**Section 02**

**Muhammad Aasif Mustafa**

**Aamir Ali**

**Voting Protocols**

1. As we know that,

Ci = (Ci-1 + Vi) % n

Where, n is the mod, and Ci is the voter encrypted sum, Ci-1 is the previous voter encrypted sum and Vi is the voter vote.

Now, if we replace each Ci-1 in Ci, we get:

Ct = (C0 + S) % n

Where, Ct is the counter encrypted sum, C0 is the initial random initialized key and t is the last voter.

Solving the equation, we get following. As n > t, then repeated modulo gives same answer.

S = (Ct – C0) % n ---------- (1)

Hence, the sum of total votes is calculated as the equation (1).

1. The distribution of the encrypted key C is uniform for all voters and lies between 0 and n - 1 because of the mathematical operation modulo. The modulo n restricts the encryption key for each voter between 0 and n – 1. Hence, the distribution is normal.

From the security point of view, if any random person vote is to be found, then for this its previous voter encryption key must be known, without it the vote cannot be found. In other words, to find any person’s vote, the encryption key of previous voter is required. Hence, the voting system protocol is full secured.

1. For any two voters i, j, they need to have only one voter k between them, such that if the Ci and Cj collude together, and Ci and Cj of both of them remain same, then k’s vote is 0, and if the Ci and Cj changes, then the k’s vote is 1.  
   Hence, the indices of voter i, k and j are for any random index ‘a’ between 1 and n - 2, the indices are “a”, “a+1” and “a+2”.