RAPPORにおけるゼロ知識証明の性能評価

プライバシー保護と性能のトレードオフ分析

2025年4月1日

研究の背景と目的

- **RAPPOR (Randomized Aggregatable Privacy-Preserving Ordinal Response)**
  - Googleが開発した差分プライバシーに基づくデータ収集システム
  - クライアント側でのデータランダム化による匿名化
- 課題: シャッフラーの信頼性担保が必要
- 目的: ゼロ知識証明(ZKP)を導入し、信頼性向上と性能評価を行う

ゼロ知識証明技術の概要

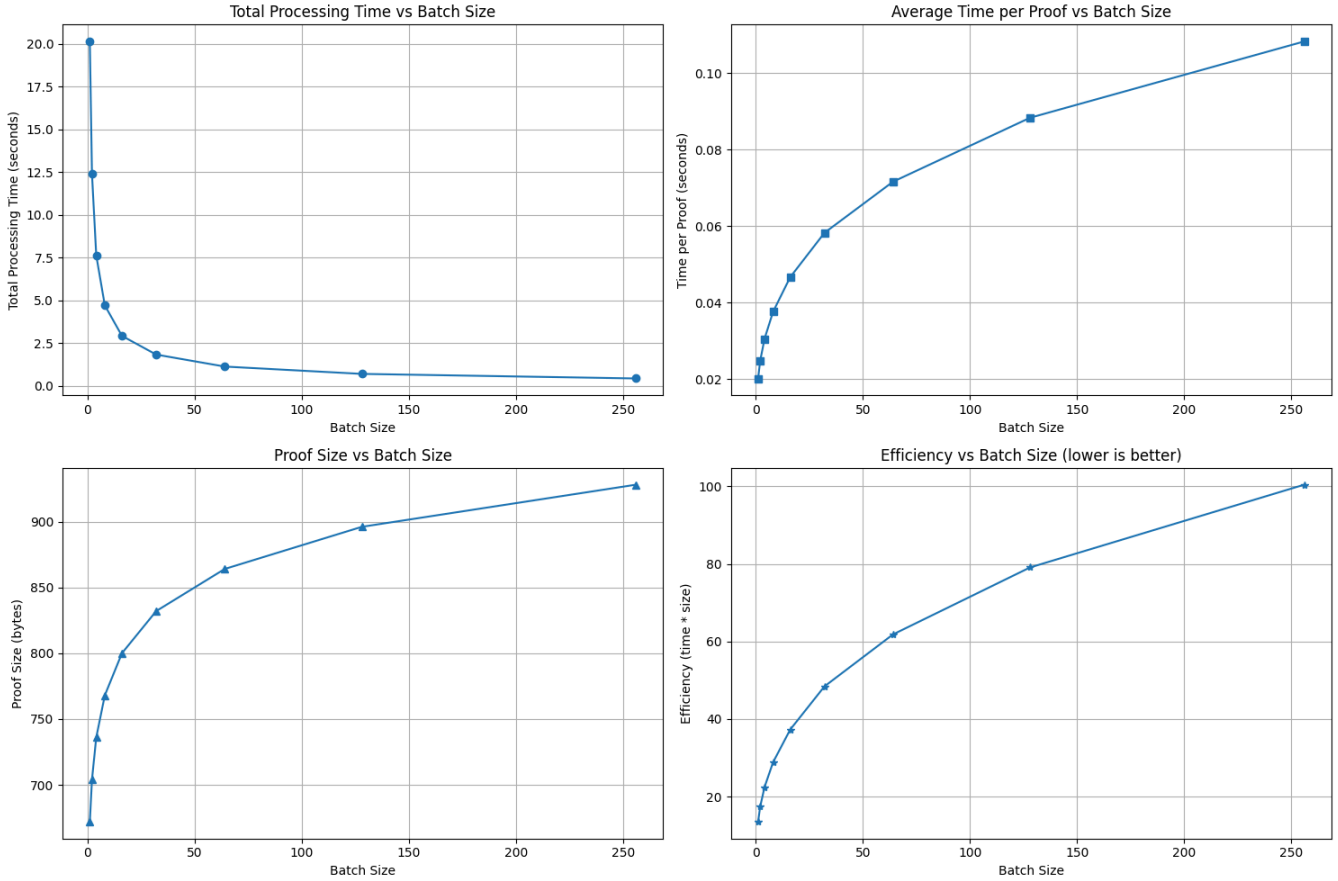
シミュレート**ZKP**

- コミットメントのハッシュ値の比較による簡易的な検証
- 低計算コストだが、暗号学的保証は限定的

Bulletproofs ZKP

- 楕円曲線暗号を用いた暗号学的に強力な証明システム
- 証明サイズが対数関数的(O(log n))に増加
- バッチ処理による効率化が可能

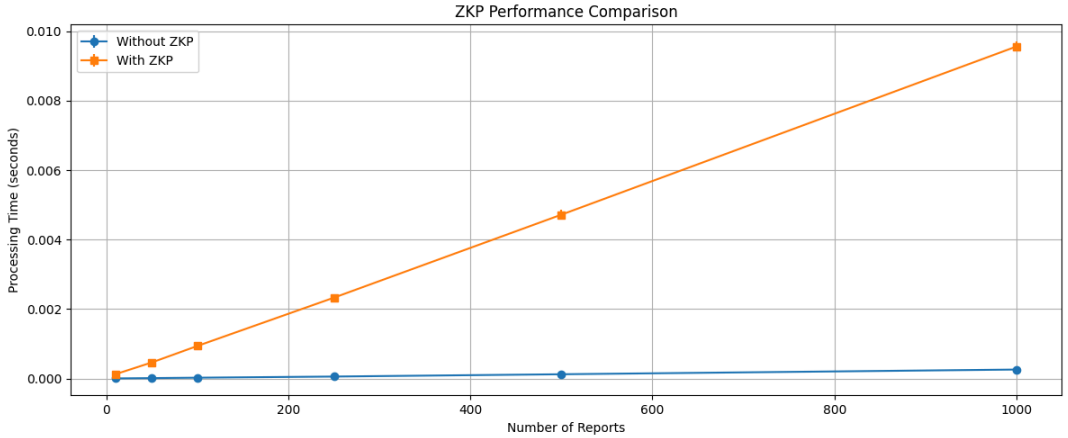
Bulletproofsのバッチ処理効果

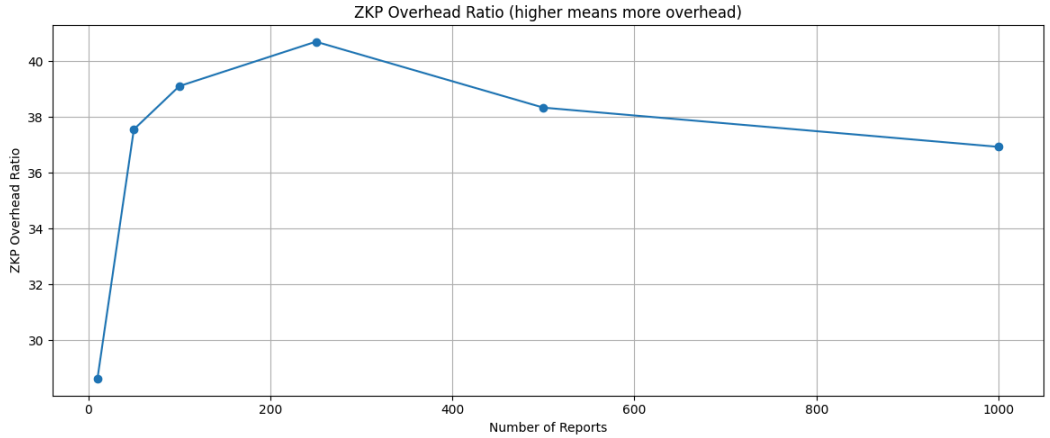


Bulletproofsのバッチ処理分析

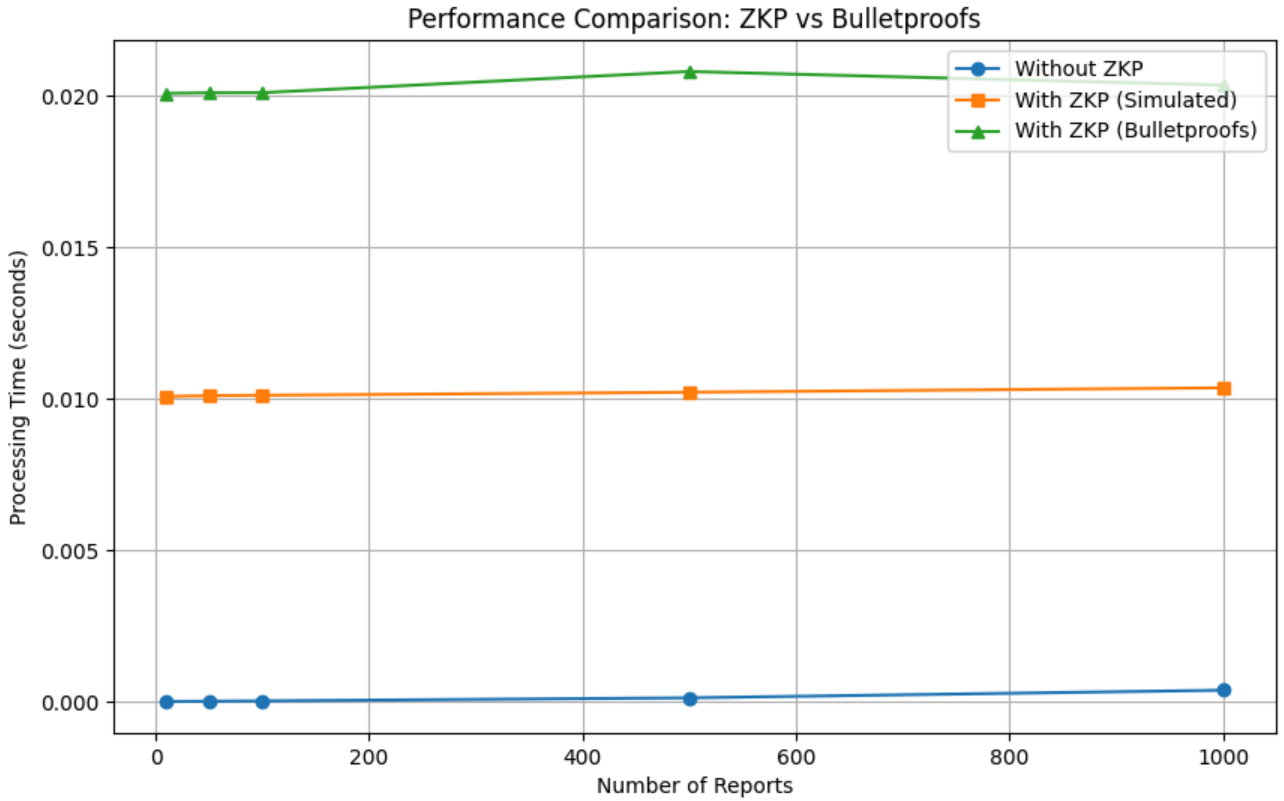
- 総処理時間: バッチサイズ1→16で20秒→2秒未満に減
- 証明あたりの時間: バッチサイズ増加で若干増加(0.02秒→0.10秒+)
- 証明サイズ: 対数関数的に増加(672バイト→950バイト程度)
- 最適バッチサイズ: 16〜64が総処理時間と効率性のバランスに優れる

ZKPの性能オーバーヘッド評価





ZKP実装方式の比較


Performance Comparison: ZKP vs Bulletproofs
Without ZKP
With ZKP (Simulated)
With ZKP (Bulletproofs)
Processing Time (seconds)
0.020
0.015
0.010
0.005
0.000
0
200
400
600
800
1000
Number of Reports

実験結果の考察

- **ZKP**オーバーヘッド: ZKP導入で約38〜42倍の処理時間増加
- 安定性: レポート数増加に伴いオーバーヘッド比率が安定(約38倍)
- 実装方式比較:
  - ZKPなし: 処理時間ほぼゼロ
  - シミュレートZKP: 約0.01秒/レポート
  - Bulletproofs: 約0.02秒/レポート(2倍の時間で強力な保証)

現状の課題

1. 高いオーバーヘッド: ZKP導入による約40倍の処理時間増加
2. バッチサイズ最適化: ユースケースに応じた適切なサイズの決定
3. システム統合: 既存RAPPORフローへのZKP統合の複雑性

提案する解決策

1. ハイブリッドアプローチ
    - 機密性の高いデータのみBulletproofsを適用
    - それ以外にはシミュレートZKPを使用
2. 適応的バッチ処理
    - システム負荷とレポート到着率に基づく動的バッチサイズ調整
3. 並列処理とハードウェアアクセラレーション
    - コホートごとの並列処理
    - GPUによるBulletproofs計算の高速化

まとめと今後の方向性

研究成果

- バッチ処理によるBulletproofsの効率化を実証
- ZKP導入の性能コストを定量化

次のステップ

- 提案解決策の実装と実環境での評価
- zk-SNARKs/zk-STARKsとの比較検討

最終目標

- プライバシー保護と計算効率を両立した実用的なRAPPOR拡張の実現