9 kwiecień 2013 r.

dr hab. Janusz Szczepański
Instytut Podstawowych Problemów Techniki
Polska Akademia Nauk

AUTOREFERAT

Moje główne badania naukowe koncentrowały się przede wszystkim na zastosowaniu metod Teorii Informacji i układów dynamicznych do analizy transmisji danych w układach biologicznych oraz sieciach teleinformatycznych. W przypadku układów biologicznych metody te przede wszystkim były skupione na badaniu procesu kodowania i wydajności transmisji natomiast w przypadku sieci teleinformatycznych celem było zapewnienie bezpieczeństwa transmisji.

W Autoreferacie omówię chronologicznie moje osiągniecie naukowe. Wyniki uzyskane po habilitacji zostały przedstawione w częściach poświęconych zastosowaniu Teorii Informacji w układach biologicznych oraz zastosowaniu chaotycznych układów dynamicznych w kryptografii. 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.

Studia magisterskie

W latach 1974 do 1979 studiowałem na Wydziale Matematyki Uniwersytetu Warszawskiego. Pracę magisterską pisałem pod kierunkiem dr hab. Z. Sawonia w Zakładzie Analizy Funkcjonalnej. Dotyczyła ona tzw. twierdzeń maksymalizacyjnych. Chodziło o warunki wystarczające dotyczące podalgebry domkniętej w algebrze funkcji ciągłych zapewniające, że algebra ta jest całą przestrzenią funkcji ciągłych C(X), gdzie X jest przestrzenią zwartą lub lokalnie zwartą. Typowym literaturowym przykładem takiego twierdzenia jest tw. Weierstrassa.

I. Problematyka związana z doktoratem

<u>Mechanika statystyczna dla układów o nieskończonej przeliczalnej liczbie stopni swobody</u>

Po obronie pracy magisterskiej w roku 1979 zdałem na studia doktoranckie w Instytucie Podstawowych Problemów Techniki PAN. Rozpocząłem pracę nad moją rozprawą doktorską pod kierunkiem Prof. H. Zorskiego. Moje badania naukowe koncentrowały się wówczas na problemach związanych ze sformułowanie odpowiedników klasycznej mechaniki statystycznej dla układów o nieskończonej przeliczalnej liczbie stopni swobody modelowanych na nieskończenie-wymiarowej ośrodkowej przestrzeni Hilberta. W przypadku modelowania układów o przeliczalnej liczbie stopni swobody zasadnicze problemy związane są z nie istnieniem na nieskończenie-wymiarowych ośrodkowych przestrzeniach Hilberta odpowiednika miary Lebesgue (tzn. miary niezmienniczej ze względu na translacje). W związku z tym funkcje gęstości prawdopodobieństwa odnosiły się do tzw. quasi-miar otrzymywanych w oparciu o tw. Kołmogorowa dla skończenie-wymiarowych rozkładów zgodnych. W 1985 roku złożyłem i obroniłem pracę doktorską pt. „Równanie Liouvilla dla

nieskończenie-wymiarowej ośrodkowej przestrzeni Hilberta" w IPPT PAN. Wyniki badań zostały przedstawione w pracach:

[Phys A] J. Szczepanski, „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*.

[AM] H. Zorski, J. Szczepanski, „Classical Mechanics in Infinite-Dimensional Hilbert Space", **Archives of Mechanics**, No. 1, 115-132 (1989).

[BPAS] 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

Za prace z tego zakresu otrzymałem nagrodę Wydziału IV PAN, im. T. Hubera.

II. Problematyka po doktoracie

A. Teoria chaosu i ergodyczności w mechanice

W roku 1985 rozpocząłem pracę w IPPT PAN na stanowisku adiunkta. Problematyka, jaką się zajmowałem w grupie Prof. Zorskiego dotyczyła zastosowań teorii chaosu i układów dynamicznych w mechanice przede wszystkim do teorii gazów rozrzedzonych. W pracy nad tymi zagadnieniami współpracowałem również z Prof. E. Wajnrybem. Prace dotyczyły głównie problemów związanych z bilardami klasycznymi (kąt padania równa się kątowi odbicia) jak też nieklasycznym. W przypadku zagadnień klasycznych chodziło o analizę gęstości trajektorii cząstek czy też ergodyczność takich systemów zaś w przypadku nieklasycznym chodziło o analizę transferowania jakościowych własności prawa odbicia (ergodyczność, chaos, stabilność) na ruch cząstek oraz ewolucję funkcji rozkładu. Bardziej szczegółowo można tą problematykę i osiągnięte rezultaty przedstawić następująco:

Zagadnienie, co dzieje się z cząsteczką, gdy dociera do brzegu jest nie tylko problemem teoretycznym, ale posiada również praktyczne znaczenie. Jednym z podejść badania zachowania cieczy (szczególnie gazów rozrzedzonych) jest przybliżenie polegające na zastąpieniu ścian pojemnika za pomocą gładkiej powierzchni (referencje w [PRA]). Gdy cząsteczka osiąga powierzchnię odbija się od niej zmieniając swoją prędkość zgodnie z pewnym prawem (przyjmujemy model deterministyczny). Zachodzi, zatem pytanie o zależność własności trajektorii cząstki od własności praw odbicia i od kształtu obszaru. W wyidealizowanym przypadku zakłada się, że „kąt padania równa się kątowi odbicia".

W podanych poniżej pracach była właśnie analizowana taka sytuacja. W pracy [PRA] analizowano ruch cząstki w obszarze wypukłym na płaszczyźnie (które to układy można zredukować do analizy ruchu cząstki w kole o „indukowanym" prawie odbicia). Pokazano, że w przypadku koła przyjmując jako prawo odbicia odwzorowanie logistyczne (z parametrem odpowiadającym odwzorowaniu ergodycznemu/ chaotycznemu) otrzymano ergodyczny/chaotyczny ruch cząstki (opisany przez korespondujący układ dynamiczny działający w przestrzeni położeń i prędkości). W pracy [Chaos] poddano analizie ruch cząstki, tym razem w obszarze z osobliwościami (w kwadracie). W pracy udowodniono (analitycznie), że dla praw odbicia zadanych odwzorowaniem logistycznym (również z parametrem ergodycznym/chaotycznym) ruch cząstki jest quasi-okresowy. Następnie w pracy

[Archives I] w celu uzyskania kompletności opisu pokazano, że nawet dwa topologicznie sprzężone prawa odbicia mogą prowadzić do kompletnie innego typu ruchu (w tym samym obszarze).

Z przeprowadzonych badań wynikało, że typ ruchu cząstki w obszarze zamkniętym o zadanym prawie odbicia jest silnie uzależniony od sprzężenia pomiędzy prawem odbicia i rodzajem obszaru, w którym się cząstka porusza. Analizy prowadzone dla gazów rozrzedzonych stanowiły później podłoże do propozycji konstrukcji kryptosystemów opartych na takich właśnie układach fizycznych [IJBC I], [Archives II].

Wyniki badań z tej tematyki opublikowano w pracach:

[BPAS] J. Szczepanski, „The Properties of the Mechanical System Equivalent to a Billiard in a Triangle", **Bulletin of the Polish Academy of Sciences**, Techn., V. 33, No. 5-6, 279-292, (1985).

[PRA] J. Szczepanski, 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*.

[Chaos] J. Szczepanski, E. Wajnryb, „Do Ergodic Properties of 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 Publishers*.

[IFTR] J. M. Amigo, J. Szczepański, A Conceptual Guide to Chaos Theory, **Institute of Fundamental Technological Reports**, 9/1999, IPPT PAN

[Archives I] J. Szczepanski, Z. Kotulski, „On Topologically Equivalent Ergodic and Chaotic Reflection Laws Leading to Different Types of Particles' Motion", **Archives of Mechanics**, vol. 50, No. 5, pp. 865-875, (1998).

B. Problem Nirenberga dla odwzorowań rozciągających

Na początku lat 90-tych i pod koniec zajmowałem się również tzw. problemem Nirenberga dla odwzorowań rozciągających w nieskończenie-wymiarowych ośrodkowych przestrzeniach Hilberta. Chodziło o to czy odwzorowanie ciągłe $f : H \to H$ spełniające warunek

$$\exists c > 1 \; \forall x, y \in H \; \|f(x) - f(y)\| \geq c\|x - y\|$$

i takie, że *f(H)* zawiera zbiór otwarty musi być odwzorowaniem „na". Innymi słowy czy wówczas równanie $f(x) = y$ musi mieć rozwiązanie dla każdego $y \in H$. Jest to problem otwarty ogłoszony w znanym podręczniku L. Nirenberga, z którym zetknąłem się jeszcze podczas studiów na wykładzie Prof. A. Pełczyńskiego. Praktyczne przykłady pojawiają się w kontekście różniczkowych operatorów eliptycznych w odpowiednich przestrzeniach Soboleva. Moje dwa wyniki dotyczące tego problemu zostały opublikowane w dwóch pracach. Na tyle na ile mi wiadomo w literaturze obecnie znajdują się ciągle częściowe wyniki związane z tym problemem, zaś pełny problem jest nadal otwarty. W przypadku przestrzeni Banach zagadnienie zostało rozstrzygnięte negatywnie (tzn. skonstruowano kontrprzykład) przez J.M. Morela i H. Steinleina.

[PAMS] J. Szczepanski, „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*.

[NA] J. Szczepanski, „A New Result on the Nirenberg Problem for Expanding Maps”, **Nonlinear Analysis: Theory Methods & Applications**, 43, 91-99 (2001), *Pergamon - Elsevier Science Publishers*.

III. Problematyka związana z habilitacją i późniejszymi badaniami

C. Zastosowanie układów dynamicznych w kryptografii

Od połowy roku 1996 zacząłem poszukiwać tematyki związanej z dynamicznie rozwijającą się technologią teleinformatyczną. Dziedziną taką jest ciągle rozwijająca się kryptografia mająca i wymagająca solidnych podstaw matematycznych oraz poszukująca nowych rozwiązań. W tamtym okresie pojawiły się możliwości wykorzystania teorii układów dynamicznych w tym również teorii chaosu właśnie do tego problemu. Pierwsze prace dotyczące zastosowań teorii chaosu w kryptografii związane były z układami dynamicznymi ciągłymi (tzn. czas jest ciągły) i z koncepcją synchronizacji takich układów. Autorami tych prac byli Pecora, Caroll, Kocarev i Parlitz (obecnie jest olbrzymia literatura na ten temat). Pierwsza wzmianka na temat zastosowania dyskretnych w czasie układów dynamicznych pojawiła się w 1991 r. w pracy Habutsu. Moje zainteresowania skupiły się na zastosowaniu w kryptografii właśnie dyskretnych układów dynamicznych. W pierwszych latach współpracowałem wraz z Prof. Z. Kotulskim (IPPT) z grupą osób zajmujących się kryptografią na Wydziale Telekomunikacji Politechniki Warszawskiej. Na początku poszukiwaliśmy modeli systemów kryptograficznych mających swoją genezę w dynamice cząstek (chodziło o wykorzystanie dużej nieprzewidywalności ich ruchu). Zainteresowaliśmy się ponadto własnościami generatorów liczb losowych bazujących na układach chaotycznych. Stanowią one m. in. podstawowy element szyfrów strumieniowych. Następnie skoncentrowaliśmy się na zastosowaniu bardziej ogólnych modeli układów dynamicznych. Tematykę tą zacząłem również rozwijać od roku 1999 z Prof. J.M. Amigo z Uniwersytetu w Alicante w Hiszpanii. Nasze prace poświecone były zastosowaniu tzw. periodycznych aproksymacji układów dynamicznych (wprowadzonych przez Halmosa i Rohlina) do projektowania kryptosystemów o udowadnialnej odporności na standardowe ataki (kryptanaliza liniowa i różnicowa). Następnie tematykę tą kontynuję także z Prof. L. Kocarevem z Uniwersytetu Kalifornijskiego w San Diego. W latach 2000-2005 odbyłem kilka wizyt naukowych (miesięcznych) jako Visiting Professor na Uniwersytecie w Alicante i Uniwersytecie Kalifornijskim w San Diego.

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 właśnie chaotycznych układów dynamicznych (Physics Letters A 2006, Physics Letters A 2007). 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 (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 IEEE 2007, Physics Letters A 2008 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 bazuje na wykorzystaniu koncepcji Rohlina-Halmosa aproksymacji układów dynamicznych periodycznymi automorfizmami.

W związku z problematyką kryptograficzną zainteresowały mnie ponadto praktyczne możliwości stworzenia generatora liczb losowych opartego na zjawiskach biologicznych. Generatory takie mogłyby mieć znaczenie do generowania tzw. ziaren (wartości początkowych) dla generatorów pseudolosowych (deterministycznych). W tym przypadku przeanalizowaliśmy (z rekomendacją pozytywną) dane biologiczne pochodzące z pomiarów odpowiedzi komórek neuronowych i z pomiarów przewodniości elektrycznej skóry (GSR – data). W przypadku tego problemu współpracowałem obok grupy ludzi z problematyki Neuroscience, także z Prof. M. Slaterem z University College London.

Wyniki dotychczasowych badań związanych z tą tematyką opublikowano w pracach:

[Annalen] Z. Kotulski, J. Szczepanski, „Discrete Chaotic Cryptography", **Annalen der Physik**, vol. 6, no. 5, pp. 381-394, (1997), *Johann Ambrosius Barth*, Heidelberg.

[IJBC I] Z. Kotulski, J. Szczepanski, 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*.

[Archives II] J. Szczepanski, K. Gorski, 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).

[BWAT] 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).

[Open] J. Szczepanski, Z. Kotulski, „Pseudorandom Number Generators Based on Chaotic Dynamical Systems", **Open Systems & Information Dynamics** 8: 137-146, (2001), *Kluwer Academic Publishers*.

[IJBC II] J. M. Amigo, J. Szczepanski, „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*.

[Computers] J. Szczepanski, 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*.

[IEEE I] J. Szczepanski, 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

[IEEE III] 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*

[PLA II] J. M. Amigo, L. Kocarev, J. Szczepanski, „Order patterns and chaos", **Physics Letters A**, 355 (1): 27-31 (2006), *Elsevier Science Publishers*

[IEEE II] 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*

[PLA III] J. M. Amigo, L. Kocarev, J. Szczepanski, „Theory and practice of chaotic cryptography", **Physics Letters A**, 366 (3): 211-216 (2007), *Elsevier Science Publishers*

[PLA I] 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*

[IS] J. Szczepanski, „On the distribution function of the complexity of finite sequences", **Information Sciences**, 179 (9): 1217-1220 (2009), *Elsevier Science Publishers*

D. Zastosowanie Teorii Informacji i teorii układów dynamicznych w układach biologicznych

W roku 2001 zainteresowałem się tematyką związaną z zastosowaniem teorii układów dynamicznych i procesów stochastycznych w naukach biologicznych a szczególnie w Neuroscience i DNA. Tematyka związana z modelowaniem układów biologicznych wydaje mi się być bardzo ciekawa i wciąż wymagająca nowych pomysłów. W moim przypadku chodziło o analizę przesyłania informacji wizualnych przez komórki neuronowe w mózgu. Podjąłem współpracę z grupą Prof. M.V. Sanchez-Vives z Institute of Neuroscience w Alicante. Ze strony polskiej w badaniach bierze udział doc. E. Wajnryb (IPPT). W oparciu o dane eksperymentalne otrzymywane w Laboratorium w Alicante i na Uniwersytecie w Yale

analizowaliśmy, w jaki sposób przekazywane są informacje dotyczące impulsów wizualnych przez komórkę neuronową. Zgodnie z przyjętą hipotezą informacje takie przekazywane są za pomocą tzw. Spików czyli gwałtownych skoków napięcia. Analizy prowadziliśmy głównie wykorzystując koncepcję złożoności w sensie Lempela_Ziva. W ogólności można powiedzieć, że złożoność L-Z mierzy tempo generowania nowych wzorców wzdłuż ciągu symboli. W przypadku procesów ergodycznych złożoność w sensie L-Z jest dobrym (szybkim) estymatorem entropii, a więc średniej ilości informacji (w sensie Shannona) przekazywanej przez proces stochastyczny. Bardziej szczegółowo można tą tematykę ująć następująco.

Mechanizmy przesyłania informacji w sieci neuronowej w mózgu są przedmiotem zainteresowań i dyskusji od wielu lat. Computational Neuroscience jest jednym z podejść [referencje w Biosystems, Network], którego celem jest zrozumienie treści i sposobu transmisji informacji właśnie w układach neuronowych. Sposób przesyłania informacji może być modelowany i analizowany na różnych poziomach. W pracach autora i współautorów analizowany jest problem takiej transmisji na poziomie przesyłania informacji przez komórkę neuronową stanowiącą element sieci wśród wielu takich komórek. Neurony odpowiadają na impulsy zewnętrzne (na przykład na stymulacje wizualne rozpatrywane w pracach autora) poprzez zmianę potencjału membrany. Jeżeli nastąpi depolaryzacja tego potencjału, który osiągnie pewien poziom (threshold) pojawiają się gwałtowne skoki potencjału charakteryzuje się pojawianiem „ostrych pików zwanych w literaturze potencjałami czynnościowymi z języka angielskiego „Spikami". Prądy takie są następnie transmitowane za pośrednictwem aksonów (axons – wypustek nerwowych) do kolejnych komórek neuronowych. Według współcześnie przyjmowanych (aprobowanych) teorii przyjmuje się, że informacja wymieniana pomiędzy neuronami zawarta jest w odstępach czasu występujących pomiędzy Spikami. Ciągle pozostaje otwartym pytaniem, w jaki sposób ta informacja jest zakodowana? Jak dalece zależy to od rodzaju komórki? Czy różne charakterystyki impulsów wejściowych są kodowane w ten sam sposób? W swoich pracach autor analizuje właśnie te problemy. Do analizy przepływu informacji stosowana jest złożoność Lempela-Ziva [referencje w Biosystems, Network, Neural]. Główna idea tego pojęcia jest taka, że unormowana złożoność Lempela-Ziva mierzy tempo generowania nowych fraz wzdłuż ciągu symboli (w szczególności stanowiącego zakodowaną odpowiedź układu na zadany impuls). Warto dodać, że w przeciwieństwie do innych ośrodków do analizy wykorzystano definicję złożoności Lempela-Ziv z roku 1976, a nie z roku 1978. Nasze badania pokazały, że estymator z roku 1976 jest zdecydowanie szybszy.

Informacja w przypadku Neuroscience jest rozumiana w sensie Shannona, a zatem, średnia ilość informacji dla zadanego źródła to entropia. Przy odpowiednich założeniach dotyczących procesu stochastycznego (stacjonarność, ergodyczność) okazuje się, że tzw. unormowana złożoność Lempela-Ziva jest estymatorem entropii tego procesu. Ta właśnie charakterystyka wykorzystywana jest do analizy w pracach autora. Istotną własnością takich estymatorów w przypadku zastosowań biologicznych musi być właśnie szybka zbieżność do entropii (procesu stochastycznego opisującego dane zjawisko biologiczne) gdyż trudno jest utrzymać stacjonarność eksperymentu biologicznego (więc mamy z konieczności krótkie ciągi bo stacjonarność doświadczenia daje się utrzymać na ogół przez relatywnie krótki czas).
W pracach rozpatrywane są dwa typy kodowania Spików stanowiących odpowiedź komórki neuronowej. W pierwszym kodowaniu, które jest rekomendowane szeroko w literaturze [referencje w Network] odcinek czasowy stanowiący odpowiedź komórki neuronowej na dany impuls dzielony jest na mniejsze (równe) przedziały (ilość przedzialików jest tutaj parametrem kodowania) i generowany jest ciąg, w którym stawiamy „zero" jeśli w przedzialiku nie było Spiku i „jeden" w przeciwnym przypadku. W drugim kodowaniu

koncentrujemy się na różnicach/interwałach pomiędzy występowaniem kolejnych Spików. Różnica pomiędzy największym i najmniejszym interwałem dzielona jest na pewną liczbę (jest to parametr kodowania) przedzialików i z każdym przedzialikiem związany jest inny symbol. Różnice pomiędzy kolejnymi interwałami określonymi przez dwa kolejne Spiki (minus najmniejszy interwał) wpada do któregoś z przedzialików i symbol korespondujący do tego przedzialika przyporządkowywany jest Spikowi.
Do analizy wykorzystano wyniki eksperymentów przeprowadzonych w Institute of Neuroscience w Alicante i częściowo w Laboratorium na Uniwersytecie w Yale.
W pracy [Network] analizowano złożoność odpowiedzi neuronów pod kątem zmiany parametrów kodowania. Zgodnie z tym co było wspomniane unormowana złożoność (przy założeniu ergodyczności źródła) może być interpretowana jako entropia źródła czyli jako średnia ilość informacji wysyłanej przez źródło. W pracy zaobserwowano dla drugiego typu kodowania (związanego z różnicami) interesujący fakt istnienia tzw. poziomów nasycenia (Rysunek poniżej). Jest to pewien zakres parametrów/częstotliwości kodowania, dla których unormowana złożoność się nie zmienia. Można takie częstotliwości rozumieć w pewnym sensie jako optymalne i wysunąć hipotezę, że kodowanie w komórce neuronowej odbywa się właśnie z takimi częstotliwościami.

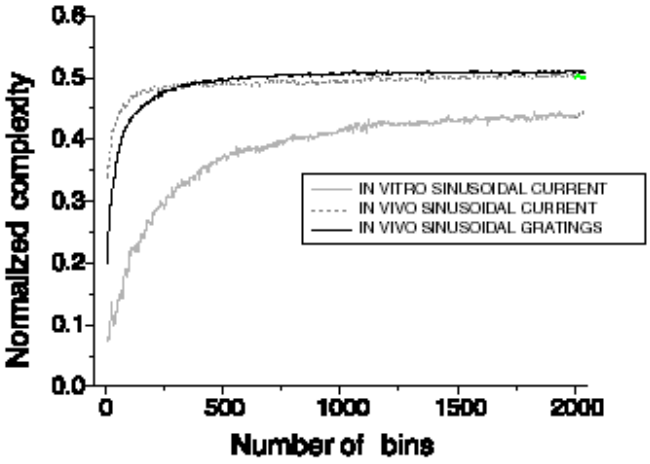

Figure 4. Interspike time coding and periodic stimuli. The curves show the normalized complexity versus number of bins for periodic stimuli (visual stimulation and current injection) both *in vivo* and *in vitro*. The curves saturate as the number of bins increases. This behaviour is typical for the interspike time coding.

Ponadto stwierdzono że poziomy nasycenia są istotnie różne dla różnych typów komórek (in vivo, in vitro) oraz są różne dla różnych typów impulsów (impulsy sinusoidalne, impulsy losowe o różnej autokorelacji) dostarczanych do komórki. Co więcej szczególnie w przypadku komórek in vivo stwierdzono, dla impulsów okresowych, bardzo ciekawy fakt utrzymywania się tej samej wartości złożoności wzdłuż całej zakodowanej trajektorii (Rysunek poniżej) dla dowolnego około 60% długości podciągu kolejnych symboli (Moving Windows).

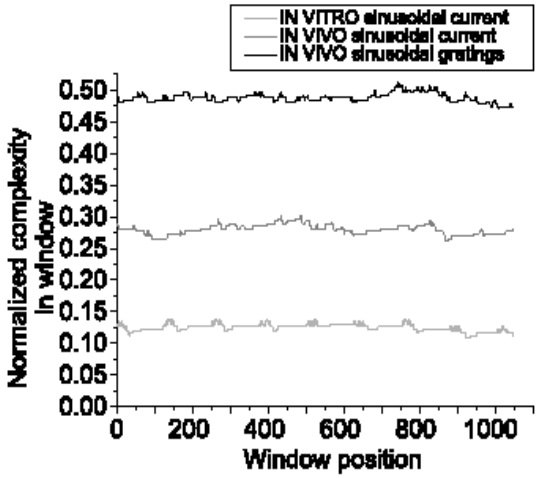

Figure 9. Calculation of normalized complexity with sliding windows—binary bin coding (2048 intervals used for encoding). The window length is 60% of the train length. The position of the left end of the window is given by the abscissa.

Potwierdzałoby to zasadność przyjętego założenia stacjonarności. Ponadto warto zauważyć, że krzywe złożoności wychodzą takie same (Rysunek poniżej) dla powtarzającego się tego samego impulsu (pomimo, że odpowiedź „w Spikach" jest inna z powodu „szumu" generowanego przez neuron).

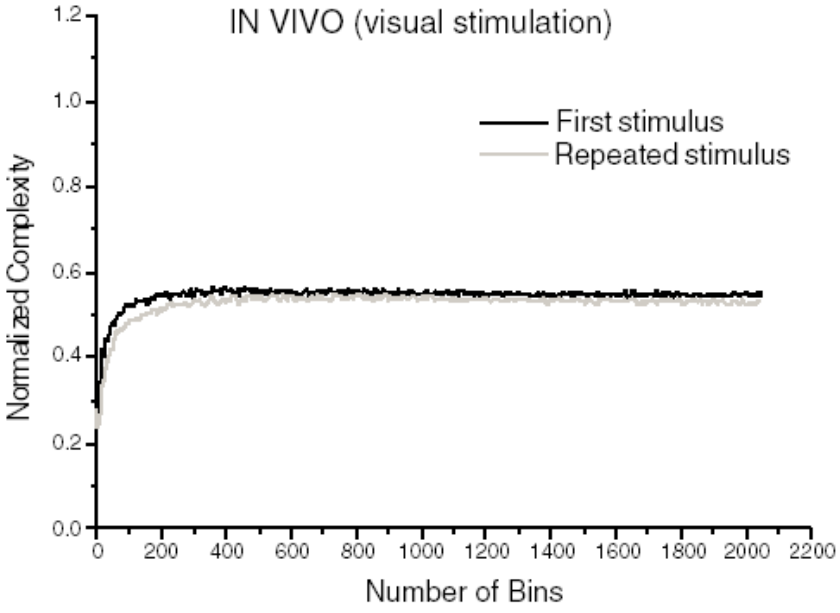

Figure 9 Interspike time coding. This figure shows the complexity curve of the neural response to a repeated application of the same stimulus (sinusoidal visual stimulation).

W pracy [Biosystems] analizowano własności źródła informacji określonego przez źródło zdefiniowane jako zespołu impulsów, komórki neuronowej i ustalonej metody kodowania. Celem było określenie liczby stanów takiego źródła dla różnych wariantów składowych kompleksu. Jako parametry kodowania przyjęto wielkości występujące dla poziomów „nasycenia" znalezione w poprzedniej pracy. Do określenia liczby stanów użyto ponownie złożoności Lempela-Ziva. Założono, że źródło jest źródłem Markowa. Główna idea estymatora liczby stanów polegała na porównywaniu wartości entropii otrzymywanej za pomocą złożoności (która działa dla dowolnego źródła) i estymatora opartego wprost na

definicji procesu Markowa (czyli estymowanie prawdopodobieństw/częstości fraz) przy założeniu, że rząd procesu Markowa jest równy zadanemu *k*. Następnie wybrano jako rząd *k* taką wartość, która była najbliższa wartości entropii estymowanej za pomocą złożoności. Wyniki obliczeń pokazały, że:

1. Dla impulsów/stumulacji okresowych liczba stanów dla komórek *in vivo* jest mniejsza niż dla komórek *in vitro* dla obu metod kodowania.
2. Ilość stanów dla komórek *in vivo* jest podobna dla okresowych (sinusoidalnych) stymulacji wizualnych i dla stymulacji prądem (o tym samym okresie).
3. Liczba stanów dla komórek *in vitro* jest znacznie większa dla okresowych stymulacji niż dla losowych stymulacji (dla kodowania interwałowego).

W pracy [Neural Computation] analizowano estymator entropii oparty na koncepcji złożoności Lempela-Ziva w kontekście jego przydatności do badania przesyłania informacji przez komórkę neuronową. Stwierdzono, że w przypadku źródeł (Zespół stymulacji + Neuron + Metoda kodowania) zdefiniowanych w pracach [Network], [Biosystems] estymator ten jest nawet szybszy niż standardowy dotychczas stosowany estymator zaczerpnięty z literatury fizycznej [referencje w Neural]. Jest to niezwykle ważny problem gdyż jak już wcześniej wspomniano w przypadku eksperymentów prowadzonych w dziedzinie Neuroscience często (ze względu na komplikacje możliwości doświadczalne i koszty) otrzymane próbki (liczba Spików) są raczej krótkie. Ponadto, w pracy pokazano, dla jakiego zakresu parametrów estymator oparty na złożoności jest szybszy od standardowego w przypadku procesu Markowa (o dwóch stanach). Zauważono, że ma to wówczas miejsce, gdy prawdopodobieństwo przejścia od jednego stanu do drugiego jest małe a w odwrotną stronę duże. Sytuacja taka ma właśnie miejsce w przypadku odpowiedzi komórek neuronowych (generowania Spików).

W kolejnej pracy autora (po habilitacji) zatytułowanej “Mutual Information and Redundancy 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 najnowszej 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 istotny wynik, że komunikacja odbywa się pakietami.

W 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.

W nurcie zastosowań procesów stochastycznych w biologii badano również możliwości konstrukcji tzw. potencjałów statystycznych dla łańcuchów DNA w oparciu o prawdopodobieństwa/częstości występowania fragmentów takich łańcuchów. Idea taka jest rozwijana w mechanice statystycznej. W ramach tego problemu współpracowałem z Prof. Zorskim i z T. Michałkiem (IPPT). Okazało się, że tak wprowadzony potencjał w znaczny sposób różnił się dla exonów (części kodujących w łańcuchu DNA) i dla intronów (części nie-kodujących). Potencjał taki można interpretować również w terminach prawdopodobieństw mutacji w tzw. kodonach (codons). Wyniki dotychczasowych badań opublikowano w pracach:

[Biosystems] M. Amigo, J. Szczepanski, 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.*

[JOBP] J. Szczepanski, T. Michalek, „Random Fields Approach to the Study of DNA Chains", **Journal of Biological Physics**, V. 29 (1): 39-54 (2003), *Kluwer Academic Publishers*.

[Network] J. Szczepanski, 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.

[Computers] J. Szczepanski, 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*.

[Neural] J. M. Amigo, J. Szczepanski, 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*.

[NeuroComputing] J. Szczepanski, 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*.

[Physica D] 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.*

[Information] J. Szczepanski, „On the distribution function of the complexity of finite sequences", **Information Sciences**, 179 (9): 1217-1220 (2009), *Elsevier Science Publishers.*

[BC] 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*.

[Biosystem II] 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.*

[JSR] 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)

[Neurocomputing II] B. Paprocki, J. Szczepanski, „How do the amplitude fluctuations affect the neuronal transmission efficiency", **Neurocomputing**, *Elsevier Science Publishers*, 104, 50-56 (2013)

E. Chaos w układach dyskretnych

W roku 2004 zainteresowałem się problemami związanymi z wprowadzeniem klasycznych odpowiedników koncepcji związanych z teorią chaosu układów dynamicznych (wykładnik Lyapunova, dziwny atraktor) dla układów o dyskretnej przestrzeni stanów. W ramach tej tematyki współpracuje z Prof. L. Kocarevem (UCSD), Prof. JM. Amigo, I. Tomovskim (UCSD) i P. Dr. P. Amato (STMicroelectronics, Arzano, Włochy). Zasadniczym wymogiem poprawności wprowadzonych koncepcji dla układów dyskretnych jest ich zbieżność do klasycznych wielkości w przypadku rozpatrywania układów dyskretnych będących aproksymacjami układów ciągłych. Problem dyskretnych wykładników Lyapunowa ma ścisły związek z oceną jakości dyskretyzacji danego ciągłego układu dynamicznego. W przypadku dyskretyzacji do celów kryptograficznych (i nie tylko) wymagane jest, aby takie cechy jak chaos zachowane również były po dyskretyzacji. W pracach (IEEE II 2007, PLA I 2008) przedstawiono możliwości zastosowania wprowadzonych koncepcji dyskretnych wykładników Lyapunova do analizy jakości systemów kryptograficznych, mianowicie do oceny odporności kryptosystemu na kryptoanalizę różnicową oraz do badania losowych permutacji. Wyniki dotychczasowych badań opublikowano w pracach:

[PRL] L. Kocarev, J. Szczepanski, „Finite-space Lyapunov exponents and pseudo-chaos", **Physical Review Letters**, 234101 1-4**,** Dec 3, (2004), *American Physical Society*.

[IEEE] 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*.

[IEEE II] 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*

[PLA I] 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*

Publikacje

Jestem autorem bądź współautorem 37 recenzowanych publikacji naukowych, z tego 34 w czasopismach z tzw. Listy Filadelfijskiej. Po złożeniu habilitacji opublikowałem 11 artykułów w czasopismach z Listy Filadelfijskiej oraz kilka publikacji w materiałach konferencyjnych.
Liczba cytowań moich prac wynosi **259**
Sumaryczny Impact Factor publikacji: **57.821 (w tym uzyskane po habilitacji: 22,207)**
Indeks Hirsha: 11

Mój dorobek naukowy obejmuje szerokie spektrum dziedzin, od prac w czasopismach o profilu informatycznym lub nawet czysto matematycznym, poprzez artykuły w czasopismach w nurcie biologicznym (Neuroinformatics), tematyce fizycznej i tematyce inżynierskiej. Współpracuję z wieloma ośrodkami na świecie (Miguel Hernandez University, Alicante; University of California, San Diego; University College London).

Obszar zainteresowań naukowych
- Modelowanie matematyczne w biologii i medycynie, zastosowanie teorii procesów stochastycznych i układów dynamicznych
- Analiza procesów transmisji informacji w sieciach neuronowych, szczególnie w mózgu (Neuroinformatyka, Teoria Informacji)
- Bezpieczeństwo danych w sieciach teleinformatycznych, m.in. związane z tym zagadnieniem aspekty kryptologiczne
- Problematyka chaosu dla układów o dyskretnej liczbie stanów

Edukacja i uzyskane stopnie naukowe
1979 – Uniwersytet Warszawski, Wydział Matematyki, mgr
1985 – Instytut Podstawowych Problemów Techniki PAN, dr
2007 – Instytut Podstawowych Problemów Techniki PAN, habilitacja (z wyróżnieniem)

Przebieg kariery naukowej
1985 – adiunkt, IPPT PAN
2007 – docent IPPT PAN
2007 – prof. nadzw. UKW
2010 – prof. nadzw. IPPT PAN

Pełnione funkcje

- Członek Komitetu Redakcyjnego czasopisma International Journal of Computational Science wydawanego w Hong Kongu przez Global Information Publisher; od 2007 r.
- Członek Komitetu Programowego Konferencji Future Generation Communication and Networking, FGCN w kolejnych latach 2007-2010
- Członek Komitetu Programowego (Technical Program Co-Chairs), International Symposium on Applied Computing and Computational Sciences, 2008, Hong Kong
- Członek American Mathematical Society (od roku 1993),
- Członek International Association for Cryptographic Research (od roku 2003).

Nagrody i inne osiągnięcia

- 1989 – Nagroda Wydziału IV PAN im. T. Hubera za prace poświecone Liouville equation in finite-dimensional Hilbert space;
- 2002 – 2004 Konsultant w zakresie kryptologii w Centrum Certyfikacji Centrast S.A., tzw. Root w systemie PKI w Polsce; spółka Centrast działała z ramienia Narodowego Banku Polskiego (75 procent udziału);
- 2002 Współuczestniczyłem w przygotowaniu Ustawy o podpisie elektronicznym;
- Przez wiele lat byłem członkiem Komisji oceniającej najlepsze prace magisterskie z zakresu kryptografii; prezentacja prac odbywa się podczas konferencji ENIGMA poświęconej bezpieczeństwu systemów teleinformatycznych;

Recenzje

- Recenzowałem kilkadziesiąt artykułów dla wielu renomowanych czasopism.
- Byłem recenzentem dwóch rozpraw doktorskich (dr S. Kotowskiego w IPPT PAN i dr Gabrieli Mochol w **Instytucie Nenckiego** PAN)
- Wykonałem pięć recenzji projektów badawczych i na rzecz obronności dla Ministerstwa Nauki i NCBiR

Działalność dydaktyczna

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.

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, w trakcie wszczynania przewodu, planowana obrona w 2013 r., promotor

Kierownictwo i uczestnictwo w projektach

- 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 Kierownictwo Projektu: "Information-Theoretical and cryptographical aspects of neuronal discharges" 17/2004/2005, joint project with Institute of Neuroscience, CSIC - Universidad Miguel Hernandez (Prof. M.V. Sanchez-Vives) Spain
- 2004, Research visit at the University of California San Diego w ramach projektu NSF. The subject: Cryptography and Coding Theory
- 2003, Research visit at the Miguel Hernandez University – Alicante. The subject: Neurosciences and Cryptography; wizyta w ramach otrzymanego grantu rządu Walencji
- 1992, Grant of Kosciuszko Foundation (New York), SIAM Conference
- 1997 - 1999 „Application of stochastic methods in cryptography", KBN 8 T11 D01112, Warsaw University of Technology, główny wykonowca
- 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 „New methods of constructions and analysis of cryptosystems", KBN 8T11 D02019, IFTR PAS, główny wykonawca
- 2000 – 2002 „Thermodynamic of biopolymers chains" KBN 8T0 7A 045 20, IFTR PAS, member of project
- 2001 – 2002 Kierownictwo Projektu: "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

Prezentacje i uczestnictwo w wybranych Konferencjach

- „Dynamics Days" – Dusseldorf i Berlin, 1988, 1990
- „SIAM Conference on Application of Dynamical Systems" – Salt Lake City, USA, Oct. 1992 (dwa referaty)
- „International Conference on Nonlinear Dynamics" – Zakopane, Poland, September 1995
- „Nonlinear Evolution Equations and Dynamical Systems" – Kolymbari, Greece, June 1997 (organizer University La Sapienza, Roma)

- **"**NATO Regional Conference on Military Communications and Information Systems – Partnership for CIS Interoperability**",** Zegrze, October 6-8, 1999 and October 10 – 12, 2001
- **"**World Congress on Neuroinformatics**" ,** Vienna, September 24-29, 2001
- **"**The Annual Computational Neurosciences Meeting**" ,** Alicante, Spain, July 5-9, 2003
- **"**International Workshop on Dynamical Systems and Complexity in Information and Communication Technology**" ,** Bologna, Italy, September 6-8, 2004
- **"**International Symposium on Nonlinear Theory and its Applications, NOLTA 2005**" ,** Bruges, Belgium, October 18-21, 2005
- **"**35th Meeting Society for Neuroscience**" ,** Washington, November 12-16, 2005
- **"**3th Congreso Iberoamericano de Seguridad Informatica**" ,** Valparaiso, Chile, November 21-25, 2005
- "10th International Neural Coding Workshop 2012", Prague, Czech, September 2–8, 2012
- "Neuroscience Congress- 8th Federation of European Neuroscience Societies (FENS) Forum", Barcelona, Spain, July 14–18, 2012
- Research visit at the Moscow University, 1989
- 1988 – participation in the course devoted to the Chaos Theory in Dynamical Systems, Udine, Italy

Współpraca z zagranicznymi ośrodkami

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.

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).