Facultatea de
Ştiințe Exacte

RAPORT DE ACTIVITATE

Seminarul catedrei de Mathematica Informatica

Centrul de cercetare: **Modele matematice si Sisteme informatice**

Universitatea Aurel Vlaicu din Arad

Septembrie 2020 – Decembrie 2023

Dragoi Vlad-Florin

1. Scop si organizare

Scopul principal al seminarul catedrei a fost de a consolida relațiile dintre membrii catedrei. Acest tel reprezintă primul pas, si poate cel mai important din strategia centrului de cercetare. Dorim ca acest seminar sa fie mai întâi suportul ce va lega temele de cercetare intre ele si va oferi o complementaritate si diversitate acestei facultăți prin activitatea de cercetare. Am spus primul pas din strategie deoarece in următorii ani ne dorim dezvoltarea unor colaborări externe cu cercetători din afara centrului, iar pasul natural ce va urma este invitarea acestora la acest seminar al catedrei.

Am încercat planificarea seminarului astfel încât majoritatea membrilor facultății sa poată participa, de aceea ziua si ora seminarului a variat de la an la an. Am urmărit ca prezentările sa fie legate de teme sau subiecte recente pentru a stimula cat mai mult interacțiunea si continuitatea activităților de cercetare. Din aceasta perspectiva am avut multe prezentări ce au fost deja făcute in cadrul unor conferințe iar mai apoi au fost extinse pentru seminar. In timpul pandemiei de COVID-19 prezentările s-au făcut online pe platforma Zoom iar in momentul trecerii la prezenta fizica am revenit in sala M111 unde obișnuiam sa ne intalnim inainte de pandemie. Am urmarit sa mentinem un ritm de 1 prezentare pe luna dar din varii motive unele luni au fost sarite, fie din motivul prezentei unor membrii la conferinte, fie din motive de sanatate, fie vacatele anuale.

Table 1

2020		
Septembrie	Marius Tomescu	Grey wolf optimizer-based approaches to path planning and fuzzy logic-based tracking control for mobile robots, IJCCC 2020
Octombrie	Sorin Nadaban	A Study of Boundedness in Fuzzy Normed Linear Spaces, Symmetry 2019
Noiembrie	SOFA 2020	
Decembrie	Vlad-Florin Dragoi	Combinatorial algorithms for integer syndrome decoding problem, SOFA 2020
2021		
Ianuarie		
Februarie	Valeriu Beiu	Consecutive k-out-of-n: F Systems (IEEE TR 2015, ICCCC2020)
Martie	Simon R. Cowell	Experimenting with beta distributions for approximating hammocks' reliability, ICCCC2020
Aprilie	Pastorel Gaspar	On random normal operators (JTP2019)
Mai	Dominic Bucerzan	Reactive-Based and Scalable-Driven Architecture for Mobile Development (SOFA2020)
Iunie	Crina Anina Bejan	Blockchain Technology (SOFA2018, IE2020)
Iulie		
August		
Septembrie		
Octombrie	Vlad-Florin Dragoi	Message-recovery laser fault injection against the McEliece scheme
Noiembrie	Lavinia Sida, Lorena Popa	Fuzzy inner product space
Decembrie		
2022		
Ianuarie		
Februarie	Vlad-Florin Dragoi	Structural properties of self-dual monomial codes with application to code-based cryptography, IMACC 2021
Martie	Valeriu Beiu	Why reliability needs rethinking (ICRC 2021)
Aprilie	Pastorel Gaspar	Wold-type structures for random operators
Mai	Sorin Hoara	How reliable are compositions of series and parallel networks compared with hammocks? (ICCCC2018, IJCCC2019)
Iunie	Mariana Nagy	Employing sorting nets for designing reliable computing nets(IEEE NANO 2020)
Iulie		
August		
Septembrie		
Octombrie	Valeriu Beiu	Optimal design of consecutive systems (ACM-ICNCC2022)
Noiembrie	Adrian Palcu	Weak charges in SU (5) L× U (1) Y gauge models
Decembrie		
2023		
Ianuarie		

Februarie	Ghiocel Mot	Fixed Point Theory for Multi-Valued Feng–Liu–Subrahmanyan Contractions (Axioms 2022)
Martie	Claudia Luminita Mihit	On uniform polynomial trichotomy of skew-evolution semiflows(CJM2022)
Aprilie	Mihaela Craciun	Perspectives of Cryptocurrency Price Prediction
Mai	Crina Bejan	Bitcoin price evolution versus energy consumption; trend analysis
Iunie	Dominic Bucerzan	Cryptocurrency Wallet Passwordless Authentication
Iulie		
August		
Septembrie		
Octombrie	Dan Deac	Nonstandard Fuzzy Sets: A General View
Noiembrie	Codruta Stoica	An approach to evolution cocycles from a stochastic point of view
Decembrie		

1. **Septembrie 2020.** Radu-Emil Precup, Emil-Ioan Voisan, Emil M Petriu, **Marius L Tomescu**, Radu-Codrut David, Alexandra-Iulia Szedlak-Stinean, Raul-Cristian Roman, *Grey wolf optimizer-based approaches to path planning and fuzzy logic-based tracking control for mobile robots,* IJCCC vol.15, no.3, 2020.

   Abstract:

   This paper proposes two applications of Grey Wolf Optimizer (GWO) algorithms to a path planning (PaPl) problem and a Proportional-Integral (PI)-fuzzy controller tuning problem. Both optimization problems solved by GWO algorithms are explained in detail. An off-line GWO-based PaPl approach for Nonholonomic Wheeled Mobile Robots (NWMRs) in static environments is proposed. Once the PaPl problem is solved resulting in the reference trajectory of the robots, the paper also suggests a GWO-based approach to tune cost-effective PI-fuzzy controllers in tracking control problem for NWMRs. The experimental results are demonstrated through simple multiagent settings conducted on the nRobotic platform developed at the Politehnica University of Timisoara, Romania, and they prove both the effectiveness of the two GWO-based approaches and major performance improvement.

2. **Octombrie 2020.** Tudor Binzar, Flavius Pater, **Sorin Nadaban,** *A Study of Boundedness in Fuzzy Normed Linear Spaces,* Symmetry vol.11,no.7, 2019.

   Abstract:

   In the present paper some different types of boundedness in fuzzy normed linear spaces of type $(X,N,*)$, where $*$ is an arbitrary t-norm, are considered. These boundedness concepts are very general and some of them have no correspondent in the classical topological metrizable linear spaces. Properties of such bounded sets are given and we make a comparative study among these types of boundedness. Among them there are various concepts concerning symmetrical properties of the studied objects arisen from the classical setting appropriate for this journal topics. We establish the implications between them and illustrate by examples that these concepts are not similar.

3. **Decembrie 2020. Vlad-Florin Dragoi**, Alin Tiberiu Lacatus, Alexandru Popoviciu, *Combinatorial Algorithms for Integer Syndrome Decoding Problem,* SOFA 2020.

   Abstract:

   Message recovery attacks against the Classic McEliece proposal to the NIST standardization process, have recently made use of the Integer syndrome decoding problem. It was demonstrated the one can modify or find extra information about the encrypted data, by means of physical attacks. The question raised by these modifications gave birth to the integer syndrome decoding problem. Here, we propose an algorithm that works as an optimized exhaustive-search, and thus finds all the solutions to the aforementioned problem. The key idea in the complexity gain is to split the binomial coefficient into product of smaller binomial coefficients. We show that this can be achieved using a permutation decomposition of the input matrix. Simulations are provided for small length and dimension matrices.

4. **Februarie 2021. Valeriu Beiu**, Leonard Daus, *Lower and Upper Reliability Bounds for Consecutive-k-Out-of-n:F Systems*, IEEE Transactions on Reliability, vol. 64, no. 3, 2015.

   Abstract:

   After a comprehensive review of reliability bounds for consecutive- k-out-of- n: F systems with statistically independent components having the same failure probability q (i.i.d. components), we introduce new classes of lower and upper bounds. Our approach is different from previous ones, and relies on alternating summation as well as on the monotony of some particular sequences of real numbers. The starting point is represented by the original formula given by de Moivre; and, by considering partial sums approximating it, new lower and upper bounds on the reliability of a consecutive- k-out-of- n: F system have been established. Simulation results show that all the lower and upper bounds considered here present very similar behaviors, as all of them are exponentially closing in on the exact reliability of a consecutive- k-out-of- n: F system. Additionally, the accuracy of the different bounds depends not only on the particular values of k and n, but also on the particular range of q (some of the new bounds being the most accurate ones over certain ranges).

5. **Martie 2021. Simon R. Cowell**, Sorin Hoara, Valeriu Beiu, *Experimenting with Beta Distributions for Approximating Hammocks' Reliability,* ICCCC 2020.

   Abstract:

It is a well-known fact that, in general, the combinatorial problem of finding the reliability polynomial of a two-terminal network belongs to the class of complete problems. In particular, hammock (aka brick-wall) networks are particular two-terminal networks introduced by Moore and Shannon in 1956. Rather unexpectedly, hammock networks seem to be ubiquitous, spanning from biology (neural cytoskeleton) to quantum computing (layout of quantum gates). Because computing exactly the reliability of large hammock networks seems unlikely (even in the long term), the alternatives we are facing fall under approximation techniques using: (i) simpler 'equivalent' networks; (ii) lower and upper bounds; (iii) estimates of (some of) the coefficients; (iv) interpolation (e.g., Bézier, Hermite, Lagrange, splines, etc.); and (v) combinations of (some of) the approaches mentioned above. In this paper we shall advocate—for the first time ever—for an approximation based on an 'equivalent' statistical distribution. In particular, we shall argue that as counting (lattice paths) is at the heart of the problem of estimating reliability for such networks, the binomial distribution might be a (very) good starting point. As the number of alternatives (lattice paths) gets larger and larger, a continuous approximation like the normal distribution naturally comes to mind. Still, as the number of alternatives (lattice paths) becomes humongous very quickly, more accurate and flexible approximations might be needed. That is why we put forward the beta distribution (as it can match the binomial distribution), and we use it in conjunction with a few exact coefficients (which help fitting the tails) to approximate the reliability of hammock networks.

6. **Aprilie 2021. Pastorel Gaspar,** *On random normal operators and their spectral measures,* Journal of Theoretical Probability, vol. 32, no.4, 2019.

   Abstract:

   The main aim of this paper is to introduce and study the subclass of not necessarily continuous, normal random operators, establishing connections with other subclasses of random operators, as well as with the existing concept of random projection operator-valued measure. Hence, after recalling some basic facts regarding random operators on a complex separable Hilbert space, theorems about transforming the class of not necessarily continuous decomposable random operators into the class of purely contractive random operators are proved. These are applied to obtain integral representations for not necessarily continuous normal or self-adjoint random operators on a Hilbert space with respect to the corresponding random projection operator-valued measures.

7. **Mai 2021. Dominic Bucerzan,** Sorin Miroiu, *Reactive-Based and Scalable-Driven Architecture for Mobile Development,* SOFA 2020,

   Abstract:

   The aim of this paper is to show and explain the implementation of this custom design pattern in developing iOS mobile applications, in regards to adopting the SOLID [14, 15] principles. We also do not rely on any interface builder tool, we code the user interface elements. One of the main purposes of this research was to find and assess the best combination of the existing software design patterns based on the ease of understanding, granularity, maintainability, modularity and scalability. The existing design patterns used in this custom implementation are Singleton, Factory, Builder, MVC, MVVM and Coordinator, all wrapped around the Rx-Swift reactive framework [1]. The study results in the performance analysis of this custom design pattern using the Swift programming language [17]. The mobile application used for case study is UBOOKER [16] which domain is business and modelling, representing the usage of algorithms, multimedia content (photos) and ample data.

8. **Iunie 2021. Crina Anina Bejan,** Dominic Bucerzan, *Blockchain. Today Applicability and Implications,* SOFA 2018. **Abstract:**
   Blockchain is an emergent technology with very rapid evolution that seems to radically reshape industry, economy and society [2]. It seems that blockchain technology triggers the beginning of the second era of digital economy. First era of digital economy is the result of the convergence of computing and communications technologies, meanwhile its second era tends to be a combination of computer science, mathematics, cryptography and behavioral economics [10]. It started back in 2008 when it was introduced for the bone structure of cryptocurrencies by a person or a group of people known for the name Satoshi Nakamoto. This paper aims to be an overview of what Blockchain currently involves, also it discusses its potential applications in different industries and its implications for society and economy in the context of next generation of internet.
9. **Octombrie 2021. Vlad-Florin Dragoi,** Pierre-Louis Cayrel, Brice Colombier, Alexandre Menu, Lilian Bossuet: *Message-Recovery Laser Fault Injection Attack on the Classic McEliece Cryptosystem,* Eurocrypt 2021.
   Abstract:
   Code-based public-key cryptosystems are promising candidates for standardization as quantum-resistant public-key cryptographic algorithms. Their security is based on the hardness of the syndrome decoding problem. Computing the syndrome in a finite field, usually , guarantees the security of the constructions. We show in this article that the problem becomes considerably easier to solve if the syndrome is computed in instead. By means of laser fault injection, we illustrate how to compute the matrix-vector product in by corrupting specific instructions, and validate it experimentally. To solve the syndrome decoding problem in N, we propose a reduction to an integer linear programming problem. We leverage the computational efficiency of linear programming solvers to obtain real-time message recovery attacks against the code-based proposal to the NIST Post-Quantum Cryptography standardization challenge. We perform our attacks in the worst-case scenario, i.e. considering random binary codes, and retrieve the initial message within minutes on a desktop computer.
   Our attack targets the reference implementation of the Niederreiter cryptosystem in the NIST PQC competition finalist Classic McEliece and is practically feasible for all proposed parameters sets of

this submission. For example, for the 256-bit security parameters sets, we successfully recover the message in a couple of seconds on a desktop computer Finally, we highlight the fact that the attack is still possible if only a fraction of the syndrome entries are faulty. This makes the attack feasible even though the fault injection does not have perfect repeatability and reduces the computational complexity of the attack, making it even more practical overall.

10. **Noiembrie 2021. Lavinia Sida**, **Lorena Popa**, *Fuzzy inner product space: literature review and a new approach,* Mathematics 2021.

    Abstract:

    The aim of this paper is to provide a suitable definition for the concept of fuzzy inner product space. In order to achieve this, we firstly focused on various approaches from the already-existent literature. Due to the emergence of various studies on fuzzy inner product spaces, it is necessary to make a comprehensive overview of the published papers on the aforementioned subject in order to facilitate subsequent research. Then we considered another approach to the notion of fuzzy inner product starting from P. Majundar and S.K. Samanta's definition. In fact, we changed their definition and we proved some new properties of the fuzzy inner product function. We also proved that this fuzzy inner product generates a fuzzy norm of the type Nădăban-Dzitac. Finally, some challenges are given.

11. **Februarie 2022. Vlad Florin Dragoi,** Andreea Szocs, *Structural Properties of Self-dual Monomial Codes with Application to Code-Based Cryptography,* IMACC2021.

    Abstract:

    This article focuses on the self-dual monomial codes that have an underlying structure of decreasing/weakly decreasing monomial codes. Having such a property permits an in-depth analysis of their structure: The permutation group of a subclass is (significantly) bigger than the affine group. Upon looking at higher powers of the code, we see that its third power is the entire space, but the dual of the square code gives information helpful for decoding. Using operations such as shortening, puncturing and taking the discrete derivative, we extract the subcode generated by the multiples of a certain variable. Recently, self-dual monomial codes have been proposed for a McEliece public key encryption scheme. They seem to possess strong security features - they have a large permutation group, they are self-dual, there are exponentially many of them by counting the possible monomial bases used in their construction. A more detailed analysis allows us to identify subclasses where the square code and shortening methods yield non-trivial results; in these cases, the security is dominated by the complexity of the Information Set Decoding, which is exponential in the square root of the length of the code. This is a solid argument for the security of the McEliece variant based on self-dual monomial codes.

12. **Martie 2022. Valeriu Beiu,** Roxana Beiu, Vlad-Florin Dragoi, *Why reliability needs rethinking,* ICRC 2021.

Abstract:

Offering high quality services/products has been of paramount importance for both communications and computations. Early on, both of these were in dire need of practical designs for enhancing reliability. That is why John von Neumann proposed the first gate-level method (using redundancy to build reliable systems from unreliable components), while Edward F. Moore and Claude E. Shannon followed suit with the first device-level scheme. Moore and Shannon's prescient paper also established network reliability as a probabilistic model where the nodes of the network were considered to be perfectly reliable, while the edges could fail independently with a certain probability. The fundamental problem was that of estimating the probability that (under given conditions) two (or more) nodes are connected, the solution being represented by the well-known reliability polynomial (of the network). This concept has been heavily used for communications, where big strides were made and applied to networks of: roads, railways, power lines, fiber optics, phones, sensors, etc. For computations the research community converged on the gate-level method proposed by von Neumann, while the device-level scheme crafted by Moore and Shannon-although very practical and detailed-did not inspire circuit designers and went under the radar. That scheme was built on a thought-provoking network called hammock, exhibiting regular brick-wall near-neighbor connections. Trying to do justice to computing networks in general (and hammocks in particular), this paper aims to highlight and clarify how reliable different types of networks are when they are intended for performing computations. For doing this, we will define quite a few novel cost functions which, together with established ones, will allow us to meticulously compare different types of networks for a clearer understanding of the reliability enhancements they are able to bring to computations. To our knowledge, this is the first ever ranking of networks with respect to computing reliability. The main conclusion is that a rethinking/rebooting of how should we design reliable computing systems, immediately applicable to networks/arrays of devices (e.g., transistors or qubits), is both timely and needed.

13. **Aprilie 2022. Pastorel Gaspar,** *Wold-type structures for random operators,* ongoing work based on (JTP2019,OT2022)

    Abstract.

    The aim is to replicate the Wold decomposition for isometries on Hilbert spaces to random isometries. Therefore the representation of random operators as acting on direct integral of Hilbert spaces is useful since a random isometry can be regrded as an arbitrary family of isometries on a Hilbert space. Each of them splits the Hilbert space into a unitary and a shift part. The resulting subspaces can be formed via a direct integral into a unitary part and a shift part direct integral for the random isometry.

14. **Mai 2022. Sorin Hoara,** Vlad Dragoi, Simon Robin Cowell, Valeriu Beiu, Pastorel Gaspar, *How reliable are compositions of series and parallel networks compared with hammocks?,* IJCCC2019.

    Abstract.

    A classical problem in computer/network reliability is that of identifying simple, regular and repetitive building blocks (motifs) which yield reliability enhancements at the system-level. Over time, this apparently simple problem has been addressed by various increasingly complex methods. The earliest and simplest solutions are series and parallel structures. These were followed by majority voting and related schemes. For the most recent solutions, which are also the most involved (eg, those based on Harary and circulant graphs), optimal reliability has been proven under particular conditions. Here, we propose an alternate approach for designing reliable systems as repetitive compositions of the simplest possible structures. More precisely, our two motifs (basic building blocks) are: two devices in series, and two devices in parallel. Therefore, for a given number of devices (which is a power of two) we build all the possible compositions of series and parallel networks of two devices. For all of the resulting twoterminal networks, we compute exactly the reliability polynomials, and then compare them with those of size-equivalent hammock networks. The results show that compositions of the two simplest motifs are not able to surpass size-equivalent hammock networks in terms of reliability. Still, the algorithm for computing the reliability polynomials of such compositions is linear (extremely effcient), as opposed to the one for the size-equivalent hammock networks, which is exponential. Interestingly, a few of the compositions come extremely close to size-equivalent hammock networks with respect to reliability, while having fewer wires.

15. **Iunie 2022. Mariana Nagy,** Vlad Dragoi, Valeriu Beiu, *Employing sorting nets for designing reliable computing nets,* IEEE-NANO 2020.

    Abstract.

    Recently, it was suggested that optimal sorting nets (which can trivially be mapped onto hardware) could be used to design highly reliable networks/systems. Sorting nets correspond to particular sorting algorithms, but it is their associated connectivity graph which seems to lead to highly reliable (minimal) two-terminal networks. Using the concept of associated connectivity graph we were able to link a reliability polynomial to any (optimal) sorting net. Here, we are going to thoroughly compare the two-terminal reliability polynomials associated to the connectivity graphs of very small optimal sorting nets, with the reliability polynomials of Moore-Shannon hammocks of similar size, as well as with size-equivalent compositions of series and parallel networks. These meticulous comparisons were done for getting a better understanding of the reliability of particular optimal sorting nets.

16. **Octombrie 2022. Valeriu Beiu,** Andreea Beiu, Roxana Beiu, *Optimal design of linear consecutive systems,* ACM-ICNCC2022.

Abstract: A critical issue for few nanometers technologies is the cost-yield balance, clearly tilted by soaring costs. An option to reduce costs, while also increasing yield, is to use reliability enhancement schemes. Unfortunately, these are considered power-hungry (due to redundancy), and entailing complex designs. From biology, neurons are prime examples of efficiency, achieving outstanding communication reliabilities, although relying on random ion channels. Aiming to bridge from biology to circuits, we will show how overlooked statistical results (about linear consecutive systems), combined with a Binet-like formula (for Fibonacci numbers of higher orders), allow avoiding lengthy reliability calculations, and present a straightforward neuron-inspired optimal design scheme for reliable communications.

17. **Noiembrie 2022. Adrian Palcu,** *Weak charges in SU (5) L× U (1) Y gauge models,* Prog. Th. Exp. Phisics 2022.

    Abstract.

    Within the framework of a renormalizable SU(5)L × U(1)Y electro-weak gauge model with no exotic electric charges, we obtain all the neutral weak charge operators and their quantization, once the diagonalization of the neutral boson mass matrix is properly performed. Our results open up the path to a rich and promising phenomenological outcome. All the Standard Model phenomenology is recovered by simply decoupling the latter's scale (vSM = 246 GeV) from the higher scale (V ~ 10 TeV) specific to our new electro-weak unification.

18. **Februarie 2023. Mot Ghiocel,** Claudia Luminiţa Mihiţ, Adrian Petruşel, *Fixed Point Theory for Multi-Valued Feng–Liu–Subrahmanyan Contractions,* Axioms 2022.

    Abstract:

    In this paper, we consider several problems related to the so-called multi-valued Feng–Liu–Subrahmanyan contractions in complete metric spaces. Existence of the fixed points and of the strict fixed points, as well as data dependence and stability properties for the fixed point problem, are discussed. Some results are presented, under appropriate conditions, and some open questions are pointed out. Our results extend recent results given for multi-valued graph contractions and multi-valued Subrahmanyan contractions.

19. **Martie 2023. Claudia Luminiţa Mihiţ,** *On uniform polynomial trichotomy of skew-evolution semiflows,* Carpathian Journal of Mathematics 2022.

    Abstract:

    The paper treats two concepts of uniform polynomial trichotomy for the skew-evolution semiflows in Banach spaces. We obtain the connection between them, a characterization for a property of uniform polynomial growth and a sufficient criteria for the uniform polynomial trichotomy.

20. **Aprilie 2023. Mihaela Craciun,** Crina Bejan, Dominic Bucerzan, *Perspectives of Cryptocurrency Price Prediction, Education,* Research and Business Technologies 2023.

    Abstract.

Cryptocurrency is a relatively young research field. Since its development, when Bitcoin was lanced (2008) (Satoshi, N.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)), until today it become a highly volatile market with more than 9 thousand types of cryptocurrencies (CoinMarketCap: preţurile criptomonedelor de ast˘azî in funcţie de capitalizare de piaţă (2021)). In latest years several algorithms and techniques have been developed in order to predict the cryptocurrency price evolution. However, a general classification of the available methods has not been proposed yet. For these reasons, in this paper the main ideas underlying cryptocurrency price forecasting are presented and compared. In the first part of the paper is presented the general framework of cryptocurrency development, namely Blockchain Technology and e-Business social environment. In the second part several techniques for cryptocurrency price prediction are presented and their main characteristics are discussed. The last section concludes.

21. **Mai 2023. Crina Bejan,** Dominic Bucerzan, Mihaela Craciun, *Bitcoin price evolution versus energy consumption; trend analysis,* Applied Economics 2022.

    Abstract.

    Digital technology developments shape the behaviour, performances, standards of society, organizations and individuals imposing new ways of payments and new forms of money. In this environment in 2008 was developed a new type of currency, namely Bitcoin. Cryptocurrency, as this new form of money has been generically called, puts pressure on the traditional concept of money. Today, the economic value of cryptocurrencies is attested by their circulation and acceptance by user communities for trade. However, establishing this value raises debates in the literature. The research from this paper investigates and analyses if there is a strong enough connectedness between Bitcoin price evolution and energy consumption tendency (for mining), to influence Bitcoin value. Public data from January 2014 to July 2021 is used. An Artificial Neural Network (ANN) was used to study and predict the tendency of Bitcoin price and energy consumption. A comparison between the forecasting trend and the real trend (the evolution of energy consumption and Bitcoin price) was made. The conducted research starts with a quantitative one and ends with a qualitative one (trends). The obtained results show that qualitatively, there is a good correlation between monthly average values of BTC prices and electricity consumption for mining.

22. **Iunie 2023. Dominic Bucerzan,** Bogdan Gros, Crina Bejan, *Cryptocurrency Wallet Passwordless Authentication,* ICIE 2021.

    Abstract.

    Cryptocurrency and Blockchain are two cutting-age topics that have a major influence in shaping our daily lives. Starting from 2009 cryptocurrency has become a presence in the ordinary economic landscape. The form of money needed a change due to technological progress, globalization and the need of faster financial transactions. This paper proposes a solution based on passwordless authentication for crypto-wallets. In the first section of the paper is presented current state of threats that target cryptocurrency wallets. In the second section of the paper, we propose a solution for authentication process based on image steganography and SmartSteg algorithm. The proposed solution aims to minimize the threats that target the security of user authentication process. It proposes another way in which users store their credentials (private keys/passwords) so they do not have to use a keyboard to retype credentials every time they login. Once the private key is generated it is stored inside a digital image in such a way that the human visual system cannot distinguish between the original image and the image with secret credential embedded. When the user logs in to the wallet it loads the image with the secret credentials from which the wallet system will extract the credentials. This method removes the need to type the any credentials or the need of showing them on the screen. This solution is in its early stages and more test are need to be done in order to detect new possible threats to crypto wallets that can emerge from the usage of the proposed solution. The main target of the work presented in this paper is to minimize as much as possible the keylogger attacks.

23. **Octombrie 2023. Dan Deac,** *Nonstandard Fuzzy Sets: A General View,* ICCCC2022.

    Abstract.

    Nonstandard fuzzy sets are extensions, generalizations of fuzzy sets introduced by Zadeh. They represent a research domain of great interest due to the multiple applications in ambiguity situations and in problems with incomplete information. We make a systematic review of these types of fuzzy sets in order to provide a framework for new research in this field, to strengthen the available theoretical results, to establish the relations among them as well as their various applications. Finally, we introduce the concept of vector fuzzy set and give different representation of Pythagorean fuzzy sets.

24. **Noiembrie 2023. Codruta Stoica,** *An approach to evolution cocycles from a stochastic point of view,* AIP Conf. Proc. 2022.

    Abstract.

    The aim of this paper is to emphasize some splitting asymptotic behaviours in mean square for stochastic cocycles, as well as connections between them. We define a general framework for the exponential splitting that includes, as a particular case, the exponential dichotomy. We will consider general splitting properties that consist in assuming the existence of a decomposition of the state space into invariant subspaces where the norms of the evolution trajectories are bounded by some functions that depend on the initial and final times. The additional conditions target the families of projections.