Secrect Sharing Progress

Joan Ngure

Report

Perfect Secrecy:
A ciphertext should not leak any additional information an attacker has prior about the plaintext.
Mathematically this can be expressed as:
An encryption scheme (gen, enc, dec) with message space M and ciphertext space C is perfectly secure iff every probability distribution over M, $\forall$m $\in$ M and $\forall$c $\in$ C with Pr(C = c) > 0 then;

$$\Pr(\text{M=m} \mid \text{C=c}) = \Pr(\text{M} = \text{m})$$

A secret sharing scheme where by shares less than the threshold leak information about secret, satisfy correctness but not secrecy (yet to find a good example).

Cheater detection:
(example lifted from previous report)
secret = $6 \in \mathbb{Z}_7$
scheme (3,5)
$P_1(1,5), P_2(2,5), P_3(3,6), P_4(4,1), P_5(5,4)$
The first three people put their shares together to reconstruct the secret. Person one decides to cheat and gives an incorrect share. The secret reconstructed is legal ($\in \mathbb{Z}_7$) but incorrect ($s' \neq s$). The cheater goes undetected since the secret is legal. [1] shows how a cheater can successfully deceive t-1 participants whereby, they reconstruct the incorrect secret and from that the cheater can learn the correct secret.
If participant one decides to cheat, he interpolation to construct a polynomial f′(x) of degree at most t-1 such that f′(0) = -1 and $f'(P_2) = \cdots = f'(P_t)$=0.
The participant therefore announces instead their share + $f'(P_1)$. Interpolation guarantees that t participants will reconstruct the polynomial f(x)+f′(x) which has constant term f(0)+f′(0) = secret - 1. Cheating will go undetected unless the secret happened to be 0. (Tried this with the above example but still don't get the correct answer. Maybe I am making mistakes somewhere in calculations or missing a concept.)