Page No.
Date

POIS EVAL 2

Rishabh Singhal
20171213

Given: k blocks of data/info (to store) in fault tolerent way using error code (e) size such that total no. of block (n)

$(k+e) \le n < k+2e$

For this we can, assume $c_1, c_2, \ldots, c_k$ (k blocks) then

A polynomial: $P = \sum_{i=1}^{k} c_i x^{k-i}$

$\Rightarrow P = c_1 x^{k-1} + c_2 x^{k-2} + \ldots + \underbrace{c_k x^0}_{c_k}$

Generate n points randomly using this polynomial i.e. $P(x_i) = x_i$

or $(x_i, P(x_i))$ pairs for $\boxed{1 \le i \le n}$

lets say e blocks are ~~are~~ corrupted out of these n blocks,

and using lagrange interpolation, we ~~need~~ can unique construct polynomial of degree m with (m+1) points

So, here k points are needed to construct back the original (P).

$\therefore \quad n - e \ge k \Rightarrow (k+e) \le n$

also from info theory ~~k~~ $\underline{n < k+2e}$

hence, using this method $\Rightarrow$ $k+e \le n < k+2e$

We can use digital signature to detect which of these are corrupted.

Page No.
Date

So, the exact steps :-

(*) → For given k blocks, generate k degree polynomial.
(*) Generate random (k+e) points (n) where e is maximum (no. of block which can be corrupted)
(*) Sign all ~~block~~ points & send.
(*) if ~~any~~ for any pair of (m, Sign(m)) ~~do~~ is not correct (we can discard it)
(*) And ~~for a~~ from remaing k uncorrupted blocks can generate the polynomial back & hence will get k blocks as its coefficients.