$

where $\mathbf{n}^\top = (p-1, 1, 2, \dots, p-2)$. Also, the Diffie-Hellman key function can be written as

$$-\mathbf{y}^\top LDL^\top \mathbf{x} = -F^\top(y)DF(x),$$

where $\mathbf{y}^\top = (y^{p-1}, y, y^2, \dots, y^{p-2})$. In the case of the Diffie-Hellman mapping (where $x = y$), we obtain the following quadratic form $-\mathbf{x}^\top LDL^\top \mathbf{x} = -F^\top(x)DF(x)$, which is computationally equivalent to the Diffie-Hellman function. The Diffie-Hellman mapping can also be written as $-\mathbf{c}^\top LDL^\top \mathbf{y}$, where $\mathbf{c}^\top = (\alpha^0, \alpha^{1^2}, \alpha^{2^2}, \dots, \alpha^{(p-2)^2})$.

Remark : Assume that $\alpha^k = x$, $0 < k < p-2$, that is, k is the Discrete Logarithm of x. Then the $k-1$ first entries of the vector $F(x)$ are 0.

3 Double and Multiple Discrete Logarithms in Terms of Matrices

In cryptography some important applications, such as group signature, e-voting and publicly verifiable secret sharing schemes, employ the double discrete logarithm problem, i.e., the discrete logarithm of the discrete logarithm [16, 17]. As a first study, consider the multiplicative group $\mathbb{Z}_p^*$. We can represent the discrete logarithm with b basis, of the discrete logarithm with α basis, as

$$\mathbf{n}^\top \cdot B \cdot N \cdot A \cdot \mathbf{x},$$

where $\mathbf{n} = (1, \ldots, p-1)^\top$, $\mathbf{x} = (x, \ldots, x^{p-1})^\top$ and $B = \{B_{ij}\}$, $1 \leqslant i, j \leqslant p-1$, with $B_{ij} = -b^{-ij}$, $A = \{A_{ij}\}$, $1 \leqslant i, j \leqslant p-1$, with $A_{ij} = -\alpha^{-ij}$ and $N = \{N_{ij}\}$, $1 \leqslant i, j \leqslant p-1$, with $N_{ij} = j^i$.

The double discrete logarithm is used as a one-way function defined over a cyclic group. In [9] it is shown that there are no low degree polynomials representing the double discrete logarithm for a large set of given data. The assumption of hardness of the double discrete logarithm is supported. Concerning repeated discrete exponentations (multiple computations of the discrete logarithm) see also [6].

Next, we consider the Multiple Discrete Logarithm Problem (MDLP), also called Representation Problem (RP), which is motivated by electronic cash, group signatures, key agreement protocols and other applications [2, 3, 10, 19].

The definition of the MDLP is given as follows. Let G be a cyclic qroup. The symbol $\langle g \rangle$ will be used for the subgroup generated by $g \in G$.

In addition, assume that G can be represented as a direct product $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_k \rangle$. Thus, every $h \in G$ can be written as $h = g_1^{z_1} g_2^{z_2} \cdots g_k^{z_k}$ in a unique way. The $k-$tuple $(z_1, \ldots, z_k)$ consists of the z_t indices, with $0 \leqslant z_t \leqslant m_t - 1$, where m_t is the order of g_t, i.e., $m_t = |\langle g_k \rangle|$. Then, the k-tuple $(z_1, \ldots, z_k)$ is called the Multiple Discrete Logarithm of h with basis $(g_1, \ldots, g_k)$.

Symmetric Vandermonde matrices can also be used for the manipulation of the MDLP. For the case where $G = \mathbb{Z}_p^*$, assume that $\mathbb{Z}_p^* = \langle \alpha_1 \rangle \times \cdots \times \langle \alpha_k \rangle$, where $\alpha_t \in \mathbb{Z}_p^*$, $|\langle \alpha_t \rangle| = m_t$, $m_1 m_2 \cdots m_k = p - 1$ and $\gcd(m_r, m_s) = 1$, for $1 \leqslant r, s \leqslant k$, with $r \neq s$. The Multiple Discrete Logarithm of x is defined as $(z_1, \ldots, z_k)$, such that $x = \alpha_1^{z_1} \alpha_2^{z_2} \cdots \alpha_k^{z_k}$, where z_t, for $1 \leqslant t \leqslant k$, is an element

of the set $\{1, \ldots, m_t\}$. Let $n_t = \frac{p-1}{m_t}$ and $\gcd(n_t, m_t) = 1$, for $1 \leqslant t \leqslant k$. Then, the following polynomial representation of z_t can be derived

$$z_t = \frac{m_t + 1}{2} x^{p-1} + \sum_{s=1}^{m_t - 1} x^{sn_t} (1 - a_t^{sn_t})^{-1}. \tag{5}$$

Also, a matrix (Discrete Fourier Transform) can be obtained

$$z_t = -m_t^{-1} \mathbf{m}_t^{\top} A \mathbf{x},$$

where $\mathbf{m}_t = (1, 2, \ldots, m_t)^{\top}$, $\mathbf{x} = (x^{n_t}, x^{2n_t}, \ldots, x^{m_t n_t})^{\top}$, and A is the $m_t \times m_t$ matrix, $A = \{A_{ij}\}$, $1 \leqslant i, j \leqslant m_t$, with $A_{ij} = -\alpha_t^{-n_t ij}$.

We note that the aforementioned representations are similar to the representations of [8], where discrete logarithms over subgroups are interpolated and represented with the help of Vandermonde matrices.

In [8] the discrete logarithm function is defined over a subgroup $\langle g \rangle$ of $\mathbb{Z}_p^*$ and the polynomial formula is

$$f(x) = (1 - (x^m - 1)^{p-1}) \bar{f}(x), \tag{6}$$

where

$$\bar{f}(x) = \frac{m+1}{2} x^m + \sum_{i=1}^{m-1} (1 - g^i)^{-1} x^i, \tag{7}$$

and $|\langle g \rangle| = m/(p-1)$, $x \in \langle g \rangle$. The corresponding matrix representation is

$$\bar{f}(x) = \frac{p-1}{m} (1, \ldots, m) A (x, \ldots, x^m)^{\top},$$

where $A = (-g^{-ij})$, $1 \leqslant i, j \leqslant m$, is $m \times m$ matrix.

The polynomials in Equations (5) and (7) are the same. Equation (5) holds for all $x \in \mathbb{Z}_p^*$, while Equation (6) is true only for elements of the subgroup $\langle g \rangle$ as $\bar{f}(x)$ is a restriction.

In the case where $|\langle g \rangle| = m$, $n = \frac{p-1}{m}$, $\gcd(m, n) = 1$, g can be considered as an element of a basis for the MDL, namely $g_1 = g, g_2, \ldots, g_k$. Every element $x \in \mathbb{Z}_p^*$ admits a unique representation as $x = g_1^{z_1} g_2^{z_2} \cdots g_k^{z_k} = g^z g_2^{z_2} \cdots g_k^{z_k}$. It can be derived that

$$z = \Big(\frac{m+1}{2}\Big) x^{p-1} + \sum_{s=1}^{m-1} x^{Ls} (1 - g^s)^{-1} = \bar{f}(x^L),$$

where $L = nN$, $N \equiv n^{-1} (\mathrm{mod}\ m)$ and the mapping $x \mapsto x^L$ is a kind of projection since $x^L = (x^n)^N = (g^{nz})^N = g^z \in \langle g \rangle$, $x^L = x$ for all $x \in \langle g \rangle$. The corresponding matrix representation is

$$z = \frac{p-1}{m}(1, \ldots, m)(-g^{-ij})(x^L, x^{2L}, \ldots, x^{mL})^\top.$$

4 Epilogue

Initially in this paper, two well-known problems from the field of cryptography, namely the Discrete Logarithm and the Diffie-Hellman problem, are studied employing matrix transformations. Specifically, using LU-decomposition for Vandermonde matrices through Newton polynomial, we are able to provide new forms of both these problems. These new forms constitute an alternative approach to view and study the equivalence of the two problems and evidence new ideas for the generation of new cryptographic functions. Additionally, two other cryptographic functions, the Double and Multiple Discrete Logarithm are considered. These functions are important for applications such as group signature, e-voting and others, and interpolation approaches to tackle them were recently tested. We extend the employment of matrices also for the representation of the Double and Multiple Discrete Logarithm.

References

[1] L. Adleman, A subexponential algorithm for the Discrete Logarithm problem with application to cryptography, In *Proc. 20th IEEE Found. Comp. Sci. Symp.*, (1979), 55–60.

[2] S. Brands, An efficient off-line electronic cash system based on the representation problem, In *Centrum voor Wiskunde en Informatica (CWI)*, **246**(77), (1993).

[3] S. Brands, Electronic cash systems based on the representation problem in groups of prime order, In *Proc. of Crypto '93*, (1993), 1–15.

[4] D. Coppersmith and I. Shparlinski, On polynomial approximation of the Discrete Logarithm and the Diffie-Hellman mapping, *J. Crypt.*, **13**(3), (2000), 339–360.

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

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

[7] E.C. Laskari, G.C. Meletiou and M.N. Vrahatis, Aitken and Neville inverse interpolation methods over finite fields, *Applied Numerical Analysis and Computational Mathematics*, **2**(1), (2005), 100–107.

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

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

[10] A. Miyaji and K. Umeda, A fully-functional group signature scheme over only known-order group, *LNCS*, **3089**, (2004), 164–179.

[11] G. Mullen and D. White, A polynomial representation for logarithms in GF(q), *A.A.E.C.C.*, **3**, (1992), 75–79.

[12] A. Odlyzko, Discrete Logarithms in finite fields and their cryptographic significance, In *Theory and Application of Cryptographic Techniques*, (1984), 224–314.

[13] J. Pollard, The fast Fourier transform in a finite field, *Math. Comput.*, **25**, (1971), 365–374.

[14] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, **26**(1), (1983), 96–99.

[15] J. Rushanan, On the Vandermonde matrix, *Amer. Math. Monthly*, **96**(10), (1989), 921–924.

[16] B. Schoenmakers, A simple publicly verifiable secret sharing scheme and its application to electronic voting, *LNCS*, **1666**, (1999), 148–164.

[17] M. Stadler, Publicly Verifiable Secret Sharing, *LNCS*, **1070**, (1996), 190–199.

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

[19] A. Yamamura and K. Kurosawa, Generic algorithms and key agreement protocols based on group actions, In *Proc. 12th ISAAC*, (2001), 208–218.