DANIEL PANARIO, Carleton University, 1125 Colonel By Dr., Ottawa

The distribution of the number of encryptions in revocation schemes for stateless receivers

We consider the problem of a center broadcasting an encrypted message to a group of users such that some subset is considered revoked and should not be able to obtain the content of the broadcasted message even if all revoked users collaborate. Various encryption schemes have been proposed to solve this problem which arises, for example, with pay-TV and satellite communications.

In one class of proposed schemes the center distributes a unique combination of keys to each user who decrypts the message individually. If keys cannot be updated once distributed the receivers are called stateless. Several key distribution schemes use a balanced binary tree structure. Some examples that we consider are the complete subtree scheme (CST), introduced independently by Wallner, Harder and Agee (1998), and Wong, Gouda and Lam (1998), the subset-difference scheme (SD), introduced by Naor, Naor and Lotspiech (2003), and the layered subset-difference scheme (LSD) by Halevy and Shamir (2002).

Park and Blake (2006) give generating functions that entail the exact mean number of encryptions for the above key distribution schemes. We extend their results by showing that the distribution of the number of encryptions is asymptotically normal.

This is joint work with C. Eagle, Z. Gao, M. Omar, and B. Richmond.