Dr.Prof.Pritam Gajkumar Shah

Contact Information

301 Subhodaya Enclave, Next to PF office RR Nagar Bangalore 560098
Email: wsnpgs@gmail.com
Phone Number: 9964485911

Education

PhD (Information Sciences and Engineering)
University of Canberra, Australia
5 Years Full Time PhD Research in Australia
From 2006 to 2010 with 4 International Scholarships
Dissertation: “An Enhancement of Elliptical Curve Cryptography in the Resource Contained Wireless Sensor Networks”.

M.Tech (Electronics Design Technology)
CEDTI, Dr.Babasaheb Ambedkar University, Aurangabad, MS, India
From August 1995 to August 1998

B.E(Electronics Engineering)
WIT, Solapur, Shivaji University India
From June 1986 to Feb 1991

Work Experience

Currently Professor in Jain University Bangalore since 21st Feb 2017.

RV College of Engineering, Bangalore India
Former Associate Professor (Computer Sciences and Engineering) since 30/07/2014

Sri Venkateshwara College of Engineering, Bangalore India
Professor in ECE and Dean (Research)
From 11/06/2012 to 28/07/2014

Dayanda Sagar Engineering College, Bangalore India
Professor (Electronics & Communication Engineering)
Associate Dean RIIC (Research Industry Incubation Centre) approved by
From 16/07/2011 to 10/06/2012

Canberra Institute of Technology, ACT, Australia
Senior Lecturer for ANU, Australia Associate Degree Students in Circuit Analysis
From Nov 2010 to June 2011

University of Canberra, Faculty of Information Sciences and Engineering, Australia
PhD Scholar and Faculty
From Jan 2008 to Dec 2010

Auckland University of Technology, New Zealand
PhD Scholar and Faculty in WSN Lab.
From March 2007 to Dec 2008

Awards , Scholarships and Research Grants

1.CV Raman Fellowship for International Researchers 2013

2.India Australia Senior Scientist Fellowship 2012

3.Australian Post Graduate Award for PhD, Australia (2009)

4.Auckland University of Technology Scholarship for PhD, New Zealand (2008)

5.University President Scholarship, Australia Australian Patents (2005)

6.Fifth Rank in the University Merit List in B.E. Examination (1991)

7.National Merit Scholarship Holder of India (1984)

Research Achievements as Per Google Scholar

Citation Index – 132

H-index 8

i-10 Index -7

Total PhD students under supervision in VTU Belgavi – 02

Jain University – 04

Phd Thesis Examiner for Curtin University Australia.

Australian and Indian Patents

1. Australian Innovative Patent Number 2009101242, “An apparatus and method for recoding of scalar based on one's complement subtraction for fast scalar multiplication in Elliptical Curve Cryptography for Wireless Sensor Network platform” , in the name of P.G.Shah ,invented by Sharma, Dharmendra; Shah, P. G.; Huang, Xu, sealed on 18/12/2009.

2. Australian Innovative Patent Number 2010100259, “An apparatus and method for Sliding window method with dynamic window size for scalar multiplication on wireless sensor network nodes”, in the name of P.G.Shah , invented by Shah, Pritam G; Huang, Xu ; and Sharma, Dharmendra , sealed on 22/03/2010.

3. Australian Innovative Patent Number 2010100508, “Apparatus and method based on hidden generator point of elliptical curve cryptography for wireless sensor networks”, in the name of P.G.Shah ,invented by Huang Xu; Shah, Pritam G; and Sharma Dharmendra, sealed on 26/05/2010.

4. Australian Innovative Patent Number 2010101116, “Apparatus and method of SPA resistant elliptical scalar multiplication on the resource constrained wireless sensor networks”, in the

name of P.G.Shah, invented by Huang Xu; Shah, Pritam G; and Sharma Dharmendra, sealed on 02/11/2010.

5. Australian Innovative Patent Number 2010100117, “Apparatus and method for selecting window size based on fuzzy controller in elliptical curve scalar multiplication on wireless sensor network platform”, in the name of P.G.Shah, invented by Huang Xu; Shah, Pritam G; and Sharma Dharmendra, sealed on 02/11/2010.

6. Australian Innovative Patent Number 2011100963,”An Apparatus and Method for Optimization of Coordinate System of Elliptical Curve Cryptography on the Wireless Sensor Network platform” in the name of P.G.Shah, invented by Shah, Pritam G; filed on 2011-08-03 .

7. Australian Innovative Patent Number 2010100316, “Apparatus and Method for Elliptical Curve Encryption Based on Hidden Generator Point for Wireless Sensor Networks” in the name of P.G.Shah, invented by Shah, Pritam G; filed on 2010-04-07 .

List of Indian Patents

1. An Apparatus and Method Based on Trust Index of Wireless Node for Multiple/Best Route Discovery Patent Number 712/CHE/2014 under examination.

2. An apparatus and method based on one’s complement subtraction recoding technique of integer in elliptical curve cryptography Patent Number 3204/CHE/2014 under examination.

3. An apparatus and method based on IoT based smart severer for controlling home security appliances Patent Number 5821/CHE/2014 Under Examination

4. An Apparatus And Method Based On Dynamic Window Fuzzy Controller For Scalar Multiplication In Elliptical cryptography patent number 398/CHE/2014 under examination

Selected Publications International Journals (Peer Reviewed)

1. “Securing Wireless Sensor Networks-Challenges and Future Scope” Pritam Gajkumar Shah, Australian Journal of Wireless Technologies, Mobility and Security, Australia, Feb 2012, ISSN 2200-1875, ISSN Online 2200-1883.

2. “Optimization of Co-ordinate System for Elliptical Curve Cryptography in Wireless Sensor Network”, Pritam Gajkumar Shah, Australian Journal of Wireless Technologies, Mobility and Security, Australia, Feb 2012, ISSN 2200-1875, ISSN Online 2200-1883.

3. “Multi-Agent System Protecting from Attacking in Elliptic Curve Cryptography”, Pritam Gajkumar Shah, Xu Huang ,Dharmendra Sharma, Australian Journal of Wireless Technologies, Mobility and Security, Australia, Feb 2012, ISSN 2200-1875, ISSN Online 2200-1883.

4. “Sliding Window Method with Flexible Window Size for Scalar Multiplication on Wireless Sensor Network Nodes” Pritam Gajkumar Shah., Xu Huang, Dharmendra Sharma, Australian Journal of Wireless Technologies, Mobility and Security, Australia, Feb 2012, ISSN 2200-1875, ISSN Online 2200-1883.

5. Algorithm based on one’s complement for fast scalar multiplication in ECC for Wireless Sensor Network, Pritam Gajkumar Shah., Xu Huang, Dharmendra Sharma, Australian Journal of Wireless Technologies, Mobility and Security, Australia, Feb 2012, ISSN 2200-1875, ISSN Online 2200-1883.

Publications International Conferences (Peer Reviewed)

1. “Optimization of Coordinate System for Elliptical Curve Cryptography on Wireless Sensor Network Platform”, Pritam Gajkumar Shah , the 5th IEEE International Conference on Sensing Technology (ICST 2011) , Nov-Dec 2011 at the School of Engineering and Advanced Technology, Massey University, Palmerston North, New Zealand, published.

2. “Analytical Study of Implementation Issues of Elliptical Curve Cryptography for Wireless Sensor networks” Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma in Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference, Perth, Australia April 2010.

3. “Algorithm based on one’s complement for fast scalar multiplication in ECC for wireless sensor network,” Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma, The 3rd International Workshop on RFID & WSN and its Industrial Applications, in conjunction with IEEE AINA 2010, April 20-23, 2010, Perth, Australia.

4. “Multi-Agent System Protecting from Attacking with Elliptic Curve Cryptography,” Xu Huang, Pritam Gajkumar Shah and Dharmendra Sharma, the 2nd International Symposium on Intelligent Decision Technologies, Baltimore, USA, 28-30 July 2010.

5. “Fast scalar multiplication for elliptic curve cryptography in sensor networks with hidden generator point,” Xu Huang, Pritam Gajkumar Shah, and Dharmendra Sharma, CyberC 2010: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, October 10-12, Huangshan, China.

6. “Minimizing hamming weight based on 1’s complement of binary numbers over GF (2m),” Xu Huang, Pritam Shah, and Dharmendra Sharma, IEEE 12th International Conference on Advanced Communication Technology, Phoenix Park, Korea Feb 7-10, 2010. ISBN 978-89-5519-146-2, pp.1226-1230.

7. “Fast Algorithm in ECC for Wireless Sensor Network,” Xu Huang, Pritam Shah, and Dharmendra Sharma, The International Multi Conference of Engineers and Computer Scientists 2010, Hong Kong, 17-19 March 2010. Proceeding 818-822.

8. “Protecting from attacking the man-in-middle in wireless sensor networks with elliptic curve cryptography key exchange,” Xu Huang, Pritam Gajkumar Shah, and Dharmendra Sharma, 4th International Conference on Network and System Security, NSS 2010, Melbourne, Australia, September 1-3, 2010.

9. “Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes,” Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma, International Conference on Wireless Communication and Sensor Computing (ICWCSC 2010), January 02-04, 2010, Chennai, India.

10. “Network Security Protocols for Wireless Sensor Networks - A Survey”, Pritam Gajkumar Shah, International Conference on Cognitive Systems ICCS, 2005, New Delhi India.

11. “Performance Evaluation of Classics Flooding and Gossiping Algorithm for Wireless Sensor Networks”, Pritam Gajkumar Shah, IEEE Conference on Signal and Processing in Mumbai, India 2007.

Travel Grant Received from IEEE

1.“Investigating Effects of Coordinate System on Elliptical Curve Protocols in Wireless Sensor Networks” Pritam Gajkumar Shah, in IEEE International Conference on Future Communication and Networking, on 3rd to 5th April 2012, Baghdad, Iraq accepted for publication and presentation with IEEE international travel and accommodation grant.

Session Chair for International Conference

1. The Fifth International Conference on Information Processing (ICIP-2011) Area: Wireless Communication Engineering and Cryptography on August 07, 2011 - August 09, 2011.
2. The International Conference on Security in Computer Networks and Distributed Systems (SNDS'12), Indian Institute of Information Technology and Management – Kerala Technopark Campus, Trivandrum-695581, Kerala, India.
3. CUBE 2012 International Information Tech. Conference & Exhibition, 3-5 Sept 2012, Pune, India. India's largest and most comprehensive Information Technology Event. (PC Member)

Book

An Enhancement of Elliptical Curve Cryptography for the Resource Constrained
Wireless Sensor Network

Subject Cryptography; Data encryption (Computer science); Wireless communication systems.

Audience Specialized

Bookmark http://trove.nla.gov.au/work/151890047

National Library of Australia- Work ID 151890047

Abstract: Analysis and mathematical modeling of Elliptical Curve Cryptography (ECC) is investigated in this thesis in regard to the Wireless Sensor Networks (WSN). Novel approaches combing use of mixed coordinate system, recoding of integer with One's Complement Subtraction (OCS) method, OCS window method to avoid Special Power Analysis (SPA) attacks, use of Dynamic Window method to avoid node failure and use of hidden generator point to avoid man-in-the-middle attack and use of uni-coordinate public key for WSN have been proposed. These six innovative, novel and industrially applicable algorithms are demonstrated which significantly improve performance of scalar multiplication processes on WSN and demonstrated to achieve node authenticity, data integrity, confidentiality on 8-bit microcontroller of sensor node. These claims are validated using simulation results obtained on MIRACL crypto library and using MATLAB analysis, appropriately provided wherever necessary

Invited Talk in Australia

Organized by: ITE&E Branch, IEE & IET, and Canberra Division Australia.
ENGINEER AUSTRALIA.
Engineering House,
11 National Circuit, , Barton, Australia.
Tuesday 16 March 2010
Topic: Elliptical Curve Cryptography in Wireless Sensor Networks
Event Contact Colleen Mays
Contact Phone +61-2-6270 6519
Contact Email cmays@engineersaustralia.org.au