

The optimized Diffie-Hellman key exchange using the graphical method

Huda Kadhim M. Aljader *

Ruma Kareem K. Ajeena [†]

Department of Mathematics

Education College for Pure Sciences

University of Babylon

Babil

Iraq

Abstract

In this paper, we describe a new contribution that uses the optimization problem to create a new version of the Diffie-Hellman key exchange (DHKE). The proposed version depended on the optimized discrete logarithm functions (ODLFs) that are given as a new definition in this work. A graphical method considers a fundamental tool to compute a shared secret key (SSK) in the proposed optimized Diffie-Hellman key exchange (ODHKE). The ODHKE is a more secure protocol for computing the SSK in comparison with the original DHKE.

Subject Classification: 11T71, 14G50, 49-xx.

Keywords: Cryptography, Optimization problem, Graphical method, ODHKE, ODLFs, Security.

1. Introduction

Many specializations in mathematics, especially graph theory and number theory, have been connected to the design of some encryption schemes [1-5].

One of the key agreement procedures established by Diffie and Hellman in 1976 is the Diffie-Hellman key exchange (DHKE). The goal is to be able to compute a shared secret key by two users which can be used

* E-mail: huda.kadom.pure347@student.uobabylon.edu.iq

(Corresponding Author)

[†] E-mail: pure.rume.k@uobabylon.edu.iq

to encrypt plaintext [6]. Many researchers introduced several research works to give different versions to improve this protocol. Recently, in 2017, Aryan et. al. [7] presented a study to obtain a stronger secret key through the extension of Diffie–Hellman protocol. In 2018, W. Jirakitpuwapat1 and P. Kumam [8] modified the key of DHKE by using the maximal abelian subgroup of automorphism of the group. In 2020, Nils Maurer et. al. [10], investigated the methods of authentication and key agreement for L-band digital aeronautical communication system (LDACS). In 2022, C. Gupta1 and N. Reddy [11] presented merging the RSA cryptosystem with the DHKE to prevent the MITM attack. In this work, a new version of DHKE is proposed based on the proposed hard mathematical problem which is ODLF. The work includes the main points: The proposed ODHKE protocol is discussed in Section 2. Section 3 explains the ODHKE protocol through a study case with a small prime number p . Furthermore, the ODHKE security considerations are specified in Section 4. Finally, in Section 5, the conclusions are drawn.

2. The Optimized Diffie-Hellman Key Exchange

A new version of the DHKE is proposed in this work. This version relies on the new optimization problem that is constructed based on the optimized discrete logarithm functions (ODLFs) that are described in the next specification.

Definition 2.1: Let g be a generator element of a prime field F_p and let h be a nonzero element of F_p . The ODLF is a function to find the exponent $a_1x_1 + a_2x_2$ such that:

$$\max(\text{or min}) g^{a_1x_1 + a_2x_2} \equiv h \pmod{p},$$

where $a_1x_1 + a_2x_2$ is a bivariate function with $a_1, a_2 \in F_p$ and the integers $x_1, x_2 \geq 0$.

The Optimized Diffie-Hellman Key Exchange (ODHKE) is explained as follows. With public domain parameters, which are a large prime p and a generator element g of a prime field F_p , Alice and Bob choose their secret keys $a = a_1x_1 + a_2x_2$ and $b = b_1x_1 + b_2x_2$ respectively. They use their shared secret constraints that are computed using the original DHKE [9] which are given by:

$$\begin{aligned}
c_{11}x_1 + c_{12}x_2 &\leq s_1 \\
c_{21}x_1 + c_{22}x_2 &\leq s_2 \\
&\vdots \\
c_{1n}x_1 + c_{1n}x_2 &\leq s_n \\
x_1, x_2 &\geq 0
\end{aligned}$$

The optimized DLF here is applied to the graphical method. Alice and Bob used their discrete logarithm objective functions:

$$\max A \equiv g^{a_1x_1 + a_2x_2} \pmod{p} \text{ and } \max B \equiv g^{b_1x_1 + b_2x_2} \pmod{p},$$

Respectively with the same shared secret constraint $c_{11}x_1 + c_{12}x_2 = s_1$ to find two points P_1 and P_2 that are computed supposing $x_1 = 0$ to get $x_2 = s_1/c_{12} = t_1$ and if $x_2 = 0$ then $x_1 = s_1/c_{11} = t_2$, so the points $P_1 = (0, t_1)$ and $P_2 = (t_2, 0)$ respectively. Similar computations are done with second, and third constraints and so on. There is a line L_1 pass through the points P_1 and P_2 that result in the first constraint. Also, a line L_2 passing through two points resulted based on the second constraint. Similarly, some lines pass through all other points that are resulted from other constraints. The intersection between these lines determines the region of the feasible solutions as shown in Figure 1. The intersection point D is computed. Based on the points that determine the shadow region which is a

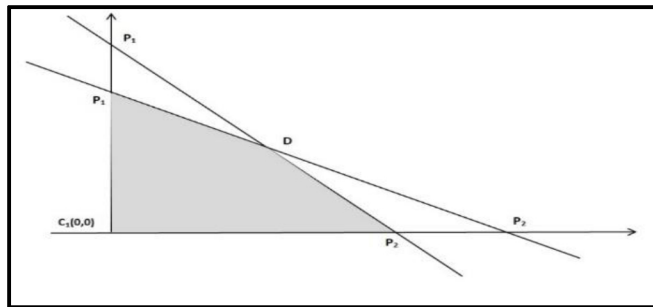


Figure 1

The region of the feasible solutions is based on intersection point D .

Region of the feasible solutions, Alice and Bob can compute their public keys A and B . In other words, using the points P_1, D, P_2 and C , Alice can compute the value of her public key A that are corresponded to these points. The optimal value is determined based on the determination of the objective function, maximum or minimum. Bob, in a similar way, uses

the same points of the feasible region to compute the values of his public key B . The optimal value of B is determined. After the computations of the keys A and B , Alice sends A to Bob and Bob sends B to Alice. Now, Alice computes A' and shared secret key by:

$A' \equiv B^{a_1x_1+a_2x_2} \pmod{p}$. Similarly, Bob computes his shared secret key $B' \equiv A^{b_1x_1+b_2x_2} \pmod{p}$. So, the shared secret key between Alice and Bob is

$$A' \pmod{p} \equiv B' \pmod{p}.$$

3. Study Case of Optimized Diffie-Hellman Key Exchange

This section discusses a study case of the proposed ODHKE as follows. Let $p = 71$ be a prime number. Suppose $g = 7$ is a generator element over F_{71} . Alice chooses her secret key $a = 5x_1 + 7x_2$ and Bob chooses his secret key $b = 3x_1 + x_2$. They use their shared secret constraints that are given by

$$2x_1 + 3x_2 \leq 18,$$

$$x_1 + x_2 \leq 8,$$

$$x_2 \leq 4,$$

$$x_1, x_2 \geq 0.$$

The proposed optimized Diffie-Hellman key exchange using the graphical method is discussed as follows. Alice and Bob compute her and his public keys A and B by using the discrete logarithm objective functions

$$\max A \equiv g^{5x_1+7x_2} \pmod{71} \text{ and } \max B \equiv g^{3x_1+x_2} \pmod{71},$$

Respectively with the same shared secret constraints. Both of them use the first constraint to find two points, so if $x_1 = 0$ then $2x_1 + 3x_2 = 18$ results $x_2 = 6$, so $P_1 = (0, 6)$ and if $x_2 = 0$ then $x_1 = 0$, therefore a resulted point is $P_2 = (9, 0)$. Now, with the second constraint $x_1 + x_2 = 8$, if $x_1 = 0$ then $P_1 = (0, 8)$ and if $x_2 = 0$ then $x_1 = 8$, therefore, $P_2 = (8, 0)$. With two resulted points from the first constraint, there is a line L_1 crossing through them. Similarly, line L_2 passes through the other two points $(0, 8)$ and $(8, 0)$. And a line L_3 pass through a point $(0, 4)$ that is resulted from a third constraint $x_4 \leq 4$ with $x_1 = 0$. The intersection between these lines determines the region of the feasible solutions as shown in Figure 2.

The intersection point D is computed by:

$$\left. \begin{array}{l} 2x_1 + 3x_2 = 18 \\ x_1 + x_2 = 8 \end{array} \right\} \times 2 = \left. \begin{array}{l} 2x_1 + 3x_2 = 18 \\ -2x_1 + 2x_2 = -16 \end{array} \right\}. \text{ So, } x_2 = 2 \text{ and } x_1 = 6.$$

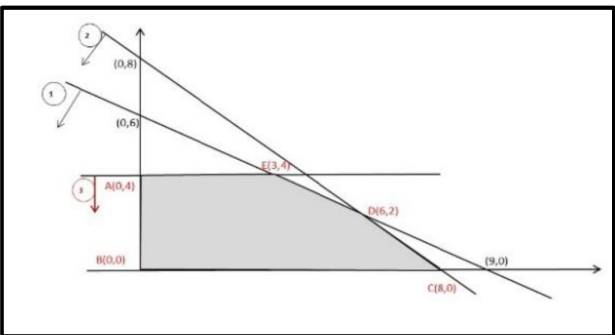


Figure 2

The region of the feasible solutions based on intersection points
 $D = (6, 2)$ and $E = (3, 4)$.

Thus, the intersection point $D = (6, 2)$ as shown in Figure 1. Another intersection point E should be computed. This computing is done as follows. Based on the substitution of the third constraint in first one, it can set $2x_1 + 3(4) = 18$. The value of $x_1 = 3$. The second intersection point $E = (3, 4)$. Based on the points that determines the region of feasible solutions, Alice and Bob can compute their public keys A and B as shown in Table 1. So, $A \equiv 44 \pmod{71}$ with a point $(3, 4)$ and $B \equiv 58 \pmod{71}$ with a point $(0, 4)$. Alice sends A to Bob and Bob sends B to Alice. Now, Alice compute her shared secret key A' by $A' \equiv B^{5x_1 + 7x_2} \pmod{71} \equiv 6 \pmod{71}$. Now, Bob computes his shared secret key B' by $B' \equiv A^{3x_1 + x_2} \pmod{71} \equiv 6 \pmod{71}$. So, the shared secret key between Alice and Bob is $A' \pmod{71} \equiv B' \pmod{71} \equiv 6 \pmod{71}$.

Table 1

Alice's and Bob's public keys A and B .

Point	$A \equiv g^{5x_1 + 7x_2} \pmod{71}$	Point	$B \equiv g^{3x_1 + x_2} \pmod{71}$
$A=(0,4)$ $B=(0,0)$ $C=(8,0)$ $D=(6,2)$ $E=(3,4)$	$5 \ 1 \ 20 \ 24 \ 44 \rightarrow$ optimal value	$A=(0,4)$ $B=(0,0)$ $C=(8,0)$ $D=(6,2)$ $E=(3,4)$	$58 \rightarrow$ optimal value $1 \ 16 \ 37 \ 28$

4. The Security Considerations on the ODHKE

The security considerations of the new proposed ODHKE are determined based on the hard computation of the ODLFs. In comparison

with the original DHKE which is dependent on the DLP, the proposed version is more secure since it is dependent on the possibilities to compute the exponent $a_1x_1+a_2x_2$ which represents the ODLF. Many cases need to guess to compute the correct $a_1x_1+a_2x_2$. In other words, the probability to choose a_1 is $1/(p-1)$ and similarly for choosing a_2 , x_1 , and x_2 , since these parameters are chosen from the range $[1, p-1]$, where p is a large prime number. So, it is more difficult to determine the value of ODLF.

5. Conclusions

A new version of DHKE based on the new computation of the hardness problem, which is ODLF, is proposed in this work. Computing the SSK in the proposed ODHKE protocol is done by employing the graphical method. The new computational result is discussed throughout the study case. The security considerations of the proposed ODHKE are determined. The ODHKE protocol is more secure for communication compared with the original DHKE protocol.

References

- [1] Ajeena, Ruma Kareem K. "The Graph and its Role for Speeding up the Elliptic Scalar Multiplication Algorithms." 2019 2nd International Conference on Engineering Technology and its Applications (IICETA). IEEE (2019).
- [2] Ajeena, Ruma Kareem K. "The soft graphic integer sub-decomposition method for elliptic scalar multiplication." *Journal of Discrete Mathematical Sciences and Cryptography* 24.6, 1751-1765 (2021).
- [3] Aljamaly, Karrar Taher R., and Ruma Kareem K. Ajeena. "The elliptic scalar multiplication graph and its application in elliptic curve cryptography." *Journal of Discrete Mathematical Sciences and Cryptography* 24.6, 1793-1807 (2021).
- [4] Aljamaly, Karrar Taher R., and Ruma Kareem K. Ajeena. "Undirected Complete Graph to Design New Public Key Cryptosystem." *Journal of Physics: Conference Series*, IOP Publishing, Vol. 1897. No. 1. (2021).
- [5] Hashim, Hashim Madlool, and Ruma Kareem K. Ajeena. "The Computational Complexity of the Elliptic Curve Factorization Algorithm over Real Field." *Journal of Physics: Conference Series*, IOP Publishing, Vol. 1897. No. 1. (2021).

- [6] Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography." *Secure communications and asymmetric cryptosystems. Routledge*, 143-180 (2019).
- [7] Kumar, Chaithanya, and PM Durai Raj Vincent. "Enhanced diffie-hellman algorithm for reliable key exchange." *IOP conference series: materials science and engineering, IOP Publishing*, Vol. 263. No. 4. (2017).
- [8] Jirakitpuwapat, Wachirapong, and Poom Kumam. "The generalized Diffie-Hellman key exchange protocol on groups." *International Econometric Conference of Vietnam. Springer, Cham* (2018).
- [9] Hoffstein, Jeffrey, et. al. *An introduction to mathematical cryptography*, New York: springer, Vol. 1. (2008).
- [10] Maurer, Nils, et. al. "Comparing different Diffie-Hellman key exchange flavors for LDACS." *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC). IEEE* (2020).
- [11] Gupta, Chiradeep, and NV Subba Reddy. "Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography." *Journal of Physics: Conference Series, IOP Publishing*, Vol. 2161. No. 1. (2022).

Received March, 2022

Revised April, 2022