

1072-68-201

Maggie Habeeb*, Mathematics Department, 365 Fifth Avenue, New York, NY 10016, and
Delaram Kahrobaei. *A New Secret Sharing Scheme using Non-abelian Groups*.

Threshold secret sharing schemes are a method to distribute a secret among n persons in such a way that any t , where $0 < t \leq n$, of the participants can recover the secret, but no $t - 1$ participants can. In this talk, we propose two new secret sharing schemes using non-abelian groups and the word problem. One scheme is the special case where all the participants must get together to recover the secret; that is, $t = n$. The second scheme we propose is a (t, n) -threshold scheme that is a hybrid of Shamir's scheme and the group theoretic scheme. (Received June 28, 2011)