[23] C. Giraud and H. Thiebeauld, \A survey on fault attacks," in Smart Card Research and Advanced Applications VI. Springer, 2004, pp. 159-176.
[24] M. Varchola, M. Drutarovsky, M. Repka, and P. Zajac, “Side channel attack on multiprecision multiplier used in protected ecdsa implementation," in 2015 International Conference on ReConFigurable Computing and FPGAs (ReCon-Fig). IEEE, 2015.
[25] G. McGraw, Software Security: Building Security In. Addison-Wesley Professional, 2006.
[26] S.-R. Oh and Y.-G. Kim, Security requirements analysis for the iot," in Platform Technology and Service (PlatCon), 2017 International Conference on. IEEE, 2017
[27] Xianmin Wei, Peng Zhang, “Research on Improved ECC Algorithm in network and Information Security” International Journal of Security and Its Applications Vol.9, No.2 (2015), pp.29-36
[28] Neetesh Saxena, Narendra S. Chaudhari, Jaya Thomas, “Solution to an Attack on Digital Signature in SMS Security”, International Conference on Modeling, Simulation and Applied Optimization,2013 IEEE
[29] Jie Liu and Jianhua Li “Cryptanalysis and Improvement on a Digital Signature Scheme without using One-way Hash and Message Redundancy”, International Conference on Information Security and Assurance, IEEE 2008.
[30] Lei Niu, Yong Yu, Jianbing Ni, Ying Sun, “Further Cryptanalysis of a Signature Scheme with Message Recovery” International Conference on Intelligent Networking and Collaborative Systems, IEEE 2012.
[31] Jianhong Zhang, Shengnan Gao, “Cryptoanlaysis of a Self-Certified Partially Blind Signature and a Proxy Blind Signature”, WASE International Conference on Information Engineering, IEEE 2009
[32] Xinghua Zhang, “Security Analysis and The Improvement of the sequential multi-signature scheme based on discrete logarithm”, International Conference on Consumer Electronics Communications and Networks,2013 IEEE
[33] Long Zhaohua, Wang Guofeng, "Multi-element Authentication method based on ECDA for Wireless Network," International Symposium on Knowledge Acquisition and Modeling Workshop, IEEE, 2008
[34] Hong Zhong, Rongwen Zhao, Jie Cui*, Xinghe Jiang and Jing Gao, “An Improved ECDSA Scheme for Wireless Sensor Network”, International Journal of Future Generation Communication and Networking Vol. 9, No. 2 2016, pp.73-82.
[35] Hansman, S, Hunt R. A taxonomy of network and computer attacks. Computer and Security, 2005.
[36] M. Varchola, M. Drutarovsky, M. Repka, and P. Zajac, “Side channel attack on multiprecision multiplier used in protected ECDSA implementation," in 2015 International Conference on ReConFigurable Computing and FPGAs (ReCon-Fig). IEEE, 2015.
[37] https://csrc.nist.gov/csrc/media/publications/fips/186/2/archive/2000-01 27/documents/fips186-2.pdf
[38] https://www.ietf.org/proceedings/92/slides/slides-92-lwig-3.pdf

Authors Profile

Dr. Dhanashree K Toradmalle is working as an Associate Professor in the Department of Computer Engineering at K J Somaiya Institute of Technology, Sion, Mumbai. Her research areas include Computer Networks, Information and Network Security, Cyber security.

Dr. Amarendra K is currently working as Professor & HoD, Dept of CSE & IT, KLEF, Vijayawada,Andhra Pradesh. He is an experienced Professor with a demonstrated history of working in the Teaching Industry. Skilled in Computer Science lecturing C / C++ Programming, Data Structures, Algorithms, Software Engineering, Cyber Laws and Security