DATA ENCRYPTION USING THE ALGEBRAIC STRUCTURE OF QUATERNIONS

Azir JUSUFI[1], Merita BAJRAMI[1], Rushadije RAMANI HALILI[1], Gazmend XHAFERI[1]

[1]*Faculty of Natural Sciences and Mathematics, University of Tetova, Tetovo, North Macedonia*
**Corresponding author e-mail: merita.azemi@unite.edu.mk*

Abstract

In this paper, a cryptographic scheme with an algebraic foundation is presented, built on the ring of quaternions. Messages are divided into blocks of length four in order to utilize quaternions of the form □ + □□ + □□ + □□. Likewise, quaternions and their algebraic properties are used for the key. To enhance the security of the cryptosystem, an S-box is incorporated, making the system more secure and nonlinear. An attacker can no longer rely on simple algebraic methods to determine the key, as the cryptosystem becomes difficult to break.
The formal construction algorithm of the encryption and decryption scheme is presented, along with its correctness, and an illustrative example is provided. The approach has a didactic and exploratory character, aiming to connect concepts of abstract algebra with cryptography, thereby opening possibilities for further developments in the field of information security.

Keywords: Encryption, decryption, ring, quaternion, S-box.

Introduction

Modern cryptography employs various algebraic structures in the construction of secure encryption schemes. Algebraic and nonlinear approaches for encryption and decryption based on polynomial and rational functions have also been studied in recent years ([2], [8]). In addition to groups, rings also provide an interesting framework for the development of alternative cryptographic mechanisms.
In this paper, by focusing on the ring of quaternions of the form $a + bi + cj + dk$, where a, b, c, and d are real numbers, we aim to construct a mathematically sound cryptosystem whose operation will be illustrated through a concrete example.

Preliminaries

This ring was discovered by the Irish mathematician William Rowan Hamilton in the 1840s and is commonly denoted by $\mathbb{H}$. The elements of $\mathbb{H}$. are called quaternions. Thus, $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$.
In $\mathbb{H}$, the operations of addition and multiplication are defined as follows. $\alpha = a + bi + cj + dk$, $\beta = a' + b'i + c'j + d'k$, where all coefficients are real.
Addition: $\alpha + \beta = (a + a') + (b + b')i + (c + c')j + (d + d')k$
Multiplication is defined as the product of two algebraic expressions, where each term of the quaternion $\alpha = a + bi + cj + dk$ is multiplied by each term of the quaternion $\beta = a' + b'i + c'j + d'k$. This yields: $\alpha \cdot \beta = A + Bi + Cj + Dk$, where: $A = aa' - bb' - cc' - dd'$; $B = ab' + ba' + cd' - dc'$; $C = ac' - bd' + ca' + db'$ and $D = ad' + bc' - cb' + da'$.
Multiplication in $\mathbb{H}$ is based on the following rules:

1. $i^2 = -1, \quad j^2 = -1, \quad k^2 = -1.$
2. $ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j.$

It is not difficult to verify that $(\mathbb{H}, +)$ forms an additive group, and moreover, the group $\mathbb{H}$ is isomorphic to the additive group of $\mathbb{R}^4 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$,, which consists of quadruples *(a, b,*

c, d) of real numbers. This isomorphism is given by the mapping: $a + bi + cj + dk \mapsto (a, b, c, d)$.
The zero element in $\mathbb{H}$ is $0 = 0 + 0i + 0j + 0k$, while the identity element is $1 = 1 + 0i + 0j + 0k$. Furthermore, we can conclude that in $\mathbb{H}$, the distributive property of multiplication over addition also holds.
For the inverse of nonzero quaternions, we have:
Let it be

$$\alpha = a + bi + cj + dk \in \mathbb{H},$$

where $a, b, c, d \in \mathbb{R}$. We consider its conjugate

$$\bar{\alpha} = a - bi - cj - dk.$$

Then, the following equality holds:

$$\alpha\bar{\alpha} = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2.$$

The expression $N(\alpha) = a^2 + b^2 + c^2 + d^2$ is called the norm of the quaternion α and is a non-negative real number.
If $\alpha \neq 0$, then $N(\alpha) > 0$, and therefore its inverse exists and is given by:

$$\alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

As a consequence, every nonzero element of the quaternion algebra is invertible, which shows that $\mathbb{H}$ is a division ring (skew field).
Since we can write $\mathbb{R} = \{a + 0i + 0j + 0k \mid a \in \mathbb{R}\}$ and the conditions for being a subring are satisfied, we conclude that the set of real numbers $\mathbb{R}$ is a subring of $\mathbb{H}$.
Basic concepts related to quaternion algebra and abstract algebra can be found in ([1], [5], [6], [7]).

Definition of a Cryptosystem
Definition 2.2.1.([3], [4], [6]) A cryptosystem is defined as a five-tuple (*P*, *C*, *K*, *E*, *D*) that satisfies the following conditions:

- *P* – is a finite set of plaintexts;
- *C* – is a finite set of ciphertexts;
- *K* – is a set of keys;
- *E*=$\{e_k | k \in K\}$ is a set of encryption functions;
- *D*=$\{d_k | k \in K\}$ is a set of decryption functions, such that $\forall x \in P, k \in K, d_k(e_k(x)) = x$.

Use of the S-box
The main reason for using an S-box is to introduce **nonlinearity** into this cryptosystem, which increases the level of security. If our cryptosystem were left as merely a series of linear operations with quaternions, then an attacker could break it quite easily by performing simple operations.
By using the S-box, we introduce exponentiation operations such as x^{-c}. This makes the cryptosystem nonlinear. An attacker can no longer use simple algebraic methods to find the key, as the resulting equations become much more difficult to solve.
In this cryptosystem, as an S-box we will use the generalized function:

$$S(x) = (ax^{-c} + b)(\mathrm{mod} p)$$

For this function to serve as a valid S-box, it must be *bijective*, which means that each input has a unique output and vice versa. For this, certain mathematical conditions must be satisfied:

1. p must be a prime number
2. The condition for $a \neq 0$ is $a \neq 0(mod p)$
3. $\gcd(a, p) = 1$.

4. $\gcd(c, p-1) = 1$.

Condition 4 is the most important one. The exponent c must be relatively prime to $p-1$, because if $gcd(c, p-1) \neq 1$, then the function x^c (and consequently x^{-c}) is not bijective on $\mathbb{Z}_p^*$.

Since 0^{-c} is not defined, we adopt the convention that if $x = 0$, then $S(0) = b$ and consequently, if $y = b$, then: $S^{-1}(b) = 0$.

Finding the inverse S^{-1}

We seek to determine x when y is known. We solve the equation step by step (always modulo p):

$$y = S(x) = (ax^{-c} + b)(\mathrm{mod}p).$$

Subtracting b from both sides, we obtain:$y - b \equiv ax^{-c}(\mathrm{mod}p)$.

Multiplying by the modular inverse of a, denoted by a^{-1}:

$$a^{-1}(y-b) \equiv x^{-c}(\mathrm{mod}p).$$

Taking the inverse of both sides in order to bring x^c to the numerator, we get:

$$(a^{-1}(y-b))^{-1} \equiv x^c(\mathrm{mod}p).$$

So,

$$x^c \equiv a^{-1}(y-b)^{-1}(\mathrm{mod}p).$$

To recover x from x^c, we must raise both sides to the power d, where d satisfies

$$c \cdot d \equiv 1(\mathrm{mod}p-1).$$

This is the reason why we required the condition $\mathrm{GCD}(c, p-1) = 1$, so that d exists (as the modular inverse of c modulo $p-1$).

By raising to the power d, we obtain

$$S^{-1}(y) = x = (a^{-1}(y-b)^{-1})^d(\mathrm{mod}p).$$

This construction guarantees that the S-box is bijective and fully invertible, thereby preserving the mathematical correctness of the cryptosystem.

Algorithm of the Cryptosystem

- At the beginning, a list consisting of *m* characters is constructed, and each character is associated with a number from 1 to *m*.
- We consider the finite field $F_p = \{0, 1, 2, \dots, p-1\}$, where *p* is the smallest prime number such that $p > m$
- The length *l* of the message *M* is divided by 4: *l* = 4*q* + *r*. Then the message *M* is divided into *q* blocks (ordered systems with 4 coordinates). If the last system does not have 4 coordinates, then it is completed at the end with as many zeros as needed.
- Each block of *M* is inserted into the S-box. For this purpose, we take as S-box $S: \mathbb{H} \to \mathbb{H}$ a nonlinear function defined as: $S(a + bi + cj + dk) = s(a) + s(b)i + s(c)j + s(d)k$, where the function *s*: $\mathbb{R} \to \mathbb{R}$ *s*(*x*) = $(ax^{-c} + b)(\mathrm{mod}p)$, where $a, b, c \in \mathbb{R}$ and *p* is a prime number.
- We choose the secret encryption keys $K \in \mathbb{H} \setminus \{0\}$ and $Q \in \mathbb{H} \setminus \{0\}$, $t \in \mathbb{Z}$.
- *Encryption* is performed by means of:

$$C = K\,S(M)\,K^{-1} + t\mathrm{Q}.$$

- *Decryption: Since* $K \neq 0$, there exists K^{-1}. Then:

$$S(M) = K^{-1}(C - tQ)K$$

and then the inverse function S^{-1} is applied to recover *M* from the S-box.

$$M = S^{-1}(K^{-1}(C - tQ)K).$$

Correct Definition of the Cryptosystem

Let the following be given:

- M the message represented as a quaternion (or a block of quaternions),
- $K \in \mathbb{H} \setminus \{0\}$ the secret key,
- S a bijective S-box function,
- The encryption function given by $E_K(M) = C = K\,S(M)\,K^{-1} + t\mathrm{Q}$ and
- The decryption function given by $M = S^{-1}(K^{-1}(C - tQ)K)$.

Theorem 4.1. For every message M, the following holds:$D_K(E_K(M)) = M$.

Proof. We start from the decryption function $D_K(C) = S^{-1}(K^{-1}(C - tQ)K)$ in which we substitute $C = E_K(M) = C = K\,S(M)\,K^{-1} + t\mathrm{Q}$ and obtain:

$$D_K(E_K(M)) = S^{-1}(K^{-1}((KS(M)K^{-1} + tQ) - tQ)K) =$$
$$= S^{-1}(K^{-1}((KS(M)K^{-1} + tQ) - tQ)K) = S^{-1}(K^{-1}(KS(M)K^{-1})K).$$

In $\mathbb{H}$ multiplication is associative, therefore:

$$D_K(E_K(M)) = K^{-1}(KS(M)K^{-1})K = (K^{-1}K)\,S(M)\,(K^{-1}K) =$$
$$= S^{-1}(1 \cdot S(M) \cdot 1) = S^{-1}(S(M)) = M.$$

Application Example

Encrypt the message UNIVERSITY and then decrypt it for verification.

Encryption:

Step 1. We choose the basic list:$A = 1, B = 2, C = 3, \dots, X = 24, Y = 25, Z = 26$.

Step 2. We transform the message UNIVERSITY into a numerical sequence:

$U = 21$, $N = 14$, $I = 9$, $V = 22$, $E = 5$, $R = 18$, $S = 19$, $I = 9$, $T = 20$, $Y = 25$

And we obtain the numerical message M: (21,14,9,22,5,18,19,9,20,25).

Step 3. The $l = 10 = 4 \cdot 2 + 2$, since the last block has two characters, we complete it with two zeros and obtain: $(21,14,9,22), (5,18,19,9), (20,25,0,0)$. Then we represent them as quaternions:

$$q_1 = 21 + 14i + 9j + 22k$$
$$q_2 = 5 + 18i + 19j + 9k$$
$$q_3 = 20 + 25i$$

Step 4. We choose $p = 29$ (29 is the first prime number greater than m=26) and work in the field $\mathbb{Z}_{29}$. As an S-box, we take $S(x) = x^3 (\mathrm{mod} 29)$, because $\gcd(3,28) = 1$, and we apply it component by component.

Block 1(21,14,9,22).

$$21^3 \equiv 10(mod29)$$
$$14^3 \equiv 18(mod29)$$
$$9^3 \equiv 4(mod29)$$
$$22^3 \equiv 5(mod29)$$

and we obtain $S(q_1) = 10 + 18i + 4j + 5k$.

Block 2 (5,18,19,9).

$$5^3 \equiv 9(mod29)$$
$$18^3 \equiv 3(mod29)$$
$$19^3 \equiv 15(mod29)$$
$$9^3 \equiv 4(mod29)$$

and we obtain $S(q_2) = 9 + 3i + 15j + 4k$.

Block 3 (20,25,0,0).

$$20^3 \equiv 25(mod29)$$
$$25^3 \equiv 23(mod29)$$
$$0^3 = 0(mod29)$$

and we obtain $S(q_3) = 25 + 23i + 0j + 0k$.

Step 5. We choose the secret keys arbitrarily from $\mathbb{H} \setminus \{0\}$. We choose $K = 1 + 2i + j + 3k$ for which we also determine the inverse quaternion, $Q = 5 - 2i + 3j - k$ and $t = 5$.
So $tQ = 5Q = 25 - 10i + 15j - 5k$.

For a quaternion $q = a + bi + cj + dk$ the inverse is given by $q^{-1} = \frac{\bar{q}}{N(q)}$ where:

- $\bar{q} = a - bi - cj - dk$ (the conjugate)
- $N(q) = a^2 + b^2 + c^2 + d^2$(the norm)

We find: $\bar{K} = 1 - 2i - j - 3k$ and $N(K) = 1^2 + 2^2 + 1^2 + 3^2 = 15$. Thus, the inverse is:

$$K^{-1} = \frac{1-2i-j-3k}{15} = \frac{1}{15} - \frac{2}{15}i - \frac{1}{15}j - \frac{1}{5}k.$$

Step 6. We encrypt using $C_i = K\,S(q_i)\,K^{-1} + tQ$, for $i = 1, 2, 3$.

- $C_1 = K\,S(q_1)\,K^{-1} + (25 - 10i + 15j - 5k) =$
  $(1 + 2i + j + 3k)(10 + 18i + 4j + 5k)(\frac{1}{15} - \frac{2}{15}i - \frac{1}{15}j - \frac{1}{5}k)+(25 - 10i + 15j - 5k)=$

$$C_1 = \left(\frac{150}{15} - \frac{28}{15}i + \frac{146}{15}j + \frac{245}{15}k\right) + (25 - 10\mathrm{i} + 15j - 5k) =$$

$$(10 - \frac{28}{15}i + \frac{146}{15}j + \frac{49}{3}k) + (25 - 10i + 15j - 5k) = 35 - \frac{178}{15}i + \frac{371}{15}j + \frac{34}{3}k$$
$$= (35, -\frac{178}{15}, \frac{371}{15}, \frac{34}{3})$$

- $C_2 = K\,S(q_2)\,K^{-1} + (25 - 10i + 15j - 5k) = (1 + 2i + j + 3k)(9 + 3i + 15j + 4k)(\frac{1}{15} - \frac{2}{15}i - \frac{1}{15}j - \frac{1}{5}k)+ (25 - 10i + 15j - 5k) =$

$$C_2 = \left(\frac{135}{15} + \frac{11}{15}i - \frac{127}{15}j + \frac{200}{15}k\right) + (25 - 10i + 15j - 5k) =$$
$$= (9 + \frac{11}{15}i - \frac{127}{15}j + \frac{40}{3}k) + (25 - 10i + 15j - 5k) = 34 - \frac{139}{15}i + \frac{98}{15}j + \frac{25}{3}k=$$
$(34, -\frac{139}{15}, \frac{98}{15}, \frac{25}{3})$

- $C_3 = K\,S(q_3)\,K^{-1} + (25 - 10i + 15j - 5k) =$
  $(1 + 2i + j + 3k)(25 + 23i + 0j + 0k)(\frac{1}{15} - \frac{2}{15}i - \frac{1}{15}j - \frac{1}{5}k) + (25 - 10i + 15j - 5k)$

$$= \left(25 - \frac{23}{3}i + \frac{46}{3}j + \frac{46}{3}k\right) + (25 - 10i + 15j - 5k)=$$
$$= (50, -\frac{53}{15}, \frac{91}{15}, \frac{31}{15}).$$

Thus, we obtain the encrypted message:

$$C = (C_1, C_2, C_3) = \left(35, -\frac{178}{15}, \frac{371}{15}, \frac{34}{3}, 34, -\frac{139}{15}, \frac{98}{15}, \frac{25}{3}, 50, -\frac{53}{15}, \frac{91}{15}, \frac{31}{15}\right).$$

Step 7. Decryption: The decryption formula is: $M_i = S^{-1}(K^{-1}(C_i - tQ)K)$, $i = 1,2,3$. But to recover them from the S-box, we must solve: $x^3 \equiv y(\mathrm{mod}29)$. Since we need $3d \equiv 1(\mathrm{mod}28)$, we take $d = 19$. Therefore, we use the power 19 as the decryption exponent.

- Decryption of C_1=$(35, -\frac{178}{15}, \frac{371}{15}, \frac{34}{3})$.

We compute $K^{-1}(C_1 - 5Q)K = 10 + 18i + 4j + 5k$ and then find $S^{-1}K^{-1}(C_1 - 5Q)K$ by calculating:

- $10^{19} \equiv 21(mod29)$
- $18^{19} \equiv 14(mod29)$

- $4^{19} \equiv 9(mod29)$
- $5^{19} \equiv 22(mod29)$.

Thus, the first decrypted block is $M_1 = (21,14,9,22)$.

- Decryption of C_2=$(9, \frac{11}{15}, -\frac{127}{15}, \frac{40}{3})$.

We compute $K^{-1}(C_2 - 5Q)K = 9 + 3i + 15j + 4k$ and then find $S^{-1}(K^{-1}(C_2 - 5Q))K$ by calculating:

- $9^{19} \equiv 5(mod29)$
- $3^{19} \equiv 18(mod29)$
- $15^{19} \equiv 19(mod29)$
- $4^{19} \equiv 9(mod29)$.

Thus, the second decrypted block is $M_2 = (5,18,19,9)$.

- Decryption of C_3=$(50, -\frac{53}{15}, \frac{91}{15}, \frac{31}{15})$.

We compute $K^{-1}(C_3 - 5Q)K = 25 + 23i + 0j + 0k$ and then find $S^{-1}(K^{-1}(C_3 - 5Q)K)$ by calculating:

- $25^{19} \equiv 20(mod29)$
- $23^{19} \equiv 25(mod29)$
- $0^{19} \equiv 0(mod29)$
- $0^{19} \equiv 0(mod29)$

Thus, the third decrypted block is $M_3 = (20,25,0,0)$.

We combine the decrypted blocks and, after removing the trailing zeros, we obtain: 21,14,9,22,5,18,19,9,20,25, which reads: **UNIVERSITY**.

Results and Interpretation

The presented cryptosystem demonstrates that structures from abstract algebra, in particular the quaternion ring $\mathbb{H}$, can serve as a powerful foundation for constructing cryptographic schemes. The combination of the following three components:

- Quaternion key transformation: $C = K \cdot S(M) \cdot K^{-1} + tQ$
- Nonlinear S-box: $s(x) = (ax^{-c} + b)(\mathrm{mod} p)$, and its inverse
- The secondary key Q and the parameter t as an additional security layer

creates a mathematically correct, fully reversible system that is resistant to linear algebraic attacks. The integration of the nonlinear S-box is essential, since it transforms the algebraic linear structure that could be exploited by attackers into a nonlinear structure, making the system resistant to classical attacks.Through the practical example of the word **"UNIVERSITY"**, we verified that the system is fully reversible, where the original message is recovered without loss of data through the application of the inverse key and the inverse function of the S-box.

Conclusion

In this paper, we have presented an innovative cryptosystem model that integrates structures from abstract algebra with modern information security techniques. The use of the quaternion ring provides a new dimension for data encryption, allowing messages to be processed as multidimensional units (blocks of length four). This approach demonstrates that quaternions are not only a theoretical mathematical tool, but also a powerful alternative for constructing modern cryptographic systems.

For future research, it is recommended to explore this system over complex number fields or through the use of quaternion matrices in order to further increase key complexity and data security.

References

[1]. Jusufi A. and Filipi K., 2022. *Matematikë Diskrete dhe Aplikime*. Prishtinë.
[2]. Zekaj B., Jusufi A. and Imeri-Jusufi B., 2022. Using incomplete polynomial functions of the odd degree n and their inverses for data encryption and decryption. *IFAC-PapersOnLine*, Vol. 55, No. 39, pp. 241–246.
[3]. Katz J. and Lindell Y., 2014. *Introduction to Modern Cryptography*. CRC Press.
[4]. Stinson D.R., 2006. *Cryptography: Theory and Practice*. CRC Press.
[5]. Ademaj E. and Gashi E., 1986. *Algjebra e përgjithshme*. Prishtinë.
[6]. Jacobson N., 1985. *Basic Algebra I*. 2nd Edition, W. H. Freeman and Company.
[7]. Atiyah M.F. and Macdonald I.G., 1969. *Introduction to Commutative Algebra*. University of Oxford.
[8]. Jusufi A., Reqica M., Reqica M. and Imeri-Jusufi B., 2025. Application of Rational Functions in Data Encryption and Decryption. *2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Paris, France, pp. 1–7. doi: 10.1109/ICECET63943.2025.11471969.