Secrect Sharing Progress

Joan Ngure

Report

cheating and cheater detection:
We know that the secret is shared using IDA while the key using perfect secrecy like shamir's secret sharing scheme. A strategic cheater knows that, submitting a wrong share of the secret will go undetected yes but he can't reconstruct the secret while deceiving others to reconstructing the incorrect secret. This is because the bit of the secret that was wrongly reconstructed is had to trace. If we have a (3,n) scheme, they know that after reconstruction the secret will be of the form $E_1E_2E_3$. After submitting an incorrect share, some or all parts maybe incorrectly reconstructed, even after gaining access to the key, you can't reconstruct the secret.
The best strategy is to submit an incorrect share of the key. The cheater can use the method we saw earlier on since in this protocol the identities are not hidden. The cheater calculates a different polynomial where by at 0 the line passes through -1 while for other identities, the line passes through 0. They therefore succeed in obtaining the secret while deceiving others. The cheater goes undetected unless the initial secret was 0.
We can use the same method we say earlier on, to prevent cheating during reconstruction of the key. That is, we make the identities private and issue different shares of the key such that the parties we reconstruct a dummy value say S which is never used as the value of the secret and the secret itself. Here we can detect cheating in key shares with a non-negligible probability.
How can we detect cheating in the overall scheme? In this paper they proposed distributed fingerprints. You submit your share, together with a fingerprint that cannot be forged.