Cryptology ePrint Archive: Report 2013/027

Anonymity Guarantees of the UMTS/LTE Authentication and Connection Protocol

Ming-Feng Lee and Nigel P. Smart and Bogdan Warinschi and Gaven Watson

Abstract: The UMTS/LTE protocol for mobile phone networks has been designed to offer a limited form of anonymity for mobile phone uses. In this paper we quantify precisely what this limited form of anonymity actually provides via a formal security model. The model considers an execution where the home and roaming network providers are considered as one entity. We consider two forms of anonymity, one where the mobile stations under attacked are statically selected before the execution, and a second one where the adversary selects these stations adaptively. We prove that the UMTS/LTE protocol meets both of these security definitions. Our analysis requires new assumptions on the underlying keyed functions for UMTS, which whilst probably true have not previously been brought to the fore.

Category / Keywords: applications /

Date: received 21 Jan 2013, last revised 25 Jan 2013

Contact author: nigel at cs bris ac uk