

A more secure new version of the encryption scheme

Banen Najah Abass *

*Department of Mathematics
Faculty of Education for Girls
University of Kufa
Kufa 540011
Al Najaf
Iraq*

Hassan R. Yassein [†]

*Department of Mathematics
College of Education
University of Al-Qadisiyah
Al-Qadisiyah
Iraq*

Abstract

Many problems have arisen due to our reliance on exchanging data via insecure media, the most important of which is the penetration of that data by unauthorized parties, which requires securing it through highly secure encryption systems while continuing to develop those systems. In this research, we introduced a highly secure public key encryption system that uses secure key exchange using the Diffie-Hellman algorithm.

Subject Classification: 94A60, 68P25.

Keywords: Diffie-Hellman, Key exchange, Public key, Security of key.

1. Introduction

The rapid expansion of communication networks in the modern world is largely attributable to the proliferation of internet-based systems. Therefore, security is essential for protecting communication data from online threats. In

* ORCID-ID: 0009-0006-5272-6868

† ORCID-ID: 0000-0002-6788-0247

* E-mail: Banenn.alkuzai@uokufa.edu.iq (Corresponding Author)

† E-mail: hassan.yaseen@qu.edu.iq

addition, a high degree of security is necessary for some applications since they deal with very sensitive data, so encryption appears to protect that data.

In 1976, Diffie-Hellman proposed a key exchange method; they also predicted that cracking their technique would be as difficult as solving discrete logarithms [8]. In 1989, Den Boer stated that there was no existing technique that could effectively address the issue of distinct records during the probability phase. Therefore, when $P - 1$ transactions are smooth or when there are priorities that meet this requirement, a multi-border algorithm exists that can solve the separate logarithm problem [6].

Citing Hoffstein et al., who first proposed a private key cryptosystem, NTRU was originally developed in 1998 using the ring of truncated polynomials [9]. In 2003, Pearson et al. studied the utilisation of generalisations of Diffie-Hellman issues in the development of cryptographic methods for practical applications [4]. In 2017, Escala et al. presented a fresh algebraic framework for studying and generalizing decisional assumptions similar to Diffie-Hellman. This framework lets them make arguments about the examination of security and applications solely through the lens of algebraic properties [7]. NTRU and some improvements were based on a truncated polynomial ring, and some of its improvements were based on changing the algebraic structure, the mathematical structure, or both [1-3, 11, 12, 14, 15, 17, 18]. Over the years, many researchers have presented new encryption methods based on algebraic or mathematical structures [5, 10, 13, 16, 19-22]. In this paper, we present a new encryption method using Diffie-Hellman, which is considered highly secure.

2. Diffie Hellman Key Exchange

Diffie and Hellman proposed the key exchange (DH) algorithm, which is a method for exchanging encryption keys between two parties in the public communications channel in a secure manner. No keys are traded explicitly but are calculated jointly by both parties. Table 1 shows a summary of the Diffie-Hellman algorithm.

Table 1
Diffie-Hellman key exchange

Create the public parameters	
We select and propagate as public parameters a (large) prime number p and an integer g that has a large prime order in F_p^*	
Private computations	
Alice Bob	
Select a secret integer a Compute $A \equiv g^a \pmod{p}$	Select a secret integer b Compute $B \equiv g^b \pmod{p}$
Public exchange of values	
Bob receives A from Alice A	
B Alice receives B from Bob	

Private computations Alice Bob	
Compute the number $\mathcal{B}^a \pmod{p}$	Compute the number $\mathcal{A}^b \pmod{p}$
The shared secret value is $\mathcal{B}^a \equiv (\mathcal{g}^b)^a \equiv \mathcal{g}^{ab} \equiv (\mathcal{g}^a)^b \equiv \mathcal{A}^b \pmod{p}$	

3. DHBH Public Key

New public keys are introduced in this section of encryption called DHBH by applying the Diffie-Hellman method for exchanging keys with the same parameters in addition to prime p . This, like other systems, consists of three phases, which are as follows:

I. Key Generation

At this phase, both the sender (Bob) and the recipient (Alice) generate public keys, which are shared between them through the following steps:

- Bob chooses private keys a, b and Alice chooses private keys c, d , such that $1 \leq a, b, c, d \leq p - 2$
- Bob calculates the public key $\mathcal{A} = \mathcal{g}^a \pmod{p}$, $\mathcal{B} = \mathcal{g}^b \pmod{p}$ and Alice calculates
- $\mathcal{C} = \mathcal{g}^c \pmod{p}$, $\mathcal{D} = \mathcal{g}^d \pmod{p}$
- Bob and Alice share the public keys $\mathcal{A}, \mathcal{B}, \mathcal{C}$, and $\mathcal{D}$ between them.
- Bob calculates $\mathcal{C}^a = \mathcal{g}^{ac} \pmod{p}$, $\mathcal{D}^b = \mathcal{g}^{dp} \pmod{p}$ and Alice calculates
- $\mathcal{A}^c = \mathcal{g}^{ac} \pmod{p}$ and $\mathcal{B}^d = \mathcal{g}^{bd} \pmod{p}$, such that $\mathcal{A}^c = (\mathcal{g}^a)^c = \mathcal{C}^a$ and $\mathcal{D}^b = (\mathcal{g}^d)^b = \mathcal{B}^d$.

II. Encryption

In order for the message $\mathcal{M}$ to be encrypted, Bob uses the following formula:

$$E = \mathcal{A}^c \mathcal{M} \mathcal{B}^d \pmod{p}.$$

III. Decryption

For the recipient (Alice) in order to recover the initial message $\mathcal{M}$ from the encrypted text E , she must follow the following steps:

Multiply E by $(\mathcal{C}^a)^{-1}$ and $(\mathcal{B}^d)^{-1}$ from left and right, respectively.

$$\begin{aligned} (\mathcal{C}^a)^{-1} E (\mathcal{B}^d)^{-1} &= (\mathcal{A}^c)^{-1} E (\mathcal{B}^d)^{-1} \pmod{p} \\ &= (\mathcal{A}^c)^{-1} \mathcal{A}^c \mathcal{M} \mathcal{B}^d (\mathcal{B}^d)^{-1} \pmod{p} = \mathcal{M} \pmod{p}. \end{aligned}$$

To illustrate the above-mentioned phases, we review the example below:

Take $p = 157$, $a = 5$, $b = 7$, $c = 8$, $d = 9$ and $\mathcal{g} = 15$.

Key generation:

Bob choose $a = 5, b = 7$ and Alice choose $c = 8, d = 9$ We calculate $\mathcal{A}, \mathcal{B}, \mathcal{C}$, and $\mathcal{D}$,

Bob calculates $\mathcal{A} = 15^5 \pmod{157} = 123 \pmod{157}$,

$B = 15^7 \pmod{157} = 43 \pmod{157}$,
 Alice calculates $C = 15^8 \pmod{157} = 17 \pmod{157}$,
 $D = 15^9 \pmod{157} = 98 \pmod{157}$,
 Bob calculates $C^5 = 106 \pmod{157}$, $D^7 = 32 \pmod{157}$,
 Alice calculates $A^8 = 106 \pmod{157}$ lculates, $B^9 = 32 \pmod{157}$.

Encryption:

$$E = A^c M B^d \pmod{p} = 17 \times 106 \times 32 \pmod{157} = 45 \pmod{157}.$$

Decryption:

$$(C^a)^{-1} E (D^b)^{-1} = (106)^{-1} \times 45 \times (32)^{-1} \pmod{157} = 40 \times 45 \times 54 \pmod{157} = 17 = M.$$

4. Security Analysis

Since the DHBH method uses the Diffie-Hellman key exchange technique; the security of this algorithm is dependent on the discrete logarithm issue as it relates to the private keys. a, b, c , and d for the public keys $A = g^a \pmod{p}$, $B = g^b \pmod{p}$, $C = g^c \pmod{p}$, and $D = g^d \pmod{p}$ respectively, which determine the security of the key.

5. Conclusion

Due to the importance of encrypting data to protect it from hackers, DHBH encryption was introduced based on Diffie-Hellman, which makes this encryption an important method in many applications that require high security. It is also difficult for hackers to penetrate and access it as a result of using more private keys, which increases the complexity of the complexity of the discrete logarithm problem.

References

- [1] A. A. Abidalzahra and H. R. Yassein, "Proposed Development of NTRU Encryption," *Int. J. Math. Comput. Sci.*, vol. 19, no. 3, pp. 715-719 (2024).
- [2] H. H. Abo-Alsood and H. R. Yassein, "QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra," *J. Phys. Conf. Ser.*, vol. 1999, no. 1, p. 012097 (2021). [Online]. Available: <https://doi.org/10.1088/1742-6596/1999/1/012097>.
- [3] H. H. Abo-Alsood and H. R. Yassein, "Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security," *AIP Conf. Proc.*, vol. 2386, no. 1, p. 060006 (2022). [Online]. Available: <http://dx.doi.org/10.1063/5.0067033>.

- [4] E. Bresson, O. Chevassut, and D. Pointcheval, "The Group Diffie-Hellman Problems," in *Selected Areas in Cryptography*, K. Nyberg and H. Heys, Eds., Berlin, Germany: Springer, pp. 325-338 (2003).
- [5] A. Chillali and M. Sahmoudi, "SCC-Cryptosystem on an algebraic closure ring," *J. Discrete Math. Sci. Cryptogr.*, vol. 23, no. 8, pp. 1475-1485 (2020). [Online]. Available: <https://doi.org/10.1080/09720529.2019.1624338>.
- [6] B. Den Boer, "Diffie-Hellman is as strong as discrete log for certain primes," in *Conf. Theory and Appl. Cryptogr.*, Springer, pp. 530-539 (1988).
- [7] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar, "An algebraic framework for Diffie-Hellman assumptions," *J. Cryptol.*, vol. 30, pp. 242-288 (2017). [Online]. Available: <https://doi.org/10.1007/s00145-015-9220-6>.
- [8] M. Hellman and W. Diffie, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644-654 (1976). [Online]. Available: <https://doi.org/10.1109/TIT.1976.1055638>.
- [9] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*, J. P. Buhler, Ed., Berlin, Germany: Springer, pp. 267-288 (1998). [Online]. Available: <https://doi.org/10.1007/BFb0054868>.
- [10] B. Imine, N. Hadj-Said, and A. Ali-Pacha, "New McEliece cryptosystem based on non-permutation equivalent polar codes," *J. Discrete Math. Sci. Cryptogr.*, vol. 23, no. 8, pp. 1-12 (2021). [Online]. Available: <https://doi.org/10.1080/09720529.2021.1933706>.
- [11] S. H. Shahhadi and H. R. Yassein, "NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra," *J. Phys. Conf. Ser.*, vol. 1999, no. 1, p. 012092 (2021). [Online]. Available: <http://dx.doi.org/10.1088/1742-6596/1999/1/012092>.
- [12] S. H. Shahhadi and H. R. Yassein, "An innovative tripternion algebra for designing NTRU-like cryptosystem with high security," *AIP Conf. Proc.*, vol. 2386, no. 1, p. 060006 (2022). [Online]. Available: <http://dx.doi.org/10.1063/5.0067023>.
- [13] D. K. Verma, M. Rani, R. K. Tyagi, and B. B. Sagar, "Baptista chaotic cryptosystem based on alternate superior dynamic lookup table," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 8, pp. 1383-1392 (2019). [Online]. Available: <https://doi.org/10.1080/09720529.2019.1692446>.

- [14] H. Yassein, N. Al-Saidi, and A. Almosawi, "A multi-dimensional algebra for designing an improved NTRU cryptosystem," *Eurasian J. Math. Comput. Appl.*, vol. 8, no. 4, pp. 97-107 (2020). [Online]. Available: <https://doi.org/10.1063/5.0067023>.
- [15] H. R. Yassein, A. A. Abidalzahra, and N. M. Al-Saidi, "A new design of NTRU encryption with high security and performance level," *AIP Conf. Proc.*, vol. 2334, no. 1, p. 080005 (2021). [Online]. Available: <https://doi.org/10.1063/5.0042312>.
- [16] H. R. Yassein, N. M. Al-Saidi, and A. K. Farhan, "A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 2, pp. 523-542 (2022). [Online]. Available: <https://doi.org/10.1080/09720529.2020.1741218>.
- [17] H. R. Yassein and H. A. Ali, "SQNTRU: New Public Key Encryption," *Int. J. Math. Comput. Sci.*, vol. 18, no. 3, pp. 381-385 (2023).
- [18] H. R. Yassein, H. N. Zaky, H. H. Abo-Alsoo, I. A. Mageed, and W. I. El-Sobky, "QuiTRU: Design Secure Variant of NtruEncrypt Via a New Multi-Dimensional Algebra," *Appl. Math. Inform. Sci.*, vol. 17, no. 1, pp. 49-53 (2023). [Online]. Available: <http://dx.doi.org/10.18576/amis/paper>.
- [19] A. H. Alwan, "Small Intersection Graph of Subsemimodules of a Semimodule," *Commun. Combin. Cryptogr. Comput. Sci.*, vol. 2022, no. 1, pp. 15-22 (2022).
- [20] S. Ediza, M. Cancana, and M. R. Farahani, "Eccentric Connectivity and Connective Eccentricity Indices of Generalized Petersen Graphs," *Commun. Combin. Cryptogr. Comput. Sci.*, vol. 2021, no. 1, pp. 1-6 (2021).
- [21] R. Ponraj, S. Prabhu, and M. Sivakumar, "Pair Mean Cordial Labeling of Total Graph of Some Graphs and Prism Related Graphs," *Commun. Combin. Cryptogr. Comput. Sci.*, vol. 2024, no. 2, pp. 181-192 (2024).
- [22] F. O. Oduol and I. O. Okoth, "Counting vertices among all noncrossing trees by levels and degrees," *Commun. Combin. Cryptogr. Comput. Sci.*, vol. 2024, no. 2, pp. 193-212 (2024).

Received May, 2024