dr hab. Janusz Szczepański, prof. IPPT PAN

Warszawa, 9 kwiecień 2013

ANKIETA OCENY OSIĄGNIĘĆ NAUKOWYCH KANDYDATA DO TYTUŁU PROFESORA

I. INFORMACJE O OSIĄGNIĘCIACH I DOROBKU

1. Informacje o osiągnięciach i dorobku naukowym:

1.1. Wykaz autorskich publikacji naukowych w czasopismach międzynarodowych, ze wskazaniem *5-letniego* wskaźnika Impact Factor publikacji oraz liczby cytowań publikacji i indeksu Hirscha wg. ISI Web of Knowledge/Web of Science.

W sumie:
• **37** autorskie recenzowane publikacje naukowe (w tym **34** z „Listy Filadelfijskiej")
• Indeks Hirscha: **11**
• Całkowita liczba cytowań: **259**
• Sumaryczny Impact Factor: **57,821 (w tym uzyskane po habilitacji 22,207)**

Po złożeniu rozprawy habilitacyjnej (11 publikacji, w tym 11 z „Listy Filadelfijskiej'' (LF)):

1. B. Paprocki, J. Szczepanski, „How do the amplitude fluctuations affect the neuronal transmission efficiency", **Neurocomputing**, *Elsevier Science Publishers*, 104, 50-56 (2013), IF= 1,595, Cyt. 0 LF
2. M. M. Arnold, J. Szczepanski, N. Montejo, J. M. Amigo, E. Wajnryb, M. V. Sanchez-Vives, „Information content in cortical spike trains during brain state transitions", **Journal of Sleep Research**, *Wiley*, 22, 13-21 (2013), IF= 3.628, Cyt. 0 LF
3. B. Paprocki, J. Szczepanski, „Efficiency of neural transmission as a function of synaptic noise, threshold, and source characteristics", **BioSystems**, 105: 62-72 (2011), *Elsevier Science Publishers*, IF=1,497, Cyt. 1 LF
4. J. Szczepanski, M. M. Arnold, E. Wajnryb, J. M. Amigo, M. V. Sanchez-Vives, „Mutual information and redundancy in spontaneous communication between cortical neurons", **Biological Cybernetics**, 104 (3): 161-174 (2011), *Springer*, IF=1,989, Cyt. 3 LF
5. J. Szczepanski, „On the distribution function of the complexity of finite sequences", **Information Sciences**, 179 (9): 1217-1220 (2009), *Elsevier Science Publishers*, IF=2,984, Cyt. 0 LF
6. J. M. Amigo, L. Kocarev, J. Szczepanski, „On some properties of the discrete Lyapunov exponent", **Physics Letters A**, 372 (41): 6265-6268 (2008), *Elsevier Science Publishers*, IF=1,731, Cyt. 1 LF
7. R. Nagarajan, J. Szczepanski, E. Wajnryb, „Interpreting non-random signatures in biomedical signals using Lempel-Ziv complexity", **Physica D**, 237 (3): 359-364 (2008), *Elsevier Science Publishers*, IF=1,737, Cyt. 2 LF
8. J. M. Amigo, L. Kocarev, J. Szczepanski, „Theory and practice of chaotic cryptography", **Physics Letters A**, 366 (3): 211-216 (2007), *Elsevier Science Publishers* , IF=1,731, Cyt. 23 LF

9. J. M. Amigo, L. Kocarev, J. Szczepanski, „Discrete Lyapunov exponent and resistance to differential cryptanalysis", **IEEE Transactions on Circuits and Systems II**, 54 (10): 882-886 (2007), *Institute of Electrical and Electronics Engineers Inc. USA,* IF=1,540, Cyt. 6 LF
10. J. M. Amigo, L. Kocarev, J. Szczepanski, „Order patterns and chaos", **Physics Letters A**, 355 (1): 27-31 (2006), *Elsevier Science Publishers,* IF=1,731, Cyt. 23 LF
11. L. Kocarev, J. Szczepanski, J. M. Amigo, I. Tomovski, „Discrete Chaos - Part I: Theory", **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications - Regular papers**, 53 (6): 1300-1309 (2006), *Institute of Electrical and Electronics Engineers Inc. USA,* IF=2,044, Cyt. 26 LF

Przed uzyskaniem stopnia doktora habilitowanego:

1. J. Szczepański, J.M. Amigo, T. Michalek, L. Kocarev, Cryptographically secure substitutions based on the approximation of mixing maps", **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications - Regular Papers**, 52 (2): 443-453 (2005), *Institute of Electrical and Electronics Engineers Inc*. USA, IF=2,044, Cyt. 14 LF
2. J. M. Amigo, L. Kocarev, J. Szczepanski, „A chaos based approach to the design of cryptographically secure substitutions", **Physics Letters A**, 343 (1-3): 55-60 (2005), *Elsevier Science Publishers* , IF=1,731, Cyt. 5 LF
3. L. Kocarev, J. Szczepański, „Finite-space Lyapunov exponents and pseudo-chaos", **Physical Review Letters**, 234101 1-4**,** Dec 3, (2004), *American Physical Society*. IF=7,013, Cyt. 12 LF
4. J. Szczepański, J. M. Amigo, E. Wajnryb, M. V. Sanchez-Vives, „Characterizing Spike Trains with Lempel-Ziv Complexity", **Neurocomputing**, 58-60: pp. 79-84, (2004), *Elsevier Science Publishers*, IF= 1,595, Cyt. 11 LF
5. J. M. Amigo, J. Szczepański, E. Wajnryb, M. V. Sanchez-Vives, „Estimating the Entropy Rate of Spike Trains via Lempel-Ziv Complexity", **Neural Computation**, Vol. 16, I. 4, pp. 717 - 736, (2004), *MIT Press*, IF=2,521, Cyt. 34 LF
6. J. Szczepański, E. Wajnryb, J. M. Amigo, M. V. Sanchez-Vives, M. Slater, „Biometric Random Number Generators", **Computers & Security**, Vol. 23, I. 1, pp. 77-84, (2004), *Elsevier Science Publishers*, IF=1,075, Cyt. 4 LF
7. J. M. Amigo, J. Szczepański, „Approximations of Dynamical Systems and Their Application to Cryptography", **International Journal of Bifurcation and Chaos**, Vol. 13, no. 7, pp. 1937-1948, (2003), *World Scientific Publishing*, IF=0.855, Cyt. 6 LF
8. J. Szczepański, M. Amigo, E. Wajnryb, M.V. Sanchez-Vives, „Application of Lempel-Ziv Complexity to the Analysis of Neural Discharges", **Network: Computation in Neural Systems** 14 (May 2003), 335-350, *Institute of Physics Publishing,* United Kingdom, IF=1,698, Cyt. 21 LF
9. J. Szczepański, T. Michalek, „Random Fields Approach to the Study of DNA Chains", **Journal of Biological Physics**, V. 29 (1): 39-54 (2003), *Kluwer Academic Publishers*, IF=1,478, Cyt. 1 LF
10. M. Amigo, J. Szczepański, E. Wajnryb, M.V. Sanchez-Vives, „On the Number of States of the Neuronal Sources", **BioSystems**, vol. 68, 1, 57-66 (2003), *Elsevier Science Publishers,* IF=1,497, Cyt. 11 LF
11. A.Górska, K.Górski, Z.Kotulski, A.Paszkiewicz, J.Szczepański, „New Experimental Results in Differential-Linear Cryptanalysis of Reduced Variants of DES", in:

Advanced Computer Systems, V. 664, pp. 335-348, J.Soldek, J.Pejas, eds, *Kluwer Academic Publishers*. Boston, January 2002. ISBN 0-7923-7651-X. (2002)
12. M.V. Sanchez-Vives, J. Szczepański, E. Wajnryb, J.M. Amigó (2001). "Medida del contenido de información en las respuestas neuronales de la corteza visual mediante el análisis de complejidad de Lempel-Ziv" **Revista de Neurología** 33, 788, (2001)
13. J. Szczepański, Z. Kotulski, „Pseudorandom Number Generators Based on Chaotic Dynamical Systems", **Open Systems & Information Dynamics** 8: 137-146, (2001), *Kluwer Academic Publishers*, IF=0,857, Cyt. 0 LF
14. J. Szczepański, „A New Result on the Nirenberg Problem for Expanding Maps", **Nonlinear Analysis: Theory Methods & Applications**, 43, 91-99 (2001), *Pergamon - Elsevier Science Publishers*, IF=1,579, Cyt. 0 LF
15. Z.Kotulski, J.Szczepański, On the Application of Discrete Chaotic Systems to Cryptography. DCC Method**, Biuletyn WAT,** Vol.48, No.10 (566), pp.111-123, (1999)
16. J. Szczepański, K. Górski, Z. Kotulski, A. Paszkiewicz, A. Zugaj, „Some Models of Chaotic Motion of Particles and Their Application to Cryptography", **Archives of Mechanics**, vol. 51, no. 3-4, pp. 509-528, (1999), IF=0,591, Cyt. 0 LF
17. Z. Kotulski, J. Szczepański, K. Gorski, A. Paszkiewicz, A. Zugaj, „Application of Discrete Chaotic Dynamical Systems in Cryptography – DCC Method", **International Journal of Bifurcation and Chaos**, Vol. 9, no. 6, pp. 1121-1135, (1999), *World Scientific Publishing*, IF=0,855, Cyt. 24 LF
18. J. Szczepański, Z. Kotulski, „On Two Motions of a Particle Driven by Equivalent Ergodic and Chaotic Reflection Laws", **Archives of Mechanics**, vol. 50, No. 5, pp. 865-875, (1998), IF=0,591, Cyt. 0 LF
19. Z. Kotulski, J. Szczepański, „Discrete Chaotic Cryptography", **Annalen der Physik**, vol. 6, no. 5, pp. 381-394, (1997), *Johann Ambrosius Barth*, Heidelberg, IF=1,063, Cyt. 19 LF
20. J. Szczepański, E. Wajnryb, „Do Ergodic or Chaotic Properties of the Reflection Law Imply Ergodicity or Chaotic Behaviour of a Particle's Motion?", **Chaos, Solitons & Fractals**, V. 5, No.1, 77-89 (1995), *Pergamon - Elsevier Science Publisher*, IF=1,414, Cyt. 5 LF
21. J. Szczepański, „On the Problem of Nirenberg concerning Expanding Maps in Hilbert Space Case", **Proceedings of the American Mathematical Society**, V. 116, No. 4, 1041-1044 (1992), *American Mathematical Society*, IF=0,648, Cyt. 2 LF
22. J. Szczepański, E.Wajnryb, „Long-Time Behaviour of the One-Particle Distribution Function for the Knudsen Gas in a Convex Domain", **Physical Review A**, V. 44, No. 6, 3615-3621 (1991), *American Physical Society*, IF=2,612, Cyt. 4 LF
23. J. Szczepański, „The Properties of the Mechanical System Equivalent to a Billiard in a Triangle", **Bulletin of the Polish Academy of Sciences**, Techn., V. 36, No. 7-9, 441-448, (1987), IF2011=0,966, Cyt. 0 LF
24. H. Zorski, J. Szczepański, „Classical Mechanics in Infinite-Dimensional Hilbert Space", **Archives of Mechanics**, No. 1, 115-132 (1989), IF=0,591, Cyt. 0 LF
25. J. Szczepański, „On the Basis of Statistical Mechanics. The Liouville Equation for Systems with Infinite Countable Number of Degrees of Freedom", **Physica A** 157, 955-982 (1989), *Elsevier Science Publishers*, IF=1,374, Cyt. 1 LF
26. J. Szczepański, "The Liouville Equation in Infinitely Dimensional Separable Hilbert Space", **Bulletin of the Polish Academy of Sciences**, Techn., V. 33, No. 5-6, 279-292, (1985), IF2011=0,966, Cyt. 0 LF

1.2 Wykaz prac o charakterze monograficznym, podręczniki, skrypty

J. M. Amigo, J. Szczepański, A Conceptual Guide to Chaos Theory, IFTR Reports, Instytut Podstawowych Problemów Techniki PAN, 9/1999

Cykl prac złożonych w ramach rozprawy habilitacyjnej ma charakter monograficzny, 2005

2. Informacje o aktywności naukowej:

2.1 we wszystkich obszarach wiedzy, z wyłączeniem obszaru wiedzy sztuka:

a) informacje o udziale w krajowych i międzynarodowych konferencjach naukowych

1. Dwukrotny udział (1988, 1991) w Konferencjach „*Dynamics Days*" organizowanych w Dusseldorfie i w Berlinie. Prezentacja łącznie pięciu prac (w formie posterów). Prace poświęcone były teorii chaosu i teorii bilardów.

2. J. Szczepanski (speaker), "On Symbolic Representation of a Dynamical Systems of a Billiard Type in a Polygon. Chaos in the Li-Yorke Sense", *Seventh Swedish-Polish Symposium on Mechanics*, Warsaw, Poland, May 27-31, 1991.

3. J. Szczepanski (speaker), E. Wajnryb, "On the Transferring of Ergodicity and Chaos", *SIAM Conference on Application of Dynamical Systems*, Snowbird, Utah, USA, October 15-19, 1992.

4. J. Szczepanski, (speaker) "On the Nirenberg Problem for Expanding Maps", *SIAM Conference on Application of Dynamical Systems*, Snowbird, Utah, USA , October 15-19, 1992.

5. J. Szczepanski (poster), "Asymptotic Behaviour of the Composition of Unimodal Map and Involution", *International Conference on Nonlinear Dynamics, Chaotic and Complex Systems*, NDCCS'95, Zakopane, Poland, 7-12 November 1995.

6. Z.Kotulski, J.Szczepański (speaker), "Discrete chaotic cryptography (DCC). New Method for Secure Communication", *Nonlinear Evolution Equations and Dynamical Systems*, Kolymbari, *(* organized by University La Sapienza, Roma), Crete, Greece, June 1997.

7. K.Górski, A.Paszkiewicz (speaker), A.Zugaj, Z.Kotulski, J.Szczepański, „Własności ciągów generowanych przez najmniejsze pierwiastki pierwotne liczb pierwszych", *Krajowe Sympozjum Telekomunikacji*, 9-11 wrzesień, Bydgoszcz, 1998.

8. S.Trznadel (speaker), A.Zugaj, K.Górski, A.Paszkiewicz, Z.Kotulski, J.Szczepański, „Przegląd stanu wiedzy na temat kryptoanalizy liniowej ze szczególnym uwzględnieniem algorytmu DES", *Poznańskie Warsztaty Telekomunikacyjne, PWT'98*, 10-11 grudzień, 1998.

9. J.Szczepański (speaker), Z.Kotulski, K.Górski, A.Paszkiewicz, A.Zugaj, "On Some Models of Pseudorandom Number Generators Based on Chaotic Dynamical Systems", *NATO Regional Conference on Military Communication and Information Systems. CIS Solutions for an Enlarged NATO*, Zegrze, October 6th-8th , 1999.
10. A.Paszkiewicz (speaker), K.Górski, Z.Kotulski, J.Szczepański, A.Zugaj, "Detection of weaknesses of pseudorandom sequences with the aid of statistical tests", *6th International Conference on Advanced Computer Systems*, ACS'99, Szczecin, November 18-19, 1999.
11. A.Zugaj (speaker), K.Górski, Z.Kotulski, J.Szczepański, A.Paszkiewicz, "Extending linear cryptanalysis - theory and experiments", *NATO Regional Conference on Military Communication and Information Systems. CIS Solutions for an Enlarged NATO*, Zegrze, October 6th-8th, 1999.
12. JM. Amigo (speaker), J. Szczepański, "On the Design of Ciphers Resistant to Linear Cryptoanalysis", European Conference on Iteration Theory 2000 (ECIT-2000), 4-9 September, Murcia, Spain, 2000.
13. Z.Kotulski (speaker), J.Szczepański, K.Górski, A.Górska, A.Paszkiewicz, "On Constructive Approach to Chaotic Pseudorandom Number Generators", *NATO Regional Conference on Military Communication and Information Systems. CIS Solutions for an Enlarged NATO,* RCMIS 2000, Zegrze, October 4-6, 2000.
14. A.Górska (speaker), K.Górski, Z.Kotulski, A.Paszkiewicz, J.Szczepański, "New Constructions in Linear Cryptanalysis of Block Ciphers", *7th International Conference on Advanced Computer Systems*, ACS 2000, Szczecin, October 23-25, 2000.
15. JM. Amigo, J. Szczepanski (speaker), "On the Design of Ciphers Resistant to Linear Cryptoanalysis", *NATO Regional Conference on Military Communications and Information Systems 2001 – Partnership for CIS Interoperability*, Zegrze, October 10 – 12, 2001.
16. J.M. Amigó (speaker), J. Szczepanski, E. Wajnryb, M.V. Sanchez-Vives, "On the Number of States of the Sources as Defined by the Neuron Responses in the Visual Cortex", *World Congress on Neuroinformatics*, Wiedeń, Austria, September 24-29, 2001.
17. A.Górska (speaker), K.Górski, Z.Kotulski, A.Paszkiewicz, J.Szczepański, "New Experimental Results in Differential-Linear Cryptanalysis of Reduced Variants of DES", *NATO International Conference on Advanced Computer Systems*, ACS 2001, Szczecin, October 17-19, 2001.
18. A.Paszkiewicz (speaker), K.Górski, A.Górska, Z.Kotulski, K.Kulesza, J.Szczepański, "Proposals of Graph-based Ciphers, Theory and Implementations", *Proceedings of the Regional Conference on Military Communication and Information Systems. CIS Solutions for an Enlarged NATO,* RCMIS 2001, Zegrze, October 4-6 2001.
19. M. V. Sanchez-Vives (poster), j. Szczepanski, E. Wajnryb, J. M. Amigo „Measurement of the Information Content in the Neuron Responses of Primary Visual Cortex", *IX Congreso de la Sociedad Espanola de Neurociencias*, Santiago de Compostela, Spain, September 9-11, 2001.

20. J. Szczepański (tutorial), Z. Kotulski, „Wykorzystanie układów dynamicznych w kryptografii", *V Krajowa Konferencja Zastosowań Kryptografii*, ENIGMA, Warszawa,15-18 maja 2001.

21. J. Szczepanski (poster), J.M. Amigo, E. Wajnryb, M.V. Sanchez-Vives, "Characterizing Spike Trains with Lempel-Ziv Complexity", *The Annual Computational Neurosciences Meeting*, Alicante, organizer Maneesh Sahani (University of California, San Francisco, USA), July 5-9, 2003.

22. J. Szczepanski (speaker), Eligiusz Wajnryb, José M. Amigó, María V. Sanchez-Vives, Mel Slater, "Construction of Random Number Generators via Biometric Methods", *NATO Regional Conference on Military Communications and Information Systems 2001 – Partnership for CIS Interoperability*, Zegrze, October 8^{th} – 10^{th} , 2003.

23. J.M. Amigo (poster), J. Szczepanski, L. Kocarev, "Cryptographically secure substitutions based on the approximation of mixing maps", *International Workshop on Dynamical Systems and Complexity in Information and Communication Technology*, Bologna Italy, Sept. 6-8, 2004.

24. L. Kocarev (University of California San Diego) speaker, J. M. Amigó (Universidad Miguel Hernández), J. Szczepański (Polish Academy of Science), "Chaos-based Cryptography: An Overview", *Special Session* „Complex Dynamics and Cryptography", *International Symposium on Nonlinear Theory and its Applications*, October 18-21, Bruges, Belgium, 2005

25. J. M. Amigó (speaker), J. Szczepański, L. Kocarev "Discrete Chaos and Cryptography", *Special Session* „Complex Dynamics and Cryptography", *International Symposium on Nonlinear Theory and its Applications*, October 18-21, Bruges, Belgium, 2005

26. M.M. Arnold (poster), J. Szczepański, N. Montejo, E. Wajnryb, M.V. Sanchez-Vives, „Information content of cortical spike trans during different brain states", *35^{th} Meeting Society for Neuroscience,* Washington, November 12-16, 2005

27. J. M. Amigó (speaker), J. Szczepański, L. Kocarev, "Caos Discreto y Criptografia", *3^{th} Congreso Iberoamericano de Seguridad Informatica,* Valparaiso, Chile, 21-25 November 2005

28. J. Szczepański (speaker), B. Paprocki, *Pierwsze Sympozjum Polskiego Węzła International Neuroinformatics Coordinating Facility* gdzie przedstawię referat zatytułowany: „"Efektywność transmisji informacji w sieciach neuronowych w ujęciu teorii Shannona", gudzień 2011, Instytut Nenckiego, Warszawa

29. J. Szczepanski (speaker), B. Paprocki, "Transmission efficiency in the brain like neuronal networks. Information and energetic aspects". *10th International Neural Coding Workshop 2012*, Prague, Czech, September 2–8, 2012

30. B. Paprocki, J. Szczepanski, “Effectiveness of information transmission in the brain-like communication models”. *10th International Neural Coding Workshop 2012*, Prague, Czech, September 2–8, 2012 (*poster)*

31. B. Paprocki, J. Szczepanski, “Long-range connections’ influence on the efficiency of transmission in brain-like neuronal networks”, *Neuroscience Congress- 8th Federation of European Neuroscience Societies (FENS) Forum*, Barcelona, Spain, July 14–18, 2012, (*poster)*

b) członkostwo w komitetach redakcyjnych i radach naukowych czasopism

Członek *Editorial Board and Review Board* czasopisma:
International Journal of Computational Science, Hong Kong, od roku 2007
http://www.gip.hk/ijcs/

Członek Programming Committee na konferencji Future Generation Communication and Networking, FGCN2012 Kangwondo, Korea

Członek Programming Committee na konferencji Future Generation Communication and Networking, FGCN2011 Jeju Island, Korea

Członek *Programming Committee* na konferencji The 3rd International Conference on Advanced Communication and Networking, ACN2011, Brno, Czechy

Członek *Programming Committee* na konferencji Future Generation Communication and Networking (FGCN 2010) Jeju Island, Korea.

Członek *Programming Committee* na konferencji The Third International Joint Conference Symposium on Computational Sciences and Optimization (CSO 2010), Huangshan Mountain, Chiny, May 28-31, 2010.

Członek *Programming Committee* na Conference on Future Generation Communication and Networking (FGCN 2009) Jeju Island, Korea.

Członek *Programming Committee* na konferencji The Second International Symposium on Applied Computing and Computational Sciences (ACCS 2009), Sanya, Chiny, April 24-26, 2009.

Członek *Programming Committee* konferencji Future Generation Communication and Networking, FGCN2008 December 13th-15th, Hainan Island, China

Członek *Programming Committee* na konferencji International Symposium on Applied Computing and Computational Sciences (ACCS2008), August 1-3, 2008, Hong Kong

Członek *Programming Committee* konferencji Future Generation Communication and Networking, FGCN2007 December 6th-8th, Jeju Island, Korea

c) wykaz zrealizowanych projektów naukowo-badawczych krajowych, europejskich i innych międzynarodowych

2011 – 2013 "Zastosowanie metod komputerowych bazujących na teorii informacji do analizy efektywności transmisji sygnałów w sieciach neuronowych", Badania własne", Grant NCN: N N519 646540, kierownik grantu

2011 – 2012 „Opracowanie wydajnych metod generowania bezpiecznych parametrów algorytmów klucza publicznego", (grant promotorski), kierownik grantu

2006 – 2009 „Stochastyczne modele ekspresji genów i sieci regulatorowych", Grant Ministerstwa Nauki, PB 4T07A00130, główny wykonawca

2005-2007 Projekt „*Caos Discreto y Sys Aplicaciones a Las Communicationes Seguras*" projekt finansowany przez Hiszpańskie Ministerstwo Nauki i Edukacji, główny wykonawca

2004 – 2005 "Information-Theoretical and cryptographical aspects of neuronal discharges", joint project with Institute of Neuroscience, CSIC - Universidad Miguel Hernandez (Prof. M.V. Sanchez-Vives) Spain, kierownik projektu

2004, Research visit at the University of California San Diego. The subject: Cryptography and Coding Theory, grant NSF USA

2003, Research visit at the Miguel Hernandez University – Alicante. The subject: Neurosciences and Cryptography

1992, Grant of Kosciuszko Foundation (New York), SIAM Conference Salt Lake City, USA

1997 - 1999 „Zastosowanie metod stochastycznych w kryptografii", KBN 8 T11 D01112, Warsaw University of Technology, główny wykonawca

2000 Grant of the Government of Valencia, INV00-01-19 for research concerning application of approximation of dynamical systems to cryptography (Miguel Hernandez University – Alicante)

2000 – 2002 „Nowe metody konstrukcji i analizy kryptosystemów", KBN 8T11 D02019, IFTR PAS, główny wykonawca

2000 – 2002 „Termodynamika łańcuchów biopolimerów w roztworze" KBN 8T0 7A 045 20, IFTR PAS, główny wykonawca

2001 – 2002 "Computational properties of cortical neurons: analysis of neural discharges complexity in the visual system" 4043/R01/R02, joint project with Institute of Neuroscience, CSIC - Universidad Miguel Hernandez (Prof. M.V. Sanchez-Vives) Spain, kierownik projektu

3. Informacje o współpracy z otoczeniem społecznym i gospodarczym:

Z-ca Przewodniczącego Rady Naukowej IPPT PAN (obecna kadencja)

Przewodniczący Komisji Rady Naukowej IPPT PAN do spraw stopni naukowych (obecna kadencja)

2002 – 2004 Konsultant w zakresie kryptologii w NBP, w Centrum Certyfikacji „Centrast S.A.", tzw. Root w systemie Infrastruktury Klucza Publicznego w Polsce. Współuczestniczenie w przygotowaniu Ustawy o podpisie elektronicznym

Pełnienie, przez trzy kadencje, funkcji Sekretarza konferencji „Polish-Swedish Symposium on Mechanics" (1991, 1993, 1995).

Recenzje dwóch rozpraw doktorskich: dr Gabrieli Mochol Instytut Nenckiego (2010), dr Stefana Kotowskiego PJWSTK (2009).

Przewodniczący Komisji doktorskiej mgr M. Kochańczyka, IPPT.

Przewodniczący Komisji Egzaminacyjnej na Wydziale Matematyki i Nauk Informacyjnych Politechniki Warszawskiej mgr inż. Jarosława Łazuki, WAT. Zakres egzaminu obejmował kryptografię – 2008.

Członkostwo w kilku komisjach doktorskich w dyscyplinie Informatyka w IPPT PAN.

Przez kilka lat członek Komisji oceniającej najlepsze prace magisterskie z zakresu kryptografii. Prezentacja prac odbywa się podczas tradycyjnych konferencji ENIGMA poświęconej bezpieczeństwu systemów teleinformatycznych.

Członek American Mathematical Society (od 1993).

Recenzje projektów badawczych NCBiR.

4. Informacje o współpracy międzynarodowej:

a) Staże zagraniczne

- Dwa miesięczne pobyty (2000, 2003) na Uniwersytecie Miguel Hernandez w Alicante.
Współpraca z Profesorem **J. M. Amigo z Miguel Hernandez University, Alicante, Spain** w problematyce związanej z bezpiecznym przesyłaniem informacji. Współpraca dotyczy zastosowania teorii chaosu i teorii aproksymacji układów dynamicznych w kryptografii. W ramach współpracy opublikowano 15 wspólnych artykułów w czasopismach z Listy Filadelfijskiej.
Współprace dwustronną pomiędzy **IPPT PAN i CISC – Miguel Hernandez University, Alicante** oraz **ICREA-IDIBAPS, Barcelona**. W ramach tej współpracy otrzymaliśmy na lata 2004-2005 grant dwustronny „Information-Theoretical and Cryptographic Aspects of Neuronal Discharges", którego byłem kierownikiem. Ze strony hiszpańskiej współpracuję z Profesor M. V. Sanchez-Vives (kierownik), Prof. J.M. Amigo i Dr M. Arnold. W badaniach

opublikowanych w Computers&Security uczestniczył także Prof. Mel Slater z **University College London**. Ze strony polskiej w badaniach uczestniczy Prof. E. Wajnryb. Badania dotyczą analizy przesyłania informacji w korze mózgowej (realizowanych przy pomocy tzw. potencjałów czynnościowych, ang. Spikes) pod wpływem stymulacji wizualnej. W Laboratoriach Neuroscience w Alicane i IDIBAPS (kierowanych przez Prof. M.V. Sanchez-Vives) przeprowadzane są eksperymenty związane z przesyłaniem sygnałów w mózgu. W ramach współpracy opublikowano 7 artykułów w czasopismach z Listy Filadelfijskiej.

- Miesięczny pobyt (2004) jako Visiting Professor na University of California San Diego. Współpraca z Prof. **L. Kocarevem z University of California (San Diego).** Tematyka współpracy obejmuje kryptografię oraz problemy związane z tzw. „dyskretnym chaosem". W ramach współpracy opublikowano 8 artykułów w czasopismach z Listy Filadelfijskiej, w tym w Physical Review Letters.

- Współpraca z **Profesorem Radhą Nagarajanem** z **University of Arkansas for Medical Sciences.** Tematyka współpracy dotyczyła analizy **sygnałów biomedycznych** pod kątem identyfikacji nielosowych wzorców. Owocem współpracy jest wspólna publikacja w Physica D (2008).

1989 – Wizyta 10 dniowa na **Uniwersytet Moskiewskim im. M. Łomonosowa.** Współpraca **z Prof. L. Bunimovichem.**

1988 – uczestnictwo w kursie Chaos Theory in Dynamical Systems, Centrum Mechaniki, Udine, Włochy

Recenzent prac publikowanych w czasopismach międzynarodowych ze wskaźnikiem impact factor (Impact Factors – 2011):

IEEE Transactions on Circuits and Systems I – Regular papers IF = 1.97
IEEE Transactions on Circuits and Systems II – Express Briefs IF = 1.410
Physics Letters A IF=1.63
Neurocomputing IF = 1.580
Information Sciences IF= 2.833
Applied Mathematical Modelling IF= 1.579
Physica Scripta IF = 1.204
IET Circuits Devices & Systems IF = 1.204
Chinese Physics Letters IF = 0.731
IEEE Sensor Journal IF = 1.520
Nonlinear Dynamics IF = 1.247
Scientia Iranica IF = 0.348
Archives of Mechanics IF = 0.396

5. Informacje o osiągnięciach i dorobku dydaktycznym i popularyzatorskim:

5.1 prowadzone wykłady i seminaria naukowe:

Od Semestru Zimowego 2007 prowadzę zajęcia dydaktyczne na Uniwersytecie Kazimierza Wielkiego w Bydgoszczy na Wydziale Matematyki, Fizyki i Techniki jako prof. nadzwyczajny. Tematyka wykładów to: rachunek prawdopodobieństwa z elementami statystyki, teoria informacji, bezpieczeństwo systemów teleinformatycznych, kryptografia. Prowadzę też Seminaria poświęcone transmisji danych w sieciach (teleinformatycznych i biologicznych). W ramach tych Seminariów obroniono pod moim kierownictwem (jestem promotorem) **5 prac magisterskich** oraz około 20 prac dyplomowych inżynierskich. Obecnie jestem promotorem 6 prac magisterskich w trakcie finalizacji.

W latach 1992, 1994 uczyłem (równolegle z pracą w IPPT) matematyki w liceum im. Ks. Poniatowskiego w Warszawie.

5.2. Opieka naukowa nad doktorantami i osobami ubiegającymi się o nadanie stopnia doktora (w charakterze promotora, promotora pomocniczego lub opiekuna naukowego)

• dr Andrzej Chmielowiec, praca doktorska pt. Generowanie parametrów algorytmów klucza publicznego uwzględniające aspekty bezpieczeństwa i wydajności, obrona z wyróżnieniem w IPPT PAN w 2012 r., promotor

• mgr Bartosz Paprocki, Uniwersytet Kazimierza Wielkiego, przygotowywana praca doktorska pt. Analiza wydajności transmisji danych w komórkach i sieciach neuronowych metodami Teorii Informacji, planowana obrona w 2013 r., promotor

5.4 Przygotowane materiały do e-learningu

W ramach wykładów prowadzonych na Uniwersytecie Kazimierza Wielkiego w Bydgoszczy przygotowałem materiały do prowadzonych zajęć w formie elektronicznej. Materiały te dotyczą
- Podstaw Probabilistyki i Statystyki
- Bezpieczeństwa Transmisji w Sieciach Teleinformatycznych. Zastosowanie Kryptografii

5.5 Indywidualna opieka naukowa nad studentami (staże naukowe)

Opieka naukowa nad studentami Wydziału Fizyki UW (praktyka w ramach programu studiów) – tematyka dotyczyła diagnozowania sygnałów biomedycznych metodami teorii złożoności.

6. Informacje o otrzymanych nagrodach oraz wyróżnieniach naukowych i dydaktycznych:

1989 – Nagroda Wydziału IV PAN im. T. Hubera za prace poświęcone równaniu Liouville'a w nieskończenie-wymiarowej przestrzeni Hilberta.

Wielokrotne wyróżnienia przez Dyrekcję IPPT PAN za osiągnięcia naukowe.

II. INFORMACJE O NAJWAŻNIEJSZYM OSIĄGNIĘCIU NAUKOWYM

Za moje najważniejsze osiągnięcia naukowe uważam opracowanie i zastosowanie metod Teorii Informacji i Układów Dynamicznych do analizy transmisji danych w układach biologicznych oraz sieciach teleinformatycznych. W przypadku układów biologicznych metody te głównie były skoncentrowane na badaniu procesu kodowania i wydajności transmisji natomiast w przypadku sieci teleinformatycznych celem było zapewnienie bezpieczeństwa transmisji. W badaniach tych mój wkład stanowiła przede wszystkim analiza teoretyczna/analityczna, propozycje zastosowania modeli teoretycznych i ich analiza, w szczególności propozycje i opracowanie zastosowanych algorytmów. Odgrywałem także istotną rolę w analizie i interpretacji otrzymanych wyników symulacji.

Neuroinformatyka: Ważne pytania związane z badaniem procesów w mózgu są następujące: w jaki sposób neurony kodują informację i w jaki sposób współpracują podczas procesu przesyłania informacji? Badania moje dotyczyły procesu przesyłania (realizowanego przy pomocy potencjałów czynnościowych ang. spikes) informacji w korze mózgowej pod wpływem bodźców wizualnych. Analizowane były głównie związki pomiędzy własnościami sygnałów wejściowych a złożonością sygnałów wyjściowych jak również własności kodowania takich układów. Aby zbadać fundamentalną w Teorii Shannona wielkość, tzw. informację wzajemną (ang. Mutual Information) zastosowano zaawansowane metody związane z szacowaniem entropii (w tym koncepcję złożoności zaproponowaną przez Lempela-Ziva, której własności rozkładu przedstawiono w pracy Information Sciences 2009). Przeprowadzenie analizy transmisji informacji w komórkach neuronowych kory mózgowej za pomocą teorii złożoności Lempela-Ziva, umożliwiło stwierdzenie: rodzaju komórki, własności sygnału wejściowego oraz ilości informacji zawartej w odpowiedzi komórki a także określenie/klasyfikacji stanów komórki. Badania te przedstawiono w pracach: Biosystems 2003, Neurocomputing 2004, Network 2003, Neural Computation 2004.
W kolejnej pracy autora " Mutual Information and in Spontanous Communication Between Cortical Neurons" (Biological Cybernetics 2011) przeprowadzono analizę procesu przesyłania informacji przez populacje neuronów pod kątem redundancji transmisji oraz informacji wzajemnej współpracujących neuronów. Wprowadzono i udowodniono własności tzw. względnego współczynnika informacji wzajemnej (charakteryzuje on jak dalece współpraca pomiędzy neuronami jest deterministyczna). W oparciu o dane eksperymentalne, pokazano, że o ile redundancja podczas transmisji może wykazywać znaczne fluktuacje, o tyle informacja względna zachowuje się w sposób stabilny. Stwierdzono, że współpraca w obrębie grupy neuronów może być bardzo elastyczna: od efektu synergii, po transmisję, w której główną rolę odgrywa pojedynczy neuron. Zjawisko te ma istotny wpływ na niezawodność transmisji.
W pracy opublikowanej w Journal of Sleep Research (2013) przeprowadzono z kolei analizę przepływu informacji w korze mózgowej dla różnych stanów mózgu. W szczególności zbadano zachowanie przepływu informacji w fazach przejścia od stanu rozbudzenia do fazy snu i odwrotnie. Pokazano ilościową symetrię transmisji w obu kierunkach. Ponadto pokazano, że transmisja informacji charakteryzuje się dużymi fluktuacjami co sugeruje ze komunikacja odbywa się pakietami.
W najnowszych pracach (Biosystem 2011, Neurocomputing 2013) przeprowadzono analizę efektywności transmisji informacji dla sieci komórek neuronowych (modelujących komórki mózgowe) w zależności od charakterystyki neuronów (m.in. fluktuacji amplitudy podczas obliczeń neuronowych) oraz takich parametrów jak: błędy w synapsie, wartości poziomu aktywacji neuronu, aktywności, entropii oraz typu źródła (zależne, niezależne). Uzyskano istotne wyniki pokazujące, że w dużym zakresie parametrów transmisja jest wydajniejsza gdy

w synapsach występuje pewien poziom szumu oraz większe tłumienie zachowań fluktuacji. Ponadto wykazano, że wzmocnienie fluktuacji zwiększa rolę szumu w synapsach dla poprawienia wydajności. Przeprowadzono też analizę efektywności transmisji uwzględniającą efekty energetyczne dla modeli sieci inspirowanych architekturą mózgu. Badania te pokazują, że w procesie ewolucji architektura neuronu i sieci zmierzała w kierunku bardziej efektywnego wykorzystania szumu, który to proces jest naturalny w układach biologicznych.

Kryptografia: Drugim ważnym nurtem moich badań jest bezpieczeństwo transmisji w sieciach teleinformatycznych pod kątem zastosowań kryptografii. W ostatnich latach nastąpił gwałtowny rozwój bezprzewodowej technologii komunikacji teleinformatycznej. Do zapewnienia bezpieczeństwa transmisji danych stosuje się coraz to nowsze metody kryptograficzne. Możliwości wykorzystania standardowych algorytmów w tych przypadkach podlegają ograniczeniom związanym przede wszystkim z poborem mocy, wielkością dostępnej pamięci i możliwościami obliczeniowymi. Dlatego w wielu ośrodkach trwają prace nad zaprojektowaniem optymalnych-dedykowanych algorytmów (m. in. kryptosystemów oraz funkcji skrótu) w przypadku tego typu ograniczeń. Ciekawym kierunkiem w tym względzie jest możliwość wykorzystania chaotycznych układów dynamicznych. Zachowanie układów chaotycznych wskazuje, że ich dynamika jest zbliżona do losowej (układ „zapomina" o danych początkowych). W oparciu o powstawanie i tworzenie wzorców przez trajektorie badano związek pomiędzy układami chaotycznymi i dynamiką losową. Zaproponowano (praca Physical Review Letters 20004) ponadto definicję wykładnika Lapunowa dla układów o skończonej liczbie stanów. Wykazano, że w granicznym przypadku wprowadzony wykładnik pokrywa się z klasycznym wykładnikiem (podstawowy wskaźnik chaosu) dla układów ciągłych. W pracach opublikowanych w Physics Letters A 2008, IEEE 2007 dokonano analizy możliwości zastosowania wprowadzonego wcześniej przez autorów pojęcia dyskretnego wykładnika Lapunowa do badania własności losowych permutacji (bijekcji) zbiorów skończonych. Badanie te umożliwiają ocenę, czy badana permutacja (w szczególności wygenerowana przez trajektorię układu chaotycznego) ma charakter losowy czy też nie. Ponadto analizowano własności cykliczne i spełnianie tzw. kryterium lawinowości. Ma to duże znaczenie przy zastosowaniach do celów kryptograficznych. W przypadku dyskretyzacji do celów kryptograficznych wymagane jest, aby takie cechy jak chaos zachowane również były po dyskretyzacji. Otrzymane wyniki pozwalają na zdefiniowanie pojęcia chaosu dla układów o dyskretnej liczbie stanów. W opublikowanych pracach (IJBC 2003, IEEE 2005, IEEE 2006) przedstawiono oryginalną metodę konstrukcji permutacji bazującą na teorii układów mieszających o „jednorodnych" własnościach parametrów *LP* i *DP* gwarantujących, że permutacje takie zastosowane do konstrukcji szyfru blokowego (lub jego komponentów) zapewniają jego odporność na kryptoanalizę liniową i różnicową. Parametry *LP* i *DP* stanowią podstawową ilościową miarę odporności kryptosystemów na ataki za pomocą kryptoanalizy liniowej i kryptoanalizy różnicowej. Główna idea prac autora bazuje na wykorzystaniu, do projektowania systemów kryptograficznych, koncepcji Rohlina-Halmosa aproksymacji układów dynamicznych periodycznymi automorfizmami.