List of Publications

International Journal (Published/Communicated)

1. **SK Hafizul Islam**, G. P. Biswas, "A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem", The Journal of Systems and Software (Elsevier Journal), vol. 84, no. 11, pp. 1892-1898, 2011.
2. **SK Hafizul Islam**, G. P. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography", Mathematical and Computer Modelling (Elsevier Journal), vol. 57, no. 11-12, pp. 2703-2717, 2013.
3. **SK Hafizul Islam**, G. P. Biswas, "A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks", Annals of Telecommunications (Springer Journal), vol. 67, no. 11-12, pp. 547-558, 2012.
4. **SK Hafizul Islam**, G. P. Biswas, "An efficient and provably-secure digital signature scheme based on elliptic curve bilinear pairings", Theoretical and Applied Informatics (Polish Academy of Science Journal), vol. 24, no. 2, pp. 109-118, 2012.
5. **SK Hafizul Islam**, G. P. Biswas, "An improved ID-based client authentication with key agreement scheme on ECC for mobile client-server environments", Theoretical and Applied Informatics (Polish Academy of Science Journal), vol. 24, no. 4, pp. 293-312, 2012.

6. **SK Hafizul Islam**, G. P. Biswas, "Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings", Journal of King Saud University - Computer and Information Sciences (Elsevier Journal), vol. 25, pp. 51-61, 2013.

7. **SK Hafizul Islam**, G. P. Biswas, "Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography", International Journal of Computer Mathematics (Taylor & Francis Journal), 2013. DOI:10.1080/00207160.2013.776674.

8. **SK Hafizul Islam**, G. P. Biswas, "A Provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings", Journal of King Saud University - Computer and Information Sciences (Elsevier Journal), 2013. DOI:10.1016/j.jksuci.2013.03.004.

9. **SK Hafizul Islam**, G. P. Biswas, "An efficient and secure strong designated verifier signature scheme without bilinear pairings", Journal of Applied Mathematics and Informatics (Korean Journal), vol. 31, no. 3 - 4, pp. 425 - 441, 2013.

10. **SK Hafizul Islam**, G. P. Biswas, "Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings", Journal of King Saud University - Computer and Information Sciences (Elsevier Journal)(Accepted).

11. **SK Hafizul Islam**, G. P. Biswas, "Cryptanalysis and improvement of a password-based user authentication scheme for the integrated EPR information system", Journal of King Saud University - Computer and Information Sciences (Elsevier Journal)(Accepted under minor revision).

12. **SK Hafizul Islam**, G. P. Biswas, "A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication" (Communicated).

13. **SK Hafizul Islam**, G. P. Biswas, "Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system" (Communicated).
14. **SK Hafizul Islam**, G. P. Biswas, "An efficient and secure ECC-based three-party authenticated key exchange protocol for mobile commerce environments" (Communicated).
15. **SK Hafizul Islam**, G. P. Biswas, "Design of two-party authenticated key agreement protocol based on ECC and self-certified public keys" (Communicated).
16. **SK Hafizul Islam**, G. P. Biswas, "Provably secure and pairing-based strong designated verifier signature scheme with message recovery" (Communicated).
17. **SK Hafizul Islam**, G. P. Biswas, "Dynamic ID-based remote user authentication scheme with smart cards using elliptic curve cryptography" (Communicated).
18. **SK Hafizul Islam**, G. P. Biswas, K-K. R. Choo,"Cryptanalysis of an Improved Smartcard-based Remote Password Authentication Scheme" (Communicated).
19. **SK Hafizul Islam**, G. P. Biswas, "Cryptanalysis of Lin et al.'s digital multi-signature scheme on the generalized conic curve over Z_n" (Communicated).

International Conference (Published/Communicated)

1. **SK Hafizul Islam**, G. P. Biswas, "An improved remote login scheme based on ECC", In: Proceedings of the International Conference on Recent Trends in Information Technology, pp. 1221-1226, 2011.

2. **SK Hafizul Islam**, G. P. Biswas, "Comments on ID-based client authentication with key agreement protocol on ECC for mobile client-server environment", In: Proceedings of the International Conference on Advanced in Computing and Communications, CCIS, Springer-Verlag, Part II, vol. 191, pp. 628-635, 2011.

3. **SK Hafizul Islam**, G. P. Biswas, "Design of an efficient ID-based short designated verifier proxy signature scheme", In: Proceedings of the International Conference in Recent Advances in Information Technology, pp. 48-53, 2012.

4. **SK Hafizul Islam**, G. P. Biswas, "An improved pairing-free identity-based authenticated key agreement protocol based on ECC", In: Proceedings of the International Conference on Communication Technology and System Design, Procedia Engineering, vol. 30, pp. 499-507, 2012.

5. **SK Hafizul Islam**, G. P. Biswas, "Certificateless strong designated verifier multisignature scheme using bilinear pairings", In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 540-546, 2012.