REZULTATELE ACTIVITĂŢILOR DE CERCETARE – DEZVOLTARE DESFĂŞURATE ÎN CADRUL TEZEI DE DOCTORAT CU TITLUL

Securitatea algoritmilor criptografici

<table>
<tr><td colspan="3">AUTOR
Dr.ing. Florin MEDELEANU</td><td colspan="3">ÎNDRUMĂTOR
Prof.univ. dr.ing. Ciprian RĂCUCIU</td></tr>
<tr><td colspan="6">DOMENIU DE DOCTORAT</td></tr>
<tr><td>Data înmatriculării</td><td>01.10.2010</td><td>Data susținerii publice</td><td>04.07.2017</td><td>Data confirmării</td><td>27.12.2017</td></tr>
<tr><td colspan="6">REZULTATELE ACTIVITĂȚII DE CERCETARE-DEZVOLTARE</td></tr>
<tr><td colspan="2">DENUMIRE REZULTAT</td><td colspan="4"></td></tr>
<tr><td colspan="2">CATEGORIA REZULTATULUI</td><td colspan="2">Rezultat final</td><td colspan="2">DETALIERE CARACTERISTICI ALE REZULTATULUI FINAL</td></tr>
<tr><td colspan="2">documentaţii, studii, lucrări</td><td colspan="2">[x]</td><td colspan="2" rowspan="24"></td></tr>
<tr><td colspan="2">planuri, scheme</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2">tehnologii</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2">procedee, metode</td><td colspan="2">[x]</td></tr>
<tr><td colspan="2">produse informatice</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2">reţete, formule</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2">obiecte fizice / produse</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2">brevet invenţie / altele asemenea</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2" rowspan="5">STADIUL DE DEZVOLTARE</td><td>soluţie / model conceptual</td><td>[x]</td></tr>
<tr><td>model experimental / funcţional</td><td>[x]</td></tr>
<tr><td>prototip</td><td>[ ]</td></tr>
<tr><td>instalaţie pilot sau echivalent</td><td>[ ]</td></tr>
<tr><td>altele ……</td><td>[ ]</td></tr>
<tr><td colspan="2" rowspan="9">DOMENIUL DE CERCETARE</td><td>tehnologiile societăţii informaţionale</td><td>[x]</td></tr>
<tr><td>energie</td><td>[ ]</td></tr>
<tr><td>mediu</td><td>[ ]</td></tr>
<tr><td>sănătate</td><td>[ ]</td></tr>
<tr><td>agricultură, securitatea şi siguranţa alimentară</td><td>[ ]</td></tr>
<tr><td>biotehnologii</td><td>[ ]</td></tr>
<tr><td>materiale, procese şi produse inovative</td><td>[ ]</td></tr>
<tr><td>spaţii şi securitate</td><td>[ ]</td></tr>
<tr><td>cercetări socio – economice şi umaniste</td><td>[ ]</td></tr>
<tr><td colspan="2" rowspan="7">CARACTERUL INOVATIV</td><td>produs nou</td><td>[]</td><td colspan="2" rowspan="7">DETALIERE CARACTER INOVATIV</td></tr>
<tr><td>produs modernizat</td><td>[x]</td></tr>
<tr><td>tehnologie nouă</td><td>[ ]</td></tr>
<tr><td>serviciu nou</td><td>[ ]</td></tr>
<tr><td>serviciu modernizat</td><td>[x]</td></tr>
<tr><td>altele…….</td><td>[ ]</td></tr>
</table>

INFORMAŢII PRIVIND PROPRIETATEA INTELECTUALĂ	
cerere înregistrare brevet de invenţie	Nr . ..... data.....
brevet de invenţie înregistrat (naţional, european, internaţional)	Nr . ..... data.....
cerere înregistrare modele şi desene industriale protejate	Nr . ..... data.....
modele şi desene industriale protejate înregistrate (naţional, european, internaţional)	Nr . ..... data.....

DOMENII DE APLICABILITATE	**DETALIERE APLICABILITATE**
În domeniul de interes al MApN	
În alte domenii	
DISEMINAREA REZULTATELOR CERCETĂRII REALIZATE ÎN CADRUL TEZEI DE DOCTORAT	**DENUMIRE ARTICOL/REVISTĂ/CONFERINȚĂ**
Articole publicate în reviste /Proceedings cotate ISI	[18] **Florin Medeleanu**, Ciprian Racuciu, Marius Rogobete, Considerations about the possibilities to improve AES S-box criptographic properties by multiplications, Series A: Mathematics, physics, technical sciences, information science, volume 16, Special issue 2015, Cryptology science [19] Ciprian Racuciu, Dan Laurenţiu Grecu, **Florin Medeleanu**, Nicolae Jula, Dan Raducanu, Comparative Analysis for the New Generation of Encryption Algorithms Involved in NESSIE and CRYPTREC Projects, in the Book "RECENT ADVANCES in COMPUTATIONAL INTELLIGENCE, MAN-MACHINE SYSTEMS and CYBERNETICS", Included in ISI/SCI Web of Science and Web of Knowledge, Cairo, Egypt, 2008, pp. 186-190, ISSN: 1790-5117, ISBN: 978-960-474-049-9
Articole publicate în reviste /Proceedings cotate BDI	[20] Ciprian Racuciu, Dan Laurenţiu Grecu, **Florin Medeleanu**, Evaluating Noise Resistance and Speed for the New Generation of Symmetric-Key Encryption Algorithms, in the Pubblication ”Scientific bulletin of the „POLITEHNICA” University of Timişoara, Transactions on Electronics and Communications, Tomul 54(68), Fascicola 2, 2009, pp.15-18, ISSN: 1583-3380 [21] Ciprian Răcuciu, Dan Laurenţiu Grecu, **Florin Medeleanu**, Symmetric Block Type Algorithm Resistance to „Key Bridging” Attacks” – Revista Tehnică Militară nr. 2 / 2010, pp.15-18, ISSN 1582-7321 [22] **Florin Medeleanu**, Securitatea în cloud: adevăr sau deziderat, Revista Infosfera nr. 3 / 2013, pp.91-96, ISSN 2065-3395
Articole susținute la conferințe internaționale	[1] Ciprian Răcuciu, Dan Laurenţiu Grecu, **Florin Medeleanu**, Comparative analysis for the new generation of encryption algorithms involved in NESSIE and CRYPTREC projects, The 38-th International Symposium of the Military Equipment & Technologies Research Agency, Bucureşti, May 29, 2008, ISBN 978-973-0-05684-6. [2] **Florin Medeleanu**, Ciprian Răcuciu, Dan Laurenţiu Grecu, Evaluation of Key Bridging Attacks on Symmetric Block Encryption Algorithms, International Conference „Education and Creativity for a Knowledge Based Society”, The 4-th Edition, Universitatea Titu Maiorescu, oct. 2010 [3] **Florin Medeleanu**, Ciprian Răcuciu, Dan Laurenţiu Grecu, Analyze of Confusion and Diffusion Properties of AES Key Schedule, International Conference „Education and Creativity for a Knowledge Based Society”, The 5-th Edition, Universitatea Titu Maiorescu, nov. 2011 [4] **Florin Medeleanu**, Dan Laurenţiu Grecu, Key Schedule Proposal For AES

	Secure Against Related Key Differential Attack, The 1-st Edition of Romanian Cryptology Days, 2011, 11-12 Nov., hosted by Foreign Intelligence Service (SIE) [8] Ciprian Răcuciu, **Florin Medeleanu**, Antonie Narcis-Florentin, The security of cloud storage systems: aspects of information security in the cloud, data integrity, proof of storage and proof of ownership protocols, Conferinţa NAVMAR-EDU-2013 [9] Ciprian Răcuciu, **Florin Medeleanu**, Dan-Laurenţiu GRECU, Anonymous signature applications in e-voting systems, International Conference „Education and Creativity for a Knowledge Based Society", The 8-th Edition, Universitatea Titu Maiorescu, nov. 2014 [13] **Florin Medeleanu**, Marius Rogobete, Ciprian Răcuciu, Considerations on differential cryptanalysis attacks on lightweight block ciphers, Conferinţa SeaConf-2015, mai 2015, Constanţa, Romania [14] Marius ROGOBETE, Ciprian RĂCUCIU, Marian-Dorin PÎRLOAGĂ, **Florin MEDELEANU**, Image Protection. A Framework Proposal, Conferinţa SeaConf-2015, mai 2015, Constanţa, Romania [15] Marius ROGOBETE, Ciprian RĂCUCIU, Marian-Dorin PÎRLOAGĂ, **Florin MEDELEANU**, Using Hide Watermark in Visual Watermark extraction.Advantages. Algorithm, Conferinţa SeaConf-2015, mai 2015, Constanţa, Romania [16] **Florin Medeleanu**, Ciprian Răcuciu, Dan Laurenţiu Grecu, Developing and modeling a new e-lottery system using anonymous signatures, Conferinţa SeaConf-2016, mai 2016, Constanţa, Romania [17] **Florin Medeleanu**, Ciprian Răcuciu, Dan Laurenţiu Grecu, Application of Anonymous Signatures in Lottery Systems, International Conference „Education and Creativity for a Knowledge Based Society", The 10-th Edition, Universitatea Titu Maiorescu, nov. 2016
Articole susținute la conferințe naționale	[5] **Florin Medeleanu**, Analiza primitivelor criptografice publice utilizate în prezent şi oportunităţi pentru serviciile de informaţii, Ed. I a Sesiunii de comunicări ştiinţifice a Scolii de Aplicaţie pentru Informaţii de Apărare, 23 nov. 2011, ISBN 978-973-663-918-0 [6] **Florin Medeleanu**, Securitatea în cloud: adevăr sau deziderat, Ed. II a Sesiunii de comunicări ştiinţifice a Scolii de Aplicaţie pentru Informaţii de Apărare, 14 nov. 2012, ISBN 978-606-660-005-7, publicat şi în Revista Infosfera, nr. 3/2013 [7] **Florin Medeleanu**, Maria Ursulean, Anonimitatea şi semnarea anonimă a datelor în format electronic, Ed. III a Sesiunii de comunicări ştiinţifice a Scolii de Aplicaţie pentru Informaţii de Apărare, 2013 [10] **Florin Medeleanu**, Hermina Dragnea, Maria Ursulean, Rezistenţa la atacuri cibernetice a algoritmilor criptografici uşor computabili, Ed. IV a Sesiunii de comunicări ştiinţifice a Scolii de Aplicaţie pentru Informaţii de Apărare, 2015 [11] **Florin Medeleanu**, Maria Ursulean, Florina Matei, Prevenirea si combaterea agresiunilor cibernetice prin utilizarea algoritmilor uşor computabili, Ed. IV a Sesiunii de comunicări ştiinţifice a Scolii de Aplicaţie pentru Informaţii de Apărare, 2015 [12] **Florin Medeleanu**, Gheorghe Lăzureanu, Protecţia împotriva atacului cibernetic utilizând semnătura electronică, Ed. IV a Sesiunii de comunicări ştiinţifice a Scolii de Aplicaţie pentru Informaţii de Apărare, 2015

Data *Semnatura*

23.01.2018