Short Curriculum Vitae

Personal Information

Full Name: Ruma Kareem K. Ajeena.
Date and Place of Birth: 22-1-1976, Baghdad -Iraq.
Gender: Female.
Matrimonial Status: Married.
Mobile No.: +60108964342 (for now).
E-mails: ruma.usm@gmail.com
Mail address: 314-28-28, Adamiya, Alsheeouokh, Baghdad, Iraq.
Working place: Mathematics school, Babylon University, Babil city, Iraq.

Areas of Specialization /Interests

Cryptography- Elliptic Curve Cryptography-ISD Method, Public Key Cryptography, Coding Theory, Linear Algebra, Abstract Algebra and Number Theory, Developing Algorithms, Parallel Numerical Computations.

Education /Career Profile

- Diploma, Mathematics & Sciences -Teachers Institute - 1990-1995.
- B.Sc. Mathematical Sciences School - Babylon University- Iraq-1995-1999.
- M. Sc. Mathematical Sciences School - Babylon University- Iraq-2003-2006.
- Ph.D. Mathematical Sciences School - USM, Penang, Malaysia 6th March 2015.
- Obtained a certification of English Language in Intensive English Levels, at School of Languages, Literacies and Translation, USM- 3.1.2011-3.6.2011.
- Obtained an appointment as Graduate Research Assistant (GRA) in the School of Mathematical Sciences, USM, 2013- 6th March 2015.

- Primary School Teacher - 1999-2000.
- Secondary School Teacher - 2001.
- Instructor at Babylon University - Mathematics Dept. - 2002-2010.
- B.Sc. Supervisor at Babylon University - Mathematics Dept. - 2006.
- Lecturer, School of Sciences for Women, Babylon University- 2008-2009.
- Researches Evaluator - Babylon University- 2006-2010.

Computer Software

Matlab, Mathematica, Sage Software.

Research and Recent Publications 2012-2015

Journal:

[1] Ajeena, R. K. K., and Kamarulhaili , H. (2014). Point Multiplication using Integer Sub-Decomposition for Elliptic Curve Cryptography. Applied Mathematics and Information Sciences, 8(2) *(Indexed in ISI, IF= 1.232).*

[2] Ajeena, R. K. K., and Kamarulhaili, H. (2013). Analysis on The Elliptic Scalar Multiplication Using Integer Sub-Decomposition Method. International Journal of Pure and Applied Mathematics, 87(1), 95-114. *(Indexed in Scopus, IF=2.68).*

[3] Ajeena, R. K. K., and Kamarulhaili, H. (2014). Comparison Studies on Integer Decomposition Method for Elliptic Scalar Multiplication. Advanced Science Letters, 20(2), 526-530. *(Indexed in Scopus, IF= 1.253).*

[4] Ajeena, R. K. K., and Kamarulhaili, H. Two Dimensional Sub-Decomposition Method For Point Multiplication on Elliptic Curves. Journal of Mathematical Sciences: Advances and Applications Volume 25, 2014, Pages 43-56.*(Indexed in MathSciNet).*

[5] Ajeena, R. K. K., and Kamarulhaili, H. GLV-ISD Method for Scalar Multiplication on Elliptic Curves. Australian Journal of Basic and Applied Sciences, 2014 *(Indexed in ISI, GIF=0.425, IF=2.684).*

[6] Ajeena, R. K., Kamarulhaili, H. Bivariate Polynomials Public Key Encryption Schemes. International Journal of Cryptology Research 4(1): 73 - 83.

[7] Ajeena, R. K., Kamarulhaili, H. Accelerating Integer Sub-Decomposition for Elliptic Scalar Multiplication using wNAF Expansion Method. Malaysian Journal of Mathematical Sciences. *(Indexed in Scopus), (Accepted).*

Conference Proceeding:

[1] Ajeena, R. K. K., and Kamarulhaili, H. *"Integer Sub-Decomposition for Point Multiplication on Elliptic Curves"*, Malaysian Cryptology and Information Security Lecture Series 3-4 July (2013).

[2] Ajeena, R. K. K., and Kamarulhaili, H. *" Bivariate Polynomials and its Application in a Public Key Encryption Schemes"*, in the 3^{rd} International Conference on Cryptology and Computer Security 2012, held on 4^{th}-6^{th} June, 2012 at Holiday Villa Beach Resort & Spa, Langkawi.

[3] Ajeena, R. K. K., and Kamarulhaili, H. *"The computational complexity of elliptic curve integer sub-decomposition (ISD) method"*, in the 21^{st} national Symposium on Mathematical Sciences, held on 6-8 November, 2013. The Gurney Resort Hotel and Residence, Penang, Malaysia. *(Proceeding Indexed in ISI, AIP).*

[4] Ajeena, R. K. K., and Kamarulhaili, H. *"A Hybrid Approach For Elliptic Scalar Multiplication"*, in the International Conference on Mathematics and Engineering and Industrial Applications 2014, held on 28-30 May 2014 at The Gurney Resort Hotel and Residence, Penang, Malaysia. *(Proceeding Indexed in ISI, AIP).*

[5] Ajeena, R. K. K., and Kamarulhaili, H. *"Fast Computation in wNAF Expansion Method for Integer Sub-Decomposition Elliptic Scalar Multiplication"*, in the 4^{rd} International Conference on Cryptology and Computer Security 2014, held on 24^{th}-26^{th} June, 2014 at Putrajaya, Malaysia.

[6] Ajeena, R. K. K., and Kamarulhaili, H. *"Elliptic scalar multiplication based on integer decomposition method for cryptographic use"*, International Congress of

Mathematicians (SEOUL-ICM 2014), held on 13^{th}-21^{th} August, 2014, Coex, Seoul, Korea, *(Abstract only).*

[**7**] Ajeena, R. K. K., and Kamarulhaili, H. *"On The Distribution of scalar k for Elliptic Scalar Multiplication"*, in the 22^{sd} national Symposium on Mathematical Sciences, held on 24^{th}-26^{th} November, 2014, at the Grand BlueWave Hotel, Shah Alam, Malaysia Malaysia. *(Proceeding Indexed in ISI).*

[**8**] Ajeena, R. K. K., and Kamarulhaili, H. *"A New Elliptic Scalar Multiplication Method Using A Generalized Extended Euclidean Algorithm"*, in the 3^{rd} International Conference on Computer Engineering and Mathematical Sciences, held on 4-5 December, 2014, Langkawi, Malaysia. *(Proceeding Indexed in ISI).*

[**9**] Ajeena, R. K. K., and Kamarulhaili, H. *"Mathematical analysis of the computational complexity of integer sub-decomposition algorithm"*, in the 3^{rd} International Conference on Science & Engineering in Mathematics, Chemistry and Physics (2015), which will be held 31 January-1 February, 2015, at the Sanur Paradise Hotel, Bali, Indonesia *(Proceeding Indexed in ISI), (Accepted).*

[**10**] Ajeena, R. K. K., and Kamarulhaili, H. *"New Algorithms to Increase Percentage of kP Computation for Elliptic Scalar Multiplications"*, in the 6^{th} International Conference on Information & Communication Systems (ICICS2015), which will be held April 7-9, 2015, Amman, Jordan. *(Proceeding Indexed in IEEE), (Accepted).*