Principles of Information Security

Indranil Pradhan

2019202008

MTech in CSIS

Question:- To store *k* blocks of data/information (say each block is of *b* bits) in a fault-tolerant way, you may encode the *k* blocks into *n* blocks (using some error-correction code) such that if any *e* of the *n* blocks are corrupted, it is still possible to retrieve the original *k* blocks of information. Specifically (for large enough *b*), coding theory suggests that this is possible if and only if $n >= (k + 2e)$. However, *show that using digital signatures, it is possible to achieve the above fault-tolerant storage even when* $(k + e) <= n < (k + 2e)$, assuming a PPTM-adversary and a negligible probability of error is permitted.

Answer:- We have k blocks of data, that needs to be encoded such that even if e blocks are corrupted we can retrieve the original k blocks.

Using something similar to Secret Sharing we can achieve that. If $c_1, c_2, c_3, \ldots\ldots, c_k$ are the k blocks to shared.

Define a polynomial,

$$Q = \sum c_i x^{k-i}$$

i.e, $Q = c_1 x^{k-1} + c_2 x^{k-2} + c_3 x^{k-3} + \ldots\ldots\ldots + c_k x^0$

We generate n points using randomly generated x.

i.e, $(x_0,Q(x_0)); (x_1,Q(x_1)); (x_2,Q(x_2)),\ldots\ldots\ldots\ldots.(x_{n-1},Q(x_{n-1}))$ n blocks.

Out of the n blocks, if at least e blocks are corrupted the (n-e) are left uncorrupted.

We need at least e points to solve a polynomial of degree (e-1) as straight line needs 2 points (degree 1).

So here k points are needed to solve a k-1 degree polynomial.

Hence,

$$n-e >= k ,$$

implies that $(k+e) <= n$

and from information theory it is that $n >= (k+2e)$

so it implies that, $(k+e) <= n <(k+2e)$

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

And the procedure follows as-

1. For k blocks generate a (k-1) degree polynomial with coefficients as each of the blocks.
2. We generate n = (k+e) points from the polynomials.
3. For each of these points we use a digital signature to tag the blocks.
4. Send each of these n = k+e blocks to the receiver.
5. Out of these n blocks, e blocks got corrupted and can be detected using digital signature.
6. The uncorrupted (n-e) = k blocks will help recovering the polynomial again.

This is how the message can be retrieved again