1072-68-232 **Ali Bagherzandi** and **Stanislaw Jarecki*** (stasio@ics.uci.edu), CA, and **Nitesh Saxena** and **Yanbin Lu**. *Password-Protected Secret Sharing.*

We revisit the problem of protecting user's private data against corruption of user's storage. To this aim we introduce Password-Protected Secret-Sharing (PPSS), which allows for secret-sharing user's data among n trustees in such a way that (1) the user can reconstruct the data by entering the correct password into a reconstruction protocol involving at least $t + 1$ honest trustees, and (2) the data remains secret even if the adversary corrupts t trustees, with the level of protection expected of password-authentication, i.e. the probability of leaking the secret is at most q/D where q is the number of reconstruction instances and D is the size of the dictionary from which user's password was chosen. We show an efficient PPSS protocol secure under the DDH assumption using three messages between the user and each server, each with constant bandwidth. As side benefit we obtain a Threshold Password Authenticated Key Exchange (T-PAKE) protocol with lower round, communication, and server computation complexities than existing T-PAKE's. (Received June 28, 2011)