Abstract

Smart Grid is a modern digital metering system that has been introduced to replace the traditional electricity infrastructure by collecting and utilizing information generated from different consumers automatically. Many researches have been conducted on the secure communication sessions to address the key issue of security in smart grid communication. Existing secure anonymous key distribution scheme for smart grid brings challenge such as key escrow problem in identity based encryption and identity based signature. In this paper we incorporate the first concept of certificateless in order to solve the key escrow problem that is found in identity based signature scheme and an identity based encryption scheme. Our proposed scheme achieves key escrow resilience which has not been achieved by previous work in this field.

References

1. Yan, Y., Qian, Y., Sharif, H. and Tipper, D. 2013 A Survey on Smart Grid Communication
Infrastructures: Motivations, Requirements and Challenges, IEEE Comm. Smart Grid
2. Fang, X., Xue, G., Yang, D., and Misra, S. 2012“Smart Grid-The New and Improved
Smart Grid
IEEE Security Privacy
6. Communications in smart distribution grid, IEEE Trans. Smart Grid
Security Privacy
Supportive Analyses and References. [Online]. Available:
11. Y. Strengers, 2010. Smart metering demand management programs: Challenging the
12. J. L. Tsai, N. W. Lo, 2015. Secure Anonymous Key Distribution Scheme for Smart Grid,
IEEE Trans. Smart Grid
CRYPTO, Santa Barbara, CA, USA
off-line dictionary attacks, in Information Security and Privacy Research. Berlin, Germany:
Springer-Verlag
15. Y. Wang, 2013. Efficient identity-based and authenticated key agreement protocol, in
Transactions on Computational Science XVI. Berlin, Germany: Springer-Verlag
17. J. H. Park, M. Kim, and D. Kwon, 2013. Security weakness in the smart grid key
distribution proposed by Xia and Wang, IEEE Trans. Smart Grid
18. S. Finster, 2013. Smart meter speed dating, short-term relationships for improved
privacy in smart metering, in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm),
Vancouver, BC, Canada, pp. 426431
IEEE Trans. Smart Grid
20. Recommendation for Key Management, Part 1: General,
22. J. L. Tsai, N. W. Lo, and T. C. Wu, Novel anonymous authentication scheme using
Grid
Proc. CRYPTO, Santa Barbara, CA, USA
Certificateless Secure Anonymous Key Distribution Scheme for Smart Grid

Cryptol. (CRYPTO), Santa Barbara, CA, USA


29. M. Myers, R. Ankney, A. Malpani, S. Galperin, and C.


**Index Terms**

Computer Science  Security

**Keywords**

Certificateless, anonymity, Smart Grid, Smart Meters.