



**Production scientifique  
2012-2015**  
**Laboratoire de mathématiques, cryptographie et mécanique et analyse numérique**

**\* Projets internationaux financés**

<b>ID</b>	<b>Intitulé</b>	<b>Responsable</b>	<b>Année</b>
202	Etude de l'écrasement de films fluides à rhéologie complexe entre deux surfaces poreuses déformables : Application à la biomécanique articulaire	Mohamed ELKHLIFI	2012
203	Informatique théorique au Maghreb	Omar KHADIR	2014
343	informatique théorique au Maghreb	KHADIR Omar	2016

**\*Projets nationaux financés**

ID	Intitulé	Responsable	Année
204	MMSY e-orientation	Omar KHADIR	2013

### \*Publications indexées

ID	Intitulé	Année	Journal	Auteurs
8513	HIGHER ORDER VIABILITY PROBLEM IN BANACH SPACES	2012	Electronic Journal of Differential Equations	Myelkebir AITALIOUBRAHIM, Said SAJID
8516	Radial orthogonality and Lebesgue constants on the disk	2012	Numerical Algorithms	Annie CUYT, Irem YAMAN, Bayram ALI IBRAHIMOGLU, Brahim BENOUAHMANE
8519	Analytical approximation of hetroclinic bifurcation in 1:4 resonance	2012	International Journal of Bifurcation and Chaos	Abdelhak FAHSI, Mohamed BELHAQ
8520	Frequency-locking in nonlinear forced oscillators near 3:1 and 4:1 resonances	2012	Annals of Solid and Structural Mechanics	Mohamed BELHAQ, Abdelhak FAHSI
8522	Combined non-Newtonian and viscous shear effects on a porous squeeze film	2012	Tribology Transactions	Mohamed NABHANI, Mohamed EL KHLIFI, Benyebka BOU-SAÏD
8523	Growth of entire solutions of singular initial-value problem in several complex variables	2012	Electronic Journal of Differential Equations	Devendra KUMAR, Mohammed HARFAOUI
8527	New digital signature protocol based on elliptic curves	2012	International Journal on Cryptography and Information Security	Abid Ounasser, Jaouad Ettanfouhi, Omar Khadir

ID	Intitulé	Année	Journal	Auteurs
8528	Non-newtonian couple stress poroelastic squeeze film	2013	Tribology International	Mohamed NABHANI, Mohamed EL KHLIFI, Benyebka BOU-SAÏD
8530	Best Polynomial Approximation in $L_p$ -Norm and $(p,q)$ -Growth of Entire Functions	2013	Abstract and Applied Analysis	Mohamed El Kadiri, Mohammed Harfaoui
8532	Best $L_p$ -Approximation of analytic functions and generalized $(\alpha, \beta)$ -Growth	2013	Gulf Journal of Mathematics	Mohammed HARFAOUI ,Devendra KUMAR
8535	Factoring cryptosystem moduli when the co-factors difference is bounded	2013	International Journal of Information Technology, Modeling and Computing	Omar AKCHICHE, Omar KHADIR
8539	A new family of multivariate matrix Padé approximants	2014	Jean Journal on Approximation	Jilali ABOUIR, Brahim BENOUAHMANE
8540	Heteroclinic connections in the 1:4 resonance problem using nonlinear transformation method.	2014	Nonlinear Dynamics	Chung K. W., Cao Y. Y, Abdelhak FAHSI, Mohamed BELHAQ
8542	Inertia effects on inclined slider bearings lubricated by a couple stress fluid	2014	Tribology Transactions	Mohamed NABHANI, Mohamed EL KHLIFI
8544	Coupled couple stress and surface roughness effects on elasto-hydrodynamic contact couple	2014	Lubrication Science	Mohamed NABHANI, Mohamed EL KHLIFI, Ory Serge Tanguy GBEHE, Benyebka BOU-SAÏD
8545	Best Approximation in $L_p$ -norm and Generalized $(\alpha, \beta)$ -growth of Analytic Functions	2014	Theory and Applications of Mathematics & Computer Science	Mohammed HARFAOUI ,Devendra KUMAR
8546	Proximate Growth and Best	2014	Theory and Applications of	Mohammed HARFAOUI

ID	Intitulé	Année	Journal	Auteurs
	Approximation in Lp-norm of Entire Functions		Mathematics & Computer Science	
8547	How can the product of two binary recurrences be constant?	2014	Boletim da Sociedade Paranaense de Matemática	Omar KHADIR, Laszlo SZALAY
8548	An integer sequence for solving the modular equation $3x = b$ , when $\frac{b}{p}$ is prime	2014	Journal of Theoretical Physics & Cryptography	Omar KHADIR, Takao KOMATSU
8549	Multivariate homogeous matrix Padé-type approximants and Padé approximants.	2015	International Journal of Pure and Applied Mathematics	Jilali ABOUIR, Brahim BENOUAHMANE
8550	Numerical study of a coastal fog event over Casablanca, Morocco	2015	Quarterly Journal of the Royal Meteorological Society	Driss BARI, Tierry BERGOT, Mohamed EL KHLIFI
8553	Fog prediction at Mohamed V international airport using Neural Network	2015	international journal multi discipline science	Driss BARI, Mohamed EL KHLIFI
8556	LVP conditions at Mohamed V airport, Morocco: Local characteristics and prediction using neural networks	2015	International Journal of Basic and Applied Sciences	Driss BARI, Mohamed EL KHLIFI
8557	Inertial MHD couple stress effects on infinitely wide slider bearings	2015	Tribology Transactions	Mohamed NABHANI, Mohamed EL KHLIFI
8559	Insecure primitive elements in an ElGamal signature protocol	2015	Journal of Discrete Mathematical Sciences & Cryptography	Omar KHADIR
8560	Factoring multi power RSA moguli with a class of secret exponents	2015	Informatica	Omar AKCHICHE, Omar KHADIR

ID	Intitulé	Année	Journal	Auteurs
8561	New variant of Guillou-Quisquater digital signature scheme	2015	International Journal of Advances in Applied Mathematics and Mechanics	Jaouad ETTANFOUHI, Omar KHADIR
14158	Alternative Equations for Guillou-Quisquater Signature Scheme	2016	International Journal of Computer Network and Information Security	J. Ettanfouhi, O. Khadir
14159	A New Signature Protocol Based on RSA and Elgamal Scheme	2016	International Journal of Information Technology, Modeling and	J. Ettanfouhi, O. Khadir
14160	Signature Algorithm based on DLP and Computing Square Roots	2016	International Journal of Information Technology, Modeling and Computing	Ounasser Abid, Omar Khadir
14161	Factoring multi-power RSA moduli with primes sharing least or most significant bits	2016	Groups Complex. Cryptol	Omar Akchiche, Omar Khadir
14163	QSAR study of 1-(3, 3-diphenylpropyl)-piperidinyl amides and ureas using genetic algorithms and artificial neural networks	2016	International Journal of Bioinformatics Research and Applications	Houda Labjar, Mohamed Kissi, Rokaya Mouhibi, Omar Khadir, Hassan Chaair
14164	Static characteristics of ferrofluid finite journal bearing considering rotational viscosity effect: Ferrofluid Finite Journal Bearing Considering Rotational Viscosity	2016	Lubrication science	Salem Laghrabli, Mohamed El Khlifi, Mohamed Nabhani, Benyebka Bou-Saïd
14165	Investigation of couple stress effects on poroelastic squeeze film of parallel plates	2016	Lubrication science	Ory Serge Tanguy Gbehe, Mohamed El Khlifi, Mohamed Nabhani, Benyebka Bou-Saïd
14166	Numerical modeling of poro-elasticity effects on squeeze film of parallel plates using homogenization method	2016	Tribology international	Ory Serge Tanguy Gbehe, Mohamed El Khlifi, Mohamed Nabhani, Benyebka Bou-Saïd

ID	Intitulé	Année	Journal	Auteurs
14978	Local Meteorological and Large-Scale Weather Characteristics of Fog over the Grand Casablanca Region, Morocco	2016	JOURNAL OF APPLIED METEOROLOGY AND CLIMATOLOGY	BARI DRISS, BERGOT THIERRY, EL KHLIFI MOHAMED
17404	Some identities involving polynomial coefficients	2016	Fibonacci Quart	Nour-Eddine Fahssi
17490	On the Heteroclinic Connections in the 1:3 Resonance Problem	2016	International Journal of Bifurcation and Chaos	B. W. Qin, K. W. Chung, FAHSI Abdelhak, M. Belhaq
17491	Non-Newtonian inertial magnetohydrodynamic porous squeeze film lubrication between circular discs	2016	Tribology International	Mohamed Nabhani, Mohamed El Khlifi
20189	Factoring RSA moduli with primes sharing bits in the middle	2017	Applicable Algebra in Engineering, Communication and Computing	AKCHICHE Omar, KHADIR Omar
20999	Near-minimal cubature formulae on the disk	2017	IMA Journal of Numerical Analysis	BENOUAHMANE Brahim, Cuyt Annie, Irem Yaman
21037	Ferrofluid lubrication of finite journal bearings using Jenkins model	2017	Lubrication Science.	Salem LAGHRABLI, Mohamed EL KHLIFI, Mohamed NABHANI, Benyebka BOU-SAÏD
28307	On the Growth Properties of Solutions for a Generalized Bi-Axially Symmetric Schrödinger Equation	2017	Journal of Mathematical Research with Applications	Devendra KUMAR , Payal BISHNOI, Mohammed HARFAOUI
28308	(p,q)- Growth of an Entire GASHE Function and the Coefficient	2018	International Journal of Mathematics and Mathematical Sciences	Harfaoui Mohammed, Mourassil Abdellah, Lakhmaili Loubna

ID	Intitulé	Année	Journal	Auteurs
28309	Multivariate homogeneous two-point Padé approximants	2018	Jaen Journal on Approximation	ABOUIR Jilali, BENOUAHMANE Brahim
28310	Factoring RSA moduli with primes sharing bits in the Middle	2018	Applicable Algebra in Engineering, Communication and Computing	Akchiche Omar, Khadir Omar
28311	Variant of Guillou-Quisquater zero-knowledge scheme	2018	International Journal of Open Problems in Computer Science and Mathematics	S. Ezziri and O. Khadir
28312	A Fast Cryptographic Protocol for Anonymous Voting	2018	MathLAB journal	L. Zahhafi, O. Khadir
28313	On sunlet graphs connected to a specific map on $\{1, 2, \dots, p - 1\}$	2018	Annales Mathematicae et Informaticae	Omar Khadir, László Németh, László Szalay
28314	Factoring RSA moduli when a message is close to a multiple of the primes	2018	INTERNATIONAL JOURNAL OF COMPUTER MATHEMATICS: COMPUTER SYSTEMS THEORY	Omar Akchiche, Omar Khadir
28315	A SECURE VARIANT OF SCHNORR SIGNATURE USING THE RSA ALGORITHM	2018	Journal of Universal Mathematics	L. ZAHHAFI AND O. KHADIR
28316	A BLIND SIGNATURE BASED ON THE DLP AND RSA CRYPTOSYSTEM	2018	Gulf Journal of Mathematics	S. EZZIRI, O. KHADIR
28317	A DIGITAL SIGNATURE SCHEME BASED SIMULTANEOUSLY ON THE DSA AND RSA PROTOCOLS	2018	Gulf Journal of Mathematics	L. ZAHHAFI, O. KHADIR
28318	Adaptation of a Cryptosystem Based on the Arithmetic of Finite Fields to Elliptic Curves	2018	Libertas Mathematica (new series)	Ounasser Abid, Omar Khadir

ID	Intitulé	Année	Journal	Auteurs
28319	Non-Newtonian effects on porous elastic journal bearings	2018	Tribology International	Anas Sakim, Mohamed Nabhani, Mohamed EL Khlifi

### \*Communications internationales

ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
6410	Inertial and non-Newtonian effects on sliders bearings load capacity	Mohamed NABHANI, Mohamed EL KHLIFI, Mohamed RIZK, Salah FADILI	12ème Congrès de Mécanique	Casablanca	Maroc	2015-04-21
6411	Magnetohydrodynamic effects on slider bearings	Mohamed NABHANI, Mohamed EL KHLIFI	12ème Congrès de Mécanique	Casablanca	Maroc	2015-04-21
6413	Combined roughness and non-Newtonian effects on elastic lubricated contacts	Ory Serge Tanguy GBEHE, Mohamed EL KHLIFI, Mohamed NABHANI, Benyebka BOU-SAÏD	12ème Congrès de Mécanique	Casablanca	Maroc	2015-04-21
6416	Roughness and couple stress effects on elastic slider bearing	Mohamed NABHANI, Mohamed EL KHLIFI, Ory Serge Tanguy GBEHE, Benyebka BOU-SAÏD	STLE 69th Annual Meeting & Exhibition	Florida	États-Unis	2014-05-18
6417	Elasticity effect on non-Newtonian porous squeeze films	Mohamed EL KHLIFI, Mohamed NABHANI	1st African Conference in Tribology	Marrakesh	Maroc	2014-04-27



ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
6420	Couple stress effects on rough flexible slider bearing: Multi-scale approach	Ory Serge Tanguy GBEHE, Mohamed EL KHLIFI, Mohamed NABHANI, Benyebka BOU- SAÏD	1st African Conference in Tribology	Marrakesh	Maroc	2014-04-27
6422	Numerical simulation of coupled roughness and couple stress effects on elasto-hydrodynamic contact	Ory Serge Tanguy GBEHE, Mohamed EL KHLIFI, Mohamed NABHANI, Benyebka BOU- SAÏD	10ème Journées d'Analyse Numérique et d'Optimisation	Essaouira	Maroc	2013-10-31
6426	Couple stress and poro-elasticity effects on squeeze film behaviour	Mohamed EL KHLIFI, Mohamed NABHANI, Benyebka Bou Said	World Tribology Congress 2013	Torino	Italy	2013-09-08
6427	Numerical simulation of non-Newtonian porous elastic squeeze film	Mohamed NABHANI, Mohamed EL KHLIFI, Benyebka BOU-SAÏD	11ème Congrès de Mécanique, Agadir	Agadir	Maroc	2013-04-23
6428	Numerical simulation of non-Newtonian effect on porous squeeze film	Mohamed NABHANI, Mohamed EL KHLIFI, Benyebka BOU-SAÏD	3rd International Conference of the Moroccan Society of Mathematics	Marrakesh	Maroc	2012-09-10
6431	Numerical study of a coastal fog over Casablanca, Morocco: effects of turbulence and radiative processes	Driss BARI, Mohamed EL KHLIFI, Tierry BERGOT	12th Workshop of Mechanic	Casablanca	Maroc	2015-04-21
6444	Investigation of Sea Surface Temperature and	Driss BARI, Tierry BERGOT, Mohamed EL	European Geosciences Union General Assembly	Vienna	Austria	2014-05-07

ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
	local topography effects on coastal fog: Case study of 21-22 January 2008 event on the west coast of Morocco	KHLIFI	Conference Abstracts			
6447	The turbulence role in a fog formation at the Mohamed V international airport	Driss BARI, Mohamed EL KHLIFI	Centre International de Mathématiques Pures et Appliquées Workshop	Tanger	Maroc	2014-05-01
6450	Fog prediction at Mohamed V international airport using Neural Network	Driss BARI, Mohamed EL KHLIFI	Journée d'Analyse Numérique et d'Optimisation	Essaouira	Maroc	2013-10-31
6478	Attacks on ElGamal digital signature scheme: an overview	Omar KHADIR	Conference on Discrete Mathematics and Computer Science	Sidi Bel Abbess	Algeria	2015-11-15
6568	Intégration symbolique-numérique et polynômes orthogonaux à plusieurs variables	Brahim BENOUAHMANE	4ème conférence internationale de la SM2A	Oujda	Maroc	2015-02-12
6577	Analytical approximation of heteroclinic bifurcations in 3:1 resonance using a nonlinear transformation method	Chung K. W., Cao Y. Y., Abdelhak FAHSI, Mohamed BELHAQ	2nd International Conference on Structural Nonlinear Dynamics and Diagnosis	Agadir	Maroc	2014-05-19
6727	A new family of	Jilali ABOUIR, Brahim	1er Congrès International	Marakech	Maroc	2014-11-19

ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
	multivariate matrix Padé approximants	BENOUAHMANE	en Modélisation et Calcul Scientifique en Ingénierie Mathématique			
6749	The Many Aspects of Polynomial Triangles	Nour-Eddine FAHSSI	Conference on Discrete Mathematics and Computer Science	Sidi Bel Abbess	Algeria	2015-11-15
7136	New digital signature protocol based on two hard problems	Jaouad ETTANFOUHI, Omar KHADIR	10ème Journées d'Analyse Numérique et Optimisation	Essaouira	Maroc	2013-10-31
10167	Insecure parameters for ElGama digital signature	Omar KHADIR	MIDI	Rouen	France	2015-09-18
10289	Cryptanalysis of RSA variant by factoring the modulus when given extra information	Omar AKCHICHE, Omar KHADIR	Le colloque International de Cybecriminalité CIC 2014	Kenitra	Maroc	2014-06-24
14167	Numerical simulation for hydrodynamic lubrication of finite porous elastic journal bearing using the Darcy Model	A.SAKIM, M. Nabhani, M.EL Khlifi	11ème Journées d'Analyse Numérique et d'Optimisation	Béni-Mellal	Maroc	2016-04-27
14168	2- Numerical simulation of poro-elasticity effects on squeeze film of parallel plates	Ory Serge Tanguy Gbehe, Mohamed El Khlifi, Mohamed Nabhani	11ème Journées d'Analyse Numérique et d'Optimisation	Béni-Mellal	Maroc	2016-04-27
14169	On the computational of multivariate homogenous	J. Abouir, Brahim benouahmane	11ème Journées d'Analyse Numérique et	Béni-Mellal	Maroc	2016-04-27

ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
	matrix Padé approximants		d'Optimisation			
14170	Experimental tests on the primality of large integers	Omar KHADIR, I. Aounil, M. Ihia, S. Moussaid El idrissi	11ème Journées d'Analyse Numérique et d'Optimisation	Béni-Mellal	Maroc	2016-04-27
20105	Numerical simulation of couple stress effect on flexible finite porous journal bearing	SAKIM Anas, NABHANI Mohamed, EL KHLIFI Mohamed	5th International Congress of the SM2A	Meknes	Maroc	2017-03-16
20106	Numerical study of non-Newtonian magnetohydrodynamic lubrication of finite slider bearing	MOUDA Mouhcine, NABHANI Mohamed, EL KHLIFI Mohamed	5th International Congress of the SM2A	Meknes	Maroc	2017-03-16
20107	Finite difference simulation of ferrofluid finite journal bearing lubrication	LAGHRABLI Salem, NABHANI Mohamed, EL KHLIFI Mohamed	5th International Congress of the SM2A	Meknes	Maroc	2017-03-16
20108	Effect of couple stress on flexible finite porous journal bearing	SAKIM Anas, NABHANI Mohamed, EL KHLIFI Mohamed	13ème Congrès de Mécanique	Meknes	Maroc	2017-04-11
20109	Couple stress and poro-elasticity effects on squeeze film	Ory Serge Tanguy Gbehe, NABHANI Mohamed, EL KHLIFI Mohamed	13ème Congrès de Mécanique	Meknes	Maroc	2017-04-11
20110	ROTATIONAL VISCOSITY	LAGHRABLI Salem, EL	The third Euro-	Marrakesh	Maroc	2017-04-16

ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
	EFFECT OF FERROFLUID ON FINITE JOURNAL BEARING: NEW MODEL OF REYNOLDS EQUATION	KHLIFI Mohamed, NABHANI Mohamed, BOU-SAÏD Benyebka	Mediterranean Conference on Bioengineering, Biomaterials and Biomedicine			
20111	COMBINED EFFECTS OF COUPLE STRESS AND POROELASTICITY ON SQUEEZE FILM: MULTI-SCALES APPROACH	Ory Serge Tanguy Gbehe, EL KHLIFI Mohamed, NABHANI Mohamed, BOU-SAÏD Benyebka	The third Euro-Mediterranean Conference on Bioengineering, Biomaterials and Biomedicine	Marrakesh	Maroc	2017-04-16
20112	Numerical simulation of non-Newtonian effect on finite flexible porous journal bearing: using Beavers-Joseph criterion of velocity slip	SAKIM Anas, NABHANI Mohamed, EL KHLIFI Mohamed	International Conference on Applied Mathematics	TAZA	Maroc	2017-10-19
20113	Effect of using magnetic field on performance of finite ferrofluid journal bearing	LAGHRABLI Salem, NABHANI Mohamed, EL KHLIFI Mohamed	Congrès International de Modélisation et Optimisation des systèmes Mécaniques	Fès	Maroc	2017-12-05
20171	The discrete logarithm problem modulo odd integers	KHADIR Omar	The International Conference on Algebra and its Applications	Errachidia	Maroc	2017-04-26
20173	Modular polynomial equations in elliptic curves	AOUNIL Ismail, IHIA Marouane, KHADIR Omar, MOUSSAID EL IDRISSEI Souhaib	5th International Congress of the SM2A	Meknes	Maroc	2017-03-16

ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
20175	An identification protocol based on Guillou-Quisquater scheme	EZZIRI Salma , KHADIR Omar	The International Conference on Applied Mathematics	TAZA	Maroc	2017-10-17
20176	Application of Paillier cryptosystem to construct a voting scheme	KHADIR Omar, ZAHHAFI Leila	The International Conference on Applied Mathematics	TAZA	Maroc	2017-10-17
20177	A generalization of the Diffie-Hellman protocol in elliptic curves	IHIA Marouane, KHADIR Omar	The International Conference on Applied Mathematics	TAZA	Maroc	2017-10-17
20179	Resolution of modular polynomial equations using lattice theory	IHIA Marouane, KHADIR Omar, MOUSSAID EL IDRISSE Sohaib	The International Conference on Applied Mathematics	TAZA	Maroc	2017-10-17
20180	Constructing a Cryptosystem Based on Diffie-Hellman and Elliptic Curves	ABID Ounasser, KHADIR Omar	The International Conference on Applied Mathematics	TAZA	Maroc	2017-10-17
20183	A practical zero-knowledge protocol based on Guillou-Quisquater scheme	EZZIRI Salma, ZAHHAFI Leila, KHADIR Omar	International Conference of Cryptology, Computer Security and Applications	Agadir	Maroc	2017-11-23
20185	An improved digital signature over elliptic curves	IHIA Marouane, KHADIR Omar	International Conference of Cryptology, Computer Security and Applications	Agadir	Maroc	2017-11-23
21203	Recursive computation of multivariate two-point	ABOUIR Jilali, BENOUAHMANE Brahim,	International Conference on Applied Mathematics	TAZA	Morocco	2017-10-19

ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
	Padé approximants	CHAKIR yassine				
21204	The Epsilon Algorithm For Two-Point Padé Approximants	CHAKIR yassine, ABOUIR Jilali, BENOUAHMANE Brahim	The second International Conference on Modeling and Scientific Computing in Mathematical engineering	Marrakesh	Morocco	2017-04-17
21205	Multivariate Two-point Padé approximants and the QD-Algorithm	ABOUIR Jilali, BENOUAHMANE Brahim, ELIDRISSI Abdennasser	International Conference on Applied Mathematics	TAZA	Morocco	2017-10-17
21206	An Algorithm For Computation Of Multivariate Two-Point Padé Approximants	ELIDRISSI Abdennasser, ABOUIR Jilali, BENOUAHMANE Brahim	The second International Conference on Modeling and Scientific Computing in Mathematical engineering	Marrakesh	Morocco	2017-04-17
28321	GAUSS-SEIDEL OVER-RELAXATION METHOD FOR SOLVING 2D REYNOLDS EQUATION IN MHD LUBRICATION PROBLEM	MOUDA Mouhcine, NABHANI Mohamed, EL KHLIFI Mohamed	International Conference on Fixed Point Theory and Applications (ICFPTA'18)	Mohammedia	Maroc	2018-05-08
28322	A numerical simulation of finite porous elastic journal bearings using Brinkman model	SAKIM Anas, NABHANI Mohamed, EL KHLIFI Mohamed	International Conference on Fixed Point Theory and Applications (ICFPTA'18)	Mohammedia	Maroc	2018-05-08
28323	A new method for speeding up the Coppersmith's algorithm	Sohaib Moussaid El Idrissi, Omar Khadir	International Conference on Fixed Point Theory and Applications	Mohammedia	Maroc	2018-05-08

ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
			(ICFPTA'18)			
28324	Reinforcement of ElGamal digital signature schemesInternational	M. IHIA, O. KHADIR	International Conference on Fixed Point Theory and Applications (ICFPTA'18)	Mohammedia	Maroc	2018-05-08
28325	NUMERICAL SIMULATION OF MHD SLIDER BEARINGS USING SUCCESSIVE OVER-RELAXATION METHOD	M. MOUDA, M. NABHANI, M. EL KHLIFI	Journes d'Analyse Numrique et Optimisation	Al-Hoceima	Maroc	2018-10-18
28326	NUMERICAL STUDY OF NON-NEWTONIAN MAGNETO-HYDRODYNAMIC LUBRICATION PROBLEM	M. MOUDA, M. NABHANI, M. EL KHLIFI	2nd International Conference On Applied Mathematics	Fés	Maroc	2018-10-26
28327	SUCCESSIVE OVER-RELAXATION METHOD AND FIXED-POINT TECHNIQUE IN FINITE FLEXIBLE POROUS JOURNAL BEARINGS	A. SAKIM, M. NABHANI, M. EL KHLIFI	Journes d'Analyse Numrique et Optimisation	Al-Hoceima	Maroc	2018-10-18
28328	ON THE CONVERGENCE OF TWO-POINT QD-ALGORITHM	Abdennasser ELIDRISSI, Jilali ABOUI, Brahim Benouahmane	Journes d'Analyse Numrique et Optimisation	Al-Hoceima	Maroc	2018-10-18
28329	TWO-POINT PADE APPROXIMANTS AND CONTINUED FRACTIONS	YASSINE CHAKIR, Jilali ABOUI, Brahim Benouahmane	Journes d'Analyse Numrique et Optimisation	Al-Hoceima	Maroc	2018-10-18



ID	Intitulé	Auteurs	Conférence	Ville	Pays	Date
28330	A method of identification based on Schnorr protocol and its application on elliptic curves	S. Ezziri, O. Khadir	International Conference on Technology, Engineering & Mathematics	Kénitra	Maroc	2018-03-26
28331	A secure variant of Schnorr signature using the RSA algorithm	Leila Zahhafi, Omar Khadir	International Conference on Intuitionistic Fuzzy Sets & Mathematics Sciences	Ifrane	Maroc	2018-04-11
28332	A blind signature based on DLP and RSA scheme	S. Ezziri, O. Khadir	2nd International Conference On Applied Mathematics	Fès	Maroc	2018-04-26
28333	A digital signature based on DSA and RSA protocols	L. Zahhafi and O. Khadir	2nd International Conference On Applied Mathematics	Fès	Maroc	2018-10-26

### \*Communications nationales

ID	Intitulé	Auteurs	Conférence	Ville	Date
6452	Etude du brouillard en zone côtière par modélisation des processus physiques de la couche limite atmosphérique: Cas du Grand Casablanca (Maroc)	Driss BARI, Mohamed EL KHLIFI	1st Journée Doctorale STI&DD FSTM	Mohammedia	2015-06-16

ID	Intitulé	Auteurs	Conférence	Ville	Date
6453	Numerical resolution of homogenized modified Reynolds equation for lubricated rough elastic contacts	Ory Serge Tanguy GBEHE, Mohamed EL KHLIFI	1st Journée Doctorale STI&DD FSTM	Mohammedia	2015-06-16
6454	Hydrodynamic lubrication of finite flexible porous journal bearing using Darcy model	Anas SAKIM, Mohamed EL KHLIFI	1st Journée Doctorale STI&DD FSTM	Mohammedia	2015-06-16
6456	Contribution à l'étude numériques des effets thermiques et inertiels sur la lubrification des coins d'huiles pour fluides non newtoniens	Mouhcine MOUDA, Mohamed EL KHLIFI	1st Journée Doctorale STI&DD FSTM	Mohammedia	2015-06-16
6509	A variant of Guillou-Quisquater signature protocol	Jaouad ETTANFOUHI, Omar KHADIR	5ème Edition des journées nationales de la sécurité	Kenitra	2015-05-07
6513	A new signature equation inspired by Guillou-Quisquater model	Jaouad ETTANFOUHI, Omar KHADIR	Le jeune chercheur : source de capital immatériel et acteur de développement	Mohammedia	2015-06-16
6515	Factoring RSA-type moduli when given some bits of the divisor	Omar AKCHICHE, Omar KHADIR	Journée Doctorale de la FSTM	Mohammedia	2015-06-16
6516	Cryptanalysis of RSA variants by factoring the modulus when given extra information	Omar AKCHICHE, Omar KHADIR	In proceedings of Colloque Internationale de Cybercriminalité CIC 2014	Kenitra	2014-06-24
6518	New attack against multi-prime RSA cryptosystems by	Omar AKCHICHE, Omar KHADIR	Journées Doctorales des Technologies d'Information et	Rabat	2014-06-19

ID	Intitulé	Auteurs	Conférence	Ville	Date
	factoring the moduli		de Communications JDTIC'14		
6519	Factoring RSA variant moduli when given additional hints	Omar AKCHICHE, Omar KHADIR	In Journée des Mathématique et Applications JMA 2014	Casablanca	2014-06-07
7125	La signature digitale de GUILOU-QUISQUATER	Jaouad ETTANFOUHI, Omar KHADIR	13ème journée de Mathématiques et Application	Casablanca	2015-06-06
7132	Extended Fermat method for factoring large RSA and Rabin moduli	Omar AKCHICHE, Omar Khadir	Journées doctorales en systeme d'information,reseaux et telecommunications	Rabat	2013-06-27
14171	Numerical solution of a new model of Reynolds equation describing the thin-film flow of a ferrofluid in finite journal bearing	S. LAGHRABLI, M. EL KHLIFI, M. NABHANI	Une Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2016-12-22
14172	6- Mathematical modeling of non-newtonian hydrodynamic lubrication of finite slider bearings	M. MOUDA, M. NABHANI, M. EL KHLIFI	Une Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2016-12-22
14173	7- Numerical modelling of elastohydrodynamic lubrication of finite porous journal bearing using darcy model	A.SAKIM, M. Nabhani, M.EL Khlifi	Une Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2016-12-22
14174	Multi-scale homogenization based modeling of poro-elasticity effects on squeeze film	O. S. T. GBEHE, M. NABHANI, M. EL KHLIFI	Une Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2016-11-22

ID	Intitulé	Auteurs	Conférence	Ville	Date
14176	Numerical analysis of hydrodynamic finite journal bearing lubricated with ferrofluid	S. LAGHRABLI, M. NABHANI, M. EL KHLIFI	Mathématiques et Applications	Casablanca	2016-12-27
14177	Modular equations with elliptic curves for cryptography	I. AOUNIL, M. IHIA, S. MOUSSAID EL IDRIS-SI, O. KHADIR	Mathématiques et Applications	Casablanca	2016-12-27
20094	Mathematical modeling of non-newtonian effects on porous elastic journal bearings	SAKIM Anas, NABHANI Mohamed, EL KHLIFI Mohamed	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20095	Numerical simulation of finite porous journal bearing using darcy-brinkman model	SAKIM Anas, NABHANI Mohamed, RIZK Mohamed, EL KHLIFI Mohamed	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20096	Mathematical modeling of non-Newtonian magneto-elastohydrodynamics lubrication of slider bearings	MOUDA Mouhcine, NABHANI Mohamed, EL KHLIFI Mohamed	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20097	Numerical study of non-Newtonian magnetohydrodynamic lubrication of inclined slider bearings	MOUDA Mouhcine, NABHANI Mohamed, RIZK Mohamed, EL KHLIFI Mohamed	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20098	Physical modelling of ferrofluid lubrication of finite journal bearings based on Jenkins	LAGHRABLI Salem, NABHANI Mohamed, EL KHLIFI Mohamed	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et	Mohammedia	2017-12-21

ID	Intitulé	Auteurs	Conférence	Ville	Date
	model		Mathématiques Appliquées		
20099	Numerical study of lubricant film behaviour subject to periodic loading between a porous surface and a rigid surface	SOBHI Said , ZARBANE Khalid, EL KHLIFI Mohamed	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20101	Surface texturing effects on the behavior of a lubricating film subject to periodic loading	LAAMIRI Mohamed, ZARBANE Khalid, EL KHLIFI Mohamed	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20115	La Modélisation Mathématiques des Plaques Minces Soumises à une flexion simple et méthodes d'Approximation des solutions de son équation différentielle aux dérivées partielles de quatrième ordre	FTOUHI Reda , HARFAOUI Mohammed	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20162	Variant of Schnorr zero-knowledge protocol	EZZIRI Salma, KHADIR Omar	Deuxièmes journées d'Algèbre Théorie des Nombres et leurs applications	Oujda	2017-11-22
20164	A practical zero-knowledge protocol inspired by schnorr scheme	EZZIRI Salma, KHADIR Omar	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20165	A protocol of a digital signature based on finite	IHIA Marouane, KHADIR Omar	2 ème Journée Scientifique sur les Méthodes de Modélisation	Mohammedia	2017-12-21

ID	Intitulé	Auteurs	Conférence	Ville	Date
	elliptic curves		en Sciences Physiques et Mathématiques Appliquées		
20166	A different approach for the comprehension of the Coppersmith's theorem	MOUSSAID EL IDRISSEI Sohaib, KHADIR Omar	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20168	A fast system of binary electronic voting based on cryptographical concept	ZAHHAFI Leila , KHADIR Omar	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
20169	VARIANT OF ELGAMAL CRYPTOSYSTEM OVER ELLIPTIC CURVES	ABID Ounasser, KHADIR Omar	15 ème Journée de Mathématiques et Applications (JMA17)	CASABLANCA	2017-07-11
20170	SIMPLIFICATION OF COPPERSMITH'S METHOD	IHIA Marouane, KHADIR Omar, MOUSSAID EL IDRISSEI Sohaib	15 ème Journée de Mathématiques et Applications (JMA17)	CASABLANCA	2017-07-11
21201	Epsilon algorithm and two-point Padé approximants	ABOUIR Jilali, BENOUAHMANE Brahim, CHAKIR yassine	2 ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
21202	The qd-algorithm for the computation of poles of meromorphic functions	ABOUIR Jilali, BENOUAHMANE Brahim, ELIDRISSI Abdennasser	2ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2017-12-21
21211	Multivariate homogeneous two-point Padé approximants	ABOUIR Jilali	Journée de Travail a l'ecole Normale Supérieure de Rabat	Rabat	2017-12-28

ID	Intitulé	Auteurs	Conférence	Ville	Date
23378	Sur certains aspects combinatoires et probabilistes des statistiques d'exclusion	FAHSSI Nouredine	Journées Nationales des doctorants et des jeunes chercheurs	Rabat	2017-07-18
28335	MATHEMATICAL MODELING OF POROUS ELASTIC JOURNAL BEARINGS OPERATING WITH COUPLE STRESS FLUIDS	SAKIM Anas, NABHANI Mohamed, M. RIZK, EL KHLIFI Mohamed	3ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2018-12-27
28336	NUMERICAL MODELING OF NON-NEWTONIAN MAGNETOHYDRODYNAMICS LUBRICATION OF SLIDER-BEARINGS	MOUDA Mouhcine, NABHANI Mohamed, EL KHLIFI Mohamed	3ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2018-12-27
28337	FINITE DIFFERENCE MODELING OF FINITE POROUS ELASTIC JOURNAL BEARING	SAKIM Anas, NABHANI Mohamed, EL KHLIFI Mohamed	3ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2018-12-27
28338	NUMERICAL STUDY OF LUBRICANT FILM BEHAVIOUR SUBJECT TO PERIODIC LOADING BETWEEN A POROUS SURFACE AND A RIGID SURFACE	SOBHI Said, NABHANI Mohamed, EL KHLIFI Mohamed	3ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2018-12-27
28339	A new alternative of Schnorr blind signature using RSA algorithm	Salma EZZIRI, Omar KHADIR	16ème Journée de Mathématiques et Applications (JMA2018)	Casablanca	2018-07-04
28340	Comparative study on Coppersmith's theorem	Sohaib MOUSSAID EL IDRISSE, Omar KHADIR	16ème Journée de Mathématiques et Applications	Casablanca	2018-07-04

ID	Intitulé	Auteurs	Conférence	Ville	Date
			(JMA2018)		
28341	Improvement of a proxy signature using RSA Algorithm	Salma Ezziri, Omar KHADIR	Troisième Congrès : Algèbre, Théorie des Nombres et leurs Applications	Oujda	2018-11-23
28342	Amelioration of the DSA signature protocol	Leila Zahhafi, Omar KHADIR	Troisième Congrès : Algèbre, Théorie des Nombres et leurs Applications	Oujda	2018-11-23
28343	Exploiting LLL-algorithm to solve cryptographic problems	Sohaib Moussaid El Idrissi, Omar KHADIR	Troisième Congrès : Algèbre, Théorie des Nombres et leurs Applications	Oujda	2018-11-23
28344	POD REDUCED-ORDER MODEL OF THE CYLINDER WAKE FLOW	EL OMARI Achraf, CORDIER Laurent, EL KHLIFI Mohamed	3ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2018-12-27
28345	Flow control over a RAMP	SERRARE Abderrahim, KOURTA azeddine, EL KHLIFI Mohamed	3ème Journée Scientifique sur les Méthodes de Modélisation en Sciences Physiques et Mathématiques Appliquées	Mohammedia	2018-12-27

### \*Thèses en cours



ID	Nom Prénom	Sujet	Directeur de thèse	Année de première inscription
945	Loubna LAKHMAILI	(p,q)-croissance et croissance générale des fonctions méromorphes et meilleure approximation polynômiale	HARFAOUI Mohammed	2015
946	Mouhcine MOUDA	Contribution à l'étude numérique des effets magnétohydrodynamiques sur la lubrification des contacts lubrifiés par fluides non newtoniens	EL KHLIFI MOHAMED	2014
947	Ory Serge Tanguy GBEHE	Etude de l'écrasement de films fluides à rhéologie complexe en présence d'un milieu poreux déformable par la méthode d'homogénéisation	EL KHLIFI MOHAMED	2011
3988	FTOUHI Reda	Approximation des solutions des équations différentielles aux dérivées partielles de quatrième ordre et applications numériques dans la théorie des plaques	HARFAOUI Mohammed	2017
948	Anas SAKIM	Modélisation des caractéristiques statiques et dynamiques des paliers poreux fonctionnant à très haute températures	EL KHLIFI MOHAMED	2013
3989	Achraf EL OMARI	Réduction de modèle paramétrique par Proper Generalized Decomposition	EL KHLIFI MOHAMED	2017
949	Marouane IHIA	Les algorithmes pour protection de données numériques et pour les signatures digitales	KHADIR Omar	2015
3990	HINDI Boullah Mohamed Said	Etude de l'écrasement des paliers poreux lubrifiés par fluides ferromagnétiques	EL KHLIFI MOHAMED	2017

ID	Nom Prénom	Sujet	Directeur de thèse	Année de première inscription
950	Tarik DRAFAT	Etude expérimentale et analytique des paliers hydrodynamiques à bague flottante	EL KHLIFI MOHAMED	2015
3991	LAKHAL Ismail	Comportement en impact d'une couche poreuse imbibée de lubrifiant	EL KHLIFI MOHAMED	2017
993	Abdellah MOURASSIL	(p,q)-croissance et croissance générale des solutions pour l'équation bi-axiale symétrique aux dérivées partielles de l'équation de Schrodinger	HARFAOUI Mohammed	2015
3992	SERRARE Abderrahime	Caractérisation du décollement turbulent et son contrôle	EL KHLIFI MOHAMED	2017
1004	Sohaib MOUSSAID EL IDRISSE	Réseaux euclidiens et cryptographie à clés publiques	KHADIR Omar	2015
4002	FATIMA EZZAHRAE HADADI	Croissance générale par rapport à une fonction entière et harmonique et meilleure approximation polynomiale en norme $L_p$ sur un compact régulier	HARFAOUI Mohammed	2017
1275	Salem LAGHRABLI	Modélisation et analyse comparative des performances d'un palier hydrodynamique lubrifié à l'aide de fluide ferromagnétique et d'un fluide à couple de contrainte	EL KHLIFI MOHAMED	2012
4039	Abdellah ZAHIR	zéros et croissance itérée et croissance générale de solutions de certaines équations différentielles et équations aux dérivées partielles d'ordre Supérieur et simulations numériques	HARFAOUI Mohammed	2017
1276	Ounasser ABID	Études des méthodes de chiffrement et de cryptanalyse en cryptographie à clé publique	KHADIR Omar	2011

ID	Nom Prénom	Sujet	Directeur de thèse	Année de première inscription
5417	ELMADDAH Youness	Perturbations convexes et non convexe de problème de la rafle	SAJID Saïd	2018
1277	Omar AKCHICHE	Primalité, factorisation des grands nombres et application à la cryptographie à clés publiques	KHADIR Omar	2012
1307	Jaouad ETTANFOUHI	Contribution aux algorithmes de cryptographie à clé publique	KHADIR Omar	2011
5419	AKERKOUCH Lahcen	Modélisation et analyse des performances d'un palier hydrodynamique lubrifié à l'aide d'un fluide magnétohydrodynamique.	EL KHLIFI MOHAMED	2018
5834	CHARRADI Nabil	Sur des inclusion différentielle avec contraintes	SAJID Saïd	2018
3083	Said SOBHI	Etude expérimentale de l'effet de la porosité de la surface de contact sur le comportement d'un film lubrifiant soumis à un écrasement périodique	EL KHLIFI MOHAMED	2016
5835	CHAHBI Chakib	Etude d'équations comportant des non linéarités asymétriques et application de la méthode de pgd pour approcher la solution	SAJID Saïd	2018
3084	Mohammed LAAMIRI	Etude expérimentale de l'effet de la texturation de surface de contact sur les performances tribologiques d'un film lubrifiant soumis à un chargement périodique	EL KHLIFI MOHAMED	2016
3163	Khalil ATLASSI	Etude des performances dynamiques d'un palier lubrifié par fluide ferromagnétique	EL KHLIFI MOHAMED	2016
3164	Leila ZAHHAFI	Méthodes d'identification, d'authentification, d'intégrité et de signature numérique en cryptographie a clé	KHADIR Omar	2016

ID	Nom Prénom	Sujet	Directeur de thèse	Année de première inscription
		publique		
3165	Salma EZZIRI	Méthode de cryptographe à clé publique, conception et cryptanalyse de signatures numériques	KHADIR Omar	2016
3166	Yassine CHAKIR	Le calcul récursif des approximants de Padé en deux points et les fractions continues à plusieurs variables	ABOUIR Jilali	2016
3167	Abdennasser ELIDRISSI	Approximants de Padé en deux points, polynômes orthogonaux et formules de cubature	BENOUAHMANE Brahim	2016

### \*Thèses soutenues

ID	Nom Prénom	Sujet	Directeur de thèse	Année de première inscription	Date de soutenance
3912	Jaouad ETTANFOUHI	Contribution aux Algorithmes de Cryptographie à Clés Publiques	KHADIR Omar	2011	2017-12-30
883	Driss BARI	Étude du brouillard en zone côtière par modélisation des processus physiques de la couche limite atmosphérique : cas du Grand Casablanca (Maroc)	EL KHLIFI MOHAMED	2011	2015-10-15
3913	Ounasser ABID	Etude des méthodes de chiffrement et de cryptanalyse en cryptographie à clé publique	KHADIR Omar	2011	2017-12-29

<b>ID</b>	<b>Nom Prénom</b>	<b>Sujet</b>	<b>Directeur de thèse</b>	<b>Année de première inscription</b>	<b>Date de soutenance</b>
3958	Omar AKCHICHE	Primalité, factorisation des grands nombres et application à la cryptographie à clé publique	KHADIR Omar	2012	2017-05-25
3959	Salem LAGHRABLI	Etude et modélisation de la lubrification des paliers hydrodynamiques de dimensions finies par ferrofluides en régime statique	EL KHLIFI MOHAMED	2012	2017-07-01
3082	Ory Serge Tanguy Gbehe	ETUDE PAR LA MÉTHODE D'HOMOGENÉISATION DES CONTACTS RUGUEUX ÉLASTIQUES ET PORO-ÉLASTIQUES LUBRIFIÉS PAR UN FLUIDE NON NEWTONIEN	EL KHLIFI MOHAMED	2011	2016-12-03