intro
background
proposal/approach
results
appendices

1. intro
   (a) what this paper is
   (b) who was involved
2. background
   (a) what is cryptography?
   (b) what is secure multiparty computation? (shamirs scheme as example)
   (c) what is the problem we are trying to solve
   (d) what solutions already exist (polynomial scheme)
3. proposal
   (a) what is hamming distance?
   (b) of n parties?
   (c) basic scheme
   (d) fully secure scheme
   (e) n sets of binary strings, if $d_h(X_1, X_2)$ is 0, they are equal for intersection
4. results
   (a) implementation of basic scheme
   (b) reasons fully secure didnt work
   (c) graph1 hamming distance vs throughput
   (d) graph2 hamming distance vs time
   (e) graph3 time vs n vs set size
5. appendecies

(a) elgamal

(b) elgamal prover

(c) basic

(d) fully secure

(e) files to generate and plot csv

1 Introduction

basldaskdlsak;asfsdfl;ksadf;lsdkf;sdlkf

2 Background

What exactly is cryptography? Cryptography is the practice and study of secure communications in the presence of adversaries. It is using Mathematics to secure information. Cryptography is very new and also very old. Julius Caesar used to encrypt his messages he deemed of military significance using the *Caesar Cipher*, which shifted every letter over by three. The field in which Dr. Rasheed and I studied is called *Secure Mulitparty Computation.* In a given system of n players, each player P_i has a secret input x_i. The players want to compute some $f(x_1, x_2, ..., x_n)$ while revealing no information about their inputs. A real world example would be if you have three co-workers, and they want to find out who has the highest salary without revealing their salaries to each other. This means we have $n = 3$ players, and $f(x1, x2, x3) = max(x1, x2, x3)$. A good MPC protocol satisfies two properties: Input privacy and correctness. In terms of input privacy, no information about the players inputs should be able to be inferred during the execution of the protocol. The only information that should be inferred is whatever could have been seen by seeing the output of the function alone.In terms of correctness, no player or players who may deviate from the protocol should be able to force honest parties to output an incorrect result.