POIS Evaluation 5

V.A. Lalitha
Kameswari
2017102S

In eval II, k blocks of information, we encode it into n blocks, such that even if atmost e are corrupted, we can still get back the k.

Now, similarly, we have the task of building a routing scheme where

- Sender and receiver have n different connections / routes
- Send k blocks of information without any corruption, even if at max e out of the n connections are damaged

Idea based on Evaluation-2

- Let's say we have e corrupt channels out of the n.
- The condition which is needed to satisfy this is $n - e \geq k$, where n = # total
  e = # corrupt
  k = number of blocks to be transmitted

Now, let d be the total data which needs to be sent across, we split into $d = d_0 d_1 \cdots d_{k-1}$ and do the same as we have done in Evaluation 2

- Create a k^{th} degree polynomial and get the k coefficients of our polynomial $f(x)$.
- Take the d blocks, put them into n blocks - $c_1, c_2 \cdots c_n$ such that
  $C_i = \{x, f(x), \text{sign}(\text{Hash}(f(x)))\}$
  where x is picked randomly from 1 to n

Scanned with CamScanner

Now when the receiver gets the k n blocks, we reconstruct the polynomial and get the k blocks.

Now, we use El Gamal public key cryptosystem to design a Robust Oblivious Transfer protocol between a client A and server B, where A has some index i, and B has an array.

We are given four different situations, and have to comment on e. We will first look at OT.

OBLIVIOUS TRANSFER PROTOCOL

→ Let A be the client who has some number between 0 and k-1, call it i.

→ Now, let B be the server who has an array B to k elements

→ Goal is for A to know bi

→ El Gamal can be used for encryption and decryption.

Now, A will send a random array R consisting of k elements to B.

Each $r_i = Enc_{K_B}(r)$ where K_B is the public key of B.

When B gets the array R, he can do:

$$D = [Dec_{K_B}(r_1), \ldots r, \ldots Dec_{K_B}(r_k)]$$

Now, using D, B will create a new array, say D'.

Scanned with CamScanner

$D' = [Dec_{K_B}(r_j) \oplus b_j \quad \forall 1 \le j \le k]$

This D' is sent to A, who can get the value of b_i by doing $D'[i] \oplus i$

Here, we see that B need not know which i is A asking for, but still A can get only b_i and not any other element.

Now, we will look at the El Gamal algorithm

Generation of the key.

→ B generates prime p and a generator g of the group $\mathbb{Z}_p$.

→ Chooses x randomly from 1 to p-1. This becomes the private key.

→ $h = g^x \bmod p$.

K_B = public key.

$= \{h, p, g\}$

Encryption

→ Let m is the message in plaintext

→ y = random number between 1 to p-1.

→ $s = h^y \bmod p$

$c_1 = g^y \bmod p$

$c_2 = ms \bmod p$

→ Now A sends (c_1, c_2) to B.

Decryption

→ $s = c_1^x \bmod p$

$p = g^{x.y} \bmod p$

$s^{-1} = s^{p-2} \bmod p$

→ $m = c_2 s^{-1}$

$= c_2 s^{p-2} \bmod p$

Now, let us look at the 4 situations given in the question

Scanned with CamScanner

Case I: Public keys of A and B are known to all

→ All clients know K_B, so they can use El Gamal.

→ OT is possible.

→ Just like evaluation II,

$(n-k) \geq e$

where n = total number of channels

k = number of blocks to be transfered

Case II: Public key of A is known to B, but public key of B is not known to A.

→ Nobody knows K_B, so El Gamal and OT are not possible

→ So, first K_B should be transferred using the robust channel

→ So, if the size of K_B is some λ blocks, we get

$e \leq \min\left((n-k), (n-\lambda)\right)$

as our new condition.

Case III: Public key of B is known to A, but public key of A is not known to B.

→ Like Case I, since K_B is known, both El Gamal and OT are possible, and the condition is the same:

$(n-k) \geq e$.

Case IV: B does not know public key of A. A does not know public key of B

→ Here, like case II, K_B is not known, so El Gamal and OT are not possible.

→ Similar to case II, let λ be the size of K_B in blocks, and we need to use robust channel to transfer K_B.

Then, we get the same condition again as

$e \leq \min\left((n-k), (n-\lambda)\right)$

Scanned with CamScanner