ANEXA 4c

FIŞA DE VERIFICARE
A ÎNDEPLINIRII STANDARDELOR MINIMALE ALE UNIVERSITĂŢII
pentru ocuparea posturilor didactice şi de cercetare (adaptată după metodologia proprie UAV)

Lector universitar/Şef lucrări

I. DATE DESPRE CANDIDAT

NUME DRĂGOI PRENUME VLAD FLORIN CNP

Postul pentru care candidează Lector universitar Disciplinele Sisteme de operare; Programare orientata pe obiecte; Dezvoltarea aplicaţiilor web; Structuri de date; Securitate informatica.

Poziţia în statul de funcţii 24

Departamentul MATEMATICA-INFORMATICA

Facultatea de Ştiinte Exacte

Gradul didactic actual Lector Poziţia în Statul de funcţii 33 Discipline Sisteme de operare;

Programare orientata pe obiecte; Dezvoltarea aplicatiilor web; Structuri de date; Securitate informatica.

Departamentul MATEMATICA-INFORMATICA

Facultatea de Ştiinte Exacte

Universitatea AUREL VLAICU din ARAD

II. DATE PRIVIND ÎNDEPLINIREA CONDIŢIILOR DE CONCURS

1.Studii universitare de licenţă şi masterat

Nr. crt.	Instituţia de învăţământ	Domeniul	Perioada	Titlul acordat
1	Universitatea "Claude Bernard" Lyon I, Lyon, Franţa	Matematică	2011	Licenţă
2	Institutul de Ştiinte Financiare si de Actuariat din cadrul Universităţii "Claude Bernard" Lyon I, Lyon, Franta	Matematici finaciare si Ingineria riscului	2013	Master

2. Studii universitare de doctorat

Nr.crt.	Instituţia organizatoare de	Domeniul	Perioada	Titlul acordat
1	Universitatea din Rouen, Franţa	Informatică	2017	Doctor in Ştiinte

3. Studii şi burse postdoctorale

Nr.crt.	Instituţia organizatoare	Domeniul	Perioada	Obs.
1	Universitatea "Aurel Vlaicu" din Arad, România	Matematică	2019	

4.Grade didactice/profesionale

Nr.crt.	Instituţia organizatoare	Domeniul	Perioada	Titlul/Funcţia
1	Universitatea "Aurel Vlaicu" din Arad, România	Informatică	2018	Lector universitar

III. DATE PRIVIND ÎNDEPLINIREA STANDARDELOR MINIMALE SPECIFICE ALE UNIVERSITAŢII

Nr.crt.	Condiţii	Document justificativ
1	Deţine titlul de doctor în domeniul disciplinelor din postul scos la concurs	Diploma doctor, Traducere legalizată diploma doctor, Adeverinţă de echivalare diploma doctor CNRED
2	Deţine diploma de master didactic/certificat de absolvire a modulului psiho-pedagogic sau alte documente echivalente	Adeverinţa de la modul psihopedagogic din cadrul Universităţii Aurel Vlaicu din Arad. Adeverinţa de activitate didactică universitară exersată în cadrul departamentului de Informatică din cadrul Universităţii din Rouen Franţa (Copie si Traducere)
3	Satisface cerinţele specifice domeniului sau facultăţii (cf. Anexa 1 şi tabel de mai jos)	Lista lucrărilor indexate BDI/WOS şi participărilor în proiecte internaţionale (cf. Documentului intitulat Lista lucrări WOS şi proiecte internaţionale)

FUNCŢII DIDAC-TICE	DOMENII					
	ŞTIINŢE EXACTE	INGINERIE	ŞTIINŢE SOCIALE	ŞTIINŢE UMANISTE	TEOLOGIE	ARTE VIZUALE
Lector /Şef Lucrări universi-tar	**-5 articole ştiinţifice publicate în reviste indexate BDI sau B+ -O participa re într-un proiect la nivel naţional sau internaţi onal, câştigat prin competi-ţie**	-3 articole ştiinţifice publicate în *extenso* în publicaţii indexate în BDI sau B+ -Realizarea unui material didactic de specialitate pentru uzul studenţilor sau o carte într-o editură recunoscută. -O participare într-un proiect la nivel naţional sau internaţional , câştigat prin competiţie	-4 articole ştiinţifice publicate în *extenso* în reviste indexate BDI sau B+; - O carte de autor publicată într-o editură recunoscută, ca unic autor; -2 participări la sesiuni ştiinţifice la nivel naţional; -O participare la o sesiune ştiinţifică de nivel internaţional; -membru în echipa unui proiect de cercetare obţinut prin competiţie naţională/ internaţională; -Realizarea unui material didactic de specialitate pentru uzul studenţilor, cel puţin în format electronic. Pentru domeniul educaţie fizică şi sport: performanţă sportivă.	-4 articole ştiinţifice publicate în *extenso* în reviste indexate BDI; -O carte de autor publicată într-o editură recunoscută, ca unic autor; -2 participări la sesiuni ştiinţifice la nivel naţional; -O participare la o sesiune ştiinţifică de nivel internaţional; -membru în echipa unui proiect de cercetare obţinut prin competiţie naţională/ internaţională; -Realizarea a minim **unui** material didactic de specialitate pentru uzul studenţilor, cel puţin în format electronic.	-2 cărţi de autor publicate în edituri de prestigiu -6 studii de specialita-te publicate; -3 comunicări ştiinţifice publicate în volume colective. -membru în echipa unui proiect de cercetare obţinut prin competiţie naţională/ internaţio-nală;	-4 participări la expoziţii de grup la nivel naţional sau 4 proiecte reale de design la cererea unui beneficiar -O carte de autor publicată într-o editură academică recunoscută sau o expoziţie personală la nivel naţional; -2 participări la un simpozion/ concurs la nivel internaţional; -membru în echipa unui proiect de cercetare obţinut prin competiţie naţională/ internaţională;

Se demonstrează cu lista articolelor/participărilor

Data completării 07/01/2019 Candidat DRĂGOI Vlad Florin

Verificat:

	Funcţia didactică, Numele şi prenumele	Semnătura
Preşedinte comisie de concurs:		
Membrii comisiei de concurs:		

Lista articole BDI/WOS şi participări proiecte naţionale/internaţionale (Condiţii Lector universitar UAV)

Drăgoi Vlad Florin

07/01/2019

1 Participări proiecte de cercetare naţionale/internaţionale

- **2018** – Director proiect de mobilitate: PN-III-P1-1.1-MC-2018-2769. Proiect naţional UEFISCDI pentru conferinţa ICCCC 2018.
- **2018-2019** – Membru în proiectul "BioCell-NanoART = Novel Bio-inspired Cellular Nano-architectures, POC-A1-A1.1.4-E-2015 nr. 30/01.09.2016". Proiect internaţional finanţat în parte de UE.
- **2013-2016** – Membru în proiectul NATO " Secure implementation of post-quantum cryptography", SPS Project Number: 984520 : `http://old2.re-search.info/`. Un proiect internaţional între Franţa, Slovacia, SUA şi Israel.

(21)

2 Lista lucrări indexate BDI/WOS

Articole - Conferinţe cu proceedings indexate WOS

Nr. art.	Titlu Articol	Autori	Conferinţa
1	On Algorithms for Evaluating the Reliability of Large Hammock Networks	Nocmi-Clara Rohatinovici, Simon R. Cowell, Leonard Daus, Philippe Poulin, **Vlad Dragoi**, Valentina Emilia Balas, Valeriu Beiu	IEEE International Conference on Computers Communications and Control (ICCCC 2018)
2	Can Series and Parallel Compositions Improve on Hammocks ?	**Vlad Dragoi**, Simon R. Cowell, Sorin Hoară, Păstorel Gaşpar, Valeriu Beiu	IEEE International Conference on Computers Communications and Control (ICCCC 2018)
3	Hammocks versus Hammock	Valeriu Beiu, Simon R. Cowell, **Vlad Dragoi**, Sorin Hoară, Păstorel Gaşpar	IEEE International Conference on Computers Communications and Control (ICCCC 2018)
4	Survey on Cryptanalysis of Code-Based Cryptography : from Theoretical to Physical Attacks	**Vlad Dragoi**, Tania Richmond, Dominic Bucerzan, Axel Legay	IEEE International Conference on Computers Communications and Control (ICCCC 2018)
5	Algebraic Properties of Polar Codes From a New Polynomial Formalism	Magali Bardet, **Vlad Dragoi**, Ayoub Otmani, Jean-Pierre Tillich	IEEE International Symposium on Information Theory (ISIT 2016)
6	Cryptanalysis of the McEliece Public Key Cryptosystem based on Polar Codes	Magali Bardet, Julia Chaulet, **Vlad Dragoi**, Ayoub Otmani, Jean-Pierre Tillich	International Workshop on Post Quantum Cryptography (PQCrypt 2016)

(22)

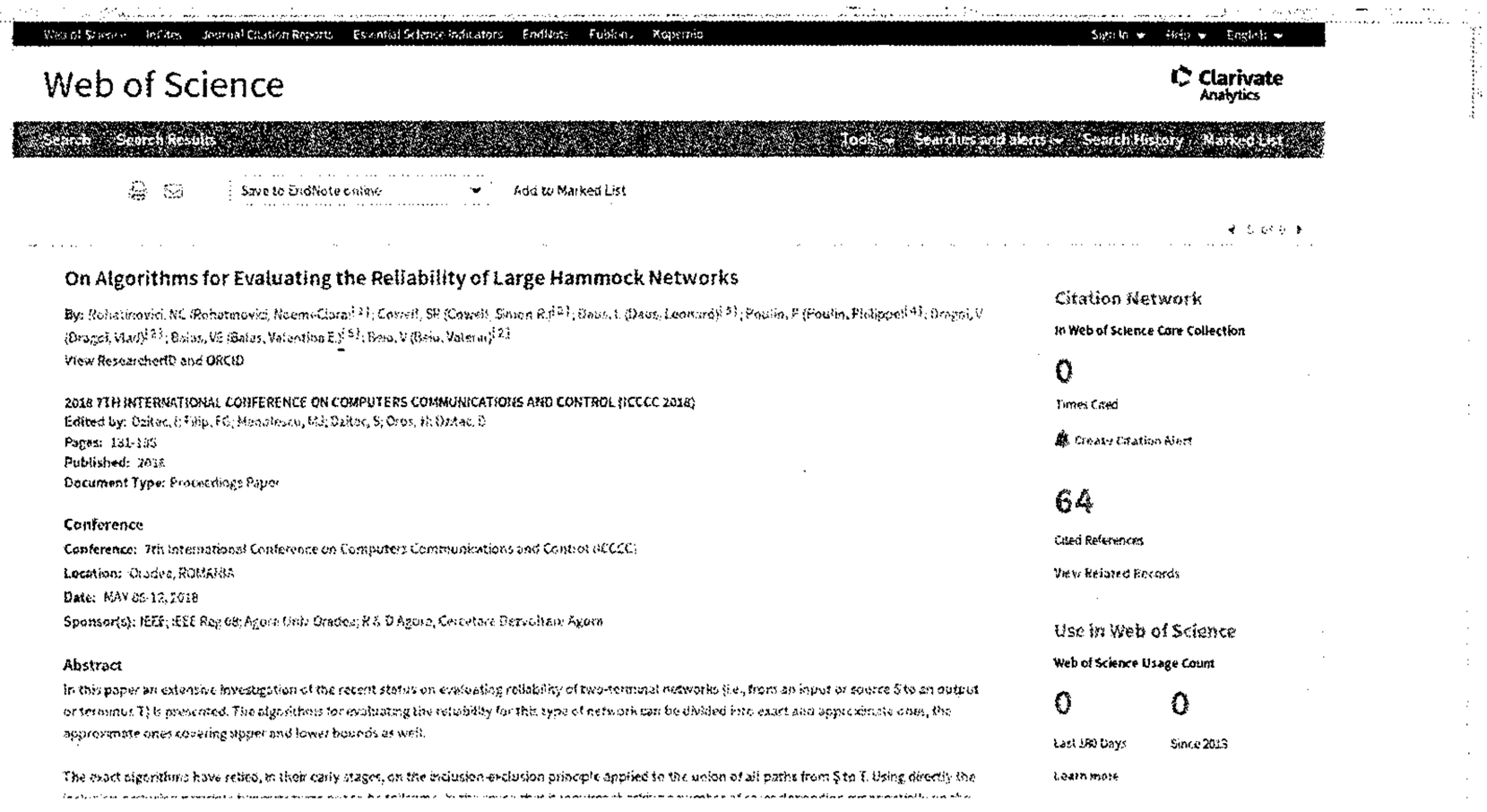
Articole - Jurnale indexate WOS

Nr. art.	Titlu Articol	Autori	Jurnal
7	How Reliable are Compositions of Series and Parallel Networks Compared with Hammocks?	**Vlad Dragoi**, Simon R. Cowell, Valeriu Beiu, S Hoară, P Gaşpar	International Journal of Computers, Communications & Control, vol. 13, no. 5, 2018
8	Cryptanalysis of a Public Key Encryption Scheme Based on QC-LDPC and QC-MDPC	**Vlad Dragoi**, Hervé Talé Kalachi	IEEE Communications Letters Volume: 22, Issue: 2, Feb. 2018
9	Improved Timing Attacks against the Secret Permutation in the McEliece PKC	Dominic Bucerzan, Pierre-Louis Cayrel, **Vlad Dragoi**, Tania Richmond	International Journal of Computers, Communications & Control, vol. 12, no. 1, 2017

23

3 Paginile WOS corespunzatoare articolelor din lista

Articolul nr. 1



Web of Science

Clarivate Analytics

Search | Search Results | Tools | Searches and alerts | Search History | Marked List

Save to EndNote online | Add to Marked List

1 of 5

On Algorithms for Evaluating the Reliability of Large Hammock Networks

By: Rohatinovici, NC (Rohatinovici, Neem-Clara)[1,2]; Cowell, SR (Cowell, Simon R.)[1,2]; Daus, L (Daus, Leonard)[1,3]; Poulin, P (Poulin, Philippe)[1,4]; Dragoi, V (Dragoi, Vlad)[1,3]; Balas, VE (Balas, Valentina E.)[1,5]; Beiu, V (Beiu, Valeriu)[1,2]

View ResearcherID and ORCID

2018 7TH INTERNATIONAL CONFERENCE ON COMPUTERS COMMUNICATIONS AND CONTROL (ICCCC 2018)
Edited by: Dzitac, I; Filip, FG; Manolescu, MJ; Dzitac, S; Oros, H; Dzitac, D
Pages: 131-135
Published: 2018
Document Type: Proceedings Paper

Conference

Conference: 7th International Conference on Computers Communications and Control (ICCCC)
Location: Oradea, ROMANIA
Date: MAY 08-12, 2018
Sponsor(s): IEEE; IEEE Reg 6; Agora Univ Oradea; R & D Agora; Cercetare Dezvoltare Agora

Abstract

In this paper an extensive investigation of the recent status on evaluating reliability of two-terminal networks (i.e., from an input or source S to an output or terminus T) is presented. The algorithms for evaluating the reliability for this type of network can be divided into exact and approximate ones, the approximate ones covering upper and lower bounds as well.

The exact algorithms have relied, in their early stages, on the inclusion-exclusion principle applied to the union of all paths from S to T. Using directly the

Citation Network

In Web of Science Core Collection

0

Times Cited

Create Citation Alert

64

Cited References

View Related Records

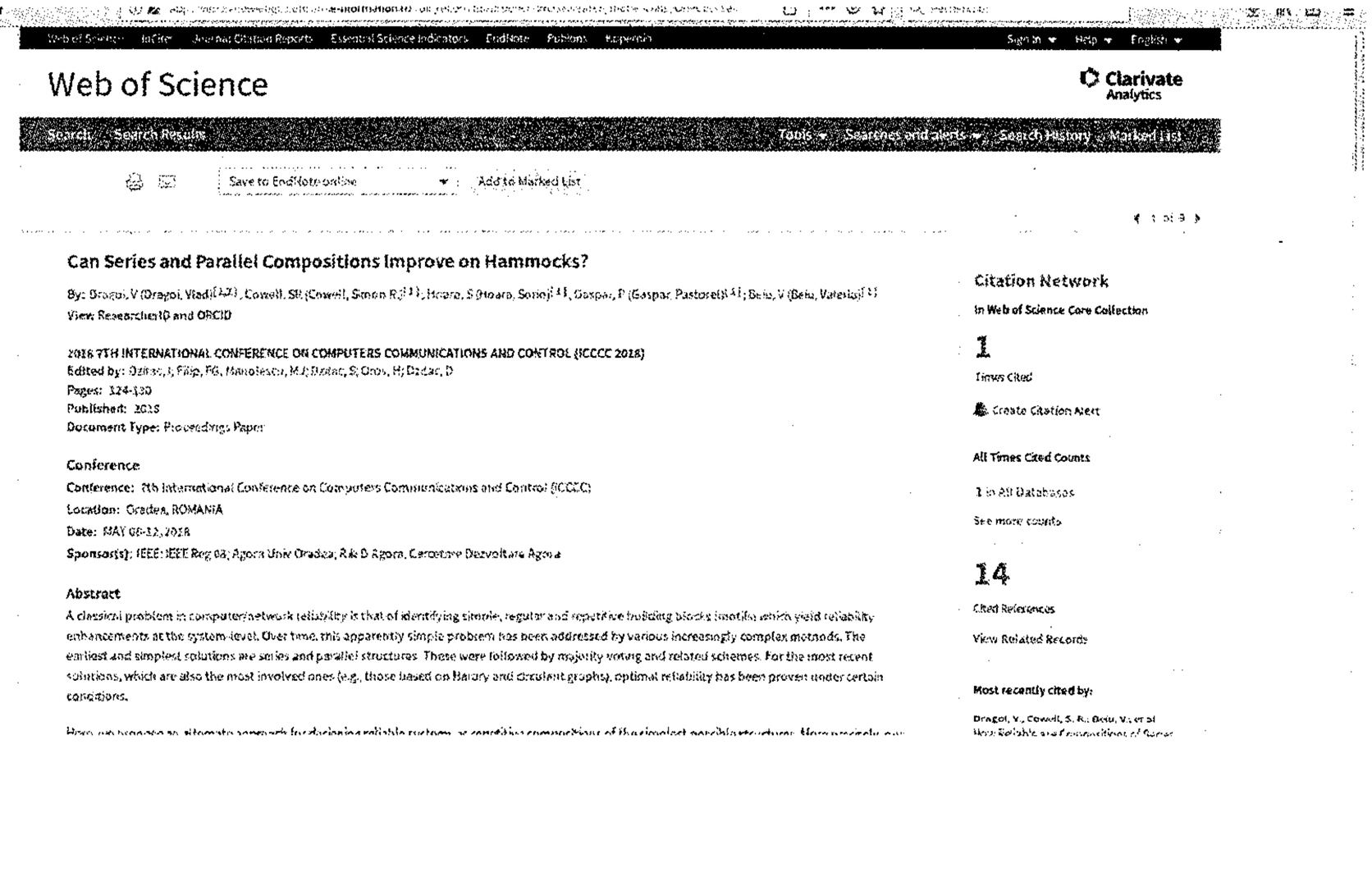
Use in Web of Science

Web of Science Usage Count

0 Last 180 Days | 0 Since 2013

Learn more

Articolul nr. 2



Web of Science

Clarivate Analytics

Search | Search Results | Tools | Searches and alerts | Search History | Marked List

Save to EndNote online | Add to Marked List

1 of 9

Can Series and Parallel Compositions Improve on Hammocks?

By: Dragoi, V (Dragoi, Vlad)[1,2]; Cowell, SR (Cowell, Simon R.)[1]; Hoara, S (Hoara, Sorin)[1]; Gaspar, P (Gaspar, Pastoret)[1]; Beiu, V (Beiu, Valeriu)[1]

View ResearcherID and ORCID

2016 7TH INTERNATIONAL CONFERENCE ON COMPUTERS COMMUNICATIONS AND CONTROL (ICCCC 2018)
Edited by: Dzitac, I; Filip, FG; Manolescu, MJ; Dzitac, S; Oros, H; Dzitac, D
Pages: 124-130
Published: 2018
Document Type: Proceedings Paper

Conference

Conference: 7th International Conference on Computers Communications and Control (ICCCC)
Location: Oradea, ROMANIA
Date: MAY 08-12, 2018
Sponsor(s): IEEE; IEEE Reg 6; Agora Univ Oradea; R & D Agora; Cercetare Dezvoltare Agora

Abstract

A classical problem in computer/network reliability is that of identifying simple, regular and repetitive building blocks (motifs) which yield reliability enhancements at the system-level. Over time, this apparently simple problem has been addressed by various increasingly complex methods. The earliest and simplest solutions are series and parallel structures. These were followed by majority voting and related schemes. For the most recent solutions, which are also the most involved ones (e.g., those based on Barlow and Proschan graphs), optimal reliability has been proven under certain conditions.

Here we propose an alternate approach for designing reliable systems: series/parallel compositions of the simplest parallel structures. More precisely, our

Citation Network

In Web of Science Core Collection

1

Times Cited

Create Citation Alert

All Times Cited Counts

1 in All Databases

See more counts

14

Cited References

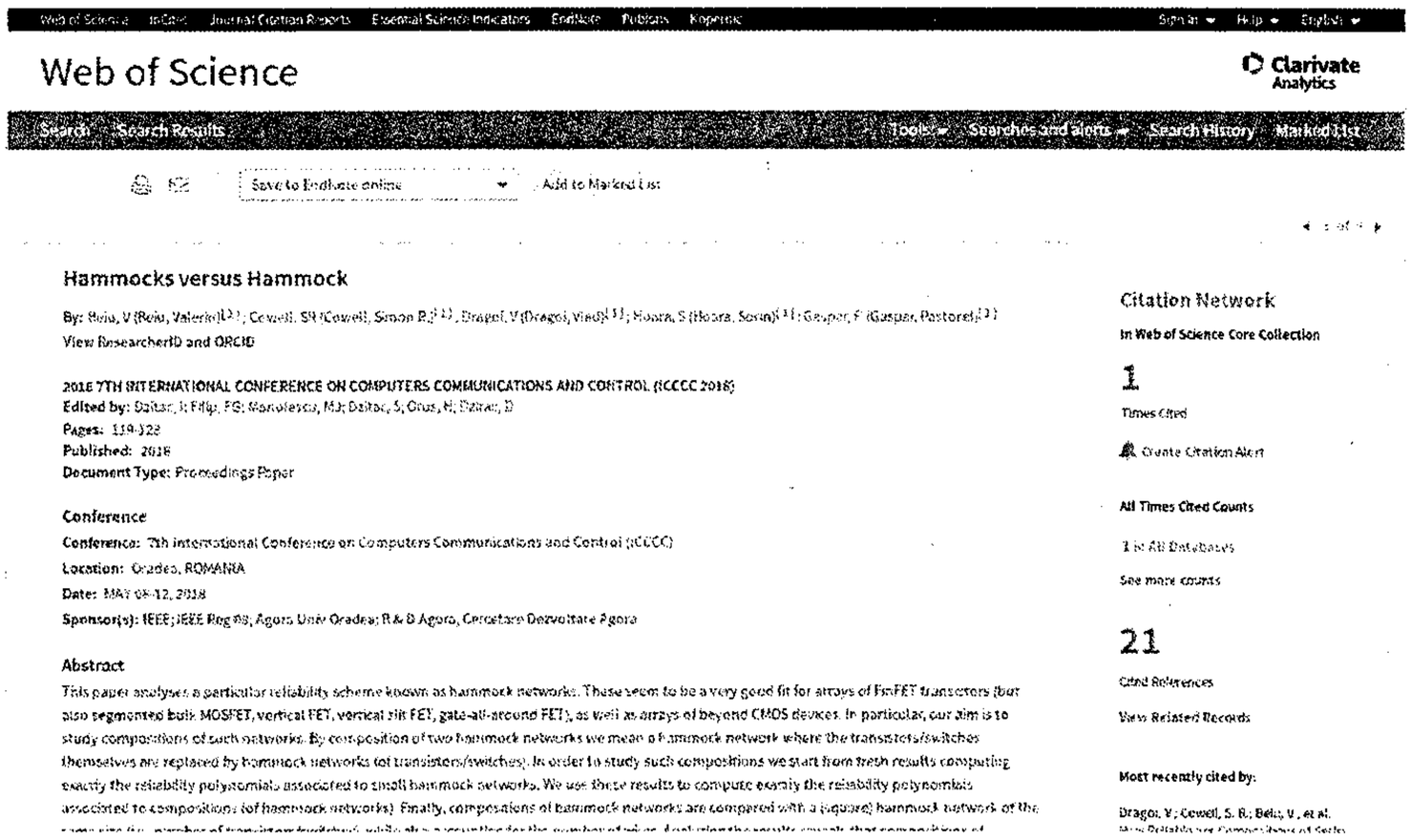
View Related Records

Most recently cited by:

Dragoi, V., Cowell, S. R., Beiu, V., et al.
How Reliable are Compositions of Series

24

Articolul nr. 3



Web of Science

Clarivate Analytics

Search | Search Results | Tools | Searches and alerts | Search History | Marked List

Save to EndNote online | Add to Marked List

Hammocks versus Hammock

By: Reis, V (Reis, Valerio)[2] ; Cowell, SR (Cowell, Simon R.)[1] ; Dragoi, V (Dragoi, Vlad)[1] ; Noora, S (Noora, Sorin)[1] ; Gasper, F (Gasper, Pastorel)[1]
View ResearcherID and ORCID

2018 7TH INTERNATIONAL CONFERENCE ON COMPUTERS COMMUNICATIONS AND CONTROL (ICCCC 2018)
Edited by: Daltac, I; Filip, FG; Manolescu, MJ; Daltac, S; Grus, H; Daltac, D
Pages: 119-122
Published: 2018
Document Type: Proceedings Paper

Conference

Conference: 7th International Conference on Computers Communications and Control (ICCCC)
Location: Oradea, ROMANIA
Date: MAY 08-12, 2018
Sponsor(s): IEEE; IEEE Reg 9; Agora Univ Oradea; R & D Agora, Cercetare Dezvoltare Agora

Abstract

This paper analyses a particular reliability scheme known as hammock networks. These seem to be a very good fit for arrays of FinFET transistors (but also segmented bulk MOSFET, vertical FET, vertical slit FET, gate-all-around FET), as well as arrays of beyond CMOS devices. In particular, our aim is to study compositions of such networks. By composition of two hammock networks we mean a hammock network where the transistors/switches themselves are replaced by hammock networks (of transistors/switches). In order to study such compositions we start from fresh results computing exactly the reliability polynomials associated to small hammock networks. We use these results to compute exactly the reliability polynomials associated to compositions (of hammock networks). Finally, compositions of hammock networks are compared with a (square) hammock network of the

Citation Network

In Web of Science Core Collection

1

Times Cited

Create Citation Alert

All Times Cited Counts

1 in All Databases

See more counts

21

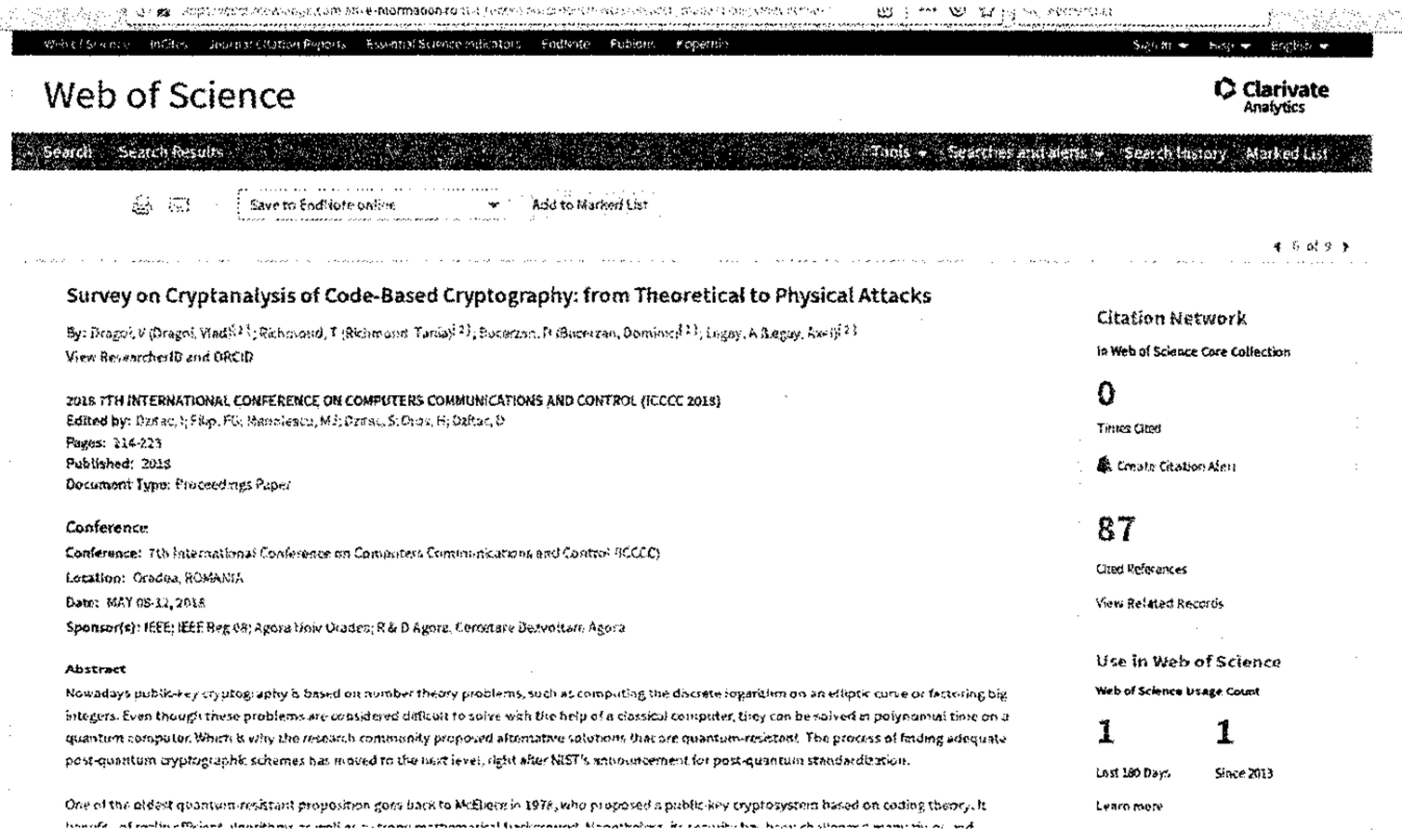
Cited References

View Related Records

Most recently cited by:

Dragoi, V ; Cowell, S. R. ; Beiu, V. , et al.

Articolul nr. 4



Web of Science

Clarivate Analytics

Search | Search Results | Tools | Searches and alerts | Search History | Marked List

Save to EndNote online | Add to Marked List

Survey on Cryptanalysis of Code-Based Cryptography: from Theoretical to Physical Attacks

By: Dragoi, V (Dragoi, Vlad)[2] ; Richmond, T (Richmond, Tania)[2] ; Bucerzan, D (Bucerzan, Dominic)[2] ; Legay, A (Legay, Axel)[2]
View ResearcherID and ORCID

2018 7TH INTERNATIONAL CONFERENCE ON COMPUTERS COMMUNICATIONS AND CONTROL (ICCCC 2018)
Edited by: Daltac, I; Filip, FG; Manolescu, MJ; Daltac, S; Grus, H; Daltac, D
Pages: 214-223
Published: 2018
Document Type: Proceedings Paper

Conference

Conference: 7th International Conference on Computers Communications and Control (ICCCC)
Location: Oradea, ROMANIA
Date: MAY 08-12, 2018
Sponsor(s): IEEE; IEEE Reg 9; Agora Univ Oradea; R & D Agora, Cercetare Dezvoltare Agora

Abstract

Nowadays public-key cryptography is based on number theory problems, such as computing the discrete logarithm on an elliptic curve or factoring big integers. Even though these problems are considered difficult to solve with the help of a classical computer, they can be solved in polynomial time on a quantum computer. Which is why the research community proposed alternative solutions that are quantum-resistant. The process of finding adequate post-quantum cryptographic schemes has moved to the next level, right after NIST's announcement for post-quantum standardization.

One of the oldest quantum-resistant proposition goes back to McEliece in 1978, who proposed a public-key cryptosystem based on coding theory. It

Citation Network

In Web of Science Core Collection

0

Times Cited

Create Citation Alert

87

Cited References

View Related Records

Use in Web of Science

Web of Science Usage Count

1 (Last 180 Days) | 1 (Since 2013)

Learn more

25

Articolul nr. 5

Web of Science

Clarivate Analytics

Search Search Results Tools Searches and alerts Search History Marked List

Save to EndNote online Add to Marked List

Algebraic Properties of Polar Codes From a New Polynomial Formalism

By: Bardet, M (Bardet, Magali)[1,2]; Dragoi, V (Dragoi, Vlad)[1,3]; Otmani, A (Otmani, Ayoub)[1,3]; Tillich, JP (Tillich, Jean-Pierre)[1]
View ResearcherID and ORCID

2016 IEEE INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY
Book Group Author(s): IEEE
Book Series: IEEE International Symposium on Information Theory
Pages: 230-234
Published: 2016
Document Type: Proceedings Paper

Conference

Conference: IEEE International Symposium on Information Theory (ISIT)
Location: Barcelona, SPAIN
Date: JUL 10-15, 2016
Sponsor(s): IEEE; IEEE Informat Theory Soc; Univ Pompeu Fabra Barcelona; NSF; Qualcomm; Huawei; Google; IEEE BigData; Gobierno Espana. Minist Economia Competitividad

Abstract

Polar codes form a very powerful family of codes with a low complexity decoding algorithm that attains many information theoretic limits in error correction and source coding. These codes are closely related to Reed-Muller codes because both can be described with the same algebraic formalism, namely they are generated by evaluations of monomials. However, finding the right set of generating monomials for a polar code which optimizes the decoding performances is a non trivial task and is channel dependent. The purpose of this paper is to reveal some universal properties of these monomials. We will namely prove that there is a way to define a nontrivial partial order on monomials so that the monomials generating a polar code

Citation Network

In Web of Science Core Collection

8

Times Cited

Create Citation Alert

All Times Cited Counts

8 in All Databases

See more counts

9

Cited References

View Related Records

Most recently cited by:

Dragoi, Vlad; Richmond, Tania; Bucerzan, Dominic; et al.

Articolul nr. 6

Web of Science

Clarivate Analytics

Search Search Results Tools Searches and alerts Search History Marked List

Save to EndNote online Add to Marked List

Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes

By: Bardet, M (Bardet, Magali)[1,2]; Chaulet, J (Chaulet, Julia)[2,1]; Dragoi, V (Dragoi, Vlad)[2,1]; Otmani, A (Otmani, Ayoub)[2,1]; Tillich, JP (Tillich, Jean-Pierre)[2,1]
View ResearcherID and ORCID

Find more records by this author

POST-QUANTUM CRYPTOGRAPHY, PQCRYPTO 2016
Edited by: Takagi, T
Book Series: Lecture Notes in Computer Science
Volume: 9606 Pages: 118-143
DOI: 10.1007/978-3-319-29360-8_9
Published: 2016
Document Type: Proceedings Paper
View Journal Impact

Conference

Conference: 7th International Workshop on Post-Quantum Cryptography (PQCrypto)
Location: Fukuoka, JAPAN
Date: FEB 24-26, 2016
Sponsor(s): CREST, Japan Sci & Technol Agcy; Inst Syst, Informat Technologies & Nanotechnologies; ID Quantique; Fukuoka Convent & Vectors Bur; Telecommunicat Advancement Foundation Found Sci

Abstract

Polar codes discovered by Arikan form a very powerful family of codes attaining many information theoretic limits in the fields of error correction and

Citation Network

In Web of Science Core Collection

2

Times Cited

Create Citation Alert

All Times Cited Counts

2 in All Databases

See more counts

39

Cited References

View Related Records

Most recently cited by:

26

Articolul nr. 7

Web of Science

Clarivate Analytics

Search | Search Results | Tools | Searches and alerts | Search History | Marked List

Look Up Full Text | Save to EndNote online | Add to Marked List

< 1 of 9 >

How Reliable are Compositions of Series and Parallel Networks Compared with Hammocks?

By: Dragoi, V (Dragoi, V)[1,2,3]; Cowell, SR (Cowell, S. R.)[4,5]; Beiu, V (Beiu, V.)[1,3]; Hoara, S (Hoara, S.)[1,3]; Gaspar, P (Gaspar, P.)[1,3]

INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Volume: 13 Issue: 5 Pages: 772-791
Published: OCT 2018
Document Type: Article
View Journal Impact

Abstract

A classical problem in computer-network reliability is that of identifying simple, regular and repetitive building blocks (motifs) which yield reliability enhancements at the system-level. Over time, this apparently simple problem has been addressed by various increasingly complex methods. The earliest and simplest solutions are series and parallel structures. These were followed by majority voting and related schemes. For the most recent solutions, which are also the most involved (e.g., those based on Harary and circulant graphs), optimal reliability has been proven under particular conditions.

Here, we propose an alternate approach for designing reliable systems as repetitive compositions of the simplest possible structures. More precisely, our two motifs (basic building blocks) are: two devices in series, and two devices in parallel. Therefore, for a given number of devices (which is a power of two) we build all the possible compositions of series and parallel networks of two devices. For all of the resulting two-terminal networks, we compute exactly the reliability polynomials, and then compare them with those of size-equivalent hammock networks.

The results show that compositions of the two simplest motifs are not able to surpass size-equivalent hammock networks in terms of reliability. Still, the algorithm for computing the reliability polynomials of such compositions is linear (extremely efficient), as opposed to the one for the size-equivalent hammock networks, which is exponential. Interestingly, a few of the compositions come extremely close to size-equivalent hammock networks with

Citation Network

In Web of Science Core Collection

0

Times Cited

Create Citation Alert

25

Cited References

View Related Records

Use in Web of Science

Web of Science Usage Count

0 (Last 180 Days) 0 (Since 2013)

Learn more

Articolul nr. 8

Web of Science

Clarivate Analytics

Search | Search Results | Tools | Searches and alerts | Search History | Marked List

Look Up Full Text | Save to EndNote online | Add to Marked List

< 2 of 9 >

Cryptanalysis of a Public Key Encryption Scheme Based on QC-LDPC and QC-MDPC Codes

By: Dragoi, V (Dragoi, Vlad)[1,2] | Kalachi, HT (Kalachi, Herve Talet)[3]
View ResearcherID and ORCID

IEEE COMMUNICATIONS LETTERS
Volume: 22 Issue: 2 Pages: 264-267
DOI: 10.1109/LCOMM.2017.2779449
Published: FEB 2018
Document Type: Article
View Journal Impact

Abstract

This letter presents a cryptanalysis of five modified McEliece cryptosystem recently proposed by Moufek et al.. The system is based on the juxtaposition of quasi-cyclic LDPC and quasi-cyclic MDPC codes. The idea of our attack is to find an alternative permutation matrix together with an equivalent LDPC code which allow the decoding of any cipher-text with a very high probability. We also apply a recent technique to determine weak keys for this scheme. The results show that the probability of weak keys is high enough that this variant can be ruled out as a possible secure encryption scheme.

Keywords

Author Keywords: Post-quantum cryptography; McEliece cryptosystem; QC-LDPC and QC-MDPC codes
KeyWords Plus: CRYPTOSYSTEMS

Author Information

Reprint Address: Kalachi, HT (reprint author)

Citation Network

In Web of Science Core Collection

1

Times Cited

Create Citation Alert

All Times Cited Counts

1 in All Databases

See more counts

35

Cited References

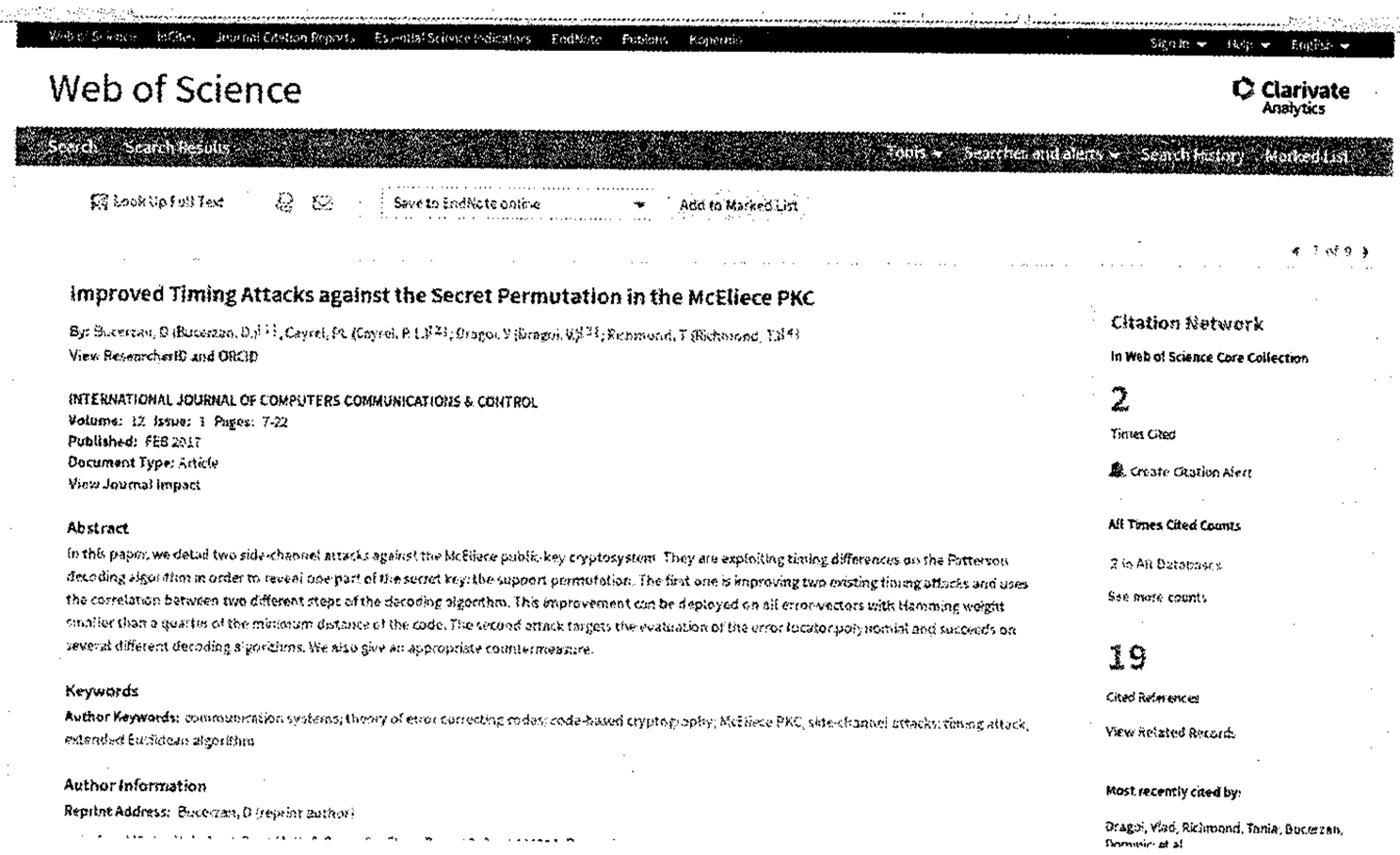
View Related Records

Most recently cited by:

Meng, Jiahui; Zhao, Danfeng; Zhang,

(27)

Articolul nr. 9



Web of Science

Clarivate Analytics

Search | Search Results

Tools | Searches and alerts | Search History | Marked List

Look Up Full Text | Save to EndNote online | Add to Marked List

1 of 2

Improved Timing Attacks against the Secret Permutation in the McEliece PKC

By: Bucerzan, D (Bucerzan, D.)[1]; Cayrel, PL (Cayrel, P. L.)[2]; Dragoi, V (Dragoi, V.)[2]; Richmond, T (Richmond, T.)[3]

View ResearcherID and ORCID

INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Volume: 12 Issue: 1 Pages: 7-22
Published: FEB 2017
Document Type: Article
View Journal Impact

Abstract

In this paper, we detail two side-channel attacks against the McEliece public-key cryptosystem. They are exploiting timing differences on the Patterson decoding algorithm in order to reveal one part of the secret key: the support permutation. The first one is improving two existing timing attacks and uses the correlation between two different steps of the decoding algorithm. This improvement can be deployed on all error vectors with Hamming weight smaller than a quarter of the minimum distance of the code. The second attack targets the evaluation of the error locator polynomial and succeeds on several different decoding algorithms. We also give an appropriate countermeasure.

Keywords

Author Keywords: communication systems; theory of error correcting codes; code-based cryptography; McEliece PKC; side-channel attacks; timing attack; extended Euclidean algorithm

Author Information

Reprint Address: Bucerzan, D (reprint author)

Citation Network

In Web of Science Core Collection

2

Times Cited

Create Citation Alert

All Times Cited Counts

2 in All Databases

See more counts

19

Cited References

View Related Records

Most recently cited by:

Dragoi, Vlad; Richmond, Tania; Bucerzan, Dominic; et al

28