

MUZAFER SARAČEVIĆ AYBEYAN SELIMI FARUK SELIMOVIĆ 

GENERATION OF CRYPTOGRAPHIC KEYS WITH ALGORITHM OF POLYGON TRIANGULATION AND CATALAN NUMBERS

Abstract *In this paper, a procedure for the application of one computational geometry algorithm in the process of generating hidden cryptographic keys from one segment of a 3D image is presented. The presented procedure consists of three phases. In the first phase, the separation of one segment from the 3D image and determination of the triangulation of the separated polygon are done. In the second phase, a conversion from the obtained triangulation of the polygon in the record that represents the Catalan key is done. In the third phase, the Catalan-key is applied in the encryption of the text based on the balanced parentheses combinatorial problem.*

Keywords computational geometry, polygon triangulation, Catalan numbers, cryptography, hidden cryptographic keys.

Citation Computer Science 19(3) 2018: 243–256

1. Introduction

Visual cryptography is a special encryption technique that allows us to hide information (secret messages) in an image in such a way that a person can decode it only if he knows and uses the correct key. Hiding information is a great area and a modern way of communication for successfully avoiding attacks and deciphering confidential information.

In this paper, a way of applying a simple polygon triangulation algorithm in the process of generating hidden cryptographic keys from one segment of a 3D image is represented. This paper determines the importance of computational geometry (polygon triangulation) and Catalan numbers that hold the cryptology, primarily in the development of algorithms for generating binary sequences that are necessary for generating keys.

Computational geometry is an integral part of mathematics that deals with the algorithmic solving of geometric problems. This discipline is considered to be a branch of computer science, which was created as a result of an attempt to solve geometric problems with a computer. From the very beginning, computational geometry has connected different areas of science and technology such as the theory of algorithms as well as combinatorial and Euclidean geometry, but also includes data structures, optimization, etc. Today, computational geometry has a great deal of application in computer graphics, visualization, GIS, CAD programs, etc.

In the background of a view (images, animations, etc.), complex geometric calculations and theories are hiding (which were confirmed and developed a long time ago); however, we are still at the beginning from the aspect of its application in modern information technologies. Triangulation of a simple polygon is one of the more important problems applied in computational geometry. This problem is applied in the process of obtaining three-dimensional representations of objects from a set of points.

Generally, the methods of counting and Catalan numbers in asymmetric cryptographic systems hold an important place in generating keys, the design of a cryptologic algorithm, and the process of cryptanalysis [1–3]. In references [4, 6, 7], the concrete applications of combinatorial problems in cryptography are listed. In papers [8, 12], concrete applications of Catalan numbers for solving of some combinatorial problems in computational geometry can be seen. Doctoral dissertation [11] presents the methods and techniques for solving some problems in the field of computational geometry based on Catalan numbers and combinatorial problems that are applied in the field of cryptography in the second paper of author [9]. So, a combination of computational geometry, cryptography, and combinatorics is made in this paper.

2. Catalan numbers and polygon triangulation algorithm

Catalan numbers represent a sequence of numbers that are primarily used in geometry as well as for solving some combinatorial problems. These were discovered by Leonard

Euler as he sought a general solution for the number of different ways in which one polygon of n sides can be divided into triangles. It should be taken into consideration not to use the diagonals of polygons that intersect each other. However, these numbers were named after Belgian mathematician Eugene Charles Catalan, who discovered the connection between these numbers and the problem of the correct sequences of n -pairs of parentheses (hereinafter referred to as balanced or paired parenthesis).

Catalan numbers $C_n, n > 0$ represent sequences of natural numbers that appear as a solution of a large number of combinatorial problems. These numbers are defined as follows:

$$C_n = \frac{(2n)!}{(n+1)!n!} = \frac{1}{n+1} \binom{2n}{n}, n \geq 0 \tag{1}$$

Table 1 shows the Catalan numbers for $n \in \{1, 2, \dots, 30\}$ calculated with formula (1).

Table 1
First 30 values of Catalan numbers

n	C_n	n	C_n	n	C_n
1	1	11	58,786	21	24,466,267,020
2	2	12	208,012	22	91,482,563,640
3	5	13	742,900	23	343,059,613,650
4	14	14	2,674,440	24	1,289,904,147,324
5	42	15	9,694,845	25	4,861,946,401,452
6	132	16	35,357,670	26	18,367,353,072,152
7	429	17	129,644,790	27	69,533,550,916,004
8	1,430	18	477,638,700	28	263,747,951,750,360
9	4,862	19	1,767,263,190	29	1,002,242,216,651,368
10	16,796	20	6,564,120,420	30	3,814,986,502,092,304

Catalan numbers are widely used in solving many combinatorial problems. In monograph [5], concrete applications of these numbers are listed along with possible solutions when it comes to representations of Catalan numbers. The author in [13] lists a set of problems that describes more than 60 different interpretations of Catalan numbers.

We can enumerate some of the interpretations: *binary trees, polygon triangulations, the problem of paired or balanced parentheses, stack permutations, Ballot problem, lattice path problem*, etc. It is generally known that all of these combinatorial problems can be solved on the basis of values that possess the properties of Catalan numbers; more precisely, the solution of these combinatorial problems are

covered with the application of these numbers. Therefore, the number of combinations and the method for generating Catalan numbers constitute a solution for certain combinatorial problems.

The procedure presented in this paper is focused on the proposal of generating a Catalan number based on the isolated triangulation from one part of a 3D image. The resulting Catalan number will represent a key for the encryption and decryption of confidential information (hereinafter referred to as a *Catalan – key*). Encryption can be implemented in combination with the aforementioned combinatorial problems that are based on (and whose solutions are given) with these numbers. For a concrete example of the encryption in this paper (in Section 4), an example with balanced parentheses is taken.

3. Connectedness of convex polygon triangulation and Catalan numbers

The triangulation of a polygon is a historically very old problem that led to the discovery of Catalan numbers. The triangulation of a simple polygon is a decomposition of the interior of the polygon into triangles with non-intersecting internal diagonals [8]. In triangulation, a maximum number of the different ways of decomposing convex n -gon to $n - 2$ triangles that are labeled with T_n are actually considered; hence, these decompositions are called triangulations. Triangulation of the n -angle polygon requires a division of triangles with $(n - 3)$ -internal non-intersect diagonals. For convex polygons, all diagonals are internal diagonals. In this case, the number of triangulations of a convex n -angle polygon is independent of the form and can be uniquely characterized by number of vertices n . In papers [8, 12], some ways of solving this type of problem have been presented.

Now, we will associate the concept of polygon triangulation and Catalan numbers. If we denote the number of triangles of the n -angle with T_n , then the following relationship holds:

$$T_n = C_{n-2}, n \geq 3 \quad (2)$$

Label n is the number of vertices in the polygon. On the basis of (2), T_n is represented in the following form:

$$T_n = \frac{1}{n-1} \binom{2n-4}{n-2} = \frac{(2n-4)!}{(n-1)!(n-2)!} \quad (3)$$

Triangulation allows for the display of three-dimensional objects from a set of points and provides a mechanism for the so-called “ironing” of three-dimensional figures (see Figure 1).

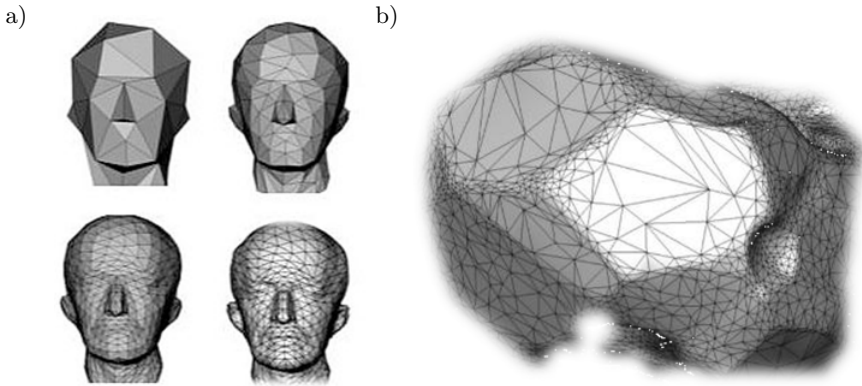


Figure 1. Method of *ironing* three-dimensional figures (a); separation of one segment from 3D image (b)

The triangulation technique in computational geometry is the most common paneling method. The easiest way of segmenting and ironing with double-curved surfaces is via a triangle network. The advantage of the triangle as a geometric figure is that the area within three points is always straight.

In the procedure developed in this research, we will apply the polygon triangulation method that has wide application in the modeling of 3D objects. The advantages of this method are the small deviations from the original shape, good structural properties, and possibility of cladding the complex free forms. We use the method of separating of one segment in the 3D image with the goal order to obtain the material for generating a hidden Catalan-key.

4. Extraction of Catalan-key from one segment of image

This section explains the work methods of generating cryptographic keys based on triangulation. This process consists of three phases:

1. Separation of one segment from a 3D image and definition of the triangulation in the separated polygon.
2. Converting the triangulation of a polygon into a binary or some other record that corresponds to the property of the Catalan number. From this phase, we get the record of the Catalan-key.
3. Application of the Catalan-key in the encryption of text on the basis of some combinatorial problem based on Catalan numbers.

In the first phase, we will extract a segment from the 3D image that will serve as the material for generating a hidden *Catalan – key* (see Figure 2).

Hence, it is now very easy to connect the binary tree with the triangulation of the polygon; thus, it is easy to represent each triangulation as a binary record or in the form of balanced parentheses (see Figure 4), provided that the last bit 0 in the binary record is eliminated in order to satisfy the condition of the *bit balance*. This does not affect the uniqueness of the binary records nor the notation of the balanced parentheses.

The resulting record from the second phase corresponds to a Catalan number or Catalan-key. The Catalan-key property is equal with the bit-balance property, which means that a number can be labeled as a Catalan number when its binary form consists of numbers equal to “1” and “0” and starting with “1”. If a binary notation of a Catalan number is connected with the mode of the balanced parentheses, then “1” represents an open parenthesis and “0” represents a closed parenthesis. It can be said that each opened parenthesis closes or each bit 1 has its pair (which is bit 0).

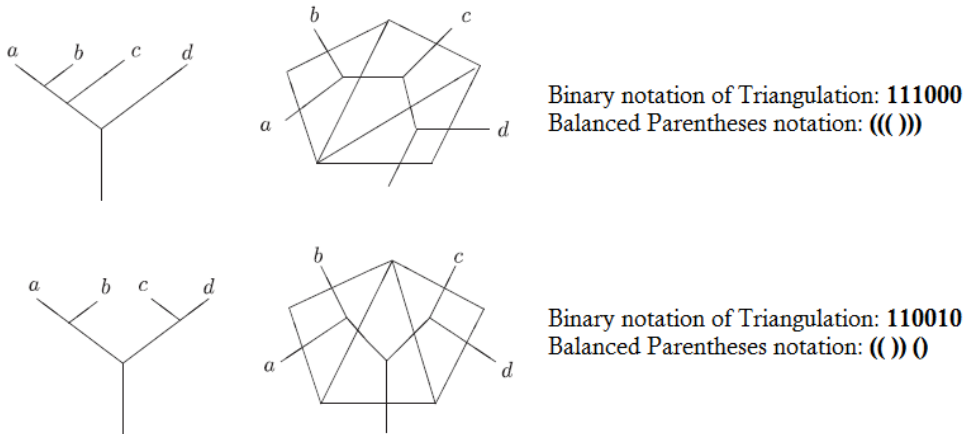


Figure 4. Second phase: triangulation and corresponding binary tree for first two cases from previous figure

Example: We are going to analyze the values that are generated in the C_3 set. For $n = 3$, we have a set of $C_3 = 5$ values that appease the Catalan number property based on formula (1).

These are the numbers $C_3 = \{42, 44, 50, 52, 56\}$ or, based on their binary format, $C_{bin} = \{101010, 101100, 110010, 110100, 111000\}$. We determine the property that corresponds to a Catalan number, which is the bit-balance property. Now, we will analyze one record that does not match the balance property; then, we will check the situation with the number that does not satisfy the bit-balance property. The first case is the number 43 its binary record is 101011. We can immediately notice that there is a balance property violation, and this happens in the sixth bit. The same case is with the number 45 (with a binary record is 101101). We can notice that there

is a balance property violation in the fourth bit. These numbers cannot be used for text encryption on the basis of a combinatorial problem that is based on the Catalan numbers.

5. Cryptanalysis of Catalan keys

In our previous papers [9, 10], we are going to analyze the values that are generated in the C_n set. For the purposes of Catalan number validity verification, we will use the binary notation. The basic feature that must be fulfilled is *bit property balance* in the binary form for a certain number from the C_n set (we will refer to this property as the bit-balance property). For example, we have the space of keys $C_{30} = 3.814.986.502.092.304$ for basis $n = 30$; i.e., the values that satisfy the property of the Catalan number. By increasing the n basis, the key space also drastically increases. In order to provide a stronger encryption (i.e., a more resistant mechanism of cryptanalysis), it is necessary to choose keys whose value bases are mainly greater than 30.

From the aspect of the cryptanalysis of Catalan keys, if n is the basis for key generation, then C_n is the total number of different binary formats that meet the Catalan number property. For example, $C_{30} = 3.814.986.502.092.304$ is calculated for basis $n = 30$ according to the formula for calculating the Catalan number. Thus, for 60-bit keys, there are 3.814.986.502.092.304 valid values that satisfy the condition of balance (i.e., the Catalan number property).

In an attempt to find all of these Catalan numbers and perform their writing on a disk, the necessary space for this is 30.519.892.016.738.432 bytes (or 28.423.864 GB, or 27.757 TB). This means that this process is very demanding when it comes to memory resources. On the other hand, if we want to find out all of the 60-bit Catalan numbers and whether 1 ms is needed for access to every element from the C_n set, the execution would take 120,972 years. The average time will be $120,972/2 = 60,486$ years. Therefore, this process is very demanding when it comes to time as well.

To provide an encryption mechanism on cryptanalysis that is as strong and resistant as possible, the keys must be chosen mainly for those values with bases greater than 30. With the application of the software solution in the *Java* programming language [9], we will show the number of values for bases n from 140 to 150:

```

C(140)= 656376399024616169349253607753345435388942038466586811952779656067170646392272840
C(141)= 2597771382055171036438595264488592497806939617029730903644099765561619037129981240
C(142)= 10282088127575012633735978459444359117193900861809983856381541729425708916192792880
C(143)= 40699932171651091675204914735300588172225857577997852764843602678976764459929805150
C(144)= 161115593562260183597018076262500259385225118963936327496691227156776984827584194180
C(145)= 637841185472509493966277041641953081675754238090104091048544721209706145413312768740
C(146)= 252533040778911922100934175670487546622645554887350891090156651320061065513932186440
C(147)= 9998943371381242321023474793439574481139884832189105555262377011307809353994353116580
C(148)= 39593131470570019928884900188787576804513637926117934749025519709205419589642069387800
C(149)= 1567888006234572789183384204747598804145874006187427021606141058048453461574982594775688
C(150)= 620925183926009621146978506218967449531342090729015621989883130549504437230725772687824

```


6. Application of Catalan keys for encryption based on combinatorial problem

In the third phase of our procedure, we present Catalan numbers as a key for text encryption over a combinatorial problem of balanced parentheses. The binary notation of the Catalan number can be represented in the form of a paired (balanced) parenthesis. The problem relates to the calculation of the number of combinations of the possible parentheses pairs. This number of possible valid combinations is directly determined by Formula (1) for calculating the set of Catalan numbers C_n . If we want to present the binary record of Catalan numbers in the Balanced Parentheses notation, then we present bit 1 with open parenthesis “(”, and bit 0 with a closed parenthesis “)”.

We will show the text encryption process where open text values are taken as a binary record (the substitution cipher is obtained). Based on the character layout “(” and “)” in the key record, the elements can have two states:

1. *Free (open) element* – this is a character from a message that is not encrypted; more accurately, it is not transferred in the cipher. A free (open) element is conditioned by the occurrence of an open parenthesis (in a key) that is waiting for its pair (i.e., a closed parenthesis).
2. *Busy (closed) element* – this is a character from a message that is encrypted and moved to the cipher. A busy (closed) element is conditioned by the occurrence of a closed parenthesis (in a key). In this way, the element is “closed” (i.e., transferred to the cipher) because the character “)” appeared, which closes the corresponding “(” character.

Example: Let character “C” is open text. If ASCII Text to Binary is applied to character “C”, then sequence of bits 0100011 is obtained. For example, if we use key $K = ()()(((())()))$ on the basis of which we will perform the permutation of the bits from the message, we obtain the following sequence of bits: 01011000 (i.e., the binary cipher). By applying Binary to ASCII Text to the given cipher, character “X” is obtained (see Figure 5).



Figure 5. Encryption of character “C” in character “X”, based on Catalan-key $K = ()()(((())()))$

Example: Let string P_{txt} ="CRYPTOLOGY" be open text. If ASCII Text to Binary is applied to P, then the following sequence of bits is obtained: P_{bin} = 01000011 01010010 01011001 01010000 01010100 01001111 01001100 01001111 01000111 01011001.

For example, if we use key $K = ((()))(())(())(())$ on the basis of which we will perform the permutation of the bits from the message, we obtain the following sequence of bits (i.e., the binary cipher): C_{bin} =01000010 01010100 01100010 01110000 00111000 01010110 01110010 01001110 01101001 01110011.

By applying *Binary to ASCII Text* to the given cipher, cipher C_{txt} ="BTbp8VrNis" is obtained.

If we compare the open text P_{txt} ="CRYPTOLOGY" and the cipher C_{txt} ="BTbp8VrNis", we can see that the first character "Y" is replaced by "b" and the other character "Y" with "s." The same case is with the "O" characters, where the first is replaced with "V" and the other with "N".

In this way, we provide a stronger encryption mechanism; that is, one character is replaced by some completely different character depending on the received bit permutation. In this case, we do not have the classic transposition cipher as in the previous examples, but we have the needed substitution cipher.

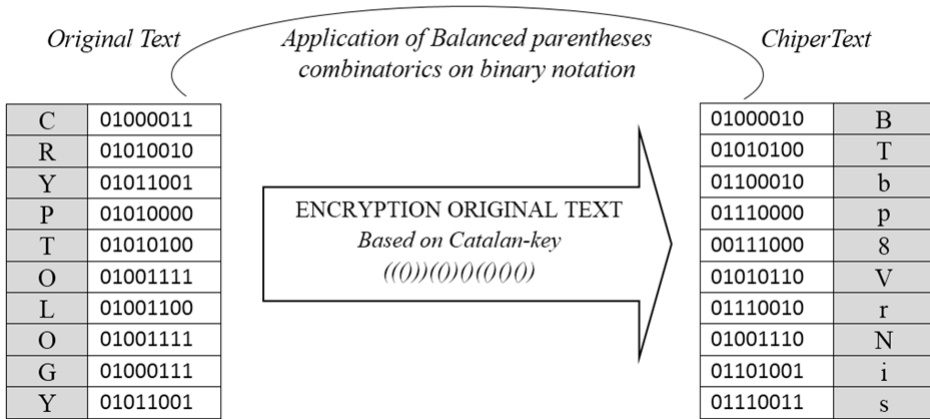


Figure 6. Encryption of string CRYPTOLOGY to string "BTbp8VrNis", based to Catalan-key $K = ((()))(())(())(())$.

It is important to note that the classic substitution isn't realized here, as one character from the message is not always replaced with the same character in the cipher. The substitution mode depends on the key itself and its length as well as from the bit key schedules. In addition, the process depends on the length of the message and the size of the segment in the message that is taken in the encryption process.

7. Application areas of proposed method

The main areas of application of our proposed method are as follows:

- Biometric authentication and generating of cryptographic keys from 3D image.
- Crypto-key management and application in cryptography as public key.
- Steganography and hiding secret information in image.

The goal of multi-factor authentication is to form a layered defense that relies on two or more different ways of determining the authenticity of the user when logging onto a system (authentication) and giving access privileges (authorization). These techniques combine what the user knows, what the user owns, and what physically identifies the user (biometric verification). The method developed in our research could find application exactly in biometric authentication. Our method is based on generating one's own key – for example, everyone has a potential key in a 3D view of their characteristic facial lines; therefore, everybody is the carrier of his/her own unique key that is generated from a triangulation of the scanned polygon. This is a pretty interesting possibility of authenticating users because there is no possibility of stealing the key (as is the case with the previous two approaches). By introducing this procedure of determining the authentication of users, unauthorized access to computers, mobile devices, physical locations, networks, or databases is made difficult.

More and more companies around the world are giving up ciphers and authentication cards and are turning to the stronger protection using biometric data. Biometric authentication uses the properties of the user for the purpose of speeding up the confirmation of someone's identity. Leading smartphone manufacturers recognize that user security is playing an increasingly important role, so they started to incorporate biometric sensors and authentication to ensure that only the authorized user can access his/her device. Different techniques are applied, such as facial recognition, fingerprint authentication, voice recognition, or retinal scanning.

Furthermore, the application of our method could have another dimension; that is, in the process of managing cryptological keys. Managing cryptographic keys is one of the most important problems in modern cryptography. Although these algorithms are based on extensive academic research, the process of creating secure and high-quality cryptological algorithms is not simple. Basically, key generation and its security is a much more difficult procedure. When attacking symmetric and asymmetric systems, cryptanalysts will first attack the key management system before attempting to discover the cryptographic algorithm that is applied. In order to safely protect an encryption system, the main purposes are to perform the generation, distribution, and management of cryptographic keys as efficiently as possible. It is precisely in these steps where the application of our method is covered.

Our method ensures the efficient generation of a key from an image; the distribution and management are done in the form of a binary Catalan-key. So, the method developed in this research ensures efficient key management with an emphasis on the

secure generation, distribution, and storage of keys. It is important to point out that the definition of absolute coincidence is difficult, and its measure is represented by entropy. On the other hand, sources of coincidence can be achieved by software. However, it should be taken into account that software is a deterministic system, while generating a key from a moving image provides a better quality random sequence (but, it must be emphasized that the number of such strings remains limited).

The security of the method of key management is of extreme importance. When the key is generated once, it must remain a secret in order to avoid situations such as impersonation. When it comes to Public Key Infrastructure (PKI), most attacks occur at the key management level in practice, and the algorithms themselves are very rarely attacked. Therefore, the proposed method can also be used in the process of hiding a key in public key cryptography.

The third aspect of applying our method is in the process of hiding information. Steganography is a technique meant to hide secret messages in such a way that no one but the transmitter and receiver is aware of the existence of the communication. Hiding messages is based on disguising the message inside images, movies, and text. The main advantage of steganography as related to cryptography is the fact that the messages do not attract attention to themselves.

We can say that this technique can avoid the “man-in-the-middle” attack since the attacker is not aware of the existence of a communication in the communication channel. In our case, the key is not transmitted by the communication channel; the unique key is contained (hidden) in the picture. In addition to the key, it is also possible to hide other information in the same way.

8. Conclusion

Bearing in mind the fact that cryptography is a very dynamic, current, and widespread discipline, a contribution to the application of combinatorics and computational geometry in the field of cryptography is given in this paper.

In this paper, the possibilities of applying polygon triangulation and Catalan numbers are considered, along with the combinatorial problems in cryptography. The theoretical bases of our research are listed where the basic properties of Catalan numbers are examined; first of all, the emphasis is placed on the bit balance property in the binary record of a Catalan number, which is related to the combinatorial problem – balanced parenthesis.

From the aspect of the achieved results, we can say that we have proposed the application of a polygon triangulation algorithm in the process of generating hidden cryptographic keys from one segment of a 3D image.

The obtained key has the property of Catalan numbers and has a large key space, which gives priority when cryptanalysis is concerned. In this case, these numbers serve as pseudo-generators that, in combination with many other combinatorial problems, can provide an effective mechanism for encrypting and decrypting text.


References

- [1] Amounas F., El-Kinani E.H., Hajar M.: Novel Encryption Schemes Based on Catalan Numbers, *International Journal of Information and Network Security*, vol. 2(4), pp. 339–347, 2013.
- [2] Cohen E., Hansen T., Itzhaki N.: From entanglement witness to generalized Catalan numbers, *Scientific Reports*, 6:30232, pp. 1–10, 2016.
- [3] Higgins P.M.: Number Story: From Counting to Cryptography, *Springer Science and Business Media, Berlin, Germany*, 2008.
- [4] Horak P., Semaev I., Tuza I.Z.: An application of Combinatorics in Cryptography, *Electronic Notes in Discrete Mathematics*, vol. 49, pp. 31–35, 2015.
- [5] Koshy T.: Catalan Numbers with Applications. *Oxford University Press, New York*, 2009.
- [6] Kościelny C., Kurkowski M., Srebrny M.: Modern Cryptography Primer: Theoretical Foundations and Practical Applications, *Springer Science and Business Media, Berlin, Germany*, 2013.
- [7] Lachaud G., Ritzenthaler C., Tsfasman M.A.: Arithmetic, Geometry, Cryptography, and Coding Theory, *American Mathematical Society, USA*, 2009.
- [8] Saračević M., Stanimirović P., Mašović S., Biševac E.: Implementation of the convex polygon triangulation algorithm. *Facta Universitatis, Series Mathematics and Informatics*, vol. 27(2), pp. 213–228, 2012.
- [9] Saračević M.: Application of Catalan numbers and some combinatorial problems in cryptography (Bachelor's thesis), *Faculty of Informatics and Computing, Singidunum University in Belgrade*, 2017.
- [10] Saračević M., Koričanin E., Biševac E.: Encryption based on Ballot, Stack permutations and Balanced Parentheses using Catalan-keys, *Journal of Information Technology and Applications*, vol. 14(2), pp. 69–77, 2017.
- [11] Saračević M.: Methods for solving the polygon triangulation problem and their implementation (PhD thesis), *University of Niš, Serbia*, 2013.
- [12] Stanimirović P., Krtolica P., Saračević M., Mašović S.: Decomposition of Catalan numbers and convex polygon triangulations, *International Journal of Computer Mathematics*, vol. 91(6), pp. 1315–1328, 2014.
- [13] Stanley R.P.: Catalan addendum to Enumerative Combinatorics, <http://www-math.mit.edu/~rstan/ec/catadd.pdf> [Available 24.05.2017.]


Affiliations

Muzafer Saračević 

University of Novi Pazar, Department of Computer Sciences, Serbia, muzafers@uninp.edu.rs,
ORCID ID: <https://orcid.org/0000-0003-2577-7927>

Aybeyan Selimi 

International Vision University, Faculty of Informatics, Macedonia, aybeyan@vizyon.edu.mk,
ORCID ID: <https://orcid.org/0000-0001-8285-2175>

Faruk Selimović 

University of Novi Pazar, Department of Computer Sciences, Serbia; faruk@uninp.edu.rs,
ORCID ID: <https://orcid.org/0000-0002-0367-9122>

Received: 09.01.2018

Revised: 26.05.2018

Accepted: 26.05.2018