Misura delle prestazioni di cifratura omomorfica per servizi di localizzazione crowd

Tesi di Laurea in

Ingegneria Informatica

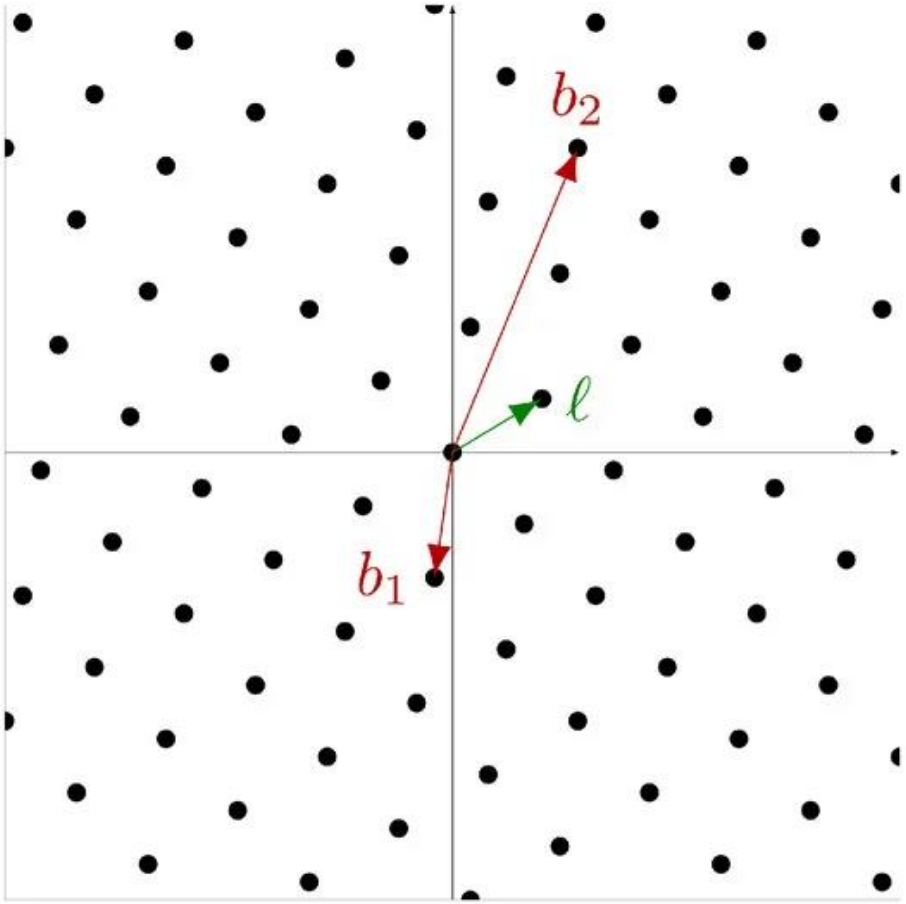
Candidato
Alessandro Corsi

Relatore
Prof. Pericle Perazzo

UNIVERSITÀ DI PISA

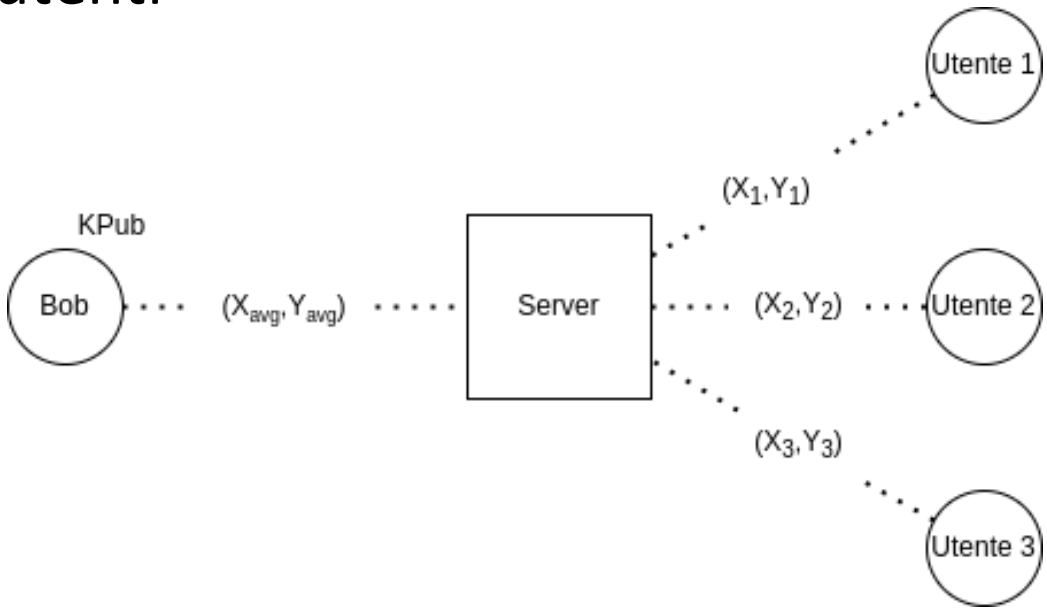
Introduzione

- La crittografia omomorfica permette di effettuare operazioni di somma e moltiplicazione su dati cifrati
  - Può essere usata per applicazioni cloud
  - È crittografia basata sui reticoli
  - Gli schemi usati sono *quantum-resistant*



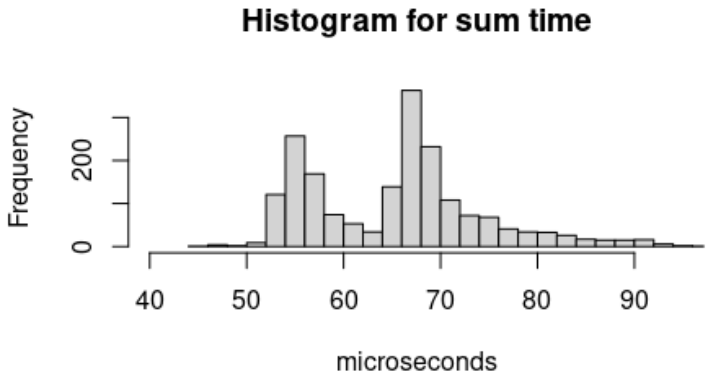
Applicazioni

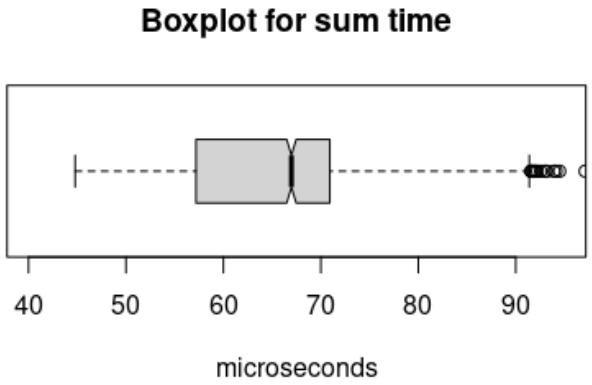
- Una particolare applicazione sono servizi di localizzazione crowd *privacy-oriented*
  - Un utente richiede la posizione media di un insieme di altri utenti
  - Il server calcola la media senza conoscere le posizioni dei singoli utenti

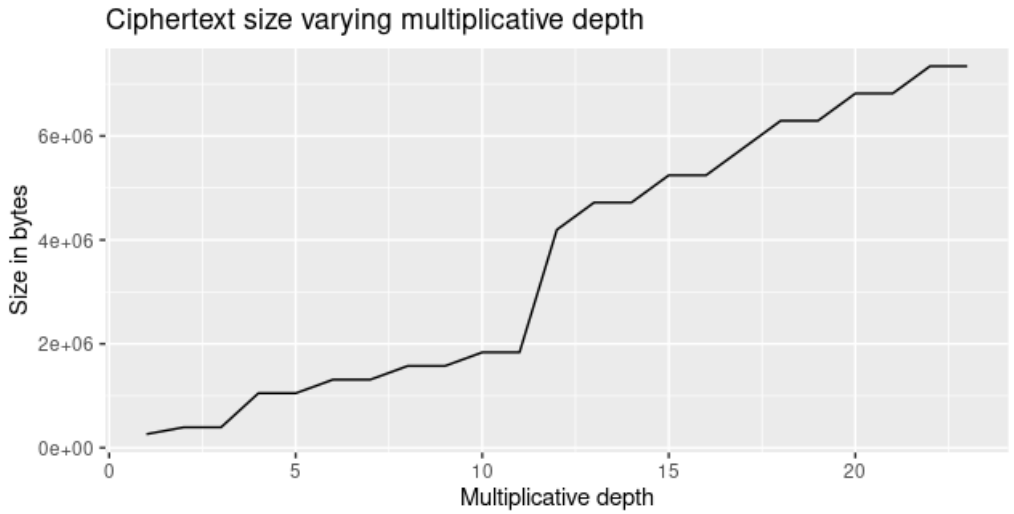


Prestazioni

- Sono state rappresentate le prestazioni della libreria OpenFHE con grafici a linee, boxplot e istogrammi

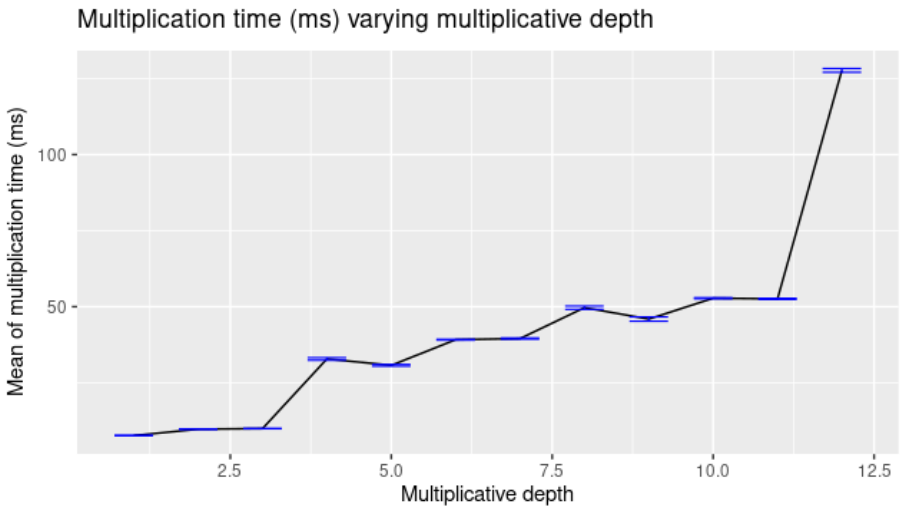


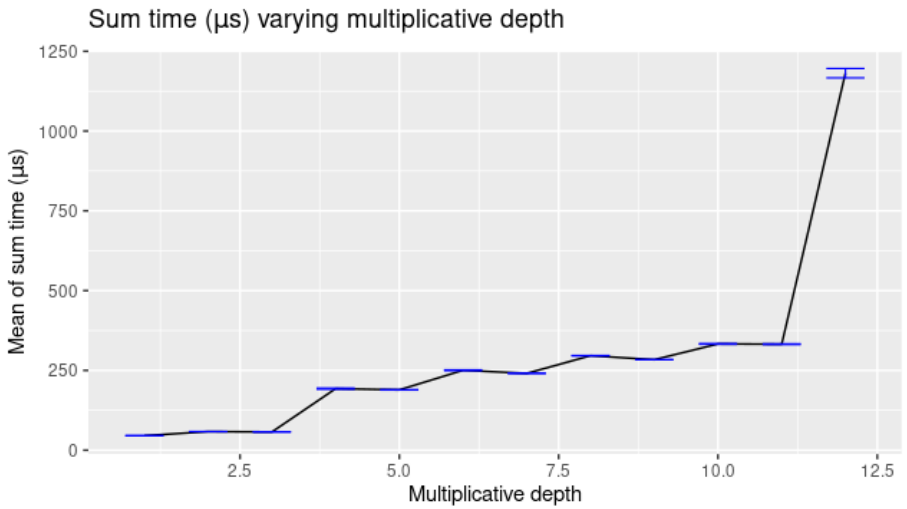




Prestazioni

- Sono state effettuate diverse misurazioni variando il parametro di MultiplicativeDepth
  - Sono stati raccolti 2000 campioni per misurazione
  - La media di ogni misurazione è stata rappresentata con line chart in cui la error bar è l'intervallo di confidenza al 95%





Conclusioni

- Nel caso in cui debbano essere effettuate molte moltiplicazioni, i calcoli possono essere lenti, e i ciphertext possono richiedere molto spazio

- Non sono stati ancora implementati metodi efficaci per effettuare la divisione tra crittogrammi