JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 37, 469-482 (2021)
DOI: 10.6688/JISE.202103_37(2).0012

Source and Channel Models for Secret-Key Agreement Based on Catalan Numbers and the Lattice Path Combinatorial Approach

MUZAFER SARAČEVIĆ[1], SAŠA ADAMOVIĆ[2], NEMANJA MAČEK[3],
AYBEYAN SELIMI[4] AND SELVER PEPIĆ[5]
[1]*Department of Computer Sciences*
University of Novi Pazar
Novi Pazar, 36300 Serbia
[2]*Faculty of Informatics and Computing*
Singidunum University
Belgrade, 11000 Serbia
[3]*Faculty of Computer Sciences*
Megatrend University
Belgrade, 11000 Serbia
[4]*Faculty of Informatics*
International Vision University
Gostivar, 1230 North Macedonia
[5]*HTM School of Professional Studies in Trstenik*
Trstenik, 37240 Serbia
E-mail: muzafers@uninp.edu.rs; sadamovic@singidunum.ac.rs;
macek.nemanja@gmail.com; aybeyan@vizyon.edu.mk; selverp@gmail.com

This paper presents a solution to secret key sharing protocol problem that establishes cryptographically secured communication between two entities. We propose a new symmetric cryptographic key exchange scenario based on the specific properties of Catalan numbers and the Lattice Path combinatorics. Our scenario consists of three phases: generating Catalan values, defining the Lattice Path movement space and defining the key equalization rules. In the experimental part of this study, we have merged our scenario with the Maurer's protocol, while in the information-theoretical approach to the key exchange we have presented how a partially split bit sequence can become the secret key that both parties in communication can use. Maurer's satellite scenario model for the exchange of the Catalan key is discussed in detail and its application is proposed. Security analysis of the protocol and testing for channel capacity or key generation speed is also suggested.

Keywords: cryptography, secret key sharing protocol, Catalan numbers, Lattice path, Maurer's satellite scenario

1. INTRODUCTION

The core of modern communication is a protocol that ensures a sufficient degree of secrecy. These protocols can be absolute, apropos theoretically or computationally safe. Storing the keys or choosing the key that one can trust to can be a major problem. The likelihood that the key and all available copies will be lost is inversely proportional to the number of instances that the copies are trusted. By increasing the number of instances,

Received September 16, 2019; revised March 9, 2020; accepted March 17, 2020.
Communicated by Sun Hung-Min.

there is a growing risk of the key being compromised.

The problem of secret key distribution is constantly present since the very beginnings of cryptography. Regardless of how much the cryptographic algorithm is theoretically secure, it can be jeopardized by key distribution. Many researchers believe that the issue of key distribution in the cryptographic system is its' the weakest point. If two entities want to exchange data in a secure environment, they must trust the third party that distributes keys (usually referred to as trusted third party in the literature). This trust relationship may become a security weak point.

Key management is extremely important for security of the entire communication system. In cryptology-based infrastructure, majority of attacks are aimed at the key management level. Participants in cryptographic systems must be able to generate keys. If the key is lost or compromised in any other way by any participant in the communication, others must be warned promptly. Otherwise, the adversary will be able to decrypt messages with the stolen key. Since the keys have a limited life expectancy, the most important reason for their periodic replacement is protection against cryptanalysis.

The main contribution of this paper is a novel symmetric cryptographic key exchange scenario based on the specific properties of Catalan numbers and the Lattice Path combinatorial approach, as well as how it can be merged with the Maurer's satellite scenario.

The rest of the paper is organized as follows. Relevant researches regarding cryptographic key distribution are discussed in section two. Section three provides the basic settings relating to the specific properties of Catalan numbers and the Lattice Path combinatorial problem as well as some of its constraints. Additionally, this section also discusses the connection between Catalan numbers and the given problem. Section four describes our symmetric cryptology key exchanging scenario consisting of three phases: generating Catalan values, defining the Lattice Path movement space and defining key equalization rules. Section five deals with a comparison and combination of our key exchange scenario with Maurer's satellite scenario. Security analysis of the protocol and testing for channel capacity or key generation speed is also discussed in that section. Concluding remarks and proposals for further work are given in the final section of this paper.

2. AN OVERVIEW OF RELATED RESEARCH

The security of cryptography-based infrastructure heavily depends on the cryptographic key management. In a two-party setup, cryptographic protocols often ignore the possibility that both parties will transmit messages simultaneously. Most two-party protocols have been designed assuming that parties alternate sending their messages.

Reyes *et al.* [1] presented the permutation parity machine, an artificial neural network proposed as a binary variant of the tree parity machine. A key agreement mechanism based on neural synchronization of two permutation parity machines is defined. Recently, it was shown that two artificial neural networks can synchronize themselves by mutual learning.

Applied number theory has numerous applications in cryptography, especially in the field of the integer sequences. Previous cryptographic algorithms were designed using the integer sequences of the Fibonacci sequence, Lucas and Catalan numbers. According to the research of Romankov and Obzor [2], many known schemes of the cryptographic key public exchange protocols in algebraic cryptography using two-sided multiplications and in most cases, such schemes are based on the platforms that are subsets of some linear spaces. This method allows computing the exchanged keys without computing any private data and without solving the hard algorithmic problems. Authors concluded that this method can be successfully applied to the further scenarios and general scheme and, thus, is a universal one. Zhang [3] presented two provably-secure protocols for two-party authenticated key exchange (AKE) which require not only a single round, but more efficient message transmission from a computational perspective. The protocol provides implicit authentication, key independence and forward secrecy.

Fahmy [4] presents protocol based on the public key cryptosystem (elliptic curve cryptosystem) that exchanges cipher keys over an insecure communication channel. It refers to key generation, distribution, storage, and deletion. The author emphasizes that designing secure cryptographic algorithms is hard, and keeping the keys secret is much harder and that cryptanalysts usually attack cryptosystems through their key management.

Barman and Chattopadhyay [5] introduced a key-exchange protocol that uses biometric data of the sender and the receiver. The session is established between enrolled users through the central server. A user generates a cryptographic key randomly and shares it with another user using biometrics-based cryptography. In this key-exchange protocol, the privacy of the biometric data for both sides is preserved.

Also, Barman *et al.* [6] introduced a CBS to exchange a randomly generated cryptographic key with user's fingerprint data. This method also protects the privacy and security of fingerprint identity of the user using cancelable biometrics. The cryptographic key is hidden within fingerprint data using a fuzzy commitment scheme and it is extracted from cryptographic construction. This concept of using cryptography for secure communication brings out the requirement of cryptographic key management. Zhou [7] examined some security issues on the Internet Key Exchange protocol. It is important to emphasize that secure communication over the Internet becomes an essential requirement for any value-added Internet application.

3. PRELIMINARIES ON CATALAN NUMBERS AND LATTICE PATH

The goal of our previous research papers [8-12] was to evaluate if Catalan numbers can be used in cryptography. So far, we have demonstrated [10] that Lattice Path combinatorial problems which are based on the properties of Catalan numbers can be used for encrypting and decrypting files and plaintext. Accordingly, we have used the NIST (National Institute of Standards and Technology) statistical battery of tests to verify the quality of generated keys.

Catalan numbers (C_n) represent a sequence of numbers which are primarily used in solving many combinatorial problems. Catalan numbers are defined as [13]:

$$C_n = \frac{(2n)!}{(n+1)!n!}\cdot \tag{1}$$

The basic feature that must be fulfilled is bit property balance, in the binary form for a certain number from the C_n set. Catalan number property is defined as follows [13]: a number can be labeled as a Catalan object when its binary form consists of numbers equal to “1” and “0” and starting with “1”. This property is known as a Dyck word in Algorithm 1.

Algorithm 1: Catalan binary (dyck) word generator.

```
INPUT: n (base for Catalan number $C_n$)
1. Initialize count=0.
2. Recursively call Step 2 until 'bit 1' count is less than the given n
2.1 If 'bit 1' count becomes more than the 'bit 0' count, then put a ‘bit 0’ and recursively call for the remaining bits.
2.2 If 'bit 1' count is less than n, then put an 'bit 1' and call step 2 for the remaining bits.
OUTPUT: Binary notation with Catalan properties (bit balance or Dyck word)
```

For example, for the basis $n = 30$, the space of value $C_{30} = 3\ 814\ 986\ 502\ 092\ 304$ *i.e.*, the values that satisfy the property of Catalan object (Catalan-key). By increasing the n basis, the key space is also drastically increasing.

Catalan numbers have found widespread usage in solving many combinatorial problems. In [13], concrete applications of these numbers are given, with possible solutions, when it comes to representation over certain combinatorial problems. The binary notation of a Catalan object can be graphically represented in the *Lattice Path* which consists of a number of points in the Cartesian coordinate system. The number of possible valid paths in the Lattice Path is directly determined by the calculating formula for the C_n set of Catalan numbers. The pathways consist of $2n$ steps with the initial point (0, 0) and the end point (n, n). If we apply a binary notation of a Catalan object, then bit 1 represents the movement to the right and bit 0 represents the movement to the up in Fig. 1.

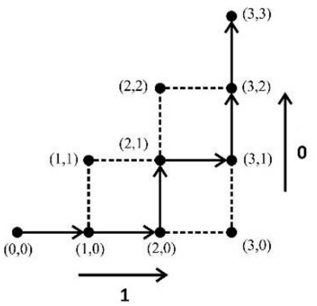


Fig. 1. Lattice path based on the Catalan key $K3 = 110100$.

As shown in Fig. 1, each path in the integer network can be encoded with a specific order of vector movement to the right (1, 0) and vector movement to the up (0, 1). Thus, for a valid Catalan object, the direction through the integer network will do exactly $2n$ movements, starting from the center point (0, 0), and finishing it at the endpoint (n, n). A restriction has been introduced on the network of the size $n \times n$ and it thus, determines how many shortest paths exist in the integer network. The path never crosses its diagonal. The main requirement is that each subsequent step must be closer to the target point. Moving through Lattice Path space can be linked with other notations, such as balanced parenthesis or Ballot problem [14].

Proposition: A number of valid paths in lattice (M_n) correspond to the Catalan number (C_n). ***Proof*:** Let M_n denote the number of possible paths. The first i pairs (bits 1 and 0) can be correctly grouped in M_i ways and the remaining $n - i - 1$ pairs in M_{n-i-1} ways. Using the multiplication principle, these two events can take place together in $M_i\, M_{n-i-1}$ different ways. Because this is true for each value of i, by the addition principle:

$$M_n = \sum_{i=0}^{n-1} M_i M_{n-i-1} = M_0 M_{n-1} + M_1 M_{n-2} + \ldots + M_{n-1} M_0 , \tag{2}$$

where $M_0 = M_1 = 1$, $M_2 = 2$, $M_3 = 5$, $M_4 = 14$, *etc.* Thus M_n satisfies the same recurrence relation and the same initial condition as C_n. Consequently, $M_n = C_n$ for every $n \geq 0$. For properties of generalized Catalan Numbers, function series, generators and random walks see papers [15-19].

4. PROPOSED SCENARIO FOR CRYPTOLOGIC KEY EXCHANGE

Our key exchange scenario consists of the following steps: generating Catalan values, defining the Lattice Path movement space and defining the key equalization rules.

1. Generating Catalan values: Both sides randomly select the Catalan number from the C_n set. The selected Catalan number (in binary form) is represented in the discrete grid with Lattice Path. If the selected value has a bit-balance property (Dyck word), then there is no possibility that side A goes to side B and vice versa. If the selected number does not meet the Catalan number (bit-balance) property then there is the possibility of switching over the diagonal or exiting the lattice. Details of the connection of Catalan numbers with lattice path combinatorial problem are given in [10].
2. Defining the Lattice Path movement space: If the moving space for A side is in the direction of the x-axis, then the movement rule is (1 → right, 0 → top), while for side B whose space is y-axis applies the rule (1 → top, 0 → right) – cf. Fig. 2 (right). There is another variant where side A is in the y-axis direction (1 → top, 0 → right), and the side B by in the x-axis (1 → right, 0 → top) – cf. Fig. 2 (left).

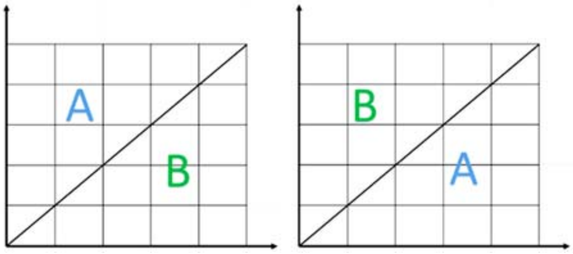


Fig. 2. Defining the lattice path movement space.

3. Defining the key equalization rules: As first, we select the main side, that is, the side that dictates the change. The other side is a secondary one, and it makes the matching of owns bits. An additional parameter is a collocation rule that is implemented in two scenarios – approximation to the diagonal or moving away from the diagonal.

Example 1: How our scenario works step by step on a concrete scenario. The first phase is *generating Catalan values.* The side A randomly selects a decimal value of 856 (binary 1101011000), while side B randomly selects a value of 684 (a binary entry of 1010101100). The condition was the selected values fulfilled the described bit-balance property (Dyck word property).

The second phase is *defining the Lattice Path movement space.* Each side selects the movement axis, and in this example let movements are with the following parameters: side A: *x*-axis (1 → right, 0 → top) and side B: *y*-axis (1 → top, 0 → right). The overall movements of both sides, based on the chosen random Catalan value, is depicted in Fig. 3 and presented in Table 1.

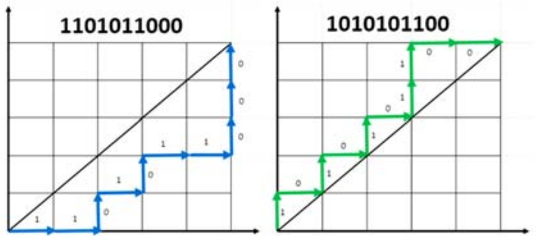


Fig. 3. Lattice Path movement space-based side A (left) and side B (right).

Table 1. Movement procedure for both sides (R for move right, T for move top).

Step	1	2	3	4	5	6	7	8	9	10
A	R	R	T	R	T	R	R	T	T	T
B	T	R	T	R	T	R	T	T	R	R

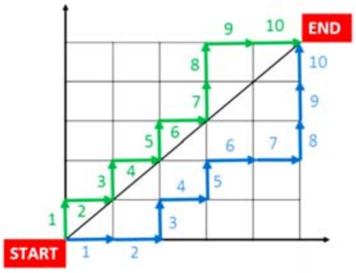


Fig. 4. Movement procedure for both sides on lattice path.

Fig. 4 depicts the unified scenario, *i.e.* the path for both sides. Both sides have chosen values that satisfy the Catalan number property, *i.e.* in this case, there is no possibility of crossing the diagonal, the conflict between the two sides or exiting from the network.

The third phase is *defining key equalization rules.* The main side is selected, that is, the side that dictates the change, and the other party agrees to the basic defined rules, which means that the additional parameter refers to the definition of the rules for the assignment which can be realized in two scenarios: scenario 1 (approximation to the diagonal) or scenario 2 (moving away from the diagonal). Below, we describe the work of both scenarios on the concrete example.

Scenario 1: *Moving towards the diagonal and A is the main:* Let A be the main side, while for the side B holds or is changed bit by the following rule: if the direction is the same on both sides (True: True or False: False) then side B retains its own bit, and if the directions differ, then the side B changes its bit. Table 2 presents the matching of the keys according to the "diagonal approximation" scenario.

Table 2. Scenario 1 – moving towards the diagonal.

Step	Moving towards the diagonal (True / False)	B – before	B – after
1	Side A – FALSE / Side B – FALSE	1	1
2	Side A – FALSE / Side B – TRUE	10	11
3	Side A – TRUE / Side B – FALSE	101	110
4	Side A – FALSE / Side B – TRUE	1010	1101
5	Side A – TRUE / Side B – FALSE	10101	11010
6	Side A – FALSE / Side B – TRUE	101010	110101
7	Side A – FALSE / Side B – FALSE	1010101	1101011
8	Side A – TRUE / Side B – FALSE	10101011	11010110
9	Side A – TRUE / Side B – TRUE	101010110	110101100
10	Side A – TRUE / Side B – TRUE	1010101100	1101011000

Finally, side B has aligned its key, which is identical to the key that has side A: 1101011000.

Scenario 2: *Movement from the diagonal and B is main:* Let B be the main side, while for the side A holds or is changed the bit, as follows: if the direction is the same on both sides (True: True or False: False), then A retains its own bit, and if the directions differ, then the side A changes its bits. Table 3 presents the matching of the keys according to moving away from the diagonal scenario.

Table 3. Scenario 2 – movement from the diagonal.

Step	Movement from the diagonal (True / False)	A – before	A – after
1	Side A – TRUE / Side B – TRUE	1	1
2	Side A – TRUE / Side B – FALSE	11	10
3	Side A – FALSE / Side B – TRUE	110	101
4	Side A – TRUE / Side B – FALSE	1101	1010
5	Side A – FALSE / Side B – TRUE	11010	10101
6	Side A – TRUE / Side B – FALSE	110101	101010
7	Side A – TRUE / Side B – TRUE	1101011	1010101
8	Side A – FALSE / Side B – TRUE	11010110	10101011
9	Side A – FALSE / Side B – FALSE	110101100	101010110
10	Side A – FALSE / Side B – FALSE	1101011000	1010101100

Finally, side A has aligned its key, which is identical to the key that has the side B: 1010101100.

The question arises, that in this case is not known to the third party (the adversary). These are the following parameters:

- "*Who is on which side?*" Whether A is on the *x*-axis, B on the *y*-axis, or vice versa.
- "*What is the main side?*" Is the main side A that dictates the change of bit on side B or vice versa.
- "*Which equalization rule is used?*" Is the bit equalization rule used to approximate or move away from the diagonal?

The safety of these three parameters is very significant. In this premature scenario, based on various combinations to define these three parameters, there are 8 different combinations of scenarios:

1. approximation to the diagonal (main side A on the x-axis, B on the y-axis),
2. approximation to the diagonal (main side A on the y-axis, B on the x-axis),
3. approximation to the diagonal (main side B on the x-axis, A on the y-axis),
4. approximation to the diagonal (main side B on the y-axis, A on the x-axis),
5. moving away from the diagonal (main side A on the x-axis, B on the y-axis),
6. moving away from the diagonal (main side A on the y-axis, B on the x-axis),
7. moving away from the diagonal (main side B on the x-axis, A on the y-axis) and
8. moving away from the diagonal (main side B on the y-axis, A on the x-axis).

5. MAURER'S PROTOCOL WITH CATALAN NUMBERS

According to Shannon's theory, cryptographic systems can be divided into two categories. The first category is related to computer security, designed in relation to the computing power of adversaries. The second one is the domain of perfect encryption systems that we consider secure even when the adversary possesses computer resources that exceed our limits of cognition. This is particularly true having in mind quantum computers that are awaiting us in the near future. *Ueli Maurer* devised his own protocol where he replaced the quantum channel with a weak source of information or a source that would definitely cause an error in the transmission [20, 21].

In the first phase of the protocol, both parties receive a broadcast signal through a noisy communication channel. In the second phase, they extract the mutual information, at the end of the third phase it is used by equalization, while the third party becomes completely independent, *i.e.*, it remains without the mutual information that initially existed initially between all participants. According to the theoretical foundations of the Maurer protocol, in this way the key is exchanged through a public channel, where the conditions are met that the adversarial party possess no information about the key or the message. According to the information theory and the definition of perfect secrecy, the mutual information between the plaintext and the ciphertext as well as between the ciphertext and the key must be zero. Also, according to *Kerckhoff's* principle, the adversary is familiar with the key exchange and encryption algorithm, while the key remains secret.

We concluded from several tests that both Catalan sequences are always completely independent. Authors in [22] introduced two new recursive bit-sequences, and then, with the help of these sequences, obtained the identities for the convolution involving the Catalan numbers. Also, authors [23, 24] discover several series of identities involving the Catalan numbers. The main purpose of paper [25] is to find expressions for two Catalan-sequences and to solve two related conjectures arising from the study of sums of finite products of Catalan numbers. In [26], the authors prove a conjecture about the equality of two generating functions for two sets whose cardinalities are given by Catalan numbers.

We will describe how we made a connection between our scenario and the aforementioned Maurer's Satellite scenario. It is important to state that we have experimentally found that if in Maurer's protocol both sides generate a random Catalan number, the mutual information will always be 0. This is a very good property of Catalan numbers, and more precisely, both sequences are always independent. Eve is a passive eavesdropper that participated in a public discussion performing the same steps as Bob in Fig. 5. If Eve does everything exactly the same as Bob, that is, imitates a participant in public discussion and realizes the protocol with Bob, by calculating mutual information it was determined that at the end of the protocol mutual information between Alice and Eve is 0. Also, the mutual information between Bob and Eve is 0, while mutual information between Alice and Bob is 1. This measuring was performed in a simulated environment.

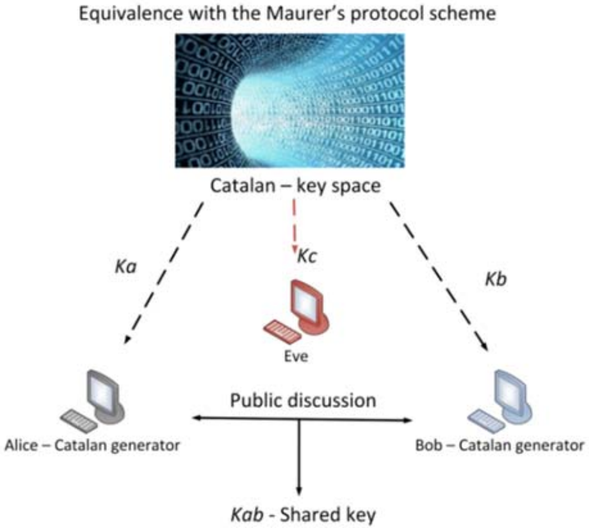


Fig. 5. Equivalent noisy channel for public discussion.

Table 4. Two random Catalan-keys.

A_key (dec): *1206719762343446959053171812826403121865940614803696816575611552645589411924*
A_key (bin): 10101010101111101010101011101001010111101010110111101001010111010101010101000101010101 010101011000111000000111010101010101101010000101010010111010011010101110000101000000101 011101011101001101011101000101110000010101010110100001011010101010100001010100
E_key (dec): *1620934935692751310532589993655837700010838143940873627601226573876598155946*
E_key (bin): 111001010101101010101010100101010101010110110111011101110110111010101011101011011111111 100101010000000100010101010100101110101010101010110101100000101000010001001100001010010 1010000111110101010001010101010101010010101010110101010101000001010101010101010
RESULT: mutual (shared) information = 0;   shared key length = 0.

Example 2: Let both sides generate a random 250-bit Catalan object. Below are the parameters from one test, where the common key cannot be separated, or the mutual information is always equal to 0, which means that the common key has length 0.

The complete scenario is based on the assumption that Eve is a passive eavesdropper. If Eve takes an active role, she may impersonate Alice or Bob, thereby compromising the security mechanisms, *i.e.* the key exchange protocol. One possible way is initial authentication based on the existing PKI infrastructure. Another possible way that is achievable on the physical layer is to remember the impulse response of the participants' channels, provided that in the first communication with them, when the impulse response is also estimated, their authenticity is trusted. Regarding practical implementation, secure channel codes would be implemented in wireless interface card drivers. With the progress of the "software-defined radios" project, it is reasonable to assume that the implementation of this type of security mechanisms on the physical layer is becoming easier for integration with forthcoming communications systems.

In order to exploit the listed Catalan sequence properties, more precisely to achieve the goal of reaching a significantly longer shared secret key from a partially known shared set of bits, we present the Maurer-Catalan protocol in Fig. 6.

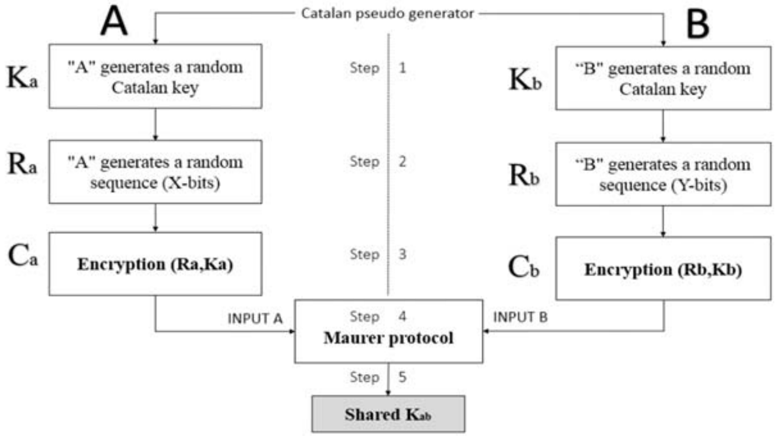

A
Catalan pseudo generator
B
Ka
"A" generates a random Catalan key
Step 1
Kb
"B" generates a random Catalan key
Ra
"A" generates a random sequence (X-bits)
Step 2
Rb
"B" generates a random sequence (Y-bits)
Ca
Encryption (Ra,Ka)
Step 3
Cb
Encryption (Rb,Kb)
INPUT A
Step 4
Maurer protocol
INPUT B
Step 5
Shared Kab

Fig. 6. Maurer protocol with Catalan-keys.

Step 1: Sides A and B randomly select Catalan key K_a and K_b (over C_n generator).
Step 2: Each side generates a random value (R_a, R_b) of an arbitrary length.
Step 3: Both sides encrypt the selected value of R_a and R_b with their chosen Catalan-key: $C_a = E\ (R_a, K_a)$ and $C_b = E\ (R_b, K_b)$.
Step 4: C_a and C_b are the initial values of the first phase of the Maurer protocol. Values A and B (key material) are completely equalized after the second phase and are usable for generating a symmetric cryptographic key through the final phase (privacy amplification) in Maurer's protocol, in which a specific class of hash codes (universal hashing) is applied. This neutralizes the mutual information between Eve and the other participants that existed at the beginning of the protocol. The bit sequence on Eve's side is completely independent of A and B.

Step 5: After the third round, the common key K_{ab} is exchanged.

Channel capacity or key generation speed refers to the amount of secret bits generated during one second of measurement, or the number of key bits shared between Alice and Bob, conditioned by the amount of randomness available for extraction. Also, the different bit rate (KDR) in the generated keys between Alice and Bob should be taken into account. Let N denote the length of the key. KDR is defined as

$$KDR = \frac{\sum_{i=1}^{N} | K_{(i)}^{A} - K_{i}^{B} |}{N}. \tag{3}$$

If KDR is not less than the correction techniques capabilities described in the information reconciliation phase, key generation will fail.

This key exchange scenario is applicable to smart city applications. In a smart city such a large set of data collections for the citizens, it represents a major security issue. For smart systems to gain widespread acceptance by users, the realization principle of smart city ideas must assure all users of the security aspect and privacy of all data online. Blockchain technology is the answer to the smart city security issue. More specifically, this technology provides the confidentiality and integrity of data in a smart environment. From a security point of view, blockchain technology is a very stable concept, but only while online users keep their private keys. This is precisely one of the weak points and challenges that creators of such systems will have to address. Also, the secret key generation and distribution are crucial to the information security of smart grids. Theft of a cryptographic key can have unprecedented consequences for the individual, and for this reason, it is often placed the emphasis on the secure distribution of keys in a smart environment.

One suggestion for implementing this proposed symmetric key exchange scenario that establishes cryptographically secured communication between two entities is in the realization of smart city applications. The first entity (user) randomly selects the function and sends its' description to the other user. The agreement on the description is done at the beginning of the protocol and it can be some parameter that selects the concrete function in the closed set. The result of this is a symmetric key of 128, 192 or 256 bits key applicable to AES algorithm.

Regarding the applicability of the protocol, it can primarily be used in 5G networks. Additionally, the application includes *LoRa* (*Long Range*), which is a relatively new IoT (internet of things) technique used widely in smart agriculture, smart cities, *etc.*, that can support long-range communications if the channel quality is good.

6. CONCLUSION AND FURTHER WORK

We have presented key exchange protocol where a string of random sequences is used as the key base. More precisely, aforementioned sequences satisfy the Catalan number property. The presented protocol for symmetric key exchange scenario consists of three phases: generating Catalan values, defining the Lattice Path movement space and defining the key equalization rules – key generation. Additionally, we have specified a concrete application in the form of Maurer-Catalan protocol combination. According to tests, we have noticed that enviable results in the key distribution process are reached. We have achieved the goal to securely exchange the significantly longer shared secret key from be from partially known shared bit string. The scenario was tested in combination with the encoding process of text or images using Catalan key and lattice path problems. Also, we have stated the security analysis of the protocol and testing for channel capacity or key generation speed.

The suggested methods can be further improved and adapted to modern approaches and protocols in cryptography. Number theory today finds increasing application in the realization of basic cryptographic techniques that deal with secure data exchange. Some studies deal with the use of number theory in the realization of visual cryptography algorithms, that is, in solving the problem of secrets sharing. In addition, it is important to note the additional possibilities of encryption and exchange data based on two-parameter Fuss-Catalan numbers. Accordingly, the proposal for future work could refer specifically to the application of Fuss-Catalan numbers in the improvement of existing protocols for managing, generation, distribution and storage of cryptographic keys.

ACKNOWLEDGEMENT

The presented study was sponsored by the Ministry of Education, Science and Technological Development of the Republic of Serbia (research grants TR32054 and III44006).

REFERENCES

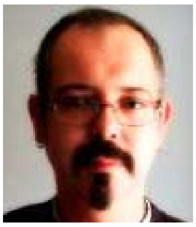
1. M. Reyes and O. K. Zimmermann, "Key exchange protocol using permutation parity machines," in *Proceedings of International Joint Conference on Computational Intelligence*, 2009, pp. 496-501.
2. V. A Romańkov and A. A. Obzor, "General algebraic cryptographic key exchange scheme and its cryptanalysis," *Prikladnaya Diskretnaya Matematika*, Vol. 37, 2017, pp. 52-61.
3. X. L. Zhang, "Authenticated key exchange protocol in one-round, algorithms and architectures for parallel processing," *Lecture Notes in Computer Science*, Vol. 5574, 2009, pp. 226-233.
4. A. Fahmy, "Key exchange protocol over insecure channel," in *Proceedings of World Academy of Science*, *Engineering and Technology*, Vol. 6, 2005, pp. 34-36.
5. S. Barman, S. Chattopadhyay, *et al.*, "A novel secure key-exchange protocol using biometrics of the sender and receiver," *Computers and Electrical Engineering*, Vol. 64, 2016, pp. 65-82.
6. S. Barman, S. Chattopadhyay, and D. Samanta, "An approach to cryptographic key exchange using fingerprint, security in computing and communications," *Communications in Computer and Information Science*, Vol. 467, 2014, pp. 162-172.
7. J. Zhou, "Further analysis of the Internet key exchange protocol," *Computer Communications*, Vol. 23, 2000, pp. 1606-1612.
8. M. Saracevic, E. Koricanin, and E. Bisevac, "Encryption based on ballot, stack permutations and balanced parentheses using Catalan-keys," *Journal of Information Tech-*

nology and Applications, Vol. 7, 2017, pp. 69-77.

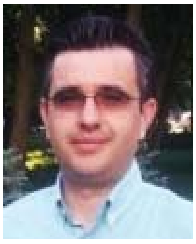
9. M. Saracevic, M. Hadzic, and E. Koricanin, "Generating Catalan-keys based on dynamic programming and their application in steganography," *International Journal of Industrial Engineering and Management*, Vol. 8, 2017, pp. 219-227.
10. M. Saracevic, S. Adamovic, and E. Bisevac, "Applications of Catalan numbers and lattice path combinatorial problem in cryptography," *Acta Polytechnica Hungarica: Journal of Applied Sciences*, Vol. 15, 2018, pp. 91-110.
11. M. Saracevic, A. Selimi, and F. Selimovic, "Generation of cryptographic keys with algorithm of polygon triangulation and Catalan numbers," *Computer Science – AGH*, Vol. 19, 2018, pp. 243-256.
12. M. Saracevic, S. Adamović, V. Miškovic, N. Maček, and M. Šarac, "A novel approach to steganography based on the properties of Catalan numbers and Dyck words," *Future Generation Computer Systems*, Vol. 100, 2019, pp. 186-197.
13. T. Koshy, *Catalan Numbers with Applications*, Oxford University Press, NY, 2009.
14. M. Saracevic, P. Stanimirovic, P. Krtolica, and S. Mašovic, "Construction and notation of convex polygon triangulation based on ballot problem," *Journal of Information Science and Technology*, Vol. 17, 2014, pp. 237-251.
15. N. R. Beaton, M. Bouvel, V. Guerrini, and S. Rinaldi, "Enumerating five families of pattern-avoiding inversion sequences and introducing the powered Catalan numbers," *Theoretical Computer Science*, Vol. 777, 2019, pp. 69-92.
16. K. Lee and L. Li, "Q, *t*-Catalan numbers and generators for the radical ideal defining the diagonal locus of $(C\text{–}2)(n)$," *Electronic Journal of Combinatorics*, Vol. 18, 2011, Article No. P158.
17. A. L. Reznik, A. V. Tuzikov, and A. A. Solovév, "Analysis of random point images with the use of symbolic computation codes and generalized Catalan numbers," *Optoelectronics Instrumentation and Data Process*, Vol. 52, 2016, pp. 529-536.
18. L. Bajunaid, J. M. Cohen, F. Colonna, and D. Singman, "Function series, Catalan numbers, and random walks on trees," *American Mathematical Monthly*, Vol. 112, 2005, pp. 765-785.
19. K. B. Davenport, "Generating function of the Catalan numbers proposal," *Fibonacci Quarterly*, Vol. 57, 2019, p. 178.
20. U. Maurer, "A universal statistical test for random bit generators," *Journal of Cryptology*, Vol. 5, 1992, pp. 89-105.
21. U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, Vol. 39, 1993, pp. 733-742.
22. W. P. Zhang and L. Chen, "On the Catalan numbers and some of their identities," *Symmetry-Basel*, Vol. 11, 2019, Article No. 62.
23. G. D. Lin, "On powers of the Catalan number sequence," *Discrete Mathematics*, Vol. 342, 2019, pp. 2139-2147.
24. L. Yin and F. Qi, "Several series identities involving the Catalan numbers," *Transactions of a Razmadze Mathematical Institute*, Vol. 172, 2018, pp. 466-474.
25. J. Zhang and Z. Y. Chen, "A note on the sequence related to Catalan numbers," *Symmetry-Basel*, Vol. 11, 2019, Article No. 371.
26. K. Aker and A. E. Gursoy, "A new combinatorial identity for Catalan numbers," *Ars Combinatoria*, Vol. 135, 2017, pp. 391-398.

Muzafer Saračević is an Associate Professor at the University of Novi Pazar, Serbia. He graduated in computer sciences (cryptography) at the Faculty of Informatics and Computing in Belgrade, obtained MSc. degree at the Faculty of Technical Sciences, University of Kragujevac, and completed his Ph.D. at the Faculty of Science and Mathematics, University of Niš, in 2013. He authored and co-authored several university textbooks and over 160 scientific papers.

Saša Adamović is an Associate Professor at Singidunum University. He received his Ph.D. title with a doctoral dissertation titled: "An class of systems for generating cryptographic keys based on biometric data," from the Singidunum University in Belgrade, in 2013. Currently, he is the Dean of the Faculty of Informatics and Computing at the University of Sinergija in Bijeljina, BiH. The research areas of Professor Adamović are cryptography and security, digital forensics and biometrics.



Nemanja Maček graduated from the University of Novi Sad in 2006 and received Advanced Security Systems Ph.D. from Sigidunum University, Belgrade in 2013. He works as a Lecturer at Department of Computer Technologies, School of Electrical and Computer Engineering of Applied Studies, Belgrade and Full Professor at Faculty of Computer Sciences, Megatrend University. He is the author of one monograph, co-author of several books and official university textbooks.



Aybeyan Selimi is an Assistant Professor at the International University Vision, Faculty of Informatics in Gostivar. He graduated in 2004 at the Institute of Mathematics in the Faculty of Natural Science and Mathematics in Skopje. In 2015 he defended his master's thesis at the Institute of Mathematics, the Faculty of Natural Sciences and Mathematics in Skopje. He completed his Ph.D. (computational geometry) at the University of Novi Pazar, Department of Computer Sciences in 2019.

Selver Pepić currently employed as a Professor at the Higher Technical Machine School of Professional Studies in Trstenik, Serbia. He graduated in 2004 at the University of Podgorica, Montenegro. In 2008 he defended his master's thesis at the Faculty of information technology – University of Novi Pazar, and completed his Ph.D. at the University of Niš, Faculty of Science and Mathematics in 2012. He authored and co-authored several university textbooks and over 40 scientific papers.