Cryptology ePrint Archive: Report 2013/206

Privacy-Preserving Billing for e-Ticketing Systems in Public Transportation

Florian Kerschbaum and Hoon Wei Lim and Ivan Gudymenko

Abstract: Many electronic ticketing systems for public transportation have been deployed around the world. Using the example of Singapore's EZ-Link system we show that it is easy to invade a traveller's privacy and obtain his travel records in a real-world system. Then we propose encrypted bill processing of the travel records preventing any kind of privacy breach. Clear advantages of using bill processing instead of electronic cash are the possibility of privacy-preserving data mining analyses by the transportation company and monthly billing entailing a tighter customer relation and advanced tariffs. Moreover, we provide an implementation to demonstrate the feasibility of our solution.

Category / Keywords: cryptographic protocols / e-ticketing system, location privacy, privacy-preserving bill computation, privacy-preserving data mining

Date: received 9 Apr 2013, last revised 9 Apr 2013

Contact author: hoonwei at ntu edu sg