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

(3s.) **v. 2026 (44) 11** : 1–6.
ISSN-0037-8712
doi:10.5269/bspm.82903

A New Public Key Cryptosystem Based on Developed Diffie-Hellman Algorithm

Fatimah H. Albakaa and Hassan Rashed Yassein*

ABSTRACT: Our current time is witnessing a very rapid development in the world of technology, which leads to the ease of inventing scientific computers and the ease of decrypting text between parties. Because of this remarkable development, we must increase the development of encryption methods and increase their security. In this research, we will present a new method called FA Polynomial Diffie-Hellman and symbolizes it FA$_{poly}$-DH, which is development of Diffie-Hellman of key exchange algorithm.

Keywords: Diffie-Hellman, polynomial Diffie-Hellman, security analysis.

Contents

1. Introduction

In 1976, Diffie and Hellman seminal work, new direction in cryptography depend on discrete logarithm problem [4]. After that, many public key cryptosystems have been created such as, in 1978, Rivest et al. proposed a new cryptosystem method is an implementation of a public key cryptosystem called RSA cryptosystem [6]. In 1985, ElGamal, introduces a new digital signature scheme together with an implementation Diffie-Hellman key exchange that depends on the difficulty of computing discrete logarithm problem. And is not yet proved that breaking the system is equivalent to computing discrete logarithm [5]. In 2025, Albakaa et al. introduced FA-algebra $FA = \left\{\lambda = \sum_{i=0}^{14} \lambda_i \vartheta_i : \lambda_i, \ldots, \lambda_{14} \in F,\ \vartheta_i = 1\right\}$ is a new 15- dimension vector space and applied on a new cryptosystem called FATRU [2]. Abass in 2024 worked on developing Diffie-Hellman in two ways. The first way by increasing the number of private keys chosen by both parties, and the second way was by replacing integers with polynomials belonging to ring $Z_q[x]/(x^N - 1)$ [1].

2. Diffie-Hellman

Let p be a prime number and g an integer. The Diffie–Hellman Problem (DHP) is the problem of computing the value of $g^{ab}\ (mod\ p)$ from the known values of $g^a\ (mod\ p)$ and $g^b (mod\ p)$ [4,3].

This common value is their exchanged key. The Diffie–Hellman key exchange algorithm is summarized in Table 1:

* Corresponding author.
2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted March 22, 2026. Published June 03, 2026.

Table 1: Diffie Hellman key exchange

A trusted party chooses and publishes a (large) prime p and an integer g having large Prime order in F_p^*	
Alice	Bob
Choose a secret integer a	Choose a secret integer b
Compute $A \equiv g^a \ (mod\ p)$	Compute $B \equiv g^b \ (mod\ p)$
Public exchange of values	
Alice sends A to Bob $\longrightarrow A$	
$B \leftarrow$ Bob sends B to Alice	
Compute the number $B^a \ (mod\ p)$	Compute the number $A^b \ (mod\ p)$
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \ (mod\ p)$	

3. FA Algebra

In this section, a new multidimensional FA algebra is defined as follows:
Let F be a field with $char(F) \neq 2$, and

$$FA = \left\{ \sum_{i=0}^{14} \lambda_i \vartheta_i | \lambda_0, \ldots, \lambda_{14} \in F, \vartheta_0 = 1 \right\}.$$

The operations addition $(+)$, multiplication $(*)$ and scalar multiplication $(\cdot)$ are defined as follows:
Suppose $u, \nu \in FA$ such that $u = \sum_{i=0}^{14} u_i \vartheta_i, \nu = \sum_{i=0}^{14} \nu_i \vartheta_i$, and a scalar $\alpha \ \in F$ then,

$$u + \nu = \sum_{i=0}^{14} u_i \vartheta_i + \sum_{i=0}^{14} \nu_i \vartheta_i = \sum_{i=0}^{14} (u_i + \kappa_i) \vartheta_i,$$

$$u * \nu = \sum_{i=0}^{14} u_i \vartheta_i * \sum_{i=0}^{14} \nu_i \vartheta_i = \sum_{i=0}^{14} (u_i v_i) \vartheta_i,$$

and

$$\alpha \cdot u = \alpha \cdot \left(\sum_{i=0}^{14} u_i \vartheta_i \right) = \sum_{i=0}^{14} (\alpha \lambda_i) \vartheta_i \text{ respectively.}$$

Then $(FA, +, \cdot)$ is a vector space with a basis $\{1, \vartheta_1, \vartheta_2, \ldots, \vartheta_{14}\}$.

Proposition 3.1. *A vector space $(FA, +, \cdot, *)$ is an algebra.*

Proof. Let $u, \nu, \omega \in FA$ and $\alpha \in F$ such that,

$$u = \sum_{i=0}^{14} u_i \vartheta_i, \nu = \sum_{i=0}^{14} \nu_i \vartheta_i, \omega = \sum_{i=0}^{14} \omega_i \vartheta_i$$

then

$$\begin{aligned} u * (\nu + \omega) &= \sum_{i=0}^{14} u_i \vartheta_i * \left(\sum_{i=0}^{14} \nu_i \vartheta_i + \sum_{i=0}^{14} \omega_i \vartheta_i \right) \\ &= \sum_{i=0}^{14} u_i \vartheta_i * \left(\sum_{i=0}^{14} (\nu_i + \omega_i) \vartheta_i \right) = \sum_{i=0}^{14} u_i (\nu_i + \omega_i) \vartheta_i \\ &= \sum_{i=0}^{14} (u_i \nu_i + u_i \omega_i) \vartheta_i = \sum_{i=0}^{14} (u_i \nu_i) \vartheta_i + \sum_{i=0}^{14} (u_i \nu_i) \vartheta_i \\ &= u * \nu + u * \omega. \end{aligned}$$

And

$$\begin{aligned}(u+\nu)*\omega &= \left(\sum_{i=0}^{14} u_i\vartheta_i + \sum_{i=0}^{14}\nu_i\vartheta_i\right) * \sum_{i=0}^{14}\omega_i\vartheta_i \\ &= \left(\sum_{i=0}^{14}\left(u_i+\nu_i\right)\vartheta_i\right) * \sum_{i=0}^{14}\omega_i\vartheta_i = \sum_{i=0}^{14}\left(\left(u_i+\nu_i\right)\omega_i\right)\vartheta_i \\ &= \sum_{i=0}^{14}\left(u_i\omega_i+\nu_i\omega_i\right)\vartheta_i = \sum_{i=0}^{14}\left(u_i\omega_i\right)\vartheta_i + \sum_{i=0}^{14}\left(\nu_i\omega_i\right)\vartheta_i \\ &= u*\omega + v*\omega.\end{aligned}$$

$$\begin{aligned}\alpha\cdot(u*\nu) &= \alpha\cdot\left(\sum_{i=0}^{14}u_i\vartheta_i * \sum_{i=0}^{14}\nu_i\vartheta_i\right) = \alpha\cdot\left(\sum_{i=0}^{14}\left(\lambda_i\nu_i\right)\vartheta_i\right) \\ &= \sum_{i=0}^{14}\alpha(\lambda_i\nu_i)\vartheta_i \ = \sum_{i=0}^{14}\left(\alpha\lambda_i\right)\nu_i\vartheta_i = (\alpha\cdot u)*\nu = u*(\alpha\cdot\nu).\end{aligned}$$

Therefore, FA is an algebra. □

Proposition 3.2. *Algebra $(FA,+,\cdot,*)$ is commutative and associative.*

Proof. Let u,ν and $\omega \in FA$ such that

$$u=\sum_{i=0}^{14}u_i\vartheta_i, \nu=\sum_{i=0}^{14}\nu_i\vartheta_i, \omega=\sum_{i=0}^{14}\omega_i\vartheta_i$$

then

1. $u*\nu=\sum_{i=0}^{14}u_i\beta_i*\sum_{i=0}^{14}\nu_i\vartheta_i=\sum_{i=0}^{14}\left(u_i\nu_i\right)\vartheta_i=\sum_{i=0}^{14}\left(\nu_iu_i\right)\vartheta_i=\nu*u.$ then FA is commutative.
2. $$\begin{aligned}(u*\nu)*\omega &= \left(\sum_{i=0}^{14}u_i\vartheta_i*\sum_{i=0}^{14}\nu_i\vartheta_i\right)*\sum_{i=0}^{14}\omega_i\vartheta_i \\ &= \sum_{i=0}^{14}\left(u_i\nu_i\right)\vartheta_i * \sum_{i=0}^{14}\omega_i\vartheta_i = \sum_{i=0}^{14}\left(\left(u_i\nu_i\right)\omega_i\right)\vartheta_i = \sum_{i=0}^{14}\left(u_i\left(\nu_i\omega_i\right)\right)\vartheta_i \\ &= \sum_{i=0}^{14}u_i\vartheta_i*\sum_{i=0}^{14}\left(\nu_i\omega_i\right)\vartheta_i = \sum_{i=0}^{14}u_i\vartheta_i*\left(\sum_{i=0}^{14}\nu_i\vartheta_i*\sum_{i=0}^{14}\omega_i\vartheta_i\right) \\ &= u*(v*\omega),\end{aligned}$$

   then FA is associative.

□

Remark 3.3.

1. *The identity element of FA algebra is* $1+\vartheta_1+\vartheta_2+\ldots+\vartheta_{14}$
2. *The inverse of* $u=\sum_{i=0}^{14}u_i\vartheta_i$ *equal to* $u_i^{-1}=\sum_{i=0}^{14}u_i^{-1}\vartheta_i$ *such that* $u_i\neq 0$ *for all* $i=0,\ldots,14$.

4. FA$_{poly}$-DH Cryptosystem

We have present the Diffie-Hellman algorithm in developer way, which is an insecure means of communication between two parties, the difficulty of which lies in finding the exponent of the discrete logarithm problem. The algorithm was developed to increase the level of security when exchanging keys by replacing integers with polynomials that fall within the algebra $FA = \left\{\lambda = \sum_{i=0}^{14} \lambda_i \vartheta_i : \lambda_i, \ldots, \lambda_{14} \in F, \vartheta_i = 1\right\}$.

4.1. Public Parameters

The FA$_{poly}$-DH cryptosystem depends on parameters (N, p, q) where N is a prime number and p, q are two coprime i.e. $gcd(p, q) = 1$, and q is much large than q. And it also depends on a sets $\mathfrak{f}$ and $\mathfrak{g} \in FA$-algebra which are defined in Table 2:

Table 2: Sets definition of FA$_{poly}$-DH cryptosystem

Symbol	Definition
$\mathcal{F}$	$\{\mathfrak{f}_0(x) + \sum_{i=0}^{14} \mathfrak{f}_i(x)\varphi_i \in FA$, the number of units is more than the number of negative ones by one and the other value is zero.$\}$.
m	$\{\mathfrak{m}_0(x) + \sum_{i=0}^{14} \mathfrak{m}_i(x)\varphi_i \in FA$, coefficients of $\mathfrak{m}$ chosen within the period $(-p/2, p/2]\}$.

4.2. The FA$_{poly}$-DH Phase

The FA$_{poly}$-DH public key cryptosystem can be summarized in Table 3:
When a trusted person selects and a truncated polynomial $\mathfrak{f}(X)$ having large prime order in FA-algebra and a large prime q. When we choose a truncated polynomial $\mathfrak{f}(X)$ of large prime order in the FA algebra and a large prime number q.

Table 3: Sets definition of FA$_{poly}$-DH cryptosystem

First party	Second party
Key Generation	
Select $\mathfrak{a}_1$ such that $1 \leq \mathfrak{a}_1 \leq q-2$	
Select $\mathfrak{f}(x) \in \mathcal{F}$	
Compute $\hbar_1(x) \equiv \mathfrak{f}^{\mathfrak{a}_1}(mod\ p)$	
Send $\hbar_1(x)$	
	Encryption
	Choose $\mathfrak{m} \in m$
	Choose $\mathfrak{a}_2, \mathfrak{a}_3$ such that
	$1 \leq \mathfrak{a}_2, \mathfrak{a}_3 \leq q-2$
	Compute $\hbar_2(x) \equiv \mathfrak{f}(x)^{\mathfrak{a}_2}(mod\ q)$
	Compute $\hbar_3(x) \equiv \mathfrak{f}(x)^{\mathfrak{a}_3}(mod\ q)$
	Compute $\mathcal{E}(x) \equiv \mathfrak{m} \cdot \left(\hbar_1(x)^{\mathfrak{a}_2}\right)^{-1} + \mathcal{P}\hbar_3(x)(mod\ q)$
	Send $(\mathcal{E}(x), \hbar_2(x))$ to first party
Decryption	
Compute	
$\mathcal{E}(x) \cdot \hbar_2(x)^{\mathfrak{a}_1} \equiv \mathfrak{m} + \mathcal{P}\hbar_3(x) \cdot \hbar_1(x)^{\mathfrak{a}_2}\ (mod\ q)$	
where,	
$\mathcal{E}(x) \cdot \hbar_1(x)^{\mathfrak{a}_2} \equiv \mathfrak{m}\ (mod\ q)$	

5. Pseudocode

The pseudocode of key generation, encryption, and decryption of FA$_{poly}$-DH show in Table 4:

Table 4: Execution time of $_{TRU}FA$

Phases	Input	Compute	Output
Key Generation	$\mathscr{P}, q, \mathfrak{f}(x)$, and $\mathfrak{a}_1$	$\hbar_1(x) \equiv \mathfrak{f}(x)^{\mathfrak{a}_1} \ (mod\ q)$	$\hbar_1(x)$
Encryption	$\mathfrak{m}, \mathfrak{a}_2$, and $\mathfrak{a}_3$	**1)** $\hbar_2(x) \equiv \mathfrak{f}(x)^{\mathfrak{a}_2} \ (mod\ q)$ **2)** $\hbar_3(x) \equiv \mathfrak{f}(x)^{\mathfrak{a}_3} (mod\ q)$ **3)** $\mathscr{E}(x) \equiv \mathfrak{m} \cdot \left(\hbar_1(x)^{\mathfrak{a}_2}\right)^{-1} + \mathscr{P}\hbar_3(x) (mod\ q)$	$\mathscr{E}(x)$
Decryption	$\mathscr{E}(x)$	**1)** $\mathscr{E}(x) \cdot \hbar_2(x)^{\mathfrak{a}_1}$ **2)** $\mathscr{E}(x) \cdot \hbar_2(x)^{\mathfrak{a}_1} \equiv \mathfrak{m} + \mathscr{P}\hbar_3(x) \cdot \hbar_1(x)^{\mathfrak{a}_2} \ (mod\ q)$ **3)** $\mathscr{E}(x) \cdot \hbar_1(x)^{\mathfrak{a}_2} \equiv \mathfrak{m} (mod\ q)$	$\mathfrak{m}$

6. Security Analysis

When exchanging keys between two parties, the hacker must break the private keys $\mathfrak{a}_1, \mathfrak{a}_2$, and $\mathfrak{a}_3$ to access the message $\mathfrak{m}$. Since the method relies on polynomial Diffie-Hellman key exchange, the difficulty lies in solving the discrete logarithm problem of polynomail. To compute the security for the keys must solving discrete logarithm problem for

$$\hbar_1(x) \equiv \mathfrak{f}(x)^{\mathfrak{a}_1} (mod\ q) \text{ and } \hbar_3(x) \equiv \mathfrak{f}(x)^{\mathfrak{a}_3} (mod\ q),$$

and to compute the security for message must solving the discrete logarithm problem for $\hbar_3(x) \equiv \mathfrak{f}(x)^{\mathfrak{a}_3} (mod\ q)$.

7. Conclusions

The FApoly-DH encryption scheme is proposed using the Diffie-Hellman polynomial algorithm, which makes this encryption an important method in many applications that require the keys to be difficult to be broken by hackers in the transmission medium of the transmitted data due to the use of polynomials in the basis instead of numbers, which greatly increases the level of security compared to methods that rely on Diffie-Hellman.

References

1. B.N. Abass. *New Encryption Schemes based on Certain Types of Public Key Cryptosystems.* PhD thesis, University of Kufa, Iraq, 2024.
2. F.H. Albakaa. *Novel Public Cryptosystems Based on NTRU, DNA and Multidimensional Algebraic Structures.* PhD thesis, University of Kufa, Iraq, 2025.
3. B. Boer. Diffie-hellman is as strong as discrete log for certain primes. In S. Goldwasser, editor, *Advances in Cryptology — CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 530–539. Springer-Verlag, 1989.
4. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
5. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithm. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.
6. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signature and public key cryptosystem. *Communications of the ACM*, 21(2):120–126, 1978.

Fatimah H. Albakaa,

Department of Mathematics,

Faculty of Education for Women, University of Kufa,

Iraq.

Department of Communication Techniques Engineering,

Al-Furat Al-Awsat Technical University,

Iraq.

E-mail address: fatimah.albakaa11@student.uokufa.edu.iq
E-mail address: fatema.albakaa@atu.edu.iq

and

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