

- [2] S. Huang and C. H. Shi, "A simple multi-proxy signature scheme," in *Proceedings of the 10th National Conference on Information Security*, Hualien, Taiwan, 2000, pp. 134-138.
- [3] H. Bao, Z. Cao and S. Wang, "Improvement on Tzeng et al's nonrepudiable threshold multi-proxy multi-signature scheme with shared verification," *Applied Mathematics and Computation*, vol. 169, no. 2, pp. 1419-1430, 2005.
- [4] C. Hsu, T. Wu, and T. Wu, "New nonrepudiable threshold proxy signature scheme with known signers," *Journal of Systems and Software*, vol. 58, no. 2, pp. 119-124, 2001.
- [5] J. Hu and J. Zhang, "Cryptanalysis and improvement of a threshold proxy signature scheme," *Computer Standards and Interfaces*, vol. 31, no. 1, pp. 169-173, 2009.
- [6] H. F. Huang and C. C. Chang, "A novel efficient (t,n) threshold proxy signature scheme," *Information Sciences*, vol. 176, no. 10, pp. 1338-1349, 2006.
- [7] S. Mashhadi, "Analysis of frame attack on Hsu et al's non-repudiable threshold multi-proxy multi-signature scheme with shared verification," *Scientia Iranica*, vol. 19, no. 3, pp. 674-679, 2012.
- [8] S. Mashhadi, "A novel non-repudiable threshold proxy signature scheme with known signers," *International Journal of Network Security*, vol. 15, no. 4, pp. 231-236, 2013.
- [9] S. Mashhadi and M. Abdi, "A Secure non-repudiable general proxy signature," *International Journal of Cyber-Security and Digital Forensics*, vol. 4, no. 2, pp. 380-389, 2015.
- [10] S. Mashhadi, "A novel secure self proxy signature scheme," *International Journal of Network Security*, vol. 14, no. 1, pp. 22-26, 2012.
- [11] J. Shao, Z. Cao, and R. Lu, "Improvement of Yang et al's threshold proxy signature scheme," *Journal of Systems and Software*, vol. 80, no. 2, pp. 172-177, 2007.
- [12] H. M. Sun, "An efficient nonrepudiable threshold proxy signature scheme with known signers," *Computer Communications*, vol. 22, no. 8, pp. 717-722, 1999.
- [13] Z. Tan, Z. Liu, and M. Wang, "On the security of some nonrepudiable threshold proxy signature schemes," in *Information Security Practice and Experience*. Heidelberg: Springer, 2005, pp. 374-385.
- [14] C. Y. Yang, S. F. Tzeng, and M. S. Hwang, "On the efficiency of nonrepudiable threshold proxy signature scheme with known signers," *Journal of Systems and Software*, vol. 73, no. 3, pp. 507-514, 2004.
- [15] K. Zhang, "Threshold proxy signature schemes," in *Information Security*. Heidelberg: Springer, 1997, pp. 191-197.



Samaneh Mashhadi

She was born in Tafresh, Iran, on March 27, 1982. She received the B.Sc. and M.Sc. degrees with honors in Mathematics from Iran University of Science and Technology (IUST), and Amirkabir University of Technology (AUT) in 2003 and 2005, respectively. She received her Ph.D. with honors in Mathematics (Cryptography) in 2008 from IUST. She is currently an Assistant Professor in Department of Mathematics of IUST. She is a member of IMS as well. Her research is the analysis, design, and application of digital signatures, secret sharing schemes, security protocols, etc.