1 ანოტაცია

სრულად ჰომომორფული დაშიფვრა(FHE) დიდი სისწრაფით იძენს პოპულარობას, როგორც ერთადერთი საშუალება, შევასრულოთ უსასრულო რაოდენობის ოპერაციები დაშიფრულ მონაცემებზე. ხელის შემშლელი ფაქტორი მხოლოდ მისი წარმადობაა, განსაკუთრებით ჰომომორფული ბუთსტრაფინგი, რომელიც განახლებას უკეთებს შეცდომას და საშუალებას გვაძლევს ახალი ოპერაცია მინიმალური შეცდომით(noise) დავიწყოთ, ოპერაციის სიმძიმის გამო გარკვეული შიფრისთვის შესაძლოა შეცდომის განახლებას რამდენიმე წუთიც კი დაჭირდეს, რაც საგრძნობლად ამცირებს პრაქტიკული აპლიკაციების რაოდენობას. ჩვენი მიზანია მასიურად გავაპარალელოთ TFHE[1]სქემა, რომელიც საუკეთესოა ნატურალურ რიცხვებზე დაფუძნებულ სქემებს შორის, და გამოირჩევა სწრაფი ბუთსტრაფინგით. ალგორითმის ბლოკების გაანალიზებით, პარალელური ალგორითმების სწორად შერჩევით და ოპტიმალური იმპლემენტაციით შევძელით გვეჩვენებინა 28x გაუმჯობესება state-of-the-art CPU იმპლემენტაციასთან შედარებით(TFHE-rs)[2][3] რომელიც მასიურად იყენებს პარალელიზაციას, და 34x აჩქარება state-of-the-art GPU იმპლემენტაციასთან(cuFHE)[4]. ძირითადი დაბრკოლება არის დიდი პოლინომების ნამრავლი, რომელიც ძირითადი ოპერაციაა ჰომომორფული ბუთსტრაფინგის, რისი გაუმჯობესებაც სხვადასხვა ალგორითმებით ნაშრომის ერთერთი მთავარი მიზანი იყო. საუკეთესო შედეგის მიღწევა შევძელით ფურიეს გარდაქმნით, რომელიც თავის მხრივ ნაშრომში განხილვის თემას წარმოადგენს.