Bimal Kumar Meher, Ph.D.

Designation : Associate Professor

Department : Department of Computer Science and Engineering

(JOINED THE INSTITUTE IN 2005)

Contact : 9078672241

Email : bimal@silicon.ac.in

RESEARCH INTERESTS

- ✓ Cryptography Based Security
- ✓ Elliptic Curve Cryptosystem
- ✓ Multifactor Authentication
- ✓ WBAN, VANET Security
- ✓ Blockchain Security

Academic Qualifications

Ph. D. (Computer Science), Utkal University, Bhubaneswar,Odisha, India

M.Tech. (Computer Science), Utkal University, Bhubaneswar, Odisha

Teaching Experience/Industrial Experience/Research Experience

- ✓ 25 years Teaching
- ✓ 08 years of Research

PUBLICATIONS

JOURNAL ARTICLES & CONFERENCE PAPERS

[1]. B. K. Meher, "A Study of Suitability and Effectiveness of Various Implementation Options of Finite Field Arithmetic on Elliptic Curve Cryptosystem," International Journal of Computer Theory and Engineering (IJCTE), Vol.1, No.4, pp.389-393 October 2009.

[2]. B. K. Meher and P. K. Meher, "A New Look-Up Table Approach for HighSpeed Finite Field Multiplication," International Symposium on Electronic System Design (IEEE Computer Society Press), Available in IEEE Xplore, Kochi, India, pp.51-55 December 2011.

[3]. B. K. Meher and P. K. Meher, "An Efficient Look-up Table-based Approach for Multiplication over GF(2^m) Generated by Trinomials," Journal ofCircuits, Systems and Signal Processing, Springer, NewYork, Vol.32, No.6, pp.2623-2638, January 2013.
[4]. C. Y. Lee, C. S. Yang, B. K. Meher, P. K. Meher, and J. S. Pan, "LowComplexityDigit-Serial and Scalable SPB/GPB Multipliers over Large Binary Extension Fieldsusing (b,2)-WayKaratsubaDecomposition," IEEE Transactions on Circuits and Systems-I, Vol. 61, No. 11, pp. 3115-3124, November 2014.
[5]. B. K. Meher and P.K. Meher, Analysis of Systolic Penalties and Design of Efficient Digit-LevelSystolic-like Multiplier for Binary Extension Fields,"Circuits, Systems and Signal Processing, Springer Journal, NewYork, Vol. 38, No. 2, pp. 774-790, July 2018.
[6]. B. K. Meher and R. Amin, "A Location-based Multi-factor Authenticationscheme for Mobile devices,"International Journal of Ad Hoc and UbiquitousComputing, Inderscience, August2022.
[7]. B. K. Meher, R. Amin, A. K. Das, M. K. Khan, "KL-RAP: An Efficient Key-less RFID Authentication Protocol Based on ECDLP for Consumer Warehouse Management System", IEEE Transactions on Network Science and Engineering. Vol. 9, Issue5, pp. 3411 – 3420, June 2022.
[8]. D. Pradhan, B. K. Meher, P. K. Meher, "Digit-Size Selection for FPGA Implementation of Generic Digit-Serial Multiplication Over GF (2^m), "1st International Conference on Circuits, Power and Intelligent Systems (CCPIS), Bhubaneswar, India (Available in IEEE Xplore), pp. 1-6, September 2023.
[9]. B. K. Meher, R. Amin, M. Abdussami, V. Sureshkumar, M. A. Hossain, "Efficient Certificateless Anonymous Mutual Authentication in WBANs for Smart Healthcare,"IEEE Transactions on Intelligent Transportation Systems, IEEE (Early Access), June 2024.
[10]. D. Pradhan, P. K. Meher, B. K. Meher, "Input–Output Scheduling and Control for Efficient FPGA Realization of Digit-Serial Multiplication Over Generic Binary Extension Fields,"Circuits, Systems, and Signal Processing, Springer Journal, (Online First), August 2024.

ANY OTHER

Awards

1. 2013 Sydney R. Parker Best Paper Award in the area of Signal Processing by Circuits, Systems and Signal Processing (CSSP), Springer
2. 2013 M.N.S. Swamy Award for being the best paper amongst all the papers published in 2012 and 2013 in CSSP, Springer
3. Best PhD Thesis award for the year 2016 by Computer Society of India (CSI) during the Annual convention of CSI in 2018.