A provably secure mix-net

Andrea Huszti[a], **Zita Kovács**[b]

[a]Faculty of Informatics
University of Debrecen
Debrecen, Hungary
huszti.andrea@inf.unideb.hu

[b]Faculty of Informatics
University of Debrecen
Debrecen, Hungary
kovacs.zita@inf.unideb.hu

Abstract

Depending on the nature and purpose of a communication, different security requirements should be accomplished. One of the most important properties is the anonymity, *i.e.* participants would like to stay hidden - or nameless -, the messages transferred cannot be linked to the sender.
In 2015 we constructed an anonymous channel, which besides anonymity provides secrecy of the messages, verification of the sender's eligibility, the possibility of answering to a message sent anonymously (anonymous reply), and in certain well-defined circumstances the possibility of revealing the senders's real identity (anonymity revocation). Applying symmetric encryption it efficiently handles arbitrarily long messages. Moreover, we used bilinear mappings for increasing the efficiency.
There are many methods (formal, simulation and experiment based techniques) to prove that a system possesses a security requirement, the goal of provable security is to provide a mathematical guarantee for that. In our case the most important objective is to prove that the mix network achieves senders' anonymity. Reductionist proofs are employed with the help of game based security definitions. The security property for a cryptographic scheme is defined as a game between a challenger and an adversary, and security is usually shown by reducing the problem of winning the game to the problem of breaking some underlying hard problem. After giving the definitions for anonymity and some variations of the Diffie-Hellman problem, we claim that if an attacker is capable of breaking the anonymity, than he can solve the hard problems.

Keywords: mixnet, anonymity, secure communication, bilinear pairings

MSC: 94A60, 11T71