NAME: AUSTIN OWINO WETOYI
REG NO.: P80/85241/12
COURSE: DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE
YEAR: 2014
TITLE: DYNAMIC SUBSET DIFFERENCE REVOCATION USING ONE BINARY TREE
ABSTRACT

Broadcast Encryption (BE), means transmitting information that anyone listening can access but only those selected by the transmitter, using a suitable criteria, can understand. An example is the pay TV system an existing solution known as the Subset Difference Revocation (SDR) performs this in a stateless manner i.e. once the system is set up, new receivers are not allowed to join though existing receivers can each be revoked and restored as necessary. The statelessness can lead to unnecessary high key storage for a receiver and messaging overhead due to potentially poor adjacency of receivers to each other on the binary key tree when the number of receivers is much smaller than the number of potential receivers

This thesis is about a scheme that converts the static SDR into a dynamic SDR scheme. Rather than use multi-tree solution which employs multiple equally sized binary trees known as allocation units that are added and discarded on demand, it uses a single binary tree that shrinks and grows on demand.

When the positions to be assigned to active members all get filled, the tree grows by one level rather than breadth. Similarly, when the members is not more than half the tree capacity, the tree shrinks by one level. Therefore, there is no need to know the maximum number of potential receivers in advance, a value that can be difficult to estimate in practice

In this thesis, we investigated how this solution compares in efficiency to the multi-tree solution that uses allocation units in terms of key storage at the receiver, the multicast cost and the inevitable unicast cost. The methodology used is simulation.

The results obtained show that the single - tree solution in typical usage performs, at worst, like the multi-tree solution and this is the major contribution

Keywords: dynamic scheme, broadcast encryption, stateless scheme, binary tree, key tree.