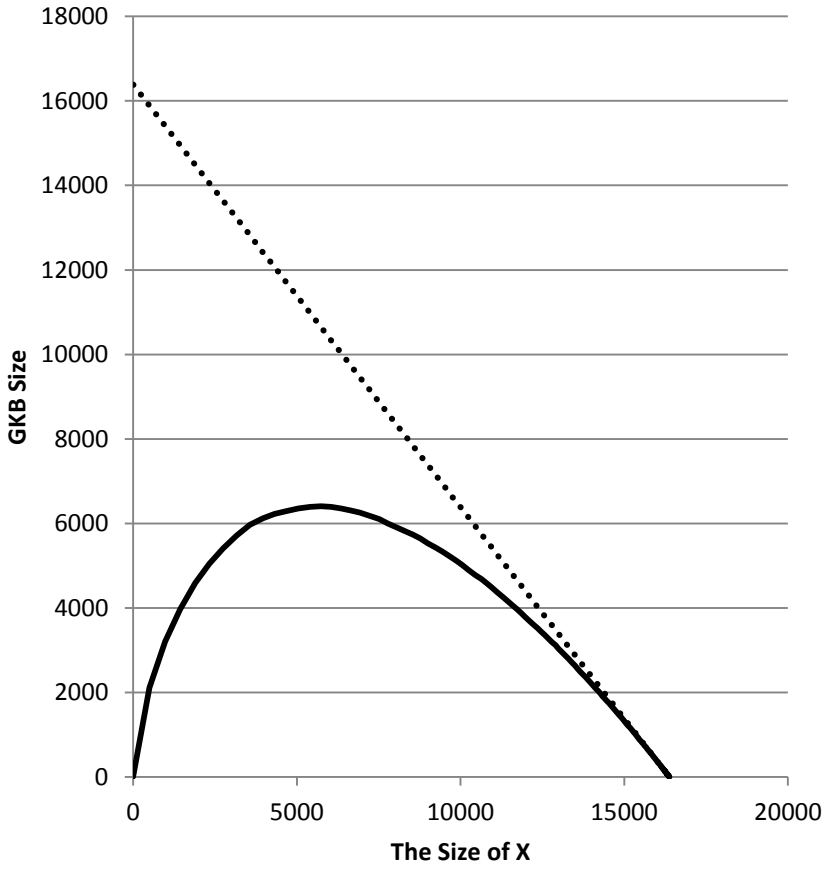
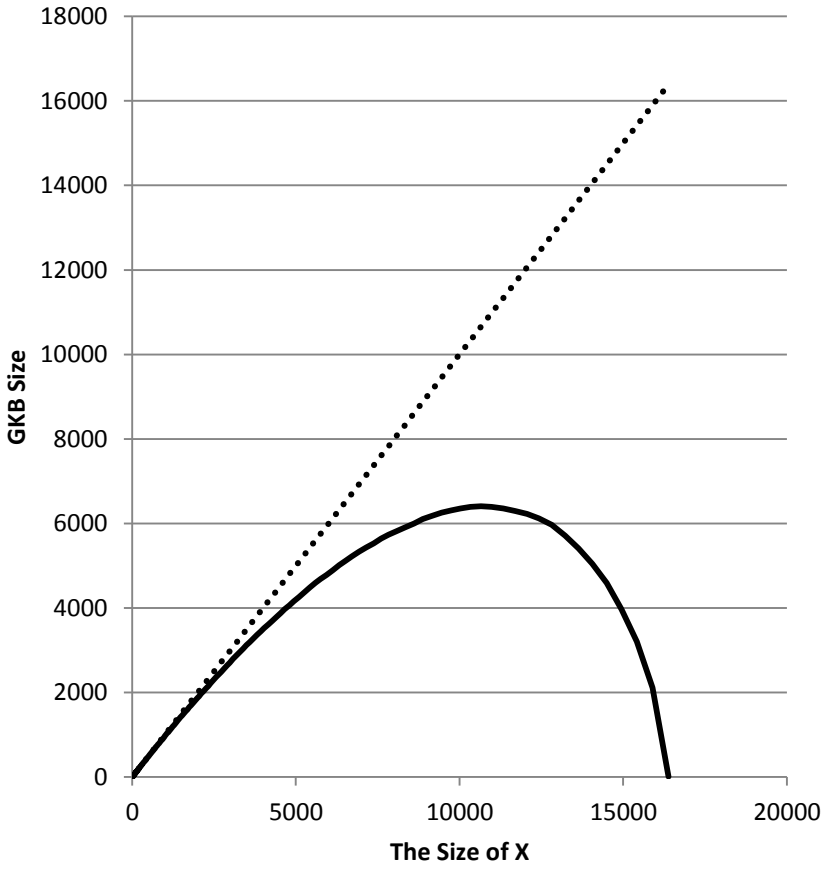
A Proposal to introduce a new flag for group leave into the group manipulation command

- Let G(X) be the GKB which covers the group X. And, let G'(X) be the smallest GKB which covers the compliment of X, i.e. U – X, where U is the whole set.
- The size of G(X) is in general larger than G'(X) if the number of members in X is larger than half of the entire group. (The members of X are randomly chosen.)
- Then, it is better to use G'(X) rather than G(X) to create the group X.
- Note that we can certainly judge which of G(X) and G'(X) is larger if we create both G(X) and G'(X)

GKB Size



The GKB covers U-X,
where U is the whole set



The GKB covers X

Cont'd

- We propose to add a new function to the group manipulation command:
- Suppose a group manipulation command is issued to create a group X and accompanies a GKB G'. Behavior of a recipient is shown in the following table (Cf. the table in the next page which shows behavior for a current command):

	Currently in X	Currently not in X
Covered by G'	Leave X	Do Nothing
Not covered by G'	Do Nothing	Join in X

- We only need a flag in the group manipulation command which indicates if the accompanying GKB is for "join" or "leave"
- Note that we cannot use this new group manipulation command to deliver a group key.

Cont’d

	Currently in X	Currently not in X
Covered by G	Do Nothing	Join in X
Not covered by G	Leave X	Do Nothing