



UNIVERSITI PUTRA MALAYSIA

CURRICULUM VITAE

A. Biodata

- a. Name: Kamel Ariffin B. Mohd. Atan
- b. Department: Mathematics
- c. Faculty: Science
- d. Field of Specialisation: Number Theory, Cryptography, History and Philosophy of Mathematics
- h. Contact:
 - Office : 03-89466872
 - Fax: 03-89466973
 - E-mail: kamel@upm.edu.my

B. Education and academic qualification

Degree	Class/Achievement	University Awarded	Year
PhD (or equivalent)		University of New South Wales, Australia	1984
Master		University of Western Ontario, Canada	1977
First Degree		University of Malaya	1972

C. Administrative duties and other relevant appointment

No.	Position	Department/Faculty/Other Institution	Year	Duration
1.	Director	Institute for Mathematical	2002-2014	12 years

		Research UPM		
2.	Deputy Vice Chancellor (Academic)	Universiti Putra Malaysia	1997-2000	3 years
3.	Director	Centre for Matriculation Studies UPM	1993-1997	4 years
4.	Acting Dean	Faculty of Science and Environmental Studies UPM	19 th Oct-7 th Dec 1992	2 months
5.	Deputy Dean	Faculty of Science and Environmental Studies UPM	1990-1993	3 years
6.	Head of Department	Department of Mathematics UPM	1986-1990 2000-2002	4 years (1 st appointment) 2 years (2 nd appointment)
7.	Acting Head of Department	Department of Mathematics UPM	1980	2 months
8.	Coordinator of Mathematics Courses	UPM branch campus in Kuching Sarawak	1978-1979	1 year
9.	Executive Cadet	Bank Negara Malaysia	1972	1 year

D. Academic awards and recognition

No.	Award/Recognition	Organisation Awarded	Date
1.	Anugerah Emerging Regional Centre of Excellence (ERCE) (INSPEM)	European Mathematics Society (EMS)	2014
2.	Anugerah PERSAMA 2008: Hadiah Utama Makalah Ilmiah 2008	Persatuan Sains Matematik Malaysia	2008
3.	Anugerah PERSAMA 2008: Hadiah Sagu hati Buku Karya Asli 2008	Persatuan Sains Matematik Malaysia	2008
4.	Anugerah Penyelidik Cemerlang UPM	Universiti Putra Malaysia	2006
5.	Anugerah Penyelidik Cemerlang Kementerian Pengajian Tinggi	Kementerian Pengajian Tinggi	2005
6.	Anugerah/Sijil Khidmat Cemerlang UPM	Universiti Putra Malaysia	1993, 1998, 2000, 2005, 2007, 2012, 2013
7.	Anugerah Penyelidik Cemerlang Fakulti Sains dan Pengajian Alam Sekitar	Fakulti Sains dan Pengajian Alam Sekitar, UPM	2001, 2003, 2007
8.	Anugerah Khidmat Setia Putra	Universiti Putra Malaysia	1999
9.	Anugerah Pengajar Cemerlang	Fakulti Sains dan Pengajian Alam Sekitar	2002, 2003, 2007, 2010
10.	Anugerah Pingat Gangsa	Invention and Research	2002

		Exhibition	
11.	Anugerah Adi Pensyarah	Fakulti Sains dan Pengajian Alam Sekitar	2003
12.	Anugerah Adi Penyelidik	Fakulti Sains dan Pengajian Alam Sekitar	2003
13.	Anugerah Pingat Emas dan Perak	Expo Science, Technology and Innovation	2004
14.	Anugerah Pingat Perak	33 rd International Exhibition for Inventions, Techniques and New Products di Geneva, Switzerland	2005
15.	Anugerah Pingat Perak	Pameran PRPI UPM	2008
16.	Darjah Kebesaran Dato Paduka Mahkota Selangor (DPMS)	DYMM Sultan Selangor	2003
17.	Darjah Kebesaran Johan Setia Mahkota (JSM)	DYMM Yang DiPertuan Agung	1997
18.	Felo Akademi Sains Malaysia (FASc)	Akademi Sains Malaysia	Mulai 2012
19.	Felo PERSAMA (FPSM)	Persatuan Sains Matematik Malaysia	Mulai Jun 2007

H. Publications

a. Cited Journals

No.	Name of Writer (s)	Year Published	Title	Name of Journal	Volume Number	Page Number
1.	S. Ismail and K.A. Mohd Atan	2013	On the Integral Solutions of the Diophantine Equation $x^4 + y^4 = Z^3$	Pertanika J. Sci & Technol.	Vol. 21(1)	119-216
2.	Yow, K.S., Sapar, S.H. and Atan K.A.	2013	On the Diophantine Equation $x^2 + 4.7^b = y^{Zr}$	Pertanika J. Sci & Technol.	Vol. 21(22)	443-458
3.	Faridah Yunos and Kamel Ariffin Mohd Atan	2013	An Average Density of τ -adic Naf (τ -NAF) Representation: An Alternative Proof	Malaysian Journal of Mathematical Sciences	Vol. 7(1)	111-123
4.	Mohamat Aidil Mohamat Johari, Kamel Ariffin Mohd Atan and Siti hasana Sapar	2013	A Combinatorial Proof for a Relation Between Certain Types of Integers	JP Journal of Algebra, Number Theory and Applications	Vol. 28(2)	129-139

5.	Isamiddin, S. Rakhimov, Kalyan Kumar Dey, Akhil Chandra Paul and Kamel A. Mohd Atan	2012	Permuting-(σ , τ)- Derivations in Prime Gamma-Near-Rings	JP Journal of Algebra, Number Theory and Applications	Vol. 26(1)	11-31
6.	M.A. Mohamed, K.A. Mohd Atan	2012	Rule Base Representation of Integer for a New Addition Chain Method	Applied Mathematical Sciences	Vol. 6, no. 30	1497-1503
7.	Seo Yoon Yang, Abasalt Bodaghi Kamel Ariffin Mohd Atan	2012	Approximate Cubic* - Derivations on Banach* - Algebras	Abstract and Applied Analysis 1.10 IF	Vo. 2012 (1)	12 page
8.	Yusof Gheisari, Abd Ghafur Ahmad, S. Seddigh Chaharbori, Siti Hasana Sapar, Kamel Ariffin Mohd Atan	2012	Spanning Trees of 2- Complexes from Diagram Groups over the Construction of Semigroup Presentation of Integers using Lifting Method	Malaysian Journal of Mathematical Sciences	Vol. 6, No. 2	213-223
9.	Isamiddin, S. Rakhimov, Kamel A. Mohd Atan	2012	On Contractions and Invariants of Leibniz Algebras	Bulletin of the Malaysian Mathematical Sciences Society	(2), 35(2A)	557-565.
10.	Mohamat Aidil Mohamat Johari, Kamel Ariffin Mohd. Atan, Siti Hasana Sapar	2012	Relation Between square and centred-Pentagonal Numbers	Malaysian Journal of Mathematical Sciences	6(2)	165-175
11.	M. Maleki, M.T. Kajani, I. Hashim, A. Kilicman, K.A. Atan	2012	A Nonclassical Radau Collocation Method for Non-linear Initial-value Problems With Applications Applications to Lane- Emden Type Equations	Journal of Applied Mathematics 0-83 IF	2012(1)	(electronic)

12.	Adem Kilicman, Hassan Eltayeb, Kamel Ariffin Mohd Atan	2011	A Note On The Comparison Between Laplace and Samudu Tranforms	Bulletin of the Iranian Mathematical Society	Vol. 37 No. 1	131-141
13.	H.K. Yap, K.A. Mohd Atan, S.H. Sapar	2011	Estimation of p-adic Sizes of Common Zeros of Partial Derivatives Associated With a Cubic Form	Sains Malaysiana	Vol. 40(8)	921-926
14.	M.A. Mohamed, M.R. Mohd Said, K.A. Mohd Atan, Z. Ahmad Zulkarnain	2011	Shorter Addition Chain for Smooth Integers Using Decomposition Method	International Journal for Computer Mathematics	Vol. 88. No. 11	2222-2232
15.	Mohammad Rezal Mamel Ariffin, Z. Mahad, Nor Azman Abu, Arif Mandangan, Kamel Ariffin Mohd Atan	2011	Linear Diophantine Equation Discrete Log Problem and the AA β Cryptosystem		Vol. ab5/1103. 4.2011	1103.4
16.	M.R. Ismail, K.A. Atan	2010	Mathematics in the Malay World Prior to the Arrival of Western Mathematics	Procedia Social and Behavioural Sciences	Vol. 8	729-734
17.	M.A. Mohamed, M.R. Md Said, K.A. Mohd Atan, Z. Ahmad Zulkarnain	2010	An Improved Binary Method for Scalar Multiplication in Elliptic Curve Cryptography	Journal of Mathematics and Statistics	6 (1)	28-33
18.	Abdul Wahed Ismail, Mohamad Rushdan Md Said, Kamel Ariffin Mohd Atan, Isamidin Rakhimov	2010	An Algorithm to Enhance Elliptic Curve Scalar Multiplication Combining MBNR With Point Halving	Applied Mathematical Sciences	Vol. 4, No. 26	1259-1272

19.	Abdul Wahed Ismail, Mohamad Rushdan Md Said, Kamel Ariffin Mohd Atan, Isamiddin Rakhimov	2010	Bilinear Pairing Computation Using the Extended Double-Base Chains Algorithm	International Journal of Math. Analysis	Vol. 4, No. 19	929- 941
-----	--	------	--	---	----------------	----------

b. Non-cited Journal

No.	Name of Writer (s)	Year Published	Title	Name of Journal	Volume Number	Page Number
1.	Isamiddin S. Rakhimov, Kamel A. Mohd. Atan	2012	On Some New Properties of Catalan Numbers	International Journal of Modern Physics: Conf. Series.	Vol. 9	537-542
2.	S. Seddighi Chaharboj, M.R. Abu Bakar, A.H. Malik, M.A. Kamel Ariffin, I. Noor Akma	2010	A New Modification of the Homotopy Perturbation Method	Ultra Science	Vol.22 (1)	309-316
3.	Nor Mazlin Zahari, Siti Hasana Sapar, Kamel Ariffin Mohd Atan	2010	A Method of Finding Integral Solution to the Diophantine Equation $x^3 + y^3 = z^8$	Jurnal Karya Asli Lorekan Matematik		9-12
4.	Wong Tze Jin, Mohamad Rushdan Md Said, Kamel Ariffin Mohd Atan, Mohamed Othman	2009	GCD Attack on the LUC4 Cryptosystem	International Journal of Cryptology Research		179-189
5.	Wong Tze Jin, Mohamad Rushdan Md Said, Kamel Ariffin Mohd Atan, Mohamed Othman	2009	Garbage-Man-In-The-Middle Attack on the Luc4 Cryptosystem	International Journal of Cryptography Research	Vol. 1 No. 1	33-42
6.	Abdul Jalil M. Khalaf, Yee-Hock Peng, Kamel Ariffin Mohd Atan	2009	The Chromatic Uniqueness of a Family of 6-Bridge Graphs	Akce J. Graphs, Combin	6, No.3	393-400

7.	Kamel Ariffin Mohd Atan, Rustem Suncheleev, Mahendran Shitan, Mohd Shafie Mustafa	2008	Animated Introductory Calculus: Development and Perception	Journal of US- China Education Review	Vol. 5, No. 3 (ser. 40)	1-15
8.	S. Alikhani, Y.H. Peng, K.A.M. Atan	2008	On the Domination Number Of Some Graphs	International Mathematical Forum	Vol. 3, No. 37-40	1879-1884
9.	S.H. Sapar, K.A.Mohd Atan	2008	On the Cardinality of the Set of Solutions to Congruence Equation Associated With a Complete Seventh Degree Form	Matematika. (Special Edition Part 1)		23-30

c. Book(s)

No.	Name of Author(s)	Year Published	Title	Publisher
1.	Isamiddin S. Rakhimov, Al Hossain Al Nashri, Kamel A. Mohd. Atan	2012	Derivations of low-Dimensional Leibniz Algebras	Lampert Academic Publishing, Germany
2.	Sozan Obaiys, Rakhimov Isamiddin Sattarovich, Kamel Ariffin Mohd Atan	2010	Classification of First Class Of Complex Filiform Leibniz Algebras	Publisher: Lampert Academic Publishing Germany
3.	K. A. Atan, R. Suncheleev	2007	Animated Introductory Calculus	Penerbit Universiti Putra Malaysia
4.	K.A. Atan	1992	Elementary Real Analsis	Dewan Bahasa dan Pustaka.
5.	K.A. Atan	1989	Principles of Mathematical Analysis	Dewan Bahasa dan Pustaka.
6.	K.A. Atan	1987	Linear Algebra	Dewan Bahasa dan Pustaka

d. Chapter(s) in Book

No.	Name of Author(s)	Year Published	Title	Publisher
-----	-------------------	-------------------	-------	-----------

1.	K.A. Atan, M.R. Ismail, O. Bakar	1996	Algebra in Islamic Mathematics	Encyclopaedia of the History of Science, Technology and Medicine In Non-Western Cultures, (Amherst, Massachusetts USA)
----	----------------------------------	------	--------------------------------	--

e. Proceeding(s)

No.	Name of Writer(s)	Year Published	Title	Name of Seminar/ Conference	Page Number
1.	Faridah Yunos, Kamel Ariffin Mohd Atan, Muhammad Rezal Kamel Ariffin and Mohamad Rushdan Md. Said	2014	Pseudo τ -adic NAF for Scalar Multiplication on Koblitz Curves	Proceedings of 4th International Cryptology and Information Security Conference 2014	120-130
2.	M.A.M. Johari, K.A.M. Atan, S.H. Sapar	2012	A General Relation Between Sums of Cubes and Triangular Pyramidal Numbers	AIP Conf. Proc.	275-279
3.	K.A. Mohd Atan, R. Suncheleev, M. Shitan, Lim S.F	2010	Animated Geometry (AG) in Education: A Case Study	Proceedings of Global Learn Asia Pacific 2010	583-588
4.	S.H. Sapar, K.A. Mohd Atan	2010	A Method of Finding an Integral Solution to $x^3 + y^3 = kz^{4x}$	Proceedings of International Conference on Mathematical Sciences	842-845
5.	M.R.M. Said, M.A. Mohamed, K.A. Mohd Atan, Z. Ahmad Zulkarnain	2010	Signed Decomposition Method for Scalar Multiplication in Elliptic Curve Cryptography	American Institute of Physics (AIP) Conference Proceedings	805-813
6.	Davood Razeipour, Mohamad Rushdan Md. Said, Kamel Ariffin Mohd Atan, Mohamed Othman	2010	The Strength of AES Cryptosystem Against the New Cryptanalytic Attacks	Proceedings of 4 th International Cryptology Conference	83-91

7.	K.S. Lee, Kamel Ariffin Mohd Atan, Siti Hasana Sapar	2010	On Positive Solutions of the Diophantine Equation $x^3 + y^3 = 2^k z^3$	Prosiding Seminar Kebangsaan Aplikasi Sains & Matematik	27-31
8.	Kamel Ariffin Mohd Atan	2010	Penentuan Penyelesaian Integer Beberapa Persamaan Diofantus	Prosiding Seminar Kebangsaan Ke-4 PBPO	
9.	Nor Mazlin Zahari, Siti Hasana Sapar, Kamel Ariffin Mohd Atan	2010	Suatu Kaedah Mencari Penyelesaian Integer Kepada Persamaan Diofantus $x^3 + y^3 = z^3$	Prosiding Seminar Kebangsaan Aplikasi Sains & Matematik	233-238
10.	K.S. Yow, Siti Hasana Sapar, Kamel Ariffin Mohd Atan	2010	On the Diophantine Equation $x^2 + 16.7^b = y^{2r}$	Prosiding Seminar Kebangsaan Aplikasi Sains & Matematik	339-346
11.	Shahrina Ismail, Kamel Ariffin Mohd Atan	2010	On the Integral Solutions for the Diophantine Equation $x^4 + y^4 = 2z^2$	Prosiding Seminar Kebangsaan Aplikasi Sains dan Matematik	307-315

f. Seminar Papers Presented (orally)

No.	Name of Writer(s)	Taraf	Title	Name of Seminar/Conference	Organiser	Place	Date
1.	Faridah Yunos, Kamel Ariffin Mohd Atan, Muhammad Rezal Kamel Ariffin and Mohamad Rushdan Md. Said	Penulis Bersama	Pseudo τ -adic NAF for Scalar Multiplication on Koblitz Curves	4 th International Cryptology and Information Security Conference 2014	Malaysian Society for Crypto- logy Research	Putra- jaya	24-26 Jun 2014
2.	K.A. Atan	Pemben- tang Kertas Kerja	On Some Exponential Sums	The 6th International Conference on Research and Education in Mathematics	Institute of Mathema- tics of Vietname Academy of Science and Tech- nology	Ho Chi Minh City	August 2013

3.	Isamiddin S. Rakhimov, Kamel A.M. Atan and Siti Hasana Sapar	Penulis Bersama	Cohomological Approach to Classify Nilpotent Leibniz Algebras	Conference on Operator Algebras and Related Topics	National University of Uzbekistan, Institute of Mathematics Ministry of Higher Education, Uzbekistan	Tashkent Uzbekistan	12-14 Sept. 2012
4.	K.A. Atan S.H. Sapar	Pembentangan Kertas Kerja	Explicit Estimation of Exponential Sums Associated With a Quintic Form	International Conference On Applied Analysis and Algebra (ICAAA 2012)	Yildiz Technical University	Istanbul Turki	20-24 Jun 2012
5.	K.A. Atan	Pengucap Utama (Key Note Speaker)	On the Estimation of Exponential Sums Associated With A Cubic Form	International Conference On Financial Mathematics and Numerical Optimization (ICFMNO 2012)	Universiti Malaysia Terengganu	Kuantan	30 Mei -1 Jun 2012
6.	K.A. Atan S. Ismail	Penulis Bersama	On the Solutions to the Diophantine Equation $x^4 + y^4 = 2z^2$	The 5 th International Conference On Research and Education in Mathematics	Institut Teknologi Bandung	Bandung Indonesia	22-14 Okt. 2011
7.	K.A. Atan M. Aidil, S.H. Sapar	Penulis Bersama	A General Relation Between Sums of Cubes and Triangular Pyramidal Numbers	The 5 th International Conference On Research and Education in Mathematics	Institut Teknologi Bandung	Bandung Indonesia	22-24 Okt. 2011
8.	K.A. Atan M. Rushdan M. Affendee Z. Zulkarnain	Penulis Bersama	A Composition method for Shorter Addition Chain	The 5 th International Conference on Research and Education in Mathematics	Institut Teknologi Bandung	Bandung Indonesia	22-24 Okt. 2011
9.	K.A. Atan F. Yunos M. Rezal M. Rushdan	Penulis Bersama	A Reduced q-adic Naf Representation for An Efficient Scalar Multiplication on Anomalous Binary Curves	The 5 th International Conference on Research and Education in Mathematics	Institut Teknologi Bandung	Bandung Indonesia	22-24 Okt. 2011
10.	K.A. Atan	Pengucap Utama (Key Note Speaker)	Number Theory and Cryptography	Seminar Kebangsaan Aplikasi Sains Dan Matematik 2010 (SKSM 18)	Universiti Teknologi Malaysia	Johor Bharu	8 Dis. 2010
11.	K.A. Atan Siti Hasana	Pembentangan	On Positive solutions of the Diophantine Equation $x^3 + y^3 = 2kz^3$	Seminar Kebangsaan Aplikasi Sains & Matematik 2010	Universiti Teknologi Malaysia	Johor Bharu	8-10 Dis. 2010

12.	K.A. Atan Siti Hasana	Penulis Bersama	Suatu Kaedah Mencari Penyelesaian Integer Kepada Persamaan Diofantus $x^3 + y^3 = z^4$	Seminar Kebangsaan Aplikasi Sains & Matematik 2010	Universiti Teknologi Malaysia	Johor Bharu	8-10 Dis. 2010
13.	K.A. Atan M. Rushdan Shahrina Ismail	Penulis Bersama	Integral Solutions for the Diophantine Equation $x^3 + y^3 = 2z^2$	Seminar Kebangsaan Aplikasi Sains & Matematik 2010	Universiti Teknologi Malaysia	Johor Bharu	8-10 Dis. 2010

g. Other Presentation (Poster/Product/Exhibition/Showcase)

No.	Name of Writer(s)	Title	Name of Seminar/Conference/Exhibition	Organiser	Place	Date
1.	K.A. Atan	Sains Matematik Pemangkin Pembangunan Modal Insan	Simposium Kebangsaan Sains Matematik 15	ITM	Shah Alam	5-7 Jun 2007
2.	K.A. Atan	Sains Matematik Pemangkin Pembangunan Modal Insan	Simposium Kebangsaan Sains Matematik 15	ITM	Shah Alam	5-7 Jun 2007
3.	K.A. Atan Rustem Sunchelev	Educational Software for the Teaching and Learning of University Level Calculus	33 rd International Exhibition of Inventions, New Techniques and Products		Geneva, Switzerland	6-11 April 2005
4.	K.A. Atan R. Sunchelev, I. Abdullah, U. Baekbaev	Educational Software in the Teaching of Introductory Calculus and Algebra at University Level	Expo Science, and Technology and Innovation		Kuala Lumpur	27-29 Ogos 2004
5.	K.A. Atan R. Sunchelev	Animation of University Level Introduction to Calculus	I-TEX Exhibition		Kuala Lumpur (MegaMall Exhibition Centre)	20 Mei 2004
6.	K.A. Atan	Peningkatan Kerjasama Antara IPT dengan sektor Industri dalam Penyelidikan Bermatematik	Seminar Kebangsaan Matematik Industri	UPM	Serdang Selangor	12 Okt. 2002

h. Other Equivalent Outcomes (Monograph/Module/Popular Writing & Article/Design etc)

No.	Name of Writer(s)	Title	Category of Outcome	Year Published
-----	-------------------	-------	---------------------	----------------

1.	S.H. Sapar, K.A. Mohd Atan	An Estimation of the p-adic Sizes of Common Zeros to Partial Derivative Polynomials of Degree Seven	Makalah	2008
2.	Siti Hasana Sapar, Kamel Ariffin Mohd Atan	An Estimation of p-adic Sizes of Common Associated With a Seventh Degree Form With Complete Dominan Terms	Makalah	2008
3.	S. H. Sapar, K. A. Atan, M. R. Said	A Method of Estimating the p-adic sizes of Common Zeros of Partial Derivative Polynomials Associated With a Quintic Form	Makalah	2007
4.	Kamel Ariffin Atan	On the Study of Numbers	Makalah	2003
5.	Kamel Atan, Thomas Bier	On the Solutions of a Semi Quadratic Pair of Diophantine Equations and Their Applications	Laporan Teknikal	2003
6.	Kamel Atan, Thomas Bier	On the Structure of Lifted Integer Solutions of the Congruence $x^2 \equiv 1 \pmod{n}$	Laporan Teknikal	2003
7.	S. H. Sapar, K.A. Atan	Estimating the p-adic Sizes of Common Zeros of Partial Derivative Polynomials,	Laporan Teknikal	2003
8.	R. Zulkapli, K.A. Atan, S.H. Sapar	A Method for Determining p-adic Orders of Factorials and Its Applications,	Laporan Teknikal	2011
9.	S.A.A. Rahman, K.A. Atan, S.H. Sapar	On the Diophantine Equations $x^2 + 3^a 5^b = y^2$	Laporan Teknikal	2011
10.	S. Ismail, K. Atan	On the Integral Solutions of the Diophantine Equation $x^4 + y^4 = z^3$	Laporan Teknikal	2011

I. Research activities

a. Research Grants

No.	Title	Role (Main/Co-researcher)	Sponsor/Grant and Amount (RM)	Period (year)	Status (Completed /Ongoing)
1.	On the Cardinality of the	Ahli	FRGS	2013-2015	Ongoing

	Set of Solutions to Congruence Equation Associated With Higher Degree Polynomial		RM61,000.00		
2.	Discrete groups, Hyperbolic & Complex Projective Geometry and Quantum States-Novel Constructions and Applications	Ahli	ERGS RM6108,000.00	2013-2016	Ongoing
3.	AA β Public Key Cryptosystem Key Generator	Ahli	PRGS RM176,000.00	2011-2013	Completed
4.	On the Cardinality of the Set of Solutions to Congruence Equation Associated With Higher Degree Polynomial	Ahli	FRGS RM61,000.00	2013-2015	Ongoing

b. Patent/Commercialisation

No.	Title	Date	File/Patent No.	Status (Granted/Pending)
1.	Chaotic Asymmetric Encryption Process for Data Security	22.05.2010	12/239,348	Granted, (US)