1020-94-164 **Brian King*** (briking@iupui.edu), Department of Elec. & Comp. Eng., 723 West Michigan Street, SL160, Indianapolis, IN 46202, Indianapolis, IN 46202. *Group Independent Secret Sharing: properties and constructions.*

Secret sharing is a cryptographic tool used to protect secret keys from being compromised. In this scenario, the secret key is shared out to a set of participants in such a manner that authorized sets of participants can reconstruct the key, whereas unauthorized sets of participants cannot recover any information concerning the key. A t out of n threshold secret sharing scheme is a secret sharing scheme for which the any set of t or more participants is an authorized set, and any set of less than t participants is unauthorized. Common methods to construct threshold sharing schemes, usually require that the secret key space possesses special algebraic properties, for example that the key space is a finite field.

A group-independent sharing scheme is a threshold secret sharing scheme that can be utilized over any finite abelian group. The topic of group-independent sharing, sometimes called Black-box threshold sharing was first introduced in the connection of creating a threshold sharing scheme for RSA keys.

In this talk we will discuss black-box secret sharing, we will then discuss equivalent definitions of black-box secret sharing, properties and the necessary requirements for black-box secret sharing and constructions for a black-box secret sharing scheme. (Received August 26, 2006)