Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43) 3** : 1–5.
ISSN-0037-8712
doi:10.5269/bspm.79595

Design a Secure Public Key Cryptosystem Based on a New Key Exchange Protocol

Banen Najah Abass*, Hassan Rashed Yassein and Banen Wafaa Abdullah

ABSTRACT: Encryption is emerging as a vital weapon in the age of digital communications, playing a crucial role in protecting and securing data. Encryption allows us to balance security with legitimate access to information, enhancing user privacy and protecting sensitive data. The continued development of encryption technologies remains of great importance in meeting the continuing challenges of data security in a world increasingly dependent on the circulation of digital information. In this work, we presented a highly secure cryptosystem by introducing a new protocol called poly Diffie-Hellman key exchange instead of Diffie-Hellman key exchange.

Key Words: Diffie-Hellman, key exchange, key security, message security.

Contents

1. Introduction

In asymmetric cryptosystem, the sender uses the public key to encrypt the data, but the recipient uses the private key to decrypt it. Because the two keys are different from each other, the public key can be shared securely without affecting the security of the private key. Every asymmetric pair of keys is unique, ensuring that messages encrypted with the public key can only be read by the person who has the corresponding private key, which means that everyone can encrypt a message with the public key, but that message cannot be decrypted only by using the recipient's secret key. In 1976, Diffie and Helmelin presented a protocol that allows two parties to create a shared key on an unsecured chat channel while keeping each party's private keys secret based on the discrete logarithm problem [1]. This protocol was used in the Al-Gamal public key cryptosystem [2]. In 1978, Rivest and others proposed the RSA algorithm, based on factorization integer numbers, which is widely used in cryptography in secure communications, data security, and financial transactions over the Internet [3].

Hoffstein and others presented in 1996 a number theory research unit cryptosystem (NTRU) public key cryptosystem depends on a ring of truncated polynomial with degree $N-1$, denoted by $\mathcal{Z}[x]/\left(x^N-1\right)$. Its plays an important role in data encryption because it is capable of offering sufficient security levels [4]. In 2003, Bresson and others studied generalizations of Diffie-Hellman protocol that were used to build encryption systems by showing the relationships between DDH, CDH, GDDH, and GCDH problems [5]. In 2017, Escala and others present a new algebraic framework for generalizing and analyzing decisional assumptions such as Diffie-Hellman [6].

* Corresponding author.
2010 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted October 16, 2025. Published December 20, 2025

Based on the truncated polynomial ring, many researchers presented encryption methods to improve NTRU by changing the shape of the elements through new rings with a different structure, which resulted in high security and efficiency, making it suitable for many applications that require these features [7,8,9,10,11,12,13,14,15,16]. Abaas and Yaseein presented a comparison between the Polynomial RSA, NTRU, and PH-RSA systems in terms of security [17]. They also proposed a development of a modified RSA key encryption called TPRSA, which via polynomials and algebra of Tri-Cartesian [18]. They also presented a highly secure public key system using the Diffie-Hellman algorithm for secure key exchange [19]. In this work, a new key exchange protocol is constructed, which called poly Diffie Hellman key exchange to construct a new cryptosystem called Poly-DHBH public key.

2. Diffie Hellman Key Exchange

Diffie and Helman introduced an algorithm that changes the key, which is considered a safe way to exchange keys between the sender and the recipient via a public communication channel [1]. Table 1 presents a synopsis of the Diffie-Hellman algorithm.

Table 1: Diffie-Hellman key exchange

Public parameter generation	
A trusted party selects and publishes an integer g with prime order (large) in F_q^* and a (large) prime q	
Private computations	
First party	Second party
Select a secret integer a Compute $\mathcal{A} \equiv g^a \ (mod\ q)$	Select a secret integer b Compute $\mathcal{B} \equiv g^b \ (mod\ q)$
Public exchange of values First part sends $\mathcal{A}$ to second part $\longrightarrow \mathcal{A}$ $\mathcal{B} \leftarrow$ Second party sends $\mathcal{B}$ to first party	
More private computations	
First party	Second party
Compute the number $\mathcal{B}^a \ (mod\ q)$	Compute the number $\mathcal{A}^b \ (mod\ q)$
The shared secret value is $\mathcal{B}^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv \mathcal{A}^b \ (mod\ q)$	

3. Poly Diffie Hellman Key Exchange

In this section, for the participation of key between two parties, through an unsafe communication means, the Deffie Hellman algorithm is used to exchange public keys, depending on the hard of discrete logarithm problem. To increase the level of the key security to the exchange, we have developed the Diffie Hellman algorithm by replacing the integer number g with a polynomial $g(x)$ that belongs to the ring $\mathcal{Z}_q[x] / \left(x^N - 1\right)$ as in the following scheme.

Table 2: Poly Diffie-Hellman key exchange

Public parameter generation	
A trusted party selects and publishes a truncated polynomial $g(x)$ having large prime order in ring $Z_q[x] / \left(x^N - 1\right)$ and a (large) prime q	
Private computations	
First party	Second party
Select a secret integer $1 \leq n_1 \leq q-2$ Compute $\mathcal{A} \equiv g(x)^{n_1} \ (mod\ q)$	Select a secret integer $1 \leq n_2 \leq q-2$ Compute $\mathcal{B} \equiv g(x)^{n_2} \ (mod\ q)$
Public exchange of values First part sends $\mathcal{A}$ to second part $\longrightarrow \mathcal{A}$ $\mathcal{B} \leftarrow$ Second party sends $\mathcal{B}$ to first party	
More private computations	
First party	Second party
Compute the number $\mathcal{B}^{n_1} \ (mod\ q)$	Compute the number $\mathcal{A}^{n_2} \ (mod\ q)$
The shared secret value is $\mathcal{B}^{n_1} \ (mod\ q) \equiv (g(x)^{n_2})^{n_1} \equiv g(x)^{n_2 n_1} \equiv (g(x)^{n_1})^{n_2} \equiv \mathcal{A}^{n_2} \ (mod\ q)$	

4. Poly-DHBH Public Key

In this section, we offer a novel public key encryption that depending on the poly Diffie-Hellman key exchange algorithm which called Poly-DHBH. The public parameters in this method are the positive integers N, p, and q suth that $gcd(p,\ q) = 1$, and the sets $\mathfrak{S}$ and $\mathfrak{M}$ which are defined as follows:

1. $\mathfrak{S} = \{g(x) \in \mathcal{Z}[x] / \left(x^N - 1\right)$ such that the number of coefficients equal to 1 is one more than the number of coefficients equal to -1, and the rest are equal to zero$\}$
2. $\mathfrak{M} = \{M \mid M$ has coefficients lying between $-p/2$ and $p/2\}$.

This method, as in the previous methods, goes through three phases, which are described as follows.

4.1. Key generation

At this phase, first party (recipient) generates public key through the following steps:

1. Selects an integer n_1 (private key) such that $1 \leq n_1 \leq q - 2$.
2. Selects polynomial $g(x) \in \mathfrak{S}$.
3. Computes $h_1(x) \equiv g(x)^{n_1} (mod\ q)$.
4. Sends public key $h_1(x)$ to second part (sender).

4.2. Encryption

To encrypt the original message $M \in \mathfrak{M}$, second part performs the following steps:

1. Selects an integer n_2, n_3 (private keys) such that $1 \leq n_2, n_3 \leq q - 2$.
2. Computes the public key $h_2(x) \equiv g(x)^{n_2} (mod\ q)$.
3. Computes the public key $h_3(x) \equiv g(x)^{n_3} (mod\ q)$.
4. Convert the original massage M to the cipher text E by the formula: $E(x) \equiv M.\left(h_1(x)^{n_2}\right)^{-1} + ph_3(x)\ (mod\ q)$ with coefficients belong to $(-\frac{q}{2}, \frac{q}{2}]$.
5. Second part send $(E(x),\ h_2(x))$ to first party.

4.3. Decryption

For the recipient (first party) to recover the original message M from the encrypted text $E(x)$, she must follow the following steps:

1. Multiply $E(x)$ by $h_2(x)^{n_1}$ from left:

$$\begin{aligned} Eh_2(x)^{n_1} &\equiv M\left(h_1(x)^{n_2}\right)^{-1} h_2(x)^{n_1} + ph_3(x)h_2(x)^{n_1}\ (mod\ q) \\ &\equiv M\left(h_1(x)^{n_2}\right)^{-1} h_1(x)^{n_2} + ph_3\ (x)h_1(x)^{n_2}\ \ (mod\ q) \\ &\equiv M + ph_3\,(x)\,h_1\,(x)^{n_2}\ \ (mod\ q) \end{aligned}$$

2. Convert $E(x)h_1(x)^{n_2} (mod\ q)$ to $mod\ p$, therefore $E(x)h_1(x)^{n_2} \equiv M\ \ (mod\ p)$.

5. Security Analysis

Since the Poly-DHBH method relies on the poly Diffie-Hellman key exchange algorithm, its security depends on discrete logarithm problem through the private keys n_1 and n_2 for the public keys $h_1(x) = g(x)^{n_1}\ (mod\ q)$ and $h_2(x) = g(x)^{n_2}\ (mod\ q)$ respectively, which determine the key security, and n_3 for the public key $h_3(x) = g(x)^{n_3}\ (mod\ q)$ which determines the message security.

6. Conclusion

Poly-DHBH, which is based on poly Diffie-Hellman, was introduced in response to the need for data encryption to safeguard it against pirates. This encryption technique is crucial for numerous applications that demand a high level of security, and hackers find it challenging to access and breach them due to the use of polynomials rather than numbers, which further complicates separate logarithm problems.

References

1. W. Diffie and M. Hellman. New directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
2. B.D. Boer. Diffie–Hellman is as strong as discrete log for certain primes. In *Advances in Cryptology — CRYPTO'88*, pages 530–539, New York, 1990. Springer.
3. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
4. J. Hoffstein, J. Pipher, and J.H. Silverman. NTRU: A ring-based public key cryptosystem. *Algorithmic Number Theory*, 1423:267–288, 1998.
5. E. Bresson, O. Chevassut, and D. Pointcheval. The group Diffie–Hellman problems. *Selected Areas in Cryptography*, 2595:325–338, 2003.
6. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie–Hellman assumptions. *Journal of Cryptology*, 30:242–288, 2017.
7. H.R. Yassein, N.M. Al-Saidi, and A.K. Almosawi. A multi-dimensional algebra for designing an improved NTRU cryptosystem. *Eurasian Journal of Mathematical and Computer Applications*, 8(4):97–107, 2020.
8. H.R. Yassein, A.A. Abidalzahra, and N.M. Al-Saidi. A new design of NTRU encryption with high security and performance level. *AIP Conference Proceedings*, 2334:080005, 2021.
9. H.R. Yassein and S.H. Shahhadi. NTRsh: A new secure variant of NTRUEncrypt based on tripternion algebra. *Journal of Physics: Conference Series*, 1999:012092, 2021.
10. H.H. Abo-Alsood and H.R. Yassein. Design of an alternative NTRU encryption with high secure and efficient. *International Journal of Mathematics and Computer Science*, 16(4):1469–1477, 2021.
11. H.H. Abo-Alsood and H.R. Yassein. QOTRU: A new design of NTRU public key encryption via Qu-Octonion subalgebra. *Journal of Physics: Conference Series*, 1999(1):012097, 2021.
12. S.H. Shahhadi and H.R. Yassein. An innovative tripternion algebra for designing NTRU-like cryptosystem with high security. *AIP Conference Proceedings*, 2386(1):060009, 2022.
13. H.H. Abo-Alsood and H.R. Yassein. Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security. *AIP Conference Proceedings*, 2386(1):060006, 2022.
14. H.R. Yassein, H.N. Zaky, H.H. Abo-Alsoo, I.A. Mageed, and W.I. El-Sobky. QuiTRU: Design secure variant of NTRU-Encrypt via a new multi-dimensional algebra. *Applied Mathematics and Information Sciences*, 17(1):49–53, 2023.
15. H.R. Yassein and H.A. Ali. SQNTRU: New public key encryption. *International Journal of Mathematics and Computer Science*, 18(3):381–385, 2023.
16. A.A. Abidalzahra and H.R. Yassein. Proposed development of NTRU encryption. *International Journal of Mathematics and Computer Science*, 19(3):715–719, 2024.
17. B.N. Abass and H.R. Yassein. Comparison between NTRU, polynomial RSA, and PH-RSA. *E3S Web of Conferences*, 508:1–5, 2024.
18. B.N. Abass and H.R. Yassein. Design of an alternative to polynomial modified RSA algorithm. *International Journal of Mathematics and Computer Science*, 19(3):693–696, 2024.
19. B.N. Abass and H.R. Yassein. A more secure new version of the encryption scheme. *Journal of Discrete Mathematical Sciences and Cryptography*, 28(2):387–392, 2025.

Banen Najah Abass,
Department of Mathematics,
Faculty of Basic Education, University of Kufa
Iraq.
E-mail address: banenn.alkuzai@uokufa.edu.iq

and

Hassan Rashed Yassein,
Department of Mathematics,
Collage of Education, University of Al-Qadisiyah,
Iraq.
E-mail address: hassan.yaseen@qu.edu.iq

and

Banen Wafaa Abdullah,
Department of Mathematics,
Faculty of Basic Education, University of Kufa
Iraq.
E-mail address: banenw.alfatlawy@uokufa.edu.iq