Mousa Farajallah

Head of the Computer Engineering and Security Department
College of Information Technology and Computer Engineering
Palestine Polytechnic University
P.O Box 198
Hebron - Palestine

Contact Information

Email Address: mousa_math@ppu.edu
Mobile No: +970599380784
Work-Phone: +97022233050, Ext 9107
Country: Palestine
Website 1: `http://staff.ppu.edu/mousa_math`

Personal Information

Birth Date: 22 May 1982
Nationality: Palestinian
Marital Status: Married
Number of Dependents: 2

EDUCATION

Ph.D in Computer Science/Engineering- Image, video and signal Crypto-Compression processing
Thesis Title: Chaos-based crypto and joint crypto-compression systems for image and video
Nantes University, Institute of Electronics and Telecommunications of Rennes University, Image Team
Location: Nantes-France
Completion Date: 30-June-2015
Build a chaos based crypto-compression system for H.265/HEVC video. It is the new video standard, it is published in 2013.
Ranked first in IETR lab-Nantes university in terms of research production between 2013 and 2015.
My PhD degree is fully supported by the French Government under the International Fellowships Program due to my high ranking in the M.Eng degree.

Master of Engineering (M.Eng)-Electronics and Computer Engineering-Cryptography.
Master Thesis Title: Developing Symmetric Encryption Algorithm based on a modified Hill cipher.
Al-Quds University, Graduate Studies
Location: Jerusalem, Palestine
Completion Date: January 2010
GPA: 90.5% Excellent-Top Rating

In January 2010, I have completed my Master degree in Electronics and Computer Engineering, specializing in **Cryptography** from Alquds University in Jerusalem in Palestine. My master degree is fully supported by the AMIDEAST under the International Fellowships Program due to my high ranking in the B.Eng degree.

Bachelor of Engineering (B.Eng) Electrical Engineering. Computer Systems Engineering
Palestine Polytechnic University, College of Engineering and Technology
Location: West Bank, Palestine
Completion Date: June 2006
GPA: 90.4%, High Honor-Top Rating
Ranked 1^{st} among all of the Electrical and Computer department of three programs contains **120** student in the year 2006.
My Engineering degree is fully supported by Hani Qaddumi Scholarship Foundation due to my high ranking in the General Secondary Education.

General Secondary Education Examination, Al-Tawjihi High school
Idna Secondary Boys School, Scientific Stream
Location: West Bank, Palestine
Completion Date: June 2001
GPA: 94.3%, Excellent

AWARDS and HONORS

- **2012, French Government Scholarship**. To complete the PhD degree between 2012 and 2015.
- **2012, Saarland University Fellowship**. To attend the Pre-PhD program (Cryptography and Information Security Course) between April 2012 and September 2012.
- **2010, AMIDEAST Fellowship**. To attend the Training of Trainers of the best 10 Palestinian student for 2010.
- **2007, AMIDEAST Fellowship**. To complete the Master of engineering in Electronic and Computer Engineering degree between 2007 and 2010.
- **2006,** 1^{st} **Rank**. Achieving the highest GPA among all Electrical and Computer Engineering department.
- **2006,** 1^{st} **Rank**. Achieving the highest GPA among Computer Engineering program.
- **2006,** 1^{st} **Rank**. Achieving the best graduation project among all Electrical and Computer Engineering department.
- **2006,** 1^{st} **Rank**. The only student achieving the High Honor rating among all Electrical and Computer Engineering department.

- **2006,** 9^{th} **Rank**. 9^{th} place of the Palestine Polytechnic University among all graduated students in 2006.
- **2002, Hani Qaddumi Scholarship**. To complete the Bachelor of engineering in computer systems engineering degree between 2002 and 2006.

Memberships

- International Journal of Signal Processing: Image Communication (Elsevier , Q1 journal) Reviewer
  Membership: Reviewer
  Member since: January 2016
- International Journal of Signal Processing (Elsevier, Q1 journal) Reviewer
  Membership: Reviewer
  Member since: September 2016
- International Journal of Bifurcation and Chaos (IJBC, Q1 journal) Reviewer
  Membership: IJBC Reviewer
  Member since: September 2014
- IEEE
  Membership: IEEE Fellow
  Member since: September 2013
- ICITST
  Membership: ICITST Fellow
  Member since: April 2013
- IFP
  Membership: IFP Fellow
  Member since: June 2010
- IEEE ICIP 2014 (SJR conference) Membership: Special Sessions organizer
  Member since: December 2014

Research Interests

- Cryptography algorithms
- Cryptography and Security Evaluation tools
- Security of HEVC standard
- Crypto-Compression algorithms
- Joint-Cryptography solutions for image and Video
- Practical Cryptanalysis
- Parallel implementation of crypto solutions
- Database Security

SKILLS

- C/C++ programming
  Level: Expert
  Experience: More than 10 years
- Java
  Level: Intermediate
  Experience: Less than one year
- ASP.NET
  Level: Expert
  Experience: Less than 5 years
- VB.Net
  Level: Expert
  Experience: Less than 10 years
- Microsoft Office 2000,2003,2007
  Level: Expert
  Experience: More than 5 years
- Matlab
  Level: Intermediate
  Experience: Less than 5 years
- Latex
  Level: Expert
  Experience: More than 3 years
- Chaos Cryptosystems
  Level: Expert
  Experience: More than 5 years
- Mathematical courses for engineering and computer science
  Level: Expert
  Experience: More than 5 years
- Video and Image courses
  Level: Expert
  Experience: Less than 5 years
- Computer Engineering/Science and IT courses
  Level: Expert
  Experience: More than 5 years
- Research and project
  Level: Expert
  Experience: More than 5 years

Languages

- Arabic
  Level: Expert
  Experience: Mother/First language
- English
  Level: Expert
  Experience: More than 18 years

Funded Training and Certification

- Saarland University -Germany
  Duration: 4 months - (From 8 April 2012 To 5 August 2012)
  Type of Training: Cryptography and Hot topics in Security
- IFP
  Duration: 10 days - (From 15 May 2010 To 24 May 2010)
  Type of Training: TOT

Work Experience

Head of the Computer Engineering and Security Department, July-2016 → current, Full time, College of Information Technology and Computer Engineering-Palestine Polytechnic University, Palestine Keeps abreast of current and future trends to develop or establish the required educational services in Computer Engineering courses. Help and resolve student complaints and other issues. Develops and maintains relationships with industry partners to support internship, graduation project collaborations. Translate the college's mission and values into students to ensure that the goals of the Computer Engineering program are attainable. Designs and implements new and innovative programs for business solutions.

Assistant Professor, August-2015 → July-2015, Full time, College of Information Technology and Computer Engineering-Palestine Polytechnic University, Palestine
Teaching up to 4 graduate and undergraduate courses in Computer Engineering each semester.

Post-Doctoral researcher, Feb-2015 → August-2015, Full time, INSA of Rennes University and AMP Visual TV company, France
I have developed with our colleagues in INSA a complete security system for the last video standard (HEVC). One of my tasks with the INSA of Rennes university includes theoretical research of HEVC encoder privacy and security while with the AMP company to implement these researches on the practical applications.

Research assistant, Oct-2013-Feb-2015, IETR Lab
I have 2 years of experience in teaching and helping first year PhD student in our lab.

Director of the computer center, April-2010-April-2012, Full time, Palestine Polytechnic University
I have worked as a director of the computer center at the college of engineering and also a lecturer at Palestine Polytechnic University, computer center is the responsible unit to provide high-quality computing facilities and services for faculty, students, and staff in order to support the practical courses, research, and educational endeavors of the college of engineering.

Lab Assistant, Sept-2006-April-2010, Full time, Palestine Polytechnic University
From 2006 till 2010 as lab supervisor teaching the practical part of the computer

courses and graduation project assistant where I gained good practical knowledge.

Teaching Courses

1- Cryptography (Master+Bachelor)
2- Cryptanalysis (Master+Bachelor)
3- Introduction to information security (Master+Bachelor)
4- Digital System Design
4- Image and video security
5- Computer Ethics
6- Signals and systems
7-Discrete Mathematics for Computer Engineering
8-Number theory. 9-Data Structures

Supervised Master/Bachelor Students

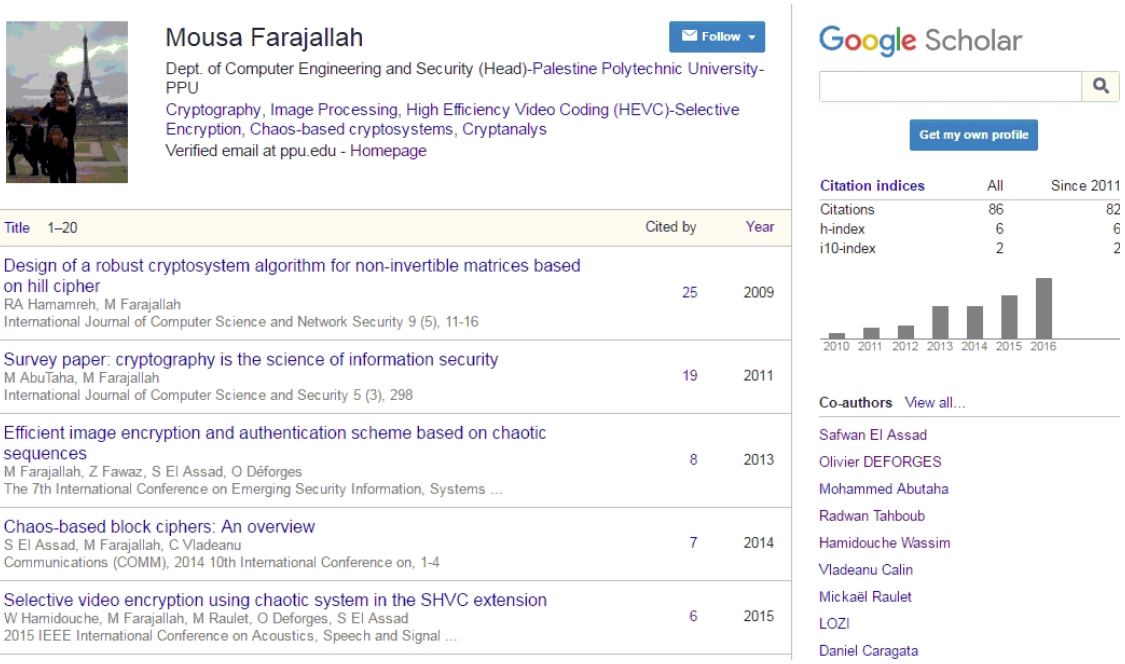
1. sahar natsha,Master of Informatics, Palestine Polytechnic University, "Joint Crypto-Compression algorithm for JPEG2000",2016.
2. Zaher Amro ,Master of Informatics, Palestine Polytechnic University, "Standard Security Evaluation using NPCR, UACI and HD",2016.
3. Amal Abuzalata ,Master of Informatics, Palestine Polytechnic University, "Designing a database encryption technique for database security solution",2016.
4. Samer Iseed, Master of Informatics, Palestine Polytechnic University, "Parallel Generator for secure real-time application",2015.
5. Rawan Qumsieh, Master of Informatics, Palestine Polytechnic University, "A lightweight image encryption algorithm", 2016.
6. Samah Asafra and Abrar Abu-Hassan, Bachelor of Computer Systems Engineering, Palestine Polytechnic University, "Virtual Reality Racing Game Using Mobile Robots", 2015.
7. Dania Jabareen, Bachelor of Computer Systems Engineering, Palestine Polytechnic University, "Musical Gloves based on Magnetic field", 2015.
8. Naji Al jazar, Saga maraqa, Bachelor of Computer Systems Engineering, Palestine Polytechnic University, "Augmented Reality of Qar Hishm", 2016
9. Rabea Altaradeh, Bachelor of Computer Systems Engineering, Palestine Polytechnic University, "Gun Simulator and AR Game", 2016
10. Saja Abu Dayyah and Raeda Abu Sabha, Bachelor of Computer Systems Engineering, Palestine Polytechnic University, "Cryptographically secure voting system", 2016.

Member of Thesis Committee

Mohammed Salem, Master of Computer Engineering, Al-Quds University- Jerusalem, "Dynamic and Efficient Protocol for Detection and Mitigation of Multiple Black Hole Attack in MANET",2016.

Papers Under Review

1. W. Hamidouche, M. Farajallah, O. Deforges, and S. El Assad,Real "Time Selective Video Encryption based on the Chaos System in the Scalable HEVC Extension", IEEE Transactions on Circuits and Systems for Video Technology, Submission date:11-Jan-2016, Q1 Journal.
2. Farajallah Mousa, El Assad Safwan and Deforges Olivier, "Partial cryptanalysis of the first Zhang algorithms", Signal Processing: Image Communication, Submission date:22-Jan-2016, Q1 Journal.



Mousa Farajallah

Follow

Dept. of Computer Engineering and Security (Head)-Palestine Polytechnic University-PPU

Cryptography, Image Processing, High Efficiency Video Coding (HEVC)-Selective Encryption, Chaos-based cryptosystems, Cryptanalys

Verified email at ppu.edu - Homepage

Title 1–20	Cited by	Year
Design of a robust cryptosystem algorithm for non-invertible matrices based on hill cipher RA Hamamreh, M Farajallah International Journal of Computer Science and Network Security 9 (5), 11-16	25	2009
Survey paper: cryptography is the science of information security M AbuTaha, M Farajallah International Journal of Computer Science and Security 5 (3), 298	19	2011
Efficient image encryption and authentication scheme based on chaotic sequences M Farajallah, Z Fawaz, S El Assad, O Déforges The 7th International Conference on Emerging Security Information, Systems ...	8	2013
Chaos-based block ciphers: An overview S El Assad, M Farajallah, C Vladeanu Communications (COMM), 2014 10th International Conference on, 1-4	7	2014
Selective video encryption using chaotic system in the SHVC extension W Hamidouche, M Farajallah, M Raulet, O Deforges, S El Assad 2015 IEEE International Conference on Acoustics, Speech and Signal ...	6	2015

Google Scholar

Get my own profile

Citation indices	All	Since 2011
Citations	86	82
h-index	6	6
i10-index	2	2

2010 2011 2012 2013 2014 2015 2016

Co-authors View all...

Safwan El Assad
Olivier DEFORGES
Mohammed Abutaha
Radwan Tahboub
Hamidouche Wassim
Vladeanu Calin
Mickaël Raulet
LOZI
Daniel Caragata

Published and Accepted Papers

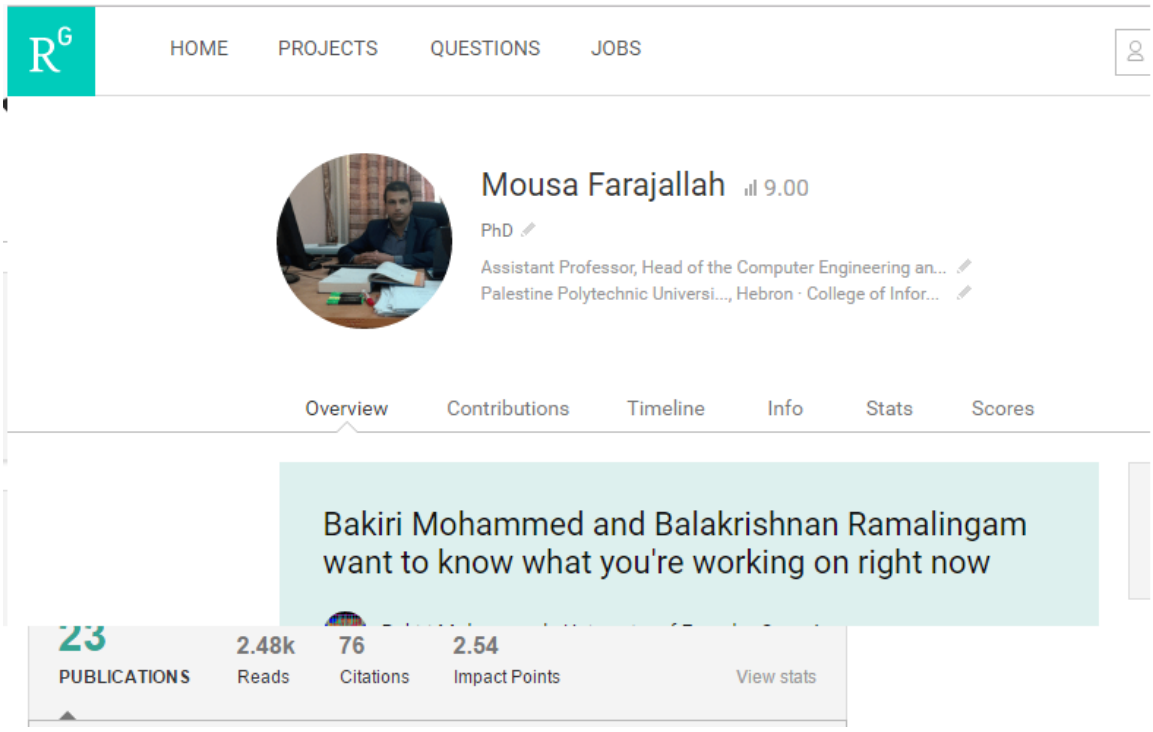
1) M. Farajallah and Rawan Qumsieh , "Selective Hybrid Chaotic-Based Cipher for Real-Time Image Application", in SECURWARE 2016, The 10^{th} International Conference on Emerging Security Information, Systems and Technologies, Nice, France, IARIA, 24-31 July, 2016.

2) El Assad Safwan and Farajallah Mousa, "A New Efficient Structure of a Cryptosystem based on Two Chaotic Layers: a Binary Diffusion Layer and a Bit-Permutation Layer", Signal Processing: Image Communication, Accepted in 20-Oct-2015, Q1 Journal.

3) AbuTaha Mohammed, El Assad Safwan and Farajallah Mousa "Chaos-based Cryptosystems using Dependent Diffusion : An Overview", IEEE ICITST-2015, December 14-16, 2015, London, UK.

4) Farajallah Mousa, El Assad Safwan and Deforges Olivier, " Fast and secure chaos based cryptosystem for images", International Journal of Bifurcation and Chaos (IJBC), Accepted in 15-June-2015, Q1 Journal.

5) M. Farajallah, W. Hamidouche, O. Deforges, and S. El Assad, "ROI selective video encryption in the hevc video standard", in IEEE International Conference on Image Processing (ICIP) SJR H Index: 40, 27-30 September 2015, Quebec City, Canada.



6) W. Hamidouche, M. Farajallah, M. Raulet, O. Deforges, and S. El Assad, "Selective video encryption using chaotic system in the SHVC extension", in 40^{th} IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) SJR H Index: 70, 19 - 24 April 2015, Brisbane, Australia.

7) M. Chetto, S. El Assad, M. Farajallah, et al., "A lightweight chaos-based cryptosystem for dynamic security management in real-time overloaded applications", Int. J. Internet Technology and Secured Transactions, vol. 5, no. 3, pp. 262274, 2014.

8) S. El Assad, M. Farajallah, C. Vladeanu, et al., "Chaos-based block ciphers: An overview", in The 10^{th} International Conference on Communications, 29-31 May, 2014.

9) Z. Fawaz, S. El Assad, M. Farajallah, A. Khalil, R. Lozi, O. Deforges, D. Battikh, B. Bakhache, M. Khalil, K. Samrouth, et al., "Lightweight chaos-based cryptosystem for secure images", in 8^{th} International Conference on Internet Technology and Secured Transactions 2013: ISTP Workshop, London, UK, 9-12 Dec, 2013.

10) M. Farajallah, Z. Fawaz, S. El Assad, and O. Deforges, "Efficient image encryption and authentication scheme based on chaotic sequences", in SECURWARE 2013, The 7^{th} International Conference on Emerging Security Information, Systems and Technologies, Barcelona, Spain, pp. 150155, IARIA, 25-31 August, 2013.

11) M. Farajallah, S. El Assad, and M. Chetto, "Dynamic adjustment of the chaos-based security in real-time energy harvesting sensors", in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, Beijing, China, pp. 282289, IEEE, 20-23 Aug, 2013.

12) M. Chetto, H. Noura, S. El Assad, and M. Farajallah, "How to guarantee secured transactions with QoS and real-time constraints", in 2012 International Conferece

For Internet Technology And Secured Transactions, London, Uk, pp. 4044, IEEE, 10-12 Dec, 2012.

13) M. Farajallah and M. Abu Taha, "A practical one way hash algorithm (POH), in The 2012 Conference on Innovations in Computing and Engineering Machinery CICEM2012, Amman, Jordan, ACM, Evaluation of reference 6, 9-11 April, 2012.

14) M. A. Taha, M. Farajallah, and R. Tahboub, "A practical one way hash algorithm based on matrix multiplication", International Journal of Computer Applications, vol. 23, 2011.

15) M. AbuTaha, M. Farajallah, R. Tahboub, and M. Odeh, "Survey paper: cryptography is the science of information security", International Journal of Computer Science and Security (IJCSS), vol. 5, no. 3, p. 298, 2011.

16) R. Hamamreh, M. Odeh, and M. Farajallah, "RAMD: Route authentication and misdirection detection protocol", in The 13^{th} IEEE Joint International Computer Science and Information Technology Conference, Chongqing, China, pp. 643648, 20-22 Aug, 2011.

17) M. Farajallah, "Self generating multi key cryptosystem for non-invertible matrices based on hill cipher", Master Thesis, Al-Quds University, Jerusalem, Palestine, Extended Book of reference 11, 2010.

18) R. A. Hamamreh and M. Farajallah, "Design of a robust cryptosystem algorithm for non-invertible matrices based on hill cipher", International Journal of Computer Science and Network Security, pp. 1116, 2009.

19) M. Farajallah and R. Hamamreh, "Self generating multi keys cryptosystem model for non-invertible matrices based on hill cipher", in SAM09 - The 2009 International Conference on Security and Management, Las Vegas, Nevada, USA, pp. 665672, 13-16 July, 2009.