Transformations of two cryptographic problems in terms of matrices *

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

[1]Computational Intelligence Laboratory, Department of Mathematics,
Univeristy of Patras, GR-26110 Patras, Greece
[2]A.T.E.I. of Epirus, P.O. 110, GR-47100 Arta, Greece
[3]University of Patras Artificial Intelligence Research Center,
University of Patras, GR-26110 Patras, Greece

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 transformations for the Double and Multiple Discrete Logarithms is also presented.

1 Introduction

Public key cryptography [4, 13] has motivated a number of very hard computational problems during the past three decades [11, 13]. These problems are related to complexity, computational algebra, computational number theory, probability, logic and others. Two of these problems, namely the Discrete Logarithm problem and the Diffie-Hellman problem, are stated below.

(a) **The Discrete Logarithm Problem (DLP)** [1, 3, 11]. Let G be a finite cyclic group generated by g and $h \in G$. Compute an integer $z : g^z = h$ from h and g.

(b) **The Diffie-Hellman Problem (DHP)** [4]. Let G be a finite cyclic group generated by g and $h, f \in G$. Suppose further that $f = g^z, h = g^w$ for some integers z, w, such that $0 \leqslant z, w \leqslant |G| - 1$. Then compute g^{zw} from g, h, f.

The computational equivalence of the two problems has been proved only for some special cases [6] and it remains a very interesting and well known open problem.

Since functions from a finite field to itself can always be represented by polynomials (Lagrangian interpolation), both interpolation and approximation techniques have been applied to address the DLP and the DHP [3, 5]. Furthermore, various attempts to reformulate these cryptographic problems, have been performed. One of these attempts exploits matrices to formulate the DLP and the DHP [8]. In this paper, LU-decomposition is applied to a Vandermonde matrix to provide simple transformations of these two problems.

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.

*elena@math.upatras.gr, gmelet@teiep.gr, dtas@math.upatras.gr, vrahatis@math.upatras.gr

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, 10]. Matrix A represents a Discrete Fourier Transform [12].

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 $y \neq 0$ [17]. The question of computational equivalence of the DLP and DHP can be formulated by matrix computations of Equations (1) and (2).

Remark 1: Let M be a $m \times m$ matrix, and v, w be m-dimensional vectors. In general the computation of $v^\top M w$ requires $O(m^2)$ operations. In some special cases this cost can be reduced. For example the computation in $\mathbb{Z}_p$ of

$$(x, x^2, \ldots, x^{p-1})\, E\, (y, y^2, \ldots, y^{p-1})^\top, \tag{3}$$

where E is the Vandermonde matrix, $E = \{E_{ij}\}$, $1 \leqslant i, j \leqslant p-1$, with $E_{ij} = -i^{-j}$, and requires $O(\log_2(p))$ operations since the quantity in Eq. (3) coincides with the modular exponentiation $x^y \bmod p$ [7].

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

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

and

$$K(x, y) = -(x^{p-1}, x, x^2, \ldots, x^{p-2})W(y^{p-1}, y, \ldots, y^{p-2})^\top, \tag{5}$$

respectively. Next, following the approach of Newton polynomials described in [14], 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, matrix W can be factorized using LU-decomposition 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

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

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. (4) and (5), 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 2: 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 e-voting and secret sharing, deal with the double discrete logarithm problem, i.e., the discrete logarithm of the discrete logarithm [15, 16]. Matrix representations can be used for this problem too. As a first study, consider the case of the multiplicative group $\mathbb{Z}_p$, where α, b are generators of $\mathbb{Z}_p^*$. 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 $\mathbf{n} = (1, \dots, p-1)^\top$, $\mathbf{x} = (x, \dots, x^{p-1})^\top$ 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 above representations can be generalized for multiple applications of the discrete logarithmic function.

Next, we consider the Multiple Discrete Logarithm Problem (MDLP) also called Representation Problem (RP) in terms of matrices. The definition of the MDLP is given as follows. Let G be a finite group and $g_1, \dots, g_k$ elements of G. By $\langle g_t \rangle$, with $1 \leqslant t \leqslant k$, we denote the cyclic subgroup generated by g_t. In addition, we 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 $(z_1, \dots, z_k)$ consists of the z_t indices, with $0 \leqslant z_t \leqslant m_t - 1$, where m_t is the order of g_t. Then $(z_1, \dots, z_k)$ is the Multiple Discrete Logarithm of h with basis $(g_1, \dots, g_k)$. For applications of the MDLP or RP to e-cash, group signatures, key agreement protocols, see [2, 9, 18]. Symmetric Vandermonde matrices can also be used for the manipulation of the MDLP. For the case where $G = \mathbb{Z}_p^*$, we assume that $\mathbb{Z}_p^* = \langle \alpha_1 \rangle \times \cdots \times \langle \alpha_k \rangle$, where $\alpha_t \in \mathbb{Z}_p^*$, $\text{Order}(\alpha_t) = m_t$, $m_1 m_2 \cdots m_k = p-1$ 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 $(z_1, \dots, z_k)$, 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 $\{1, \dots, m_t\}$. Let $n_t = \frac{p-1}{m_t}$ and $\gcd(n_t, m_t) = 1$. It can be shown that z_t amounts to

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

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 $A_{ij} = -\alpha_t^{-n_t ij}$. The above representations can be generalized in the case of G being a subgroup of $\mathbb{Z}_p^*$ and in the case of a finite field of prime power order.

4 Epilogue

In this paper, new forms of the Discrete Logarithm and the Diffie-Hellman problem have been presented. These new forms include transformations using LU-decomposition for Vandermonde matrices through Newton polynomials. By these transformations, the equivalence of the two cryptographic problems can be viewed and studied using an alternative approach and ideas for the generation of new cryptographic functions can be derived. Lastly, a first study on matrix transformations for the Double and Multiple Discrete Logarithms is given.

References

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

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

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

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

[5] 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):100-107, 2005.

[6] U. Maurer and S. Wolf. The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms. *SIAM J. Comp.*, 28(5):1689–1721, 1999.

[7] G. Meletiou. A polynomial representation for exponents in $\mathbb{Z}_p$. *Bull. Greek Math. Soc.*, 34:59–63, 1992.

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

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

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

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

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

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

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

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

[16] M. Stadler, Publicly Verifiable Secret Sharing. *LNCS*, 1070:190–199, 1996.

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

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