HSH-algebra with application

1Husein Hadi Abbass, 2Salah Albermany, 3Hussein saad mazel
1,3Department Mathematics, 2Computer Science
Faculty of Computer science and Mathematics, University of Kufa, Iraq

husseinh.abbas@uokufa.edu.iq
salah.albermany@uokufa.edu.iq
husseins.aloffie@student.uokufa.edu.iq

Abstract. In this paper we will study a new notion called HSH-algebra with his application in coding and the encryption data.

Keywords. bh-algebra; BCK-algebra; BCI-algebra; block codes; DES.

1. Introduction
The notion of BCK-algebra introduced by Y. Imai and K. Iseki in 1966[13]. In the same year, K. Iseki introduced the notions of a BCI-algebra as a generalization of a BCK-algebra and the notion of ideal of a BCK-algebra[5]. In 1998, Y. B. Jun, E. H. Rogh and H. S. Kim introduced the notion of BH-algebra[11]. in 2017 H.H. Abbass and A.H. Nouri introduced the notions 'On some types of ideals of pseudo BH-algebra' [3].in 2018 R.H.Abbas introduced ' On the normed BH-algebras' [7]. In the same year S.A. Neamah and A.A. Neamah introduced ‘ On the Sub-implicative ideal of a BH-algebra [10]. In other hand, studied One of the recent applications of BCK-algebras was given in the Coding Theory (see [12]). In 2014 intruded " On coded on BCK-algebras" by [1]. The paper also has several connections between BCK-algebras and n-ary block codes (A. Borumand Saeid et al)(2018) [2]. In the other hand, Data Encryption Standard “DES” algorithm are one of the most widely used encryption algorithm in the world[6]. in 2018 I.B.A.I. Iswara and et al introduced Application of Data Encryption Standard and Lempel-Ziv-Welch Algorithm for File Security see [4].

2. Preliminaries
Definition (2.1) [6] :
A BH-algebra is a nonempty set X with a constant "0" and a binary operation"*" satisfying the following conditions:
(BH-I)x * x = 0, for all x ∈ X.
(BH-II)x * y = 0 and y * x = 0 ⇒ x = y, ∀ x, y ∈ X.
(BH-III)x * 0 = x, ∀ x ∈ X.

Definition (2.2): [1] A mapping ̃A: A→X is called a BCK-function on A, which A and X is a nonempty set and a BCK-algebra, respectively.

Definition (2.3): [1] A cut function of ̃A, for q ∈ X, is defined to be a mapping ̃Aq : A → {0,1} such that
\((\forall x \in A)(\bar{A}_q = 1 \leftrightarrow q \ast \bar{A}(x) = 0)\)

3. **Main Results**

**Definition (3.1):**
An algebra \((X, \ast, 0)\) is a nonempty set \(X\) with a binary operation \(\ast\) and a constant 0 is called HSH-algebra if it have the following axioms:

- (HSH-I) if \(x \ast y = 0\) and \(y \ast x \neq 0\) then \(y \ast x = x\), \(\forall x \in X/\{0\}, y \in X\).
- and when \(x = 0\) then \(y \ast x = y\).
- (HSH-II) \(x \ast x = 0, \forall x \in X\).
- (HSH-III) \(0 \ast x = 0, \forall x \in X\).
- (HSH-IV) \((x \ast (x \ast y)) \ast y = 0, \forall x, y \in X\).
- (HSH-V) if \(x \ast y = 0\) and \(y \ast x = 0\) then \(x = y, \forall x, y \in X\).

**Lemma (3.2):**
Every HSH-algebra is BH-algebra.

**Proof:**
Direct from (HSH-I)

**Example (3.3):**
Let \((X, \ast, 0)\) be a HSH-algebra when \(X = \{0, a, b, c, d\}\), 0 is constant and \(\ast\) is the binary operation with the following cayley table:

|     | 0   | a   | b   | c   | d   |
|-----|-----|-----|-----|-----|-----|
| 0   | 0   | 0   | 0   | 0   | 0   |
| a   | a   | 0   | a   | 0   | a   |
| b   | b   | b   | 0   | b   | 0   |
| c   | c   | a   | c   | 0   | c   |
| d   | d   | d   | d   | b   | d   |

**Theorem (3.4):**
Let \(X\) be HSH-algebra and \(x, y, z \in X\), such that \(x \ast y = 0\) and \(y \ast x \neq 0\) then

i) \(x \ast (y \ast x) = 0\)

ii) \((y \ast x) \ast y = 0\)

iii) \(((y \ast x) \ast x) \ast z = 0, \forall z \in X, x \neq 0\).

iv) \((x \ast y) \ast (y \ast x) = 0\)

v) \((x \ast y) \ast (x \ast y) = x, x \neq 0\)

**Proof:**

i) If \(x = 0\) then \(0 \ast (y \ast 0) = 0\) since (HSH-III), if \(x \neq 0\) By (HSH-I) we have \(y \ast x = x\)

Then \(x \ast (y \ast x) = x \ast 0\) [by (HSH-I) and (HSH-II)]

ii) when \(x = 0\), we have \((y \ast 0) \ast y\) and by [ (HSH-I) we have \(y \ast 0 = y\).

then \(y \ast y = 0\) [by (HSH-II)]

If \(x \neq 0\) and by (HSH-I) we get

\((y \ast x) \ast y = x \ast y\)

iii) Since \(x \neq 0\) then \(y \ast x = x\) by (HSH-I) so, this yield

\(((y \ast x) \ast x) \ast z = (x \ast x) \ast z = 0 \ast z = 0\) [by HSH-II and HSH-III]

iv) if \(x = 0\) we have

\((0 \ast y) \ast (y \ast 0)\) and by [ (HSH-III) and (HSH-I)] get that

\(0 \ast (y) = 0\) [by (HSH-III)]

If \(x \neq 0\) then \(x \ast y = 0\) [by (HSH-I)]

\(0 \ast x = 0\) [ (HSH-I)].
v) If $x \neq 0$ then $(\text{HSH-I})$ we get 
$x*0=x$ [by (\text{HSH-I})]

**Theorem (3.5):**

Let $(X,*,0)$ be HSH-algebra if $x*y \neq 0, \forall x,y \in X$, when $x \neq 0$ and $x \neq y$ then must the following cases are hold HSH-algebra:

1) $x*y=x$  
2) $x*y=y$  
3) if $x*y=z$ then $x*z=y$

Then this theorem called Twice-theorem.

**Proof:**

1) we need just to satisfy the condition (HSH-IV), if $x*y=x$, then 
$(x*(x*y))*y=(x*x)*y=0*y=0$ then the condition is hold

2) if $x*y=y$ then 
$(x*(x*y))*y=(x*y)*y=y*y=0$

3) If $x*y=z$, then $x*z=y$

Suppose $x\neq y\neq z\neq w \neq 0$ when $x,y,z,w \in X$

Consider $x*y=z$ and $x*z=w$, since $(x*(x*y))*y=0$

Then $(x*(x*y))*y=(x*z)*y$

But $w*y=0$, this contradiction then $w=y$

**Defined (3.6):**

The partial order relation "$\leq$" on a HSH-algebra is defined as

$x \leq y \iff x*y=0$

**The coding in HSH-Algebra:**

In this section, we defined function of HSH-algebra, this function convers table of HSH-algebra to block code.

**Definition (3.5.1):**

A mapping $\overline{H} : H \rightarrow X$ is called a HSH-function on $H$, Which $H$ and $X$ is a nonempty set. And $(X,*,0)$ is HSH-algebra.

**Definition (3.5.2):**

cut function of $\overline{H}$ is a map $\overline{H}h : H \rightarrow \{0,1\}$, $h \in X$, such that $(\forall x \in H)(\overline{H}h(x) = 0)$. $X,H$ are set when $(X,*,0)$ is HSH-algebra.

**Example (3.5.3):**

Let $X=\{0, 1, 2,3,4,5,6\}$ is the set and * is a binary operation and let $(X,*,0)$ is HSH-algebra, the cayley table of $(X,*,0)$ is

|   | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 |
| 3 | 3 | 1 | 3 | 0 | 3 | 3 | 0 |
| 4 | 4 | 1 | 2 | 4 | 0 | 4 | 0 |
| 5 | 5 | 5 | 2 | 5 | 5 | 0 | 0 |
| 6 | 6 | 6 | 1 | 2 | 3 | 4 | 5 |

So, the graph of above table and by using definition (3.6) is following
Graph 1. HSH-algebra from table 2

Then the table of $H_h$ is following

| $H_h$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|-------|---|---|---|---|---|---|---|
| $H_0$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $H_1$ | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| $H_2$ | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| $H_3$ | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| $H_4$ | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| $H_5$ | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| $H_6$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

Graph 2. $H_h$

Then the block code is

$V = \{1111111, 0101101, 0010111, 0001001, 0000101, 0000011, 0000001\}$

**Data encryption by HSH-algebra:**

Confidentiality of in Cryptography, it’s to convert the plaintext (or changes message) into a form that cannot be read from unauthorized user called ciphertext, the above processing is by use a special encryption algorithms, and where the receiver wanted to return the original message from ciphertext, it’s by use mathematical algorithm called decryption. The string code of encryption or decryption process on the plaintext and ciphertext may ascii code or any suitable code that sent from the sender. the using HSH-algebra to encode the plaintext into HSH-code, and the HSH-code encrypted by encryption method, for example use the DES ( Data Encryption Standard ) method of 64bits. In our proposer denoted the method of encryption and use HSH-code by “E-HSH”, under using the DES ( 64 bits) algorithm or AES ( 128 bits) algorithm, ..... The key generation and strong ( security , and implementation ) of E-HSH encryption dependent onto the encryption method [8],[9].

**Definition (3.6.1):**

The table HSH-algebra of size N, satisfy HSH-II , and HSH-III of definition (3.1), and lemma(3.2), and other square is empty elements, called Main Structure Table, denoted by MST and the number of empty squares in MST denoted by ES(N).

**Remark(3.6.2)**
all HSH-algebra tables of size $N$ denoted by $\rho(N)$, all zero-classes (there exist at least one zero in empty sequars of MST) denoted by $P_z$, and all nonzero-classes (all empty sequars are non-zero of MST) denoted by $P_{nz}$.

Example (3.6.3):
$\rho(3)=6$, and $ES(3)=2$, the Main Structure Table (MST) of HSH-algebra of $N=3$, is

|   | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 |
| 2 | 2 | 0 | 0 |

The tables of $N=3$, are where $P_z=2$, and $P_{nz}=4$:

|   | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 |
| 2 | 1 | 0 | 0 |

|   | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 |
| 2 | 2 | 0 | 0 |

Encryption algorithm (E-HSH Method)

**Input:**
- random HSH-algebra table selected
- $K$: key of encryption method (for example DES(64 bit))
- $P$: plaintext (message)

**Output:**
- $C$: ciphertext
1. Select the HSH-code from the HSH-algebra table
2. Enhancement of code for increase efficiency code
3. Encryption HSH-code the plaintext $E_k$(HSH-code), where $E_k(P)$ encryption method to encrypt $P$ by use encryption method (for example DES) and the key $K$.

Decryption algorithm (E-HSH Method)

**Input:**
- HSH-algebra table
- $K$: key of encryption method
- $C$: ciphertext

**Output:**
- $P$: plaintext
1. decrypt $C$ by $M = D_k(C) = A$
2. convert code $M$ into code of HSH-algebra
3. use HSH-code method to convert $M$ into plaintext $P$.
   where $D_k(C)$ decryption method by use encryption method, and key $K$.

Example (3.6.4):
Consider the key $=1256984563214569$ size of key is 64bits, the method of encryption is DES, $N=4$ the size of set $X$ of HSH-algebra, and the HSH-table key is $K=10$, and the plaintext is hi
The plaintext $\text{hi}$ corresponding ASCII code in hexacode is $68\ 69$, and in binary is: $01101000\ 01101001$.

Since the number of empty squares of upper MST is
$$\frac{ES(4)}{2} = \frac{6}{2} = 3$$

and the number of zero-classes of HSH-algebra size $N=4$ is
$$P_z = 2\left(\binom{4}{1} + \binom{4}{2} + \binom{4}{3}\right) = 2 \times 7 = 14 = 2(2^3 - 1).$$

with the HSH-table with non-zero element in MST satisfy $x \cdot y = x$, then the order the $K=10$ of $14$ classes is:

Table 6. HSH-algebra satisfy $x \cdot y = x$

|   | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 1 | 1 | 4 | 1 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 2 | 1 | 0 | 1 | 0 | 3 | 1 | 0 | 1 | 1 | 4 | 1 | 0 | 0 | 0 |
| 2 | 1 | 0 | 2 | 2 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 1 | 0 | 2 | 2 | 1 | 0 | 2 |
| 3 | 3 | 3 | 0 | 3 | 1 | 3 | 0 | 3 | 3 | 0 | 0 | 3 | 3 | 0 | 3 | 1 | 3 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 7 | 1 | 0 | 0 | 0 | 8 | 1 | 0 | 2 | 1 |
| 7 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 2 | 0 | 0 | 2 |

$$C_{10} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 2 & 0 & 3 \\ 3 & 3 & 0 & 0 \end{pmatrix}$$

Then the matrix code corresponding is
$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Since $K=10$, then to selection the permutation of $N=4$, where $N!=24$, on the set $X=\{0,1,2,3\}$ by $K=10 \rightarrow 22_4$

then the order corresponding to $22_4$ is:

Table 7. permutation of code

|   | 1 | 0 | 2 | 3 |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 |

The code corresponding read in column, then the message

Table 8. HSH-code
Then the plaintext of 64-bit is
\[
M = 8BBC8BB800000000
\]

K = 1256984563214569 is the key of DES cryptosystem

By using DES encryption algorithm steps the ciphercode is
\[
C = 5A81d2DEA95D1AEC
\]

By use the Decryption algorithm D-HSH Method, To decrypt the ciphertext C, the first step is use DES algorithm to find M, and change it to base 4, then from HSH-table convert it to binary corresponding HSH-code, then every 8-bit corresponding the character in ASCII code, it's represent the plaintext.

4. Conclusion

The paper introduced a new notion denoted by HSH-algebra, given some theorems, definitions, examples, and with implement it to encode data, and decoded by HSH-function. Finally, HSH-algebra used the HSH-code algebraic with encryption method to encrypt, and decrypt message, the strong (security, and implementation) of E-HSH encryption dependent onto the encryption method.

References

[1] Borumand Saeid, H. Fatemidokht, C. Flaut and M. Kuchaki Rafsanjani "On Codes based on BCK-algebras" 06F35, 94B60, (2014).
[2] A. Borumand Saeid and et al "Some connections between BCK-algebras and n-ary block codes" Soft Comput 22:41–46 (2018).
[3] H.H. Abbass and A.H. Nouri “On some types of pseudo ideals “Applied Mathematical Sciences, Vol.11, no. 43, 2113-2120, (2017).
[4] I.B.A.I.Iswarana and et al “introduced Application of Data Encryption Standard and Lempel-Ziv-Welch Algorithm for File Security “International Journal of Engineering & Technology, 7 (3.2) 783-785, (2018).
[5] K. ISEKI, “An algebra related with a propositional calculus”, Proc.Japan Acad. 42, 26-29, (1966).
[6] Ratnadewi, R. P. Adhie, Y. Hutama, A. Saleh Ahmar, and M. I. Setiawan, “Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC),” J. Phys. Conf. Ser., vol. 954, no. 1, p. 012009, (2018).
[7] R.H. Abass"On the normed BH-algebra”(2018), 339-348, vol.119
[8] S. Albermany and F. Radi “Block cipher Methods” international journal of advancements in research & technology, vol. 5, Issue 11, (2016).
[9] S. Albermany, F. Radi and G.A. Safdar " New random block cipher algorithm" International Conference on Current Research in Computer Science and Information Technology (ICCIT) (2017)
[10] S.A. Neamah and A.A. Neamah “On the Sub-implicative ideal of a BH-algebra” journal university of kerbula vol.16, (2018).
[11] Y. B. Jun, E. H. Roh and H. S. Kim, "On BH-algebras"Scientiae Mathematica 1(1), 347–354, (1998).
[12] Y. B. Jun, S. Z. Song, “Codes based on BCK-algebras” Inform Sciences, 181,5102-5109(2011).
[13] Y. IMAI and K. ISEKI, "On axiom system of propositional calculi XIV, Proc. Japan Acad. 42, 19-20, (1966).