Modern Applied Science; Vol. 13, No. 5; 2019
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Applications of Algebraic Geometry in Cryptography

Nada Yassen Kasm[1] & Zyiad Adrees Hamad[2]

[1] Department of Mathematics, College of Education for pure Sciences, University of Mosul, Mosul, Iraq

[2] Department of Mathematics, College of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq

Correspondence: Nada Yassen Kasm, Department of Mathematics, College of Education for pure Sciences, University of Mosul, Mosul, Iraq. E-mail: drnadaqasim1@gmail.com

Received: March 23, 2019 Accepted: April 26, 2019 Online Published: April 30, 2019

doi:10.5539/mas.v13n5p130 URL: https://doi.org/10.5539/mas.v13n5p130

Abstract

One of the most important applications of algebraic geometry, known as linguistics, has been used in linguistics, military and diplomatic. It was said that the first to mobilize a comment between the army is the Pharaohs. He also mentioned that the Arabs have old attempts at encryption. The Chinese used many methods in conveying messages during war. Their intention was to get the wrong signals. This research is a general study on science (word) searching for several methods in English linguistics, a word of thanks and a message.

Keywords: cryptography, caesar code, linear code, rotation code, polypus box

1. Introduction

1.1 Introduce the Problem

The best method used in ancient times. In today's era, it is urgent to use this "encryption" science to link its universes through open networks. And called human rights in Saudi Arabia. The confidentiality of information must be kept confidential. Considerable efforts have been made from all over the world to find the best ways in which data exchange can be simplified and data can not be detected. Be a great verification tool, designed especially for all concepts. There is a need for strong encryption methods because with the rapid development of the computer, it reduces the strength of encryption; because increasing the speed of the computer means shortening the time needed by the computer to break or detect a certain encryption key. It also uses encryption to protect information that can be accessed by illegal access attempts When the rest of the protection measures are inefficient to prevent such access, encryption can be applied to protect the communication channels and physical databases. Also, codes and codes have been used throughout European history to help plan the overthrow of the kings, draw up battle plans and send important messages. For the American Revolution George was introduced. Washington has an espionage system to report on the ability and movements of British forces to send this information to his supporters. Each spy has a symbolic book containing symbolic numbers, each of which represents a specific word. The letter contains a series of numbers used to send intelligence about the enemy. In modern warfare, codes and codes have been used to ensure that secret information is not leaked to the enemy. There are many books about military intelligence in World War II and about the process of breaking symbols to reveal enemy plans. Each side tried to break the symbols of the other side (Yan, Wang, Niu & Yang, 2015, pp.317-333).

1.1.1 Definition

"Cryptoanalysis is the science that uses mathematics to encrypt and decrypt data Encryption enables you to store or transmit sensitive information over insecure networks - such as the Internet - and therefore can not be read by anyone other than the person sending it. To save the security and confidentiality of information, the analysis and decryption. It is a flag to break and break secure communication.(Shukla ,Khare, Rizvi, Stalin& Kumar 2015,pp. 1387-1410).

1.1.2 Encryption Objectives

"(1) There are four main objectives behind the use of cryptography as follows: - Confidentiality and privacy

A service that is used to store information content from all persons except those who have been informed of it.

2) Data integration

It is a service used to save information from change (delete, add or modify) by unauthorized persons.

3) Proof of identity

A service used to authenticate the handling of authorized data.

4) Do not be arrogant

It is a service used to prevent a person from denying something"

1.1.3 How Encryption Works

"Encryption algorithm is a mathematical function used in the process of encryption and decryption It works in union with the key, password, number or phrase, to encrypt the read texts The same readable text encodes to different encrypted texts with different keys The security in encrypted data depends on two important things The strength of encryption algorithm is confidential"

2. Types of Encryption

2.1 Traditional Encryption

"Broadcast and symmetric device (Synaptic Encryption). It uses one key to encrypt and decrypt the data. This type of encryption depends on the secret of the key used. Where the person who owns the key is the key. For example, if Zaid wanted to send an encrypted message to slaves, it was a good way. Any third person has got this key on him and his eye, all things encrypted between Zaid and Obaid, and examples of this kind. (Kahrobaei, Tortora & Tota, 2019).

2.2 Code of Caesar

"It is an old method invented by Tsar Julius to work encrypted messages between the sectors of the army has proved effective in his time But in modern times and with the development of the computer can not be used this way for the rapid detection of the content of messages, we will give two examples of applications on the code Caesar (Yan & Wang & Niu & Yang, 2015,pp.317-333)(Hong & Cheon , 2012,pp.133-150)

2.2.1 Example

"If we coded the word "SECRET" and used the value of "3", we would change the position of the characters beginning with the third letter, "D", so the order of the letters will be as follows:

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 The letters after using the new value of the "3" key are in the current form

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Now the value of A = D, B = E, C = F and so on

In this way, the word "SECRET" will be "VEFUHW" to give anyone else the possibility of reading your encrypted message should send him the value of the key "

"3".

2.2.2 Example

If we encode the word "ZYIAD" and use the value of the key "5", we change the position of the letters beginning with the letter V, "F" and therefore the order of the letters will be as follows:

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

The characters after using their new value of the "5" key are as current

F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

Now the value of A = F, B = G, C = H and so on

In this way, the word "ZYIAD" will be "EDNEF" to give anyone else the possibility to read your message. You should send the value of the key "5".

3. Standard Data Encryption

"This system was developed at the end of the 1970s by the US National Security Agency, and it is not feasible to use it with the development of computer systems and the faster processing of data, as the content of encrypted messages may be detected in a short time"

3.1 Measuring Strength of Encryption

"Encryption may be strong or weak, since the strength meter for encryption is the time and resources required for unencrypted text detection of encrypted texts. A strong encryption result is encrypted text that is difficult to detect with time or provides tools for it."

3.1.1 Modern Methods of Encryption, The Decryption Process

"changes one character from plaintext to another to produce encoded text. (In order to open the code, we execute the reverse of the encryption steps). In other words, the order of the characters is changed. Examples of the encryption method are the following."

3.1.2 Method of Reverse Message

"In this method of encryption, the characters of the message are reversed for the purpose of generating encrypted text. It is usual that if someone wants to read any text and the text is very English, he reads it from left to right which is the familiar style in reading any text. Left-to-right text characters characters. "

3.1.3 Example

" We assume the following message Separation question focuses on them before encoding meht sucof noitseuq noittarapes after encryption. Note in this example Then e then h until the end of the sentence. "

Note in this example that the encrypted text was created by reading the right-to-left message where the m character was turned on in their word Them the letter e , the letter h, and so on to the end of the sentence"

3.1.4 Example

"If we have the following encrypted text Eab doog"

For the purpose of generating clear text we read the text from right to left ie start from the right of the letter g in the word doog and move left to read o then o then d and so to become the text of the coli Eab doog encrypted text Good bay Clear text after decryption.

Note in the process of opening the code that the method used to find the clear text of the encrypted text is the same method used in the encryption process to find the encrypted text. In other words, when the encrypted text is encoded in the encryption process, the text is read from right to left. When the text is clearly defined in the code opening process, the text is also read from right to left, which is the opposite of the message (whether encrypted message or clear text)"

4. Method of Engineering Modeling

"In this method we use the message to create a specific geometry model in a rectangular shape of the different dimensions according to the length of the message and here we must emphasize the need to calculate the length of the message before the start of the encryption process"

4.1 Example

"Assume we have the following message CONCEAL SAM MESSAGES The message contains 18 characters so the length of the message is 18. The message above can be divided to form a rectangle with the following tests:"

(1) The letter can be written in two equal rows and each row contains nine characters by reading the message horizontally as shown in the Table1.

Table 1. Table CONCEAL SAM MESSAGES

Letter	C	O	N	C	E	A	L	S	A
Characters	M	M	E	S	S	A	G	E	S

(2) The geometrical shape (rectangle) shall be in the form of two equal columns by writing the above letter vertically, one letter as in the following Table2.

Table 2. Table geometrical shape (rectangle)

Letter	C	O	N	C	E	A	L	S	A
Characters	M	M	E	S	S	A	G	E	S

The letter was read in a specific way to form an engineering form where the first nine letters of the letter were placed in the first column while the second nine were placed in the second column.

4.2 Methods of Alternative Coding

"Cryptography is a cryptographic method by which units of clear text are replaced by other units of encrypted text in a special regulatory system. These modules may be one character per unit or two pairs of characters per unit or three characters per unit or a combination of all the above. The receiver of the message (receiever) opens the code by executing the steps inversely. The replacement encoder can be compared with Transposition Ciphers, In the eternal encodings, clear text units are rearranged in a sorted order In the usual P it is complicated but not taken to change the same units In contrast, in the alternative encoding, plain text units retain their order in the same sequence in the encrypted text, but the text units change clearly"

Now we take some type of encoders, which is simple-instance encryption and give an example of how encryption is applied

4.2.1 The Method of Encryption to Replace the Simple

Only one letter is used in this method and the following example is explained in detail in the above. (Escala, Herold, Kiltz,afols, & Villar, 2013, pp.129-147).

4.2.2 Example

" Use the simple-mode encryption method using the zebras and encrypt the word "Math"?

The solution /

We initialize the encryption method using the given keyword and the method is coli

Plaintext alphapet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY

In other words, the letter A encodes the clear text into the letter Z and the letter B to the letter E and so on.

If the word (Math) will be encoded word (JZQD)"

4.2.3 Example

Use the substitution encoding method using the DOCTOR and the

NAdA YASSEN KASM?

4.2.4 The Solution

"We start by configuring the encryption method using the given keyword and the method is coli

Plaintext alphapet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext alphabet: DOCTORABEFGHIJKLMNPQSUWXYZ

If the letter A will be encoded to D and the letter B to O and so on. In this encryption the required text will be encoded as follows"

JDTD YDPPOJ GDP

4.2.5 Number Cipher

The method of digital encryption includes the characterization of 26 letters in the form of numbers as shown in the following Table3.

Table 3. Table Number Cipher

Character	Numerical value	Character	Numerical value	Character	Numerical value
A	1	J	10	S	19
B	2	K	11	T	20
C	3	L	12	U	21
D	4	M	13	V	22
E	5	N	14	W	23
F	6	O	15	X	24
G	7	P	16	Y	25
H	8	Q	17	Z	26
I	9	R	18		

4.2.6 Example

If we assume that we have the text Mathematics Department under this numbering

we get the following digital encoded text as shown in the following Table 4.

Table 4. Table text Mathematics Department under this numbering

Clear text	M	A	T	H	E	M	A	T	I	C	S	D	E	P	A	R	T	M	E	N	T
Encrypted text	13	1	20	8	5	13	1	20	9	3	19	4	5	16	1	18	20	13	5	14	20

Let the text be encrypted

13 1 20 8 5 13 1 9 3 19 5 16 1 18 5 14 20

The coded text and any number separated by commas are written for the purpose of non-ambiguity because if the numbers are merged, for example, the number 25 symbol, which corresponds to Y, and when merged with another letter, it can be separated into two numbers, meaning that 2 represents the letter B and 5 is the letter E.

Digital codes of this type provide very simple security because everyone knows the letters and numbers of the alphabetical code and does not contain a key word so it can only be used in some very simple issues

4.2.7 Wireless Encryption Method (ASCII CODE)

"This method is similar to the previous digital encoding, but the alphabetic characters are encoded as they are in the wireless table shown in the following table5.

Table 5. Table alphabetic characters

Character	Remix for wireless	Character	Remix for wireless	Character	Remix for wireless
A	65	J	74	S	83
B	66	K	75	T	48
C	67	L	76	U	85
D	68	M	77	V	86
E	69	N	78	W	87
F	70	O	79	X	88
G	71	P	80	Y	89
H	72	Q	81	Z	26
I	73	R	82		

4.2.8 Example

Encrypt the following clear text using wireless encryption

WALAA SHEET KHLEEF

Under the radio schedule we produce the following encrypted text

87 65 76 65 65 83 72 69 69 84 75 72 76 69 69 70

4.3 Fraxttional Systems

"The Transposittion method will be more effective when used with Fractionation, ie, an initial phase that divides each of the clear text symbols into several symbols of the encoded text. For example, the plain text characters are written into a matrix. Each letter of the letter is then replaced by its coordinates (See box Polybius square) There is a method of encryption is the relative conversion code to Morse code (Morse code) where will include each character Vbmp of the spaces in addition to points and dashes. The most important types of these types of codes Come on"

4.3.1 Polypropylene Box Blade

"In cryptography, Polypus is a device invented by the Greek world Polypus, which describes relatively literal text so that it can be represented by a small set of symbols. The Polypus was introduced in 200 BC by what is now known as the polypus square, which is a 5x5 matrix and uses 24 Of each letter. Each letter has a single position known as the coordinates of the system, which lines the lines and columns of the matrix. For example, if the letter A is in one column at the right of the point of origin and one line down, this has its coordinates 11. In the English alphabet, Fit the hottest P 26 to a box consists of 25 cells. Force the merging of the letters I and J when that character K will be in the location (Coordinates) 25, in other words, in two lines down and five squares upward. The basic shape of the polypus square model (after deleting J from the vulgar characters to be a 5X5 matrix) appears as shown (Budaghyan & Parker, 2019, pp.). table shown in the following Table6.

Table 6. Table polypropylene box blade

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

"Each letter of this matrix represents its coordinates in the array. In other words, each character takes vertical and horizontal coordinates, as shown in the shaded numbers. For example, the coordinates of the letter T are 44 starting with the vertical coordinate number followed by the horizontal coordinate number. The following figure shows how these coordinates are chosen for letter T" table shown in the following Table7.

Table 7. Table coordinates are chosen for letter "T"

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

4.3.2 Example

To encrypt the word (THEORM) we take each letter from the letters of this word and find the coordinates of each character of the box polypus as shown in the following Table8.

Table 8. Table word (THEORM)

T	H	E	O	R	M
44	23	15	34	42	32

So the code output for this keyword will be 442315344232

"If we want to open the previous code 442315344232 we take every two digits of this encrypted text. The reason is that each character is encoded into two numbers and represent its numerical coordinates in the array. For example, the 44 numbers represent the 4 vertical coordinates while the second 4 represents the horizontal coordinate as agreed In the Polypus box, go back to the Polypus square. Look for these two events where they are interspersed with the letter T and so on for the rest of the letters of the encrypted word"

4.3.3 Bified Cipher

"The code (Bified) uses a polypeous box to encrypt the message in a way that makes it difficult to open the code without knowing the secret information. The reason for this is that each letter of the encoded text is supported by two characters of the text. As a result, the frequency analysis of the characters becomes more difficult. In classical coding, the code is a cryptographic method that connects the polypus square using substitution and uses relative encryption with it. In the year 1901 by) (Felix Delastell)

(Bennett& Brassard& Breidbart,2014, pp. 453-458)

To illustrate this method, a 5x5 matrix containing a different combination of alphabetical characters will be created first without using the letter as shown in the following Table9.

Table 9. Table Bified Cipher

	1	2	3	4	5
1	B	G	W	K	Z
2	Q	P	N	D	S
3	I	O	A	X	E
4	F	C	L	U	M
5	T	H	Y	V	R

"Note that the distribution of the letters in this matrix is an irregular distribution, which is not to write the set of alphabetical characters in the usual sequence as was followed in the distribution of alphabetical characters in the polypus box. The letter is converted to the corresponding letter of each letter with its coordinates in the matrix (column number - row number) You then write the coordinates vertically under each row"

4.3.4 Example

We assume the following message FLEE AT ONCE according to the Bified matrix, the coordinates of the letter characters can be configured as shown as shown in the following Table10.

Table 10. Table Bified matrix

Character	F	L	E	E	A	T	O	N	C	E
Coordinates	14	34	53	53	33	15	23	32	24	53

Then write these coordinates under each number vertically as shown Table11.

Table 11. Table Bified matrix

F	L	E	E	A	T	O	N	C	E
1	3	5	5	3	1	2	3	2	5
4	4	3	3	3	5	3	2	4	3

"These numbers are arranged by the coordinates of each letter vertically under each letter. For example, the coordinates of the letter F are 14 and these numbers are written vertically under each letter 1 and 4 then the numbers are read horizontally to form a series of the following numbers 13553123254433353243 Then write this letter of numbers in units of each unit Of two numbers as shown below and start from the right 43 32 35 33 44 25 23 31 55 13

The next step is to take two numbers (which represent the coordinates of one of the numbers) to see the corresponding character of these coordinates. Where each two digits are the coordinates of one of the letters of the matrix of the paveid to have the following output" as shown Table12.

Table 12. Table letters of the matrix

13	55	31	23	25	44	33	35	32	43
I	R	W	O	H	U	A	Y	N	X

"The coordinates will be read first by reading the column number and second by the row number. For example, the number 25, 5 represents the column number, 2 represents the row number, and the intersection gives us the letter H and so on the other coordinates.

The result of this procedure is the final text of the word

FLEE AT ONCE is IRWOHUAYNX.

Now we will take a new code and apply it to field 19, which we mentioned earlier in

Chapter 2, and give an applied example to encrypt the field word."

4.3.5 Rotating Blade (ROT19)19

"One way of coding is called ROT19 (19). Its method of operation depends on the composition or creation of a mapping of all 26 letter letters of the English alphabet so that this number is from 0 to 25 as shown in the Table 13."

Table 13. Table Rotating blade(ROT19)19

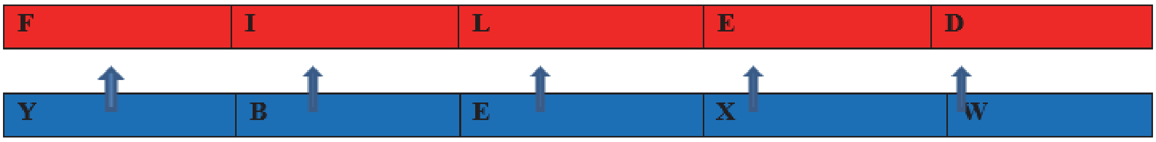
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

"This method displaces each character with 19 characters from the character within the alphabetical sequence to give an example of an application to this type of code (Budaghyan & Parker, 2019, pp.)

4.3.6 Example

If we have a (field) word, we can encrypt it. The work involves finding the number of the character and adding 19. The remainder must be 26 in order to find the new number. Finally, we find the corresponding character of the resulting number, where the result of the combination is 19, within the limit of the 26 letters. The process of adding the word (FILED) to the word (YBEXW) as shown in the following Table 14."

Table 14. Table The process of adding the word (FILED) to the word (YBEXW)



F	I	L	E	D
Y	B	E	X	W

4.4 Method of Linking Linear Codes [n, k, d] $_{19}$ and Coding Methods

"This method involves linking between the linear codes obtained in the second chapter and the methods of coding mentioned earlier in Chapter 3. The method is to link the linear code with the code and the digital code, using the polypus box and configuring the password On the linear code numbers, this method differs from previous methods. The password we draw and the characters we arrange with the polypus box and give the letter J the coordinates 00 and the first number of the vertical coordinates and the

second number of the horizontal coordinate, as shown in the following examples"

4.4.1 Example

Encode the text IRWOHUAYNX using the linear code [325,3,307] 19 and the code

(Baybed) using a polypus box?

First we assign the numbers of the linear code 325330719 and find the literal value of each number through the following table15.

Table 15. Table text IRWOHUAYNX using the linear code [325,3,307] $_{19}$

Character	Numerical value	Character	Numerical value	Character	Numerical value
A	0	J	9	S	18
B	1	K	10	T	19
C	2	L	11	U	20
D	3	M	12	V	21
E	4	N	13	W	22

F	**5**	**O**	**14**	**X**	**23**
G	**6**	**P**	**15**	**Y**	**24**
H	**7**	**Q**	**16**	**Z**	**25**
I	**8**	**R**	**17**		

From the table, the numbers of the linear code will be 3 = D, 2 = C, 5 = F, 0 = A, 7 = H, 1 = B, 9 = J The key word will be the linear code, DCFDDAHBJ,

DCFDDAHBJEGIKLMNOPQRSTUVWXYZ Now we take these characters arranged by the Piolis box without duplicating the symmetry and give J coordinate 00as shown in the following Table 16."

Table 16. Table linear code, DCFDDAHBJ

	1	**2**	**3**	**4**	**5**
1	**D**	**C**	**F**	**A**	**H**
2	**B**	**E**	**G**	**I**	**K**
3	**L**	**M**	**N**	**O**	**P**
4	**Q**	**R**	**S**	**T**	**U**

Then write the numbers under each letter vertically as shown below: as shown in the following Table 17."

Table 17. Table letter vertically

I	**R**	**W**	**O**	**H**	**U**	**A**	**Y**	**N**	**X**
4	**2**	**2**	**4**	**5**	**5**	**4**	**4**	**3**	**3**
2	**4**	**5**	**3**	**1**	**4**	**1**	**5**	**3**	**5**

"These numbers are arranged by typing the coordinates of each letter vertically under each character. For example, the coordinates of the letter R are 24 and these numbers are written vertically under each letter, ie 2 and 4. Then the numbers are read horizontally to form the following series of numbers:

4224554433245314153 5.

This series of numbers is then written in units of each unit consisting of two numbers separately as shown below:

42 24 55 44 33 24 53 14 15 35

The next step is to take every two numbers (which represent the coordinates of one of the numbers) to see the corresponding letter of these coordinates. Each two digits are considered to be events of one of the letters of the matrix in order to have the following output"as shown in the following Table 18.

Table 18. Table series of numbers

42	24	55	44	33	24	53	14	15	35
R	I	Z	T	N	I	X	A	H	P

"The coordinates will be read first, the column number and second the row number, for example, the number 42, 2 represents the column number, 4 represents the row number, and so on the other coordinates

The result of the IRWOHUAYNX text encoding using the linear code, the PEPOLIS box, the BEFID code, and the numeric code is the RIZTNIXAHP text.

We use the same method in all the codes obtained through the engineering construction proces"

References

Alex, E., Gottfried, H., Eike, K., Carla, R., & Jorge, V. (2013). An algebraic framework for Di_e-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, Advances in Cryptology {CRYPTO 2013, Part II, *volume 8043 of Lecture Notes in Computer Science, 129-147*. Springer. https://doi.org/10.1007/978-3-642-40041-4

Bennett, C. H., Brassard, G., & Breidbart, S. (2014). Quantum cryptography II: How to re-use a one-time pad safely even if P= NP. *Natural computing, 13*(4), 453-458. https://doi.org/10.1007/s11047-014-9453-6

Budaghyan, L., Li, C., & Parker, M. G. (2019). Special Issue on Mathematical Methods for Cryptography. https://doi.org/10.1007/s12095-019-00356-8

Jae Hong, S., & Jung, H. Ch. (2012). Beyond the limitation of prime-order bilinear groups, and round optimal blind signatures. In Ronald Cramer editor, TCC 2012: 9th *Theory of Cryptography Conference, volume 7194 of Lecture Notes in Computer Science,* pages 133-150. Springer, March 2012. https://doi.org/10.1007/978-3-642-28914-9

Kahrobaei, D., Tortora, A., & Tota, M. (2019). Multilinear Cryptography using Nilpotent Groups. arXiv preprint arXiv:1902.08777

Nilsson, A., Johansson, T., & Wagner, P. S. (2019). Error Amplification in Code-based Cryptography. IACR *Transactions on Cryptographic Hardware and Embedded Systems,* 238-258. https://doi.org/10.13154/tches.v2019.i1.238-258

Shukla, P., Khare, A., Rizvi, M., Stalin, S., & Kumar, S. (2015). Applied cryptography using chaos function for fast digital logic-based systems in ubiquitous computing. *Entropy*, *17*(3), 1387-1410. https://doi.org/10.3390/e17031387

Yan, X., Wang, S., Niu, X., & Yang, C. N. (2015). Generalized random grids-based threshold visual cryptography with meaningful shares. *Signal Processing, 109,* 317-333. https://doi.org/10.1016/j.sigpro.2014.12.002

Copyrights