1125-94-1508 **Wentao Huang**, **Michael Langberg** and **Joerg Kliewer*** (jkliewer@njit.edu), New Jersey Institute of Technology, Department of Electrical and Computer Eng., Newark, NJ 07102, and **Jehoshua Bruck**. *Communication Efficient Secret Sharing.*

A secret sharing scheme is a method to store information securely and reliably. Particularly, in a threshold secret sharing scheme, a secret is encoded into n shares, such that any set of at least t_1 shares suffice to decode the secret, and any set of at most $t_2 < t_1$ shares reveal no information about the secret. Assuming that each party holds a share and a user wishes to decode the secret by receiving information from a set of parties; the question we study is how to minimize the amount of communication between the user and the parties. We show that the necessary amount of communication, termed "decoding bandwidth", decreases as the number of parties that participate in decoding increases. We prove a tight lower bound on the decoding bandwidth, and construct secret sharing schemes achieving the bound. Particularly, we present a scheme that achieves the optimal decoding bandwidth when d parties participate in decoding, universally for all $t_1 \leq d \leq$. (Received September 17, 2016)