**ETSWD002-2016-Efficient Anonymous Message Submission**

**Abstract** — In online surveys, many people are reluctant to provide true answers due to privacy concerns. Thus, anonymity is important for online message collection.Existing solutions let each member blindly shufﬂe the submitted messages by using an IND-CCA2 secure cryptosystem. In the end, the message sender’s identities are protected since no one knows the message submission order. These approaches cannot efﬁciently handle groups of large size. In this paper, we propose an efﬁcient anonymous message submission protocol aimed at a practical group size. Our protocol is based on a secret sharing scheme and a symmetric key cryptosystem. We propose a novel method to aggregate members’ messages into a message vector such that a group member knows only his own position in the submission sequence. The protocol is accountable for capturing malicious members breaking the protocol execution. We provide a theoretical proof showing that our protocol is anonymous under malicious attacks. We also discuss our simulation results to demonstrate the efﬁciency of our protocol.