

**REZULTATELE ACTIVITĂȚILOR DE CERCETARE-DEZVOLTARE
DESĂȘURATE ÎN CADRUL TEZEI DE DOCTORAT CU TITLUL**

**CONTRIBUȚII LA OPTIMIZAREA GENERATOARELOR DE SECVENȚE
PSEUDOALEATOARE CRIPTOGRAFICE PE BAZA TEORIEI MATEMATICE A
HAOSULUI**

AUTOR Cornaciu Veronica		ÎNDRUMĂTOR Prof. Dr. Ing. Ciprian Răcuciu	
DOMENIUL DE DOCTORAT			
INGINERIE ELECTRONICĂ, TELECOMUNICAȚII ȘI TEHNOLOGII INFORMAȚIONALE			
Data înmatriculării	01.10.2018	Data susținerii publice	03.10.2025
Data confirmării			
REZULTATELE ACTIVITĂȚII DE CERCETARE-DEZVOLTARE			
DENUMIRE REZULTAT			
CATEGORIA REZULTATULUI	Rezultat final	DETALIERE CARACTERISTICI ALE REZULTATULUI FINAL	
documentații, studii, lucrări	[X]	<p>- Analiza generatoarelor pseudoaleatoare și a generatoarelor hibride din perspectiva performanțelor criptografice:</p> <ul style="list-style-type: none"> o Studiul comparativ al generatoarelor existente, cu accent pe criteriile de selecție bazate pe robustețea criptografică, calitatea secvențelor generate și rezistența la atacuri statistice. <p>- Metode de selecție a generatoarelor în funcție de cerințele specifice ale aplicațiilor criptografice:</p> <ul style="list-style-type: none"> o Propunerea unui set de criterii de selecție și clasificare a generatoarelor în funcție de parametrii specifici (entropie, perioadă, sensibilitate la condițiile inițiale) și de domeniul de aplicabilitate (securitate criptografică, simulare stocastică, etc.). o Aplicarea algoritmilor de asociere (ex. Apriori) pe un set de date sintetice care simulează rețete medicale, cu scopul de a descoperi medicamente frecvent prescrise împreună. 	
planuri, scheme	[X]		
tehnologii	[X]		
procedee, metode	[X]		
produse informatice	[X]		
rețete, formule	[]		
obiecte fizice/ produse	[]		
brevet invenție/ altele asemenea	[]		
STADIUL DE DEZVOLTARE	soluție/ model conceptual	[X]	
	model experimental/ funcțional	[X]	
	prototip	[]	
	instalație pilot sau echivalent	[]	
	altele	[X]	
DOMENIUL DE CERCETARE	tehnologiile societății informaționale	[X]	
	energie	[]	
	mediu	[]	
	sănătate	[]	
	agricultură, securitatea și siguranța alimentară	[]	
	biotehnologii	[X]	
	materiale, procese și produse inovative	[X]	
	spații și securitate	[X]	

<p>cercetări socio –economice și umaniste</p>	<p>[]</p>	<p>- Analiza comparativă a generatoarelor bazate pe funcții haotice:</p> <ul style="list-style-type: none"> ○ Evaluarea performanțelor criptografice ale unor generatoare bazate pe funcții haotice prin aplicarea unor metode avansate de analiză statistică și criptografică, evidențiind vulnerabilitățile și punctele forte ale acestora. ○ Investigarea utilizării funcțiilor bent ca o clasă specială de funcții haotice discrete, evidențiind contribuția acestora la creșterea nelinearității, îmbunătățirea distribuției statistice și sporirea rezistenței criptografice a generatoarelor în care sunt integrate. <p>- Analiza comparativă a generatoarelor cuantice:</p> <ul style="list-style-type: none"> ○ Realizarea unei analize detaliate a generatoarelor care utilizează metode cuantice, subliniind avantajele în ceea ce privește imprezizibilitatea secvențelor generate și potențialul acestora în criptografia cuantică. ○ Propunerea și modelarea unui protocol original de comunicare directă cuantică securizată (Quantum Secure Direct Communication – QSDC), bazat pe gruparea fotonilor individuali, utilizarea fotonilor falși, multiple baze ortogonale de polarizare și stocare în memorie cuantică, asigurând astfel detectarea eficientă a interceptării și eliminarea necesității distribuirii prealabile a unei chei criptografice. <p>- Analiza comparativă a generatoarelor bazate pe algoritmi genetici:</p> <ul style="list-style-type: none"> ○ Studiul algoritmilor genetici utilizați pentru generarea numerelor pseudoaleatoare, cu accent pe eficiența acestora în generarea secvențelor cu distribuție uniformă și pe optimizarea parametrilor algoritmilor. <p>- Analiza generatoarelor de ultimă generație bazate pe rotații de biți:</p>
--	------------	---

		<ul style="list-style-type: none"> ○ Realizarea unei analize comparative asupra generatoarelor hibride și a celor de ultimă generație care integrează rotații pe biți, așa cum sunt cele propuse de Agner Fog, evidențiind impactul acestor tehnici asupra distribuției secvențelor, entropiei și comportamentului criptografic al generatoarelor. ○ Identificarea vulnerabilităților și avantajelor acestor metode prin aplicarea unor teste criptografice avansate și propunerea de strategii de optimizare. <p>- Introducerea unor pseudo-operatori și generalizarea acestora:</p> <ul style="list-style-type: none"> ○ Definirea unor pseudo-operatori de tip Ben-Tal și extinderea acestor structuri la nivelul analizelor matematice aplicate în optimizare și criptografie. ○ Studiul proprietăților acestor operatori, incluzând asociativitatea, comutativitatea și distributivitatea, precum și construcția derivatei generalizate după o direcție. <p>- Obținerea unor condiții de optimizare de tip Karush-Kuhn-Tucker:</p> <ul style="list-style-type: none"> ○ Reformularea condițiilor de optimizare de tip KKT în contextul aplicării operatorilor pseudo-algebrici generalizați, demonstrând utilitatea acestora în problemele de programare semi-infinită și multi-criterială. <p>- Implementarea unor generatoare hibride bazate pe funcții haotice și pseudo-operatori generalizați de tip Ben-Tal:</p> <ul style="list-style-type: none"> ○ Dezvoltarea unor structuri algoritmice hibride care combină funcții haotice cu pseudo-operatori de tip Ben-Tal și rotații de biți, astfel încât să se maximizeze imprevizibilitatea și rezistența la atacuri criptografice. <p>- Testarea și validarea generatoarelor propuse prin suite de teste criptografice NIST:</p> <ul style="list-style-type: none"> ○ Aplicarea suitei NIST asupra generatoarelor propuse pentru a
--	--	---

			<p>evalua calitatea statistică a secvențelor și pentru a identifica posibile puncte slabe în structura algoritmică.</p> <p>- Interpretarea rezultatelor obținute și formularea unor metode de optimizare în vederea îmbunătățirii performanțelor criptografice</p> <p>- Interpretarea criptografică a rezultatelor obținute și propunerea unor metode de optimizare :</p> <ul style="list-style-type: none"> o Identificarea corelațiilor dintre structura generatorului, tipologia operatorilor utilizați și caracteristicile secvențelor generate, propunând strategii de optimizare orientate către utilizarea practică a acestor generatoare în aplicații criptografice.
--	--	--	---

CARACTERUL INOVATIV	produs nou	[]	
	produs modernizat	[X]	
	tehnologie nouă	[]	
	serviciu nou	[]	
	serviciu modernizat	[]	
	altele	[X]	
INFORMAȚII PRIVIND PROPRIETATEA INTELECTUALĂ			
Cerere înregistrare brevet de invenție		-	
Brevet de invenție înregistrat (național, european, internațional)		-	
Cerere înregistrare modele și desene industriale protejate		-	
Modele și desene industriale protejate înregistrate (național, european, internațional)		-	
DOMENII DE APLICABILITATE		DETALIERE APLICABILITATE	
În domeniul de interes al MapN		<p>1. Analiza și clasificarea generatoarelor pseudoaleatoare cu aplicabilitate în criptografia militară</p> <ul style="list-style-type: none"> • Realizarea unei evaluări comparative a generatoarelor pseudoaleatoare (PRNG) și a generatoarelor hibride, în vederea identificării celor cu grad ridicat de entropie, robustețe criptografică și rezistență la atacuri statistice, criterii esențiale pentru sistemele de comunicații militare securizate. • Propunerea unui set de criterii de selecție a generatoarelor în funcție de cerințele aplicațiilor din domeniul apărării, precum criptarea comunicațiilor radio, generarea de chei unice și protecția datelor clasificate. 	

	<p>2. Securizarea comunicațiilor și a canalelor de comandă-control</p> <p>Generatoarele hibride propuse pot fi integrate în sisteme de criptare în timp real, asigurând:</p> <ul style="list-style-type: none"> • protecție sporită împotriva interceptării și injectării de date; • performanțe robuste în medii ostile (interferențe, perturbări). <p>3. Suport pentru infrastructuri distribuite și sisteme autonome</p> <p>Datorită dimensiunii reduse și a complexității controlabile, generatoarele propuse sunt:</p> <ul style="list-style-type: none"> • compatibile cu platforme militare mobile (dronă, UAV, satelit); • aplicabile în rețele distribuite cu cerințe ridicate de securitate și latență minimă.
--	--

<p>În alte domenii Aplicații în domeniul optimizării matematice</p>	<p>- Obținerea unor condiții de optimalitate de tip Karush-Kuhn-Tucker:</p> <ul style="list-style-type: none"> • Reformularea condițiilor de optimizare de tip KKT în contextul aplicării operatorilor pseudo-algebrici generalizați, demonstrând utilitatea acestora în problemele de programare semi-infinită și multi-criterială.
<p>DISEMINAREA REZULTATELOR CERCETĂRII REALIZATE ÎN CADRUL TEZEI DE DOCTORAT</p>	<p style="text-align: center;">DENUMIRE ARTICOL/REVISTĂ/CONFERINȚĂ</p>
<p>Articole publicate în reviste/ proceedings cotate ISI</p>	<ol style="list-style-type: none"> 1. V. Cornaciu, I. Ileana, , <i>The Avriel-Ben-Tal algebraic operations approach for a short version proof of the Karush-Kuhn-Tucker optimality conditions</i>, Analele Stiintifice ale Universitatii Ovidius Constanta, Seria Matematica, Vol. 25(2), 2017, 3948, DOI: 10.1515/auom-2017-0019, WOS:000411439100003. 2. A. Bobe, C. Racuciu, V. Cornaciu, <i>Karush-Kuhn-Tucker Necessary Optimality Conditions for $(h, \varphi)\epsilon$-Multiobjective Optimization Problems Based on Pseudo-Avriel-Ben-Tal Algebraic Operation</i>, Analele Stiintifice ale Universitatii Ovidius Constanta, Seria Matematica, articol acceptat spre publicare.
<p>Articole publicate în reviste / proceedings cotate BDI</p>	<ol style="list-style-type: none"> 1. V. Cornaciu, $(h, \varphi)_\epsilon$ – <i>Optimality conditions for multi-objective fractional semi-infinite programming with uniform $K - (F_b, \rho)$ – convexity</i>, “Mircea cel Batran” Naval Academy Scientific Bulletin, 19(1), 359-366, 2016. DOI: 10.21279/1454-864X-16-I1-060.

2. V. Preda., **V. Cornaciu**, (h, φ) – *Optimality conditions for locally Lipschitz generalized B-vex semi-infinite programming*, “Mircea cel Batran” Naval Academy Scientific Bulletin, 19(2), 387-393, 2016. DOI: 10.21279/1454-864X-16-I2-056.
3. **V. Cornaciu**, *Applications of the pseudo-operators in differential equations*, Conferința internațională “Educație și creativitate pentru o societate bazată pe cunoaștere”, Universitatea Titu Maiorescu, secțiunea Știința și tehnologia informației, Ediția a X-a, București, 17-19 noiembrie, 2016, ISSN 2248-0056, ISBN 978-3-9503145.
4. **V. Cornaciu**, *Pseudo-operators and generalized directional derivative*, Conferința internațională “Educație și creativitate pentru o societate bazată pe cunoaștere”, Universitatea Titu Maiorescu, secțiunea Știința și tehnologia informației, Ediția a XI-a, București, 2017. ISSN 2248-0056, ISBN 978-3-9503145-5-7.
5. L., Zisu, **V. Cornaciu**, *Quantum Secure Direct Communication With Single Photons And Quantum Memory*, Conferința internațională “Educație și creativitate pentru o societate bazată pe cunoaștere”, Universitatea Titu Maiorescu, secțiunea Știința și tehnologia informației, Ediția a XIII-a, București, 2019. ISSN 2248-0056, ISBN 978-3-9503145-5-7.
6. **V. Cornaciu**, C. Răcuciu, *Multi-criteria method for evaluation of the pseudorandom number generators used in the study of thermodynamic systems*, The 5th International Scientific Conference SEA-CONF 2019, Constanța, Romania. Lucrarea este publicată în Scientific Bulletin of Naval Academy, Vol. XXII 2019, issue no. 2, pp.305-312. ISSN: 2392-8956; ISSN-L: 1454-864X, doi: 10.21279/1454-864X-19-I2-036.
7. **V. Cornaciu**, C. Răcuciu, *An overview of hybrid random number generators*, The 6th International Scientific Conference SEA-CONF 2020, Constanța, Romania. Lucrarea este publicată în Scientific Bulletin of Naval Academy, Vol. XXIII 2020, issue no. 1, pp.248-252. ISSN: 2392-8956; ISSN-L: 1454-864X, doi: 10.21279/1454-864X-20-I1-034.
8. **V. Cornaciu**, C. Răcuciu, L. Zisu, *An short analysis of modern methods in random number generators*, The 7th International Scientific Conference SEA-CONF 2021, Constanța, Romania. Lucrarea este publicată în Proceedings of the International Scientific Conference SEA-CONF, ISSN: 2457-144X; ISSN-L: 2457-144X, pp . 224-232, doi: 10.21279/1454-864X-19-I1-023.
9. **V. Cornaciu**, C. Răcuciu, C. Dascalescu, V. Garban, C. Dinuca, *A short analysis over bent functions in cryptography*, Conferința internațională “Educație și creativitate pentru o societate bazată pe cunoaștere”, Universitatea Titu Maiorescu, secțiunea Știința și tehnologia informației, Ediția a XVIII-a, București, 2024. ISSN 2248-0056, ISBN 978-3-9503145-5-7.
10. E. C. Dinuca, D. Joita, A. C. Dascalescu **V. Cornaciu**, , *Using data mining algorithms on medical prescriptions*, Conferința internațională “Educație și creativitate pentru o societate bazată pe cunoaștere”, Universitatea Titu Maiorescu, secțiunea Știința și tehnologia informației, Ediția a XVIII-a, București, 2024. ISSN

	<p>2248-0056, ISBN 978-3-9503145-5-7..</p> <p>11. V. Cornaciu, C. Răcuciu „An Overview of Pseudorandom Number Generators With Bit Rotations”, în Proceedings of the 17th International Conference on Electronics, Computers and Artificial Intelligence (ECAI 2025), 26-27 iunie 2025, Targoviste, România, pp. 1-4. doi: 10.1109/ECAI65401.2025.11095541. Conferință indexată IEEE Xplore, ISI Proceedings (WoS) și Scopus.</p> <p>12. V. Cornaciu, C. Răcuciu „An Analysis of Genetic Algorithms in Cryptography”, în Proceedings of the 17th International Conference on Electronics, Computers and Artificial Intelligence (ECAI 2025), 26-27 iunie 2025, Targoviste, România doi: 10.1109/ECAI65401.2025.11095532. Conferință indexată IEEE Xplore, ISI Proceedings (WoS) și Scopus.</p> <p>13. M. Rogobete, C.-S. Oprina, V. Cornaciu, M. Rogobete, „A Quantum Resistant Authentication Survey – ID87,” Proc. 11th Int. Sci. Conf. SEA-CONF 2025, Constanța, Romania, <i>Scientific Bulletin of Naval Academy</i>, vol. XXVIII, 2025.</p> <p>14. V. Cornaciu, C. Răcuciu, „Chaos-Based Pseudorandom Number Generators: A Theoretical Overview and Simulation-Based Analysis”, <i>Journal of Military Technology</i>. Articol în curs de apariție.</p> <p>15. V. Cornaciu, C. Răcuciu, „Survey and Analysis of Optical Implementation of Quantum Random Number Generators”, <i>Journal of Military Technology</i>. Articol în curs de apariție.</p>
<p>Articole susținute la conferințe internaționale</p>	
<p>Articole susținute la conferințe naționale</p>	

Data

05.09.2025

Semnătura

