Statistiques Sécurisées

Chiffrement Homomorphe

Angel Bochenko
Céline Mafetgo
Julien Wirth
Mohamed Zouhair

Introduction

- Le Context

- Choix des différents outils

Le chiffrement Homomorphe

- Opérations sur des valeurs chiffrées
- Différents types de chiffrement :
  - Partiellement Homomorphe
  - Totalement homomorphe
  - Presque homomorphe
- Le Bruit
- Les schémas de chiffrement
  - BFV
  - CKKS

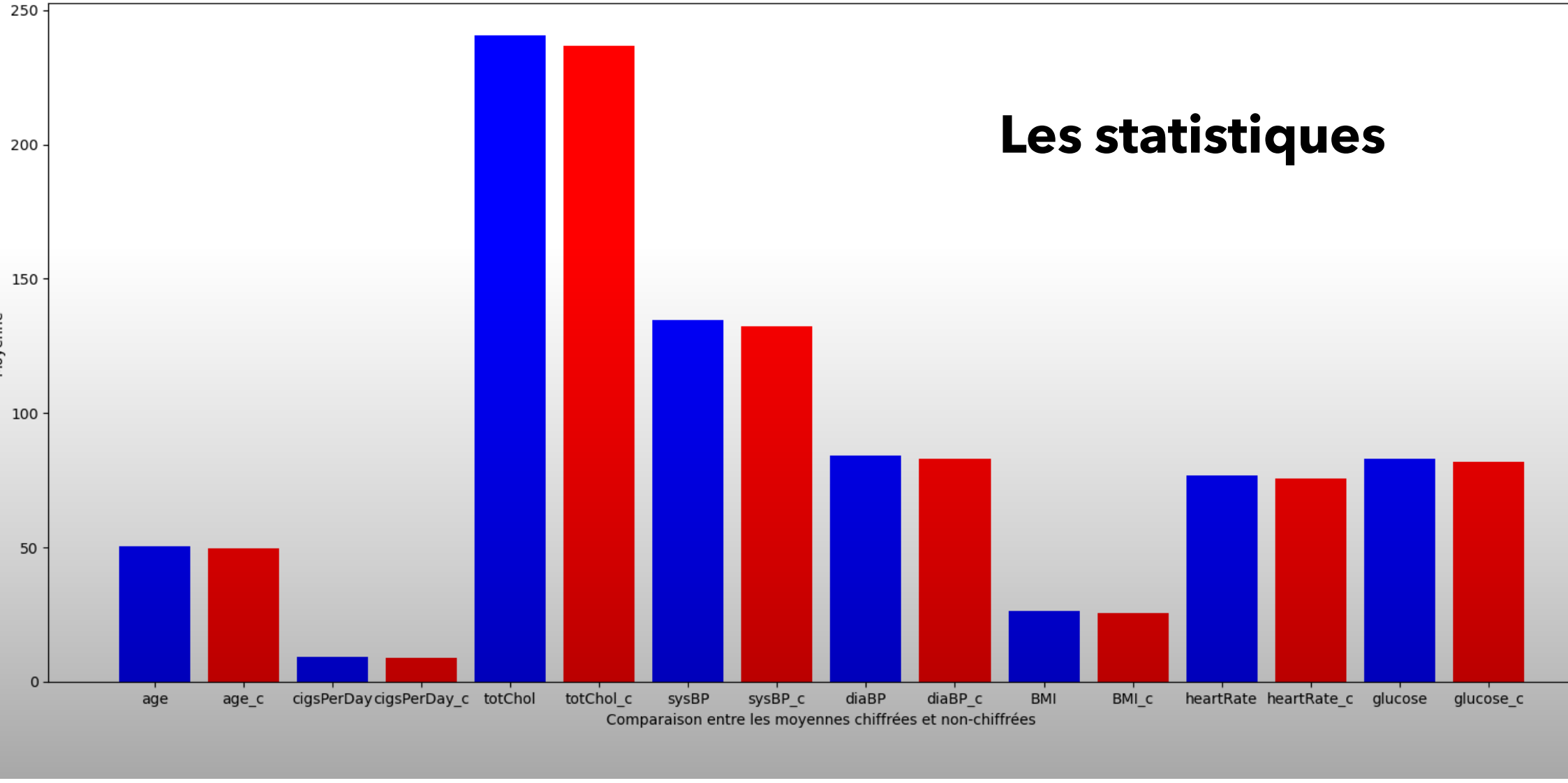
CKKS

- Encodage en polynôme
- LWE/RWLE
  - Encryption of μ using p: output $c=(\mu,0)+p=(\mu-A.s+e,A)=(c0,c1)$.
  - Decryption of c using s: output $\mu\sim=c0+c1.s=\mu-A.s+e+A.s=\mu+e\approx\mu$
- L'addition :
  - $CAdd(c,c')=(c0+c'0,c1+c'1)=c+c'=cadd$
  - $Decrypt(cadd,s)=c0+c'0+(c1+c'1).s=c0+c1.s+c'0+c'1.s=Decrypt(c,s)+Decrypt(c',s)\approx\mu+\mu'$
- La multiplication
  - $cmult=CMult(c,c')=(d0,d1,d2)$
  - $crelin=Relin((d0,d1,d2),evk)$
  - $\mu mult=Decrypt(crelin,s)\approx\mu.\mu'$
- Le rescaling

Implémentation

- Chiffrement côté Client :
  - Création du contexte
  - Chiffrement
- Calculs côté serveur
  - Récupération context public
  - Les calculs
- Dechiffrement côté Client, calcul et génération des graphes
  - Génération des graphiques

Les statistiques



Comparaison des données

```
male              :       0.443654267,       0.4505009774 | diff=0.006846710441808568
age               :      49.5574398249,      50.3773341292 | diff=0.8198943042939177
education         :       1.9797592998,       2.012196737 | diff=0.0324743722560488
currentSmoker     :       0.489059081,       0.4966347287 | diff=0.0075756477180154436
cigsPerDay        :       9.0221553611,       9.1715966081 | diff=0.14944124704342165
BPMeds            :       0.0303610503,       0.0304858846 | diff=0.00012483423346732955
prevalentStroke   :       0.0057439825,       0.0058411108 | diff=9.712833000705915e-05
prevalentHyp      :       0.3115426696,       0.3171064402 | diff=0.005563706133461196
diabetes          :       0.0270787746,       0.0285455409 | diff=0.001466766321751467
totChol           :     236.8730853392,     240.7922584686 | diff=3.919173129415526
sysBP             :     132.3680251641,     134.5578752054 | diff=2.189850041305789
diaBP             :      82.9120623632,      84.2816745389 | diff=1.3696121756152024
BMI               :      25.7841849015,      26.2116479625 | diff=0.42746306098323217
heartRate         :      75.7305798687,      76.9845781699 | diff=1.253998301206508
glucose           :      81.8561269147,      83.2105828504 | diff=1.3544559357343928
TenYearCHD        :       0.1523522976,       0.1552045407 | diff=0.002852243068939997
```

Difficultés

- Les contraintes de la bibliothèque
- Agencement des données
- Taille des données

Améliorations possibles

- Améliorer l'interaction client/serveur (faciliter l'échange de données et améliorer la scalabilité)
- Produire plus de statistiques
- Changer la structuration des données chiffrées

Conclusion