小口研究室　研究紹介　(2018年度)
(お茶の水女子大学理学部情報科学科)

完全準同型暗号を用いたゲノム秘匿検索の高速化
（研究担当:山田　優輝）

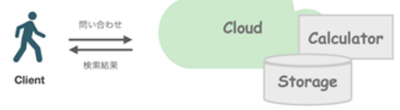
研究背景

◆ ゲノムデータ委託システム

大型のストレージと計算機を所有するクラウドにデータと計算を委託
→ 膨大なゲノムデータを用いた統計処理を行うことができる
特定の文字列がゲノム配列に含まれているかどうか判定する問い合わせを行う

◆ プライバシ保護・計算量

個人のゲノムデータは住所などとは異なり変更することができない
→ 暗号化によるプライバシー保護が必要
膨大なデータを暗号化して処理するため計算量が課題となる



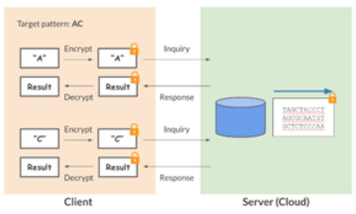
提案手法

◆ 完全準同型暗号 FHE を利用

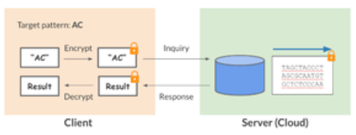
暗号文同士での加算と乗算が成立する完全準同型暗号 FHE を利用
メリット
　復号せずに演算を行うことが出来る
デメリット
　計算量が大きい
　演算を行いすぎると復号することが出来なくなる

◆ システムデザイン

復号を保証するために二つのアプローチを比較する
1. 計算量の少ない問い合わせを複数回行う
2. 暗号文内のノイズを除去する演算 bootstrap を行う



デザイン 1



デザイン 2

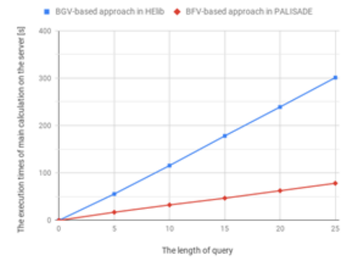
実験と考察

◆ 条件設定

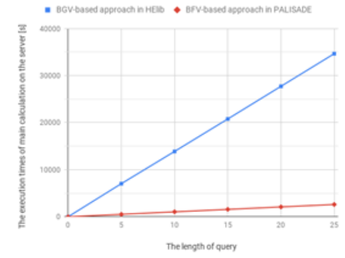
- 各デザインについて異なる暗号スキーム・暗号ライブラリを用いて実行時間の測定を行う
- BGV: HElib
- BFV: PALISADE
- クエリ長: 5～25
- サンプル: 10,000文字×512サンプル

◆ 実験結果

- デザイン
  デザイン 1 では実用可能な時間で検索が完了する
- スキーム
  両方のデザインについてBFV(PALISADE) の方が演算が高速
- Bootstrap
  デザイン 2 では bootstrap を行っているがこの演算は非常に計算量が大きいため、デザイン 1 と比較して実行時間が長くなっている



デザイン 1



デザイン 2

今後の課題

- デザイン 2 について bootstrap の有無とスキームの条件を変えて更に実験を行う
- クライアント・サーバ間の通信時間を比較する
- クライアント・サーバ間のデータ通信量を比較する
- ポジション数・サンプル数を変えて実験を行う

深層学習を用いた無線LAN通信時の端末情報を考慮したパケット喪失に基づく輻輳の予測
（研究担当:山本　葵）

研究背景

- スマートフォン、タブレット端末などのワイヤレスデバイスの普及によるトラフィックの増加
- 帯域の取り合いによる輻輳の発生

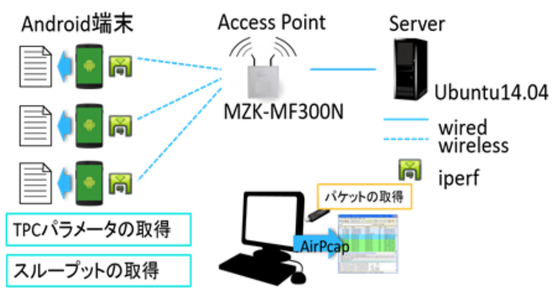
→

- 無線LANのトラフィックの深層学習による解析
- 解析によるトラフィックの予測
- →輻輳の極めて早期な検出、予兆の発見

帯域をコントロールして使うことが必要　　輻輳が起こることを予想して制御

実験概要

アクセスポイントに接続した複数のAndroid端末からiperfによってデータをサーバに送信、データの取得



- カーネルモニタ
  通信時におけるLinuxシステムのカーネル内部の処理を解析するシステムツールで、カーネル内部のパラメータ値の変化を記録可能

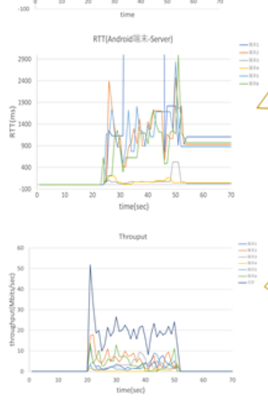
実験①
カーネルモニタで通信中の各端末のTCPパラメータを出力、輻輳状態の観察
実験②
深層学習を用いて輻輳発生時のAPまわりのパケットの解析、予測実験

実験結果

実験1 通信中の各端末のTCPパラメータの観察

- データ通信(70秒)
- 端末6台で同時通信
- 20－50秒のみパケット送信

- 出力
- 各端末のTCPパラメータ
- CWNDサイズ
- RTT
- 各端末のスループット



端末3と端末4の2台が帯域の大部分を圧迫している

通信開始直後から値は大幅増加
キューが溜まるのが早くパケットの処理が追い付かなかったと考えられる

CWND値が小さくなるときにスループット値も減少
→十分なスループットを確保できていない

実験2 深層学習を用いた予測実験

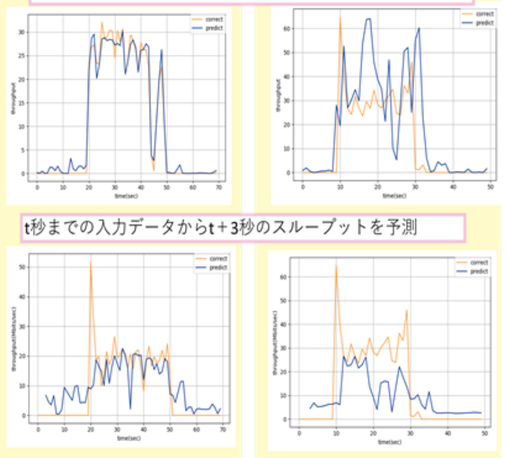
学習に用いるデータ

入力データ(特徴量)		正解データ
1秒間	[length sequence_number … etc …cwnd1 … cwnd N]（1パケット+cwnd）	スループット
	[length sequence_number … etc …cwnd1 … cwnd N]	
	…	
	[length sequence_number … etc …cwnd1 … cwnd N]	

学習データ(70秒)(20-50秒で通信)を用いた予測

テストデータ(70秒)(10-30秒で通信)を用いた予測

t秒までの入力データからt秒のスループットを予測



t秒までの入力データからt＋3秒のスループットを予測

http://ogl.is.ocha.ac.jp/
oguchi@is.ocha.ac.jp