ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.11, 10055–10066
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.11.113

A NOTE ON POINT HYPERPATH CRYPTOGRAPHY

MAITRAYEE CHOWDHURY

ABSTRACT. In this paper we give a technique of encryption relating to the point hyperpath of a hypergraph. The technique would relate an n length point hyperpath of which each hyperedge is of order n. For encryption of a message with n characters, this would associate a vetex set of order $n^2 - (n-1)$ giving rise to an $n \times n$ matrix. Together with this encryption, the existing available cryptosystem would finally lead to the expected result.

1. INTRODUCTION

Cryptography is the study of sending and receiving unrevealed messages. The aim of cryptography is to send messages across a route so that only the intended recipient of the message can interpret it. In addition, when a message is received, the recipient usually needs some affirmation that it is genuine; and has not been sent by someone who is trying to cheat the recipient. Modern cryptography is heavily dependent on abstract algebra and number theory.

The message to be sent is the **plaintext** message. The disguised message is the **ciphertext**. The plain text and the ciphertext are both written in an **alphabet**, consisting of **letters** or **characters**. Characters can include not only the familiar alphabetic characters A,...,Z and small a,...,z but also digits, punctuation marks and blanks. A **cryptosystem** or **cipher** has two parts: **encryption**, the process of transforming a plaintext message to a ciphertext message and the **decryption**, the

2020 *Mathematics Subject Classification.* 05C65, 05C25, 94A60, 94A62, 54A05, 54B05.
Key words and phrases. Hypergraph, point hyperpath, encrypted message, decrypted message, non-singular matrix.

reverse transformation of changing a ciphertext message into a plaintext message [9]. There are many different families of cryptosystems, each distinguished by a particular encryption algorithm. Cryptosystems in a specified cryptographic family are distinguished from one another by a parameter to the encryption function called a key. A classical cryptosystem has a single **key**, which must be kept secret, known only to the sender and the receiver of the message. If a person A wishes to send secret messages to two different people B and C, and do not wish to have B understand C's messages or vice-versa, A must use two seperate keys, so one cryptosystem is used for exchanging mesages with B, and another is used for exchanging messages with C.

Systems that use two seperate keys, one for encoding and another for decoding, are **public key cryptosystems**. Since knowledge of the encoding key does not allow anyone to guess at the decoding key, the encoding key can be made public. A public key cryptosystem allows A and B to send messages to C using the same encoding key. Anyone is capable of encoding a message to be sent to C, but only C knows how to decode such a message [9]. In **single** or **private key cryptosytems** the same key is used for both encrypting and decrypting messages. To encrypt a plaintext message, we apply to the message some function which is kept secret, say, f. This function will yield an encrypted message. Given the encrypted form of the message, we can recover the original message by applying the inverse transformation f^{-1}. The transformation f must be relatively easy to compute, as must f^{-1}; however, f must be extremely difficult to guess at if only examples of coded messages are available [9].

One of the uses of hypergraph in cryptography is in the process of encryption of a secret image into n share images where it uses the construction of a 'hyperstar access structure VCS' from a hyperstar without center access structure VCS [8]. Another interesting use is related with key hypergraph that is defined as a pair of vertex and hyperedges such that a party is represented as a vertex and a group of parties is represented as a hyperedge. A key agreement protocol for a key hypergraph establishes all the keys for hyperedges in a key hypergraph at the same time. It provides key independence and forward secrecy in the random oracle model under the computational Diffie-Hellman assumption [7]. Also there are articles where we observe the use of Diffie-Hellman method used in the topological

basic concepts such as sub base, base and topology [5]. A technique for cryptography depending on the connected components of a topological space is introduced by Abedal and Saba [2] where a basis for a topology is chosen for the purpose.

In this article our main aim is to relate a point hyperpath with relevant cryptanalysis together with usual existing cryptosystem. The method of encryption would relate a point hyperpath with each hyperedge that would further relate a vertex set giving rise to a square matrix that would act as the key for encryption. Together with this encryption, the existing available RSA system would finally lead to the expected result. However, in this article our main endeavor would be on hypergraphic aspect of the encryption technique for obvious reason. For the purpose we begin with the following preliminaries. We refer [3, 6] and [1] for hypergraphic and cryptographic fundamentals.

2. PRELIMINARIES

Definition 2.1. *[1] A **hypergraph** is a pair $H = (V, \mathcal{E})$ where $\mathcal{E} \subseteq P(V)\backslash\{\phi\}$ and $P(V)$ is the power set of V.*

Definition 2.2. *[1] The **order** of the hypergraph $H = (V, E)$ is the cardinality of V, i.e. $|V| = n$; its **size** is the cardinality of E, i.e., $|E| = m$.*

Reviewing the definition of **hyperpath** due to Kannan and Dharmarajan [4] we redefine it as **point hyperpath** to suit our purpose.

Definition 2.3. *A **point hyperpath** in $H = (V, E)$ between two distinct vertices x_1 and x_2 is a sequence $x_1E_1x_2E_2...x_{k-1}E_{k-1}x_k$ with the following properties*

(i) *k is a positive integer.*
(ii) *$x_1, x_2, ..., x_k$ are distinct vertices.*
(iii) *$E_1, E_2, ..., E_{k-1}$ are hyperedges (not necessarily distinct).*
(iv) *$x_j, x_{j+1} \in E_j$ for $j = 1$ through $j = k - 1$ and we call it a $x_1 - x_k$ hyperpath.*
(v) *$E_i \cap E_{i+1} = \{x_{i+1}\}$, [$i = 1, .., n - 1$] and $E_i \cap E_j = \emptyset$ iff $|i - j| > 1$.*

Note: The condition (v) stated in the definition above indicates that any two adjacent edges possesses a single point in common.

Example 2.1. *Let $H = (V, E)$ be a hypergraph, where $V = \{v_1, v_2, ..., v_{16}\}$ and $E = \{E_1, E_2, ..., E_8\}$ having size 8 and order 16 such that $E_1 = \{v_0, v_7, v_6\}$, $E_2 =$*

$\{v_6, v_{10}, v_{11}\}$, $E_3 = \{v_{11}, v_{14}, v_{15}, v_5\}$, $E_4 = \{v_5, v_8, v_9, v_{13}\}$, $E_5 = \{v_6, v_{16}\}$, $E_6 = \{v_2, v_5\}$, $E_7 = \{v_9, v_4, v_{12}\}$, $E_8 = \{v_1, v_3, v_{13}\}$.

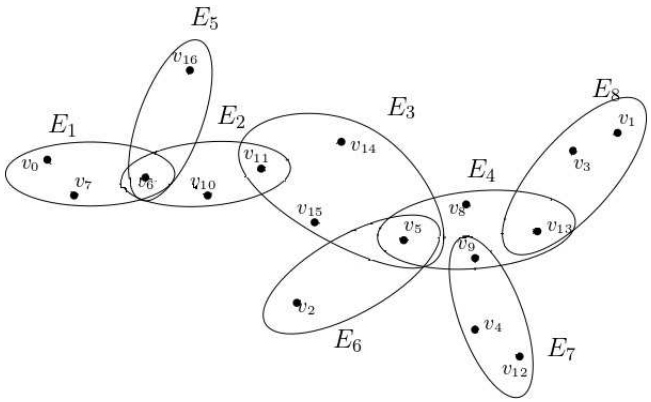

FIGURE 1. Point hyperpath

P_1 : $v_0E_1v_6E_2v_{11}$ is a point hyperpath of length 2.
Here, P_2 : $v_6E_2v_{11}E_3v_5E_4v_{13}$ is a point hyperpath of length 3.
P_3 : $v_0E_1v_6E_2v_{11}E_3v_5E_4v_{13}E_8v_1$ is a point hyperpath of length 5.

Definition 2.4. *A **replaced point** $(r-p)$ **hyperpath** of a point hyperpath is another point hyperpath obtained on replacing the common vertex of two hyperedges by any other vertex of any one of them.*

It is to be noted that for any pair of edges of such a point hyperpath, there is a scope of various types of such interchanging and this very character of the point hyperpath may contibute in a positive sense that we are going to propose.

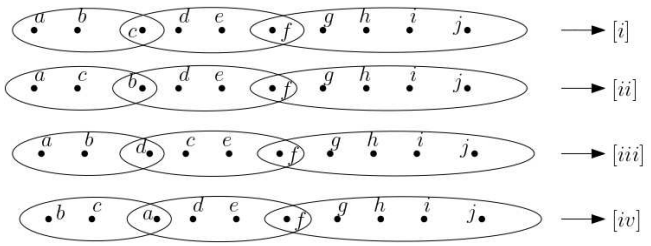

FIGURE 2. [ii],[iii],[iv] are (r-p) hyperpaths of [i]

3. Application of point hyperpath to Cryptography

Let M be a message with number of characters n. Take a hypergraph $H = (V, \mathcal{E})$ forming a point hyperpath such that the $|V| = n^2 - (n-1)$ and for each $E_i \in \mathcal{E}$, $|E_i| = n$.

We can encrypt the entire message or deducting parts and encrypt them on alone and in both cases the number of elements of this set depends on the number of characters taken from the message. We have chosen the vertex set V such that each hyperedges (forming the point hyperpath) forms a column basis of the key matrix described below.

We chose the finite set A depending on M so that A represents different representative numbers of the elements of M. For the purpose it seems useful to write down the english alphabet system with its normal ascending numeric decimal presentation shown below:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

FIGURE 3. Numeric correspondence of alphabets

Now we assign a number to each of the characters from M in A from figure 3. Then we send this number to a fixed vector of the set of vectors (set of hyperedges of the point hyperpath each of size n).

This vector is sent to the first hyperedge of size n, in the point hyperpath. Finally we'll get an $n \times n$ matix B for operation on the set of vectors each of size n (the hyperedges of the point hyperpath in consideration). And this would give us a map:

$$h : \mathbb{R}^n \to \mathbb{R}^n$$
$$h(u) = Bu$$

where B is the non singular matrix, whose columns are the elements of the hyperedges of the point hyperpath each of size n.

3.1. **The Encryption and Decryption Algorithm.**

(i) M: Message space: A set of strings (plain text messages) over some alphabet that needs to be encrypted.

(ii) A: Set of different numbers: To assign a number for each letter of the message and $|M| = |A| = |Y| = |V| = |C| = n$, $|X| = n^2$.

(iii) $X = (V, \mathcal{E})$ with $|V| = n^2 - (n-1)$ and $|\mathcal{E}| = n$ and for each $E_i \in \mathcal{E}$, $|E_i| = n$, constituting a point hyperpath.
(iv) $Y =$ transform the message in numeric form to the vector of FIXED NUMBERS.
(v) V: This vector transforms to the hyperedge of the point hyperpath.
(vi) C : Transformed vector is the cipher vector.

3.1.1. *The Encryption Process(Algorithm).*

$$\mathbb{R} \xrightarrow{q} \mathbb{R}^n \xrightarrow{f} \mathbb{R}^n \xrightarrow{h} \mathbb{R}^n$$
$$A \mapsto Y \mapsto V \mapsto C$$
$$(hofoq) : \mathbb{R} \to \mathbb{R}^n$$

[$(hofoq)$ is one to one map from A onto C]

$$\begin{aligned}(hofoq)(x_i) &= h(f(q(x_i))) \\ &= h(f(y_i)) \\ &= h(v_i) \\ &= Bv_i \quad [|B| \neq 0] \\ &= c_i\end{aligned}$$

3.1.2. *The Decryption Process (Algorithm).*

$$(hofoq)^{-1} : \mathbb{R}^n \to \mathbb{R}$$
$$C \mapsto V \mapsto Y \mapsto A$$

[$(hofoq)^{-1}$ is one to one map from C onto A.]

$$\begin{aligned}(hofoq)^{-1}(c_i) &= (q^{-1}(f^{-1}(h^{-1}(c_i))) \\ &= q^{-1}(f^{-1}(B^{-1}(c_i))) \\ &= q^{-1}(f^{-1}(v_i)) \\ &= q^{-1}(y_i) \\ &= x_i\end{aligned}$$

Example 3.1. *Encrypt the message 'get'.*

M :	m_i	g	e	t
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
A :	a_i	6	4	19

$|V| : n^2 - (n-1) = 3^2 - 2 = 7$

H : Hypergraph with the following point hyperpath

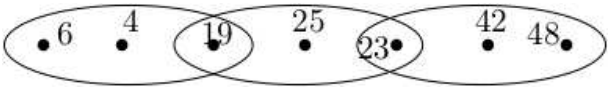

FIGURE 4. Point hyperpath

$$\begin{aligned} V &= \{6, 4, 19, 19+6, 19+4, 2\times 19+4, 2\times 19+25\} \\ &= \{6, 4, 19, 25, 23, 42, 48\} \\ \mathcal{E} &= \{\{6, 4, 19\}, \{19, 25, 23\}, \{23, 42, 48\}\} \end{aligned}$$

$$Y : y_i \quad \begin{pmatrix} 6 \\ 6 \\ 6 \end{pmatrix} \quad \begin{pmatrix} 4 \\ 4 \\ 4 \end{pmatrix} \quad \begin{pmatrix} 19 \\ 19 \\ 19 \end{pmatrix}$$

$$v_i : \quad \begin{pmatrix} 6 \\ 19 \\ 23 \end{pmatrix} \quad \begin{pmatrix} 4 \\ 25 \\ 42 \end{pmatrix} \quad \begin{pmatrix} 19 \\ 23 \\ 48 \end{pmatrix}$$

$$\begin{aligned} h : &\quad \mathbb{R}^3 \to \mathbb{R}^3 \\ h(u) &= Ku \end{aligned} \tag{3.1}$$

$$K = \begin{pmatrix} 6 & 4 & 19 \\ 19 & 25 & 23 \\ 23 & 42 & 48 \end{pmatrix}, \quad [|K| \neq 0]$$

Note:

$$Kv_1 = c_1, Kv_2 = c_2, Kv_3 = c_3$$

$$K^{-1}c_1 = v_1, K^{-1}c_2 = v_2, K^{-1}c_3 = v_3$$

$$Kv_1 = \begin{pmatrix} 6 & 4 & 19 \\ 19 & 25 & 23 \\ 23 & 42 & 48 \end{pmatrix} \begin{pmatrix} 6 \\ 19 \\ 23 \end{pmatrix}$$

$$= \begin{pmatrix} 549 \\ 1118 \\ 2040 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 0 \\ 12 \end{pmatrix} \quad \text{[using the available modulo encryption]} \tag{3.2}$$

$\equiv (dam)$

[g$\longrightarrow$dam]

$$Kv_2 = \begin{pmatrix} 6 & 4 & 19 \\ 19 & 25 & 23 \\ 23 & 42 & 48 \end{pmatrix} \begin{pmatrix} 4 \\ 25 \\ 42 \end{pmatrix} = \begin{pmatrix} 922 \\ 1667 \\ 3158 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 3 \\ 12 \end{pmatrix} \equiv (mdm)$$

[e$\longrightarrow$mdm]

$$Kv_3 = \begin{pmatrix} 6 & 4 & 19 \\ 19 & 25 & 23 \\ 23 & 42 & 48 \end{pmatrix} \begin{pmatrix} 19 \\ 23 \\ 48 \end{pmatrix} = \begin{pmatrix} 1118 \\ 2040 \\ 3707 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 12 \\ 15 \end{pmatrix} \equiv (amp)$$

[t$\longrightarrow$amp]

get$\longrightarrow\longrightarrow\longrightarrow$(dam)(mdm)(amp), [the encrypted message]

The encrypted matrix form is,

$$\begin{pmatrix} d & m & a \\ a & d & m \\ m & m & p \end{pmatrix} \equiv \begin{pmatrix} 3 & 12 & 0 \\ 0 & 3 & 12 \\ 12 & 12 & 15 \end{pmatrix} \equiv \begin{pmatrix} 549 & 922 & 1118 \\ 1118 & 1667 & 2040 \\ 2040 & 3158 & 3707 \end{pmatrix} = (c_1 \quad c_2 \quad c_3)$$

Now for decryption we'll use the inverse of K. Here,

$$K^{-1}(c_1 \quad c_2 \quad c_3) = (K^{-1}c_1 \quad K^{-1}c_2 \quad K^{-1}c_3) = (v_1 \quad v_2 \quad v_3)$$

And,

$$\begin{aligned} q^{-1}(f^{-1}(v_1)) &= a_1 \\ q^{-1}(f^{-1}(v_2)) &= a_2 \\ q^{-1}(f^{-1}(v_3)) &= a_3 \end{aligned}$$

Now, from (3.1)

$$K^{-1} = \begin{pmatrix} 0.056948 & 0.147481 & -0.093210 \\ -0.093210 & -0.036261 & 0.054271 \\ 0.054271 & -0.038938 & 0.018009 \end{pmatrix}, \quad c_1 = \begin{pmatrix} 549 \\ 1118 \\ 2040 \end{pmatrix}$$

Therefore, [keeping active modulo encryption as in (3.2)]

$$K^{-1}c_1 = \begin{pmatrix} 0.056948 & 0.147481 & -0.093210 \\ -0.093210 & -0.036261 & 0.054271 \\ 0.054271 & -0.038938 & 0.018009 \end{pmatrix} \begin{pmatrix} 549 \\ 1118 \\ 2040 \end{pmatrix}$$

$$= \begin{pmatrix} 5.9981 \\ 19.0007 \\ 23.0004 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 19 \\ 23 \end{pmatrix}$$

And,

$$f^{-1} \begin{pmatrix} 6 \\ 19 \\ 23 \end{pmatrix} = \begin{pmatrix} 6 \\ 6 \\ 6 \end{pmatrix}$$

Finally, we get

$$q^{-1} \begin{pmatrix} 6 \\ 6 \\ 6 \end{pmatrix} = 6 \equiv g$$

Thus,

$$dam \longrightarrow\longrightarrow g$$

Similarly,

$$mdm \longrightarrow\longrightarrow e$$

$$amp \longrightarrow\longrightarrow t$$

Thus the decrypted message is get.

4. USE OF $(r-p)$ HYPERPATH WHEN THE KEY MATRIX IS SINGULAR

Suppose as in the above case, we got a string of message of say, 3 characters. With the help of these 3 we form a point hyperpath of length $3^2 - 3 = 7$, may be in a different way from the above. Suppose this time our message is 'dip'. For this we take the following point hyperpath,

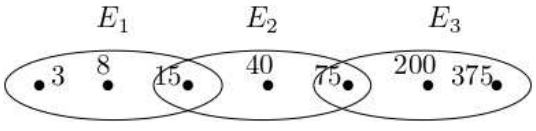

FIGURE 5. Point hyperpath

In this case we note that the determinant of the corresponding key matrix,

$$\begin{pmatrix} 3 & 8 & 15 \\ 15 & 40 & 75 \\ 75 & 200 & 375 \end{pmatrix}$$

is zero. And therefore we interchange the vertices 8 and 15 as already said. And the resulting (r-p) hyperpath appears as,

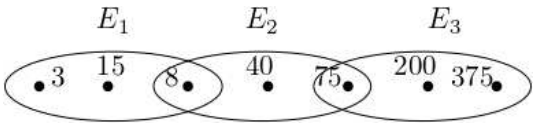

FIGURE 6. (r-p) hyperpath

And now this time the corresponding key matrix is,

$$K = \begin{pmatrix} 3 & 15 & 8 \\ 8 & 40 & 75 \\ 75 & 200 & 375 \end{pmatrix}$$

and here $|K| = 28175(\neq 0)$. Now,

$$K \begin{pmatrix} 3 \\ 8 \\ 75 \end{pmatrix} = \begin{pmatrix} 729 \\ 5969 \\ 29950 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 15 \\ 24 \end{pmatrix} \equiv (bpy)$$

$$K \begin{pmatrix} 15 \\ 40 \\ 200 \end{pmatrix} = \begin{pmatrix} 2245 \\ 16720 \\ 84125 \end{pmatrix} \equiv \begin{pmatrix} 9 \\ 2 \\ 15 \end{pmatrix} \equiv (jcp)$$

$$K \begin{pmatrix} 8 \\ 75 \\ 375 \end{pmatrix} = \begin{pmatrix} 4149 \\ 31189 \\ 156225 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 15 \\ 17 \end{pmatrix} \equiv (ppr)$$

Again,

$$K^{-1} = \begin{pmatrix} 0 & -0.142857 & 0.028571 \\ 0.093167 & 0.018633 & -0.005714 \\ -0.049689 & 0.018633 & 0 \end{pmatrix}$$

And also,

$$K^{-1}\begin{pmatrix}729\\5969\\29950\end{pmatrix} = \begin{pmatrix}2.988\\8.004\\74.997\end{pmatrix} \equiv \begin{pmatrix}3\\8\\75\end{pmatrix}$$

Now, we have,

$$f^{-1}\begin{pmatrix}3\\8\\75\end{pmatrix} = \begin{pmatrix}3\\3\\3\end{pmatrix}$$

And finally we get,

$$g^{-1}\begin{pmatrix}3\\3\\3\end{pmatrix} = 3 = d$$

Thus,

$$\text{bpy} \longrightarrow \text{d}$$

Similarly,

$$\text{jcp} \longrightarrow \text{p}$$
$$\text{ppr} \longrightarrow \text{i}$$

That is,

$$(bpy)(jcp)(ppr) \longrightarrow dpi \longrightarrow dip$$

It is interesting to note that our decrypted message would depend on the chosen point hyperpath, not on the (mid way) $(r-p)$ hyperpath.

5. Conclusion

We use here a point hyperpath (may be a subhypergraph) of length coinciding with the order of each hyperedge forming the hyperpath. This helps in giving rise to a square matrix to act as the key for playing the pivotal role in our proposed encryption technique. Moreover, the possibility of occurrence of singular matrix in

the process is overcome by introducing the notion of (r-p) hyperpath. In this article our main endeavor is on the hypergraphic aspect of the encryption technique for obvious reason with the help of the existing cryptosystem that would finally lead to the expected result.

6. Acknowledgement

I would like to acknowledege my supervisor Dr. Saifur Rahman of Rajiv Gandhi University, Itanagar, for his relentless guidance and encouragement in my work.

References

[1] A. Bretto: *Hypergraph theory- an introduction*, Springer Int. Publishing Switzerland, 2013.
[2] A. H. M. Hamza, S. N. F. Al-khafaji: *Using connected components of topological spaces in cryptography*, Int. Journal of Mathematics Trends and Technology, **12**(1), 2014, 31-33.
[3] J. Hoffstein, J. Pipher, J. H. Silverman: *An Introduction to Mathematical Cryptography*, Springer, 2008.
[4] K. Kannan, R. Dharmarajan: *Hyperpaths and Hypercycles*, Int. Journal of Pure and Applied Mathematics, **98**(3) (2015), 309-312.
[5] K. Polat: *On Key Exchange Method via Topological Concepts*, TWMS J. App. Eng. Math., **9**(1) (2019), 151-158.
[6] N. Koblitz: *A Course in Number Theory and Cryptography*, Springer-Verlag New York, 1994.
[7] R. Jeong, D. H. Lee: *Key agreement for key hypergraph*, Computers and Security, **26**(7-8) (2007), 452-458.
[8] T. Guo, L. N. Zhou: *Constructing visual cryptography scheme by hypergraph decomposition*, Procedia Computer Science, **131** (2018), 336-343.
[9] T. W. Judson: *Abstract Algebra Theory and Applications*, Orthogonal publishing L3C, 2018.

Department of Mathematics
Rajiv Gandhi University
address: Itanagar, India
Email address: maitrayee3.1415@gmail.com