A Hybrid Mix based on Bilinear Maps*

Andrea Huszti[a], **Zita Kovács**[b]

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

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

Abstract

We introduce a hybrid mix network based on bilinear maps. A mix is a cryptographic construction for providing anonymity of the sender. Our solution is based on a mix proposed in [1]. Messages are encrypted via symmetric encryption, increasing efficiency of the submission process. There are cases when a sender does not submit all the documents necessary, or after opening the submission the committee needs more documents. Our solution enables postulating supplements. We modified the one-way mix in [1], so that the receiver is capable of resending a message to the anonymous sender. This extension makes for the principle possible communicating with the sender without revealing his anonymity, and decreasing efficiency of the mix. We provide eligibility verification and the revocation of the sender's anonymity when it is necessary without a trusted third party.

Zhong proposed an identity-based mix [2] which based on bilinear maps and it is only appropriate for sending short messages. Our mix is length-flexible, which means it efficiently handles short and long messages.

We applied commitment schemes, blind signatures, secret sharing and distributed anonymity revocation to accomplish the desired security requirements. Our solution based on bilinear maps and thus saves significant communication and computational costs.

References

[1] Ohkubo, M., Abe, M., A Length-Invariant Hybrid Mix, *Advances in Cryptology - ASIACRYPT* LNCS Vol. 1976 (2000), 178–191.

[2] Zhong, S. Identity-based Mix: Anonymous Communications without Public Key Certificates, *Comp. and Elect. Eng.*, Vol. 35(5) (2009), 705–711.

*The publication was supported by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project has been supported by the European Union, co-financed by the European Social Fund.