Abstract: Efficient Privacy-preserving Path Authentication using RFID for Supply Chain Management

Younho Lee[1], Yongsu Park[2]
[1] *Department of Information and Communication Engineering, Yeungnam University, Korea, younholee@yu.ac.kr*
[2] *Division of Computer Science and Engineering, Hanyang University, Korea, yongsu@hanyang.ac.kr*

Abstract

This paper presents a privacy-preserving path-authentication method using RFID for supply chain management (SCM). Compared to past work, our scheme employs only symmetric encryption and message authentication code, which reduces the computation and communication overhead, while the proposed method also supports high-level privacy without using the tamper-proof tags as [1]. Performance analysis demonstrates that the proposed scheme needs less than 1% of clock cycles and 50% tag storage compared to [1].

Acknowledgement

This work was supported by the 2011 Yeungnam University.