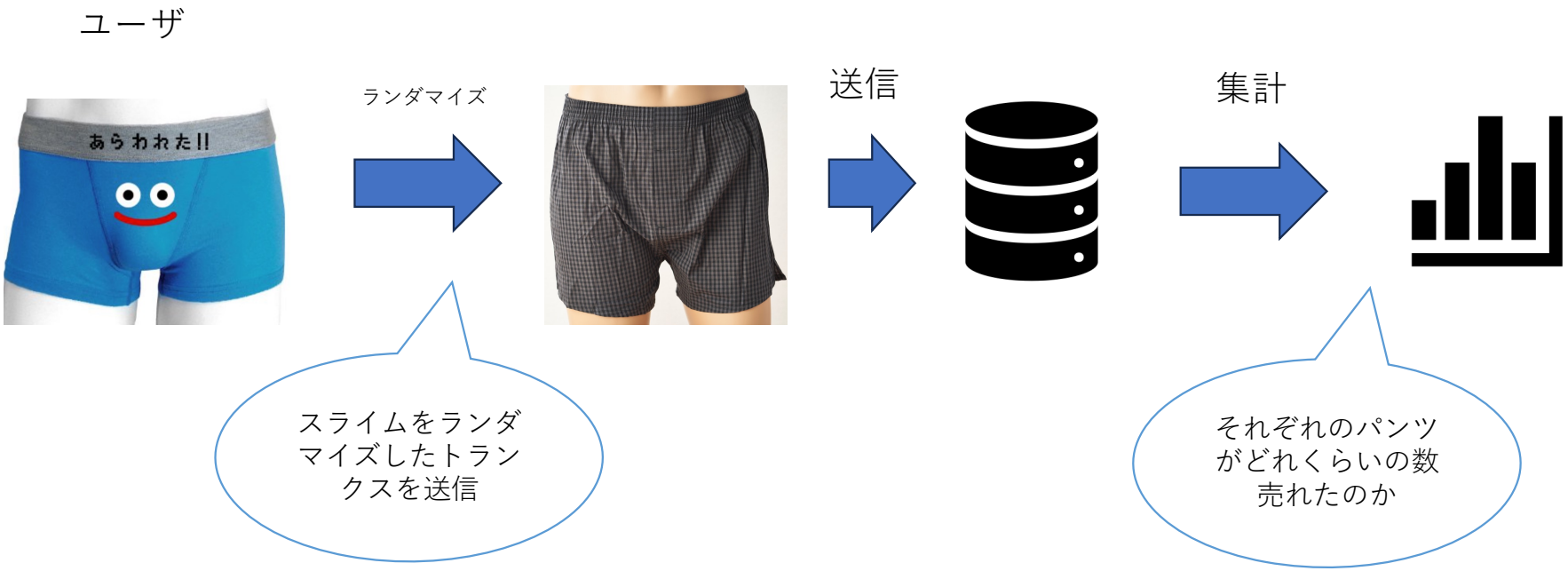
紛失通信とアダマール行列を用いてポイズニング安全性を強化したLDP方式の提案

総合数理学部　先端メディアサイエンス学科

菊池研4年　清水正浩

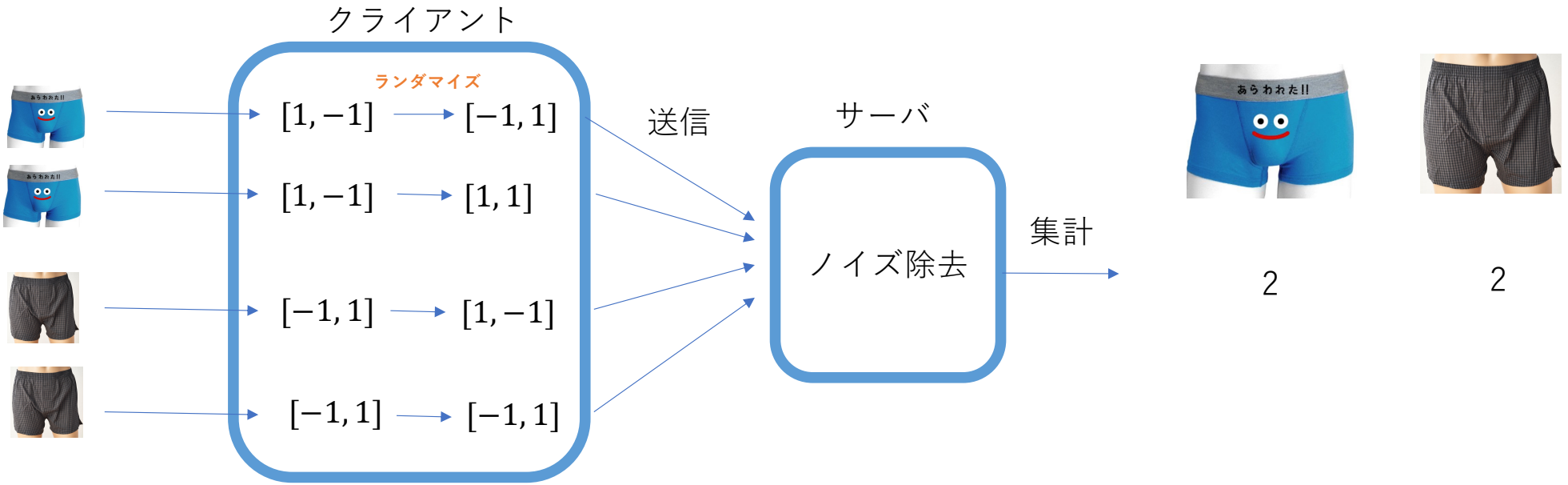
背景

- データの利活用が盛んになり、サービス事業者はユーザの**パーソナルデータ**を利用したい。
- 一方で、ユーザは自身の**プライバシーを守りたい。→局所差分プライバシ**

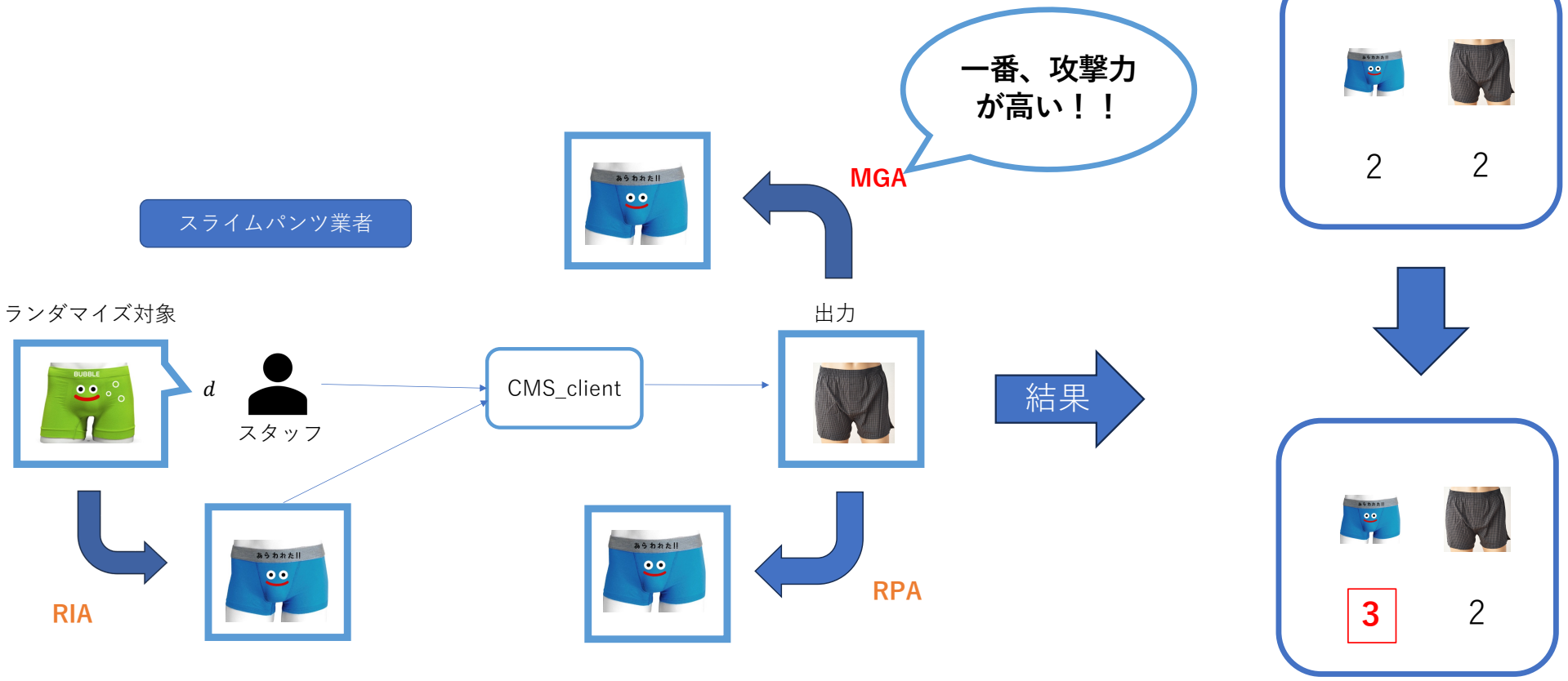


局所差分プライバシ CMS

- データの収集者を信頼しないモデル
- ユーザ側でデータに**ランダマイズして**からサーバに送信。



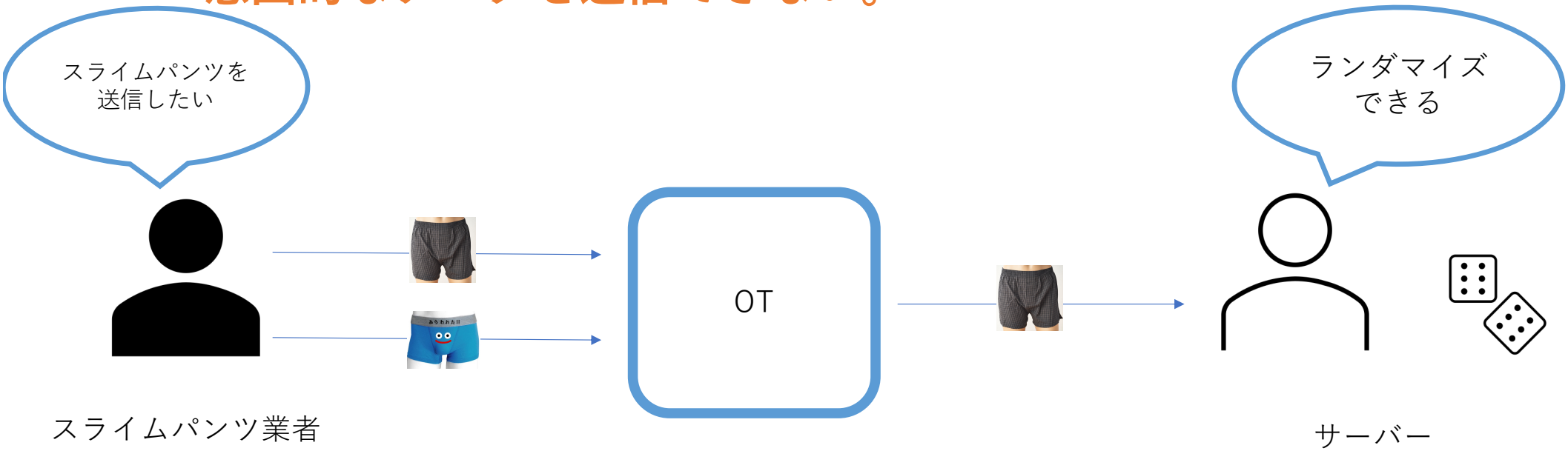
ポイズニング攻撃[Cao 2021]



Ex:スライムパンツ業者はスライムパンツがよく売れている見せかけたい！！

提案方式 紛失通信(OT)(Shimon 1985)

- 紛失通信(OT) は、公開鍵を使うことによって、ユーザが送信したサーバがどのデータを得たか知ることができないプロトコル
  →意図的なデータを送信できない。



紛失通信の課題

- 各ビットごとに暗号化、復号するため、**ドメイン長**が大きくなると**送信時間**が大きくなってしまう。
- 例えば、

$[1,-1]$

2bit

OT

$[-1,1]$

2bitであればそんなに
時間がかからない。

$[1,-1,1,1,1,1,1,1]$

8bit

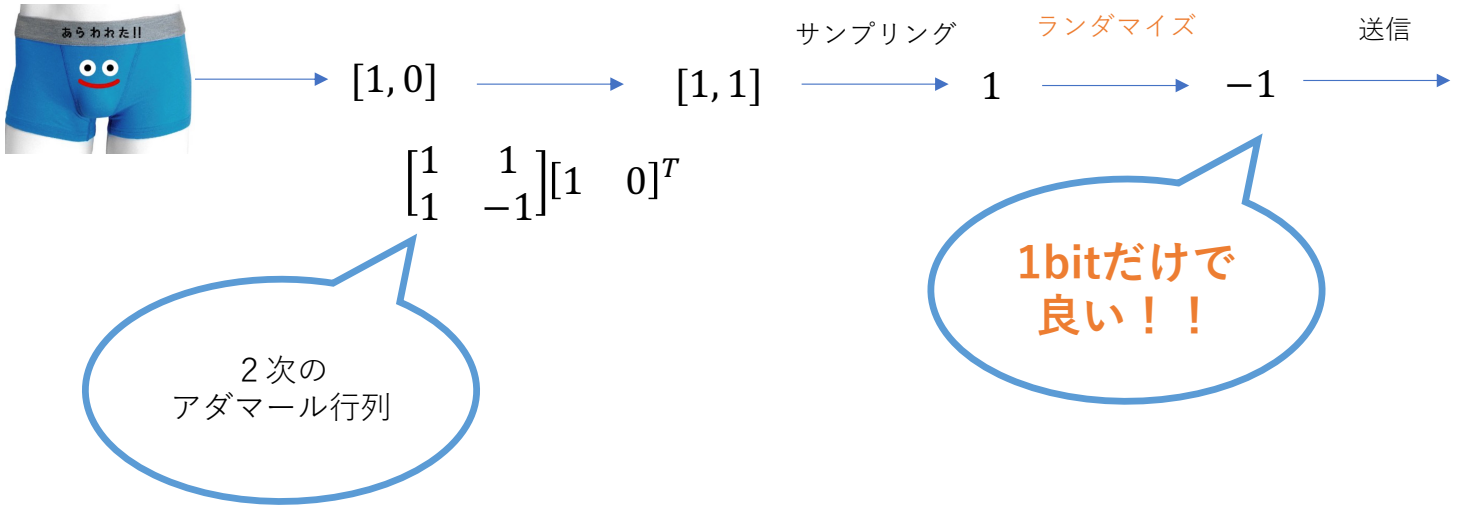
OT

$[1,-1,1,1-1,1,-1,1]$

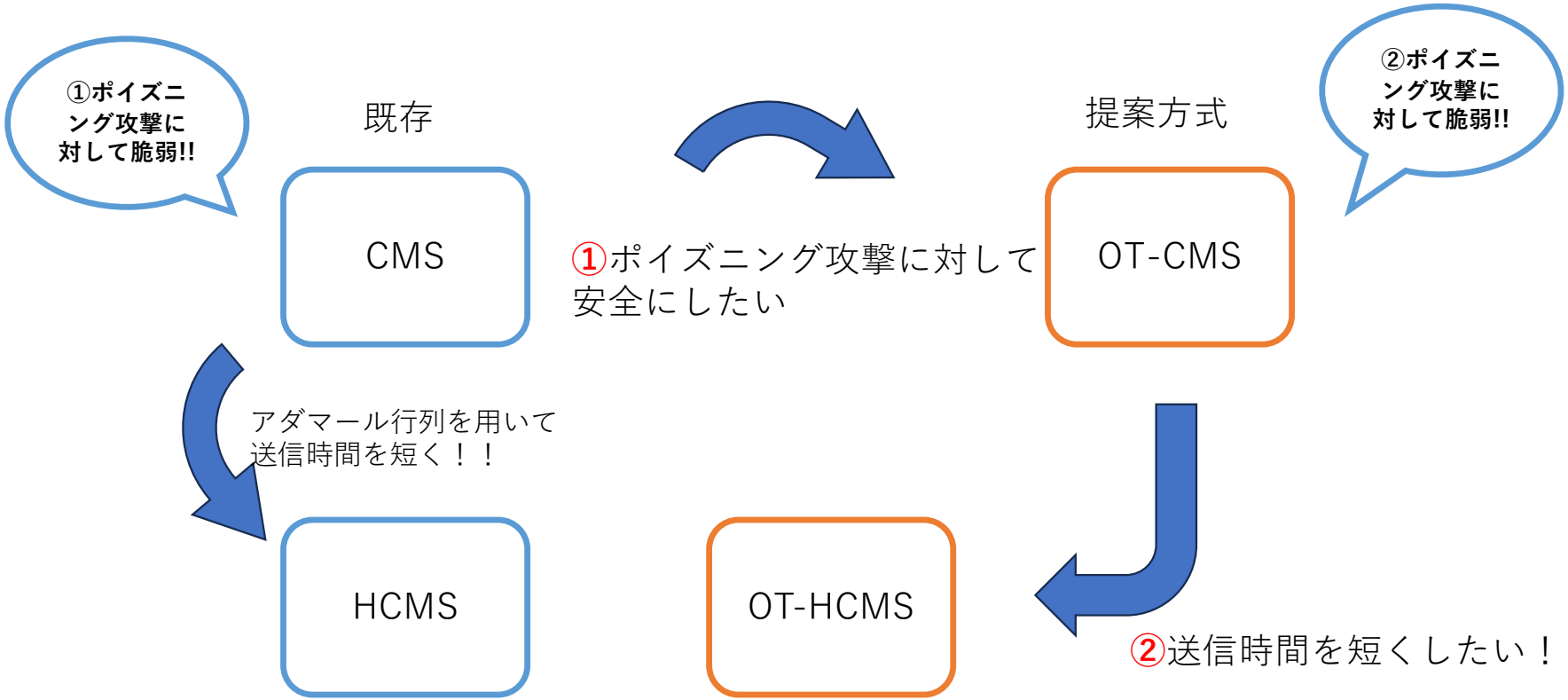
2bitのときより時間がかかる

CMSとHCMS(先行研究)

- HCMSは頻度推定を行うLDPの実装の１つ。CMSの亜種
- HCMSのHはHadamardのH
- CMSの送信量を減らすために提案された方式



既存の方式と提案方式の関係



Research Question

Q1. **OTを適用した方式は既存の方式より安全にすることができるか？**

Q2. HCMSではどれ位、**推定精度**が落ちるのか？

Q3. CMSとHCMSではどちらの方がポイズニング攻撃に対して**脆弱**なのか？

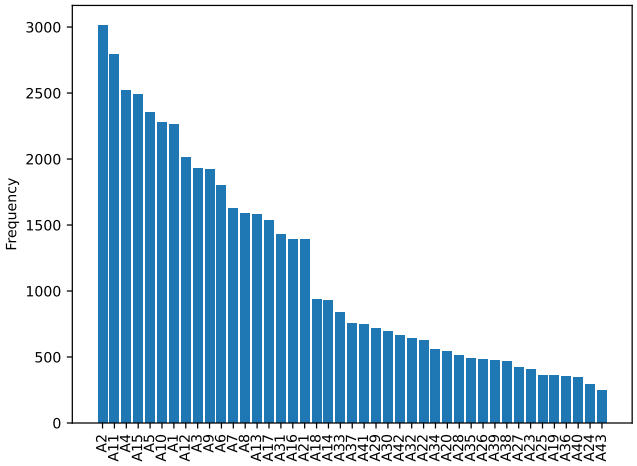
実験、評価指標

- 推定精度の評価指標：MSE
- 脆弱さの評価指標：Frequency Gain

$$FG = \sum_{t \in T} E[\tilde{f}_t - \hat{f}_t]$$

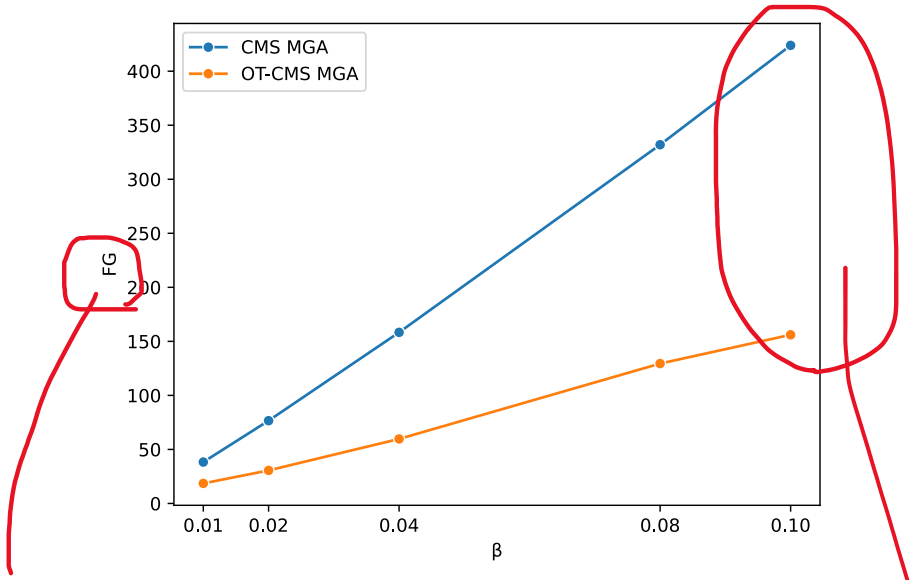
T:ターゲットアイテムの集合
$\tilde{f}_t$：アイテムtのポイズニング後の推定値
$\hat{f}_t$：アイテムtのポイズニング前の推定値

オンラインショッピングの購入頻度のデータ



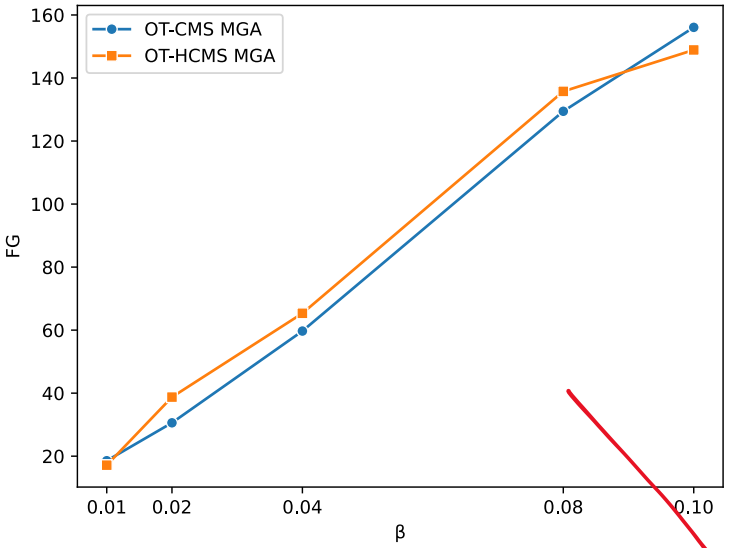
レコード数：49742　　アイテム数：43

実験結果（Oblivious Transfer）



小さくなるほど安全！！

不正ユーザの割合



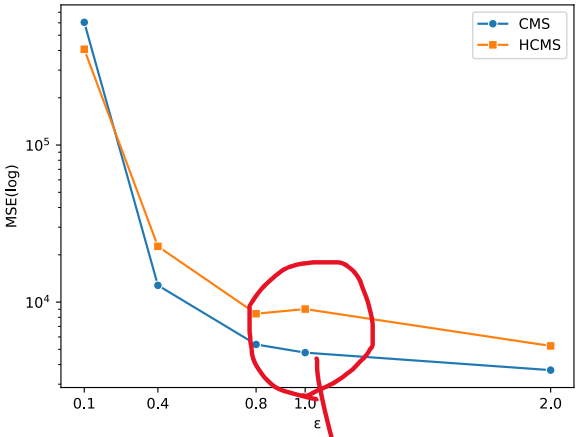
不正ユーザの割合

ほぼ変わらない

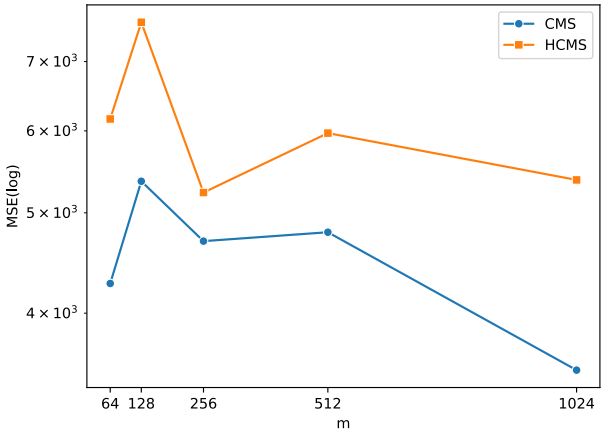
OTを適用した方が小さい→安全

実験結果（推定精度）

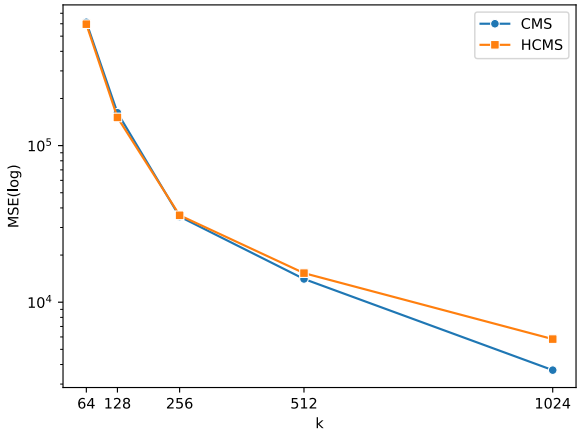
誤差



プライバシー予算



ドメイン長

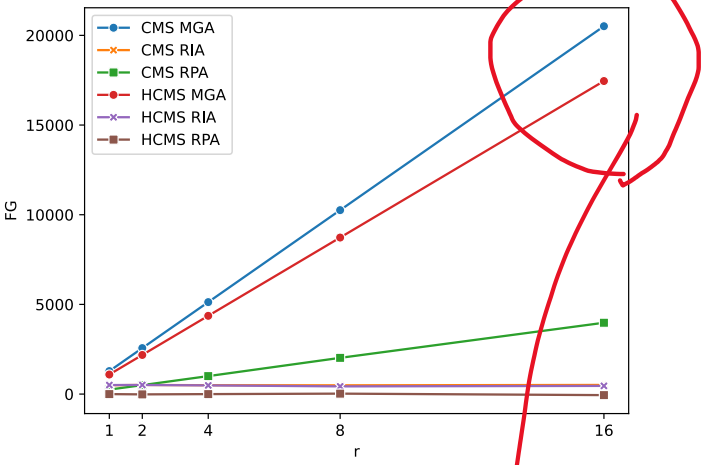


ハッシュ関数の数

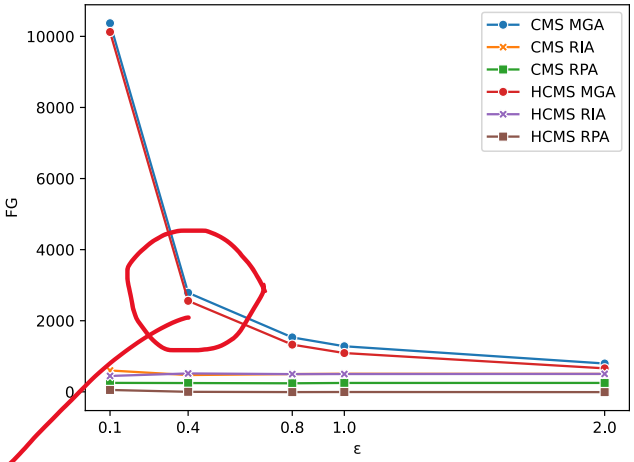
HCMSの方が89.7%大きい

全体としてHCMSの方が誤差が大きい!!

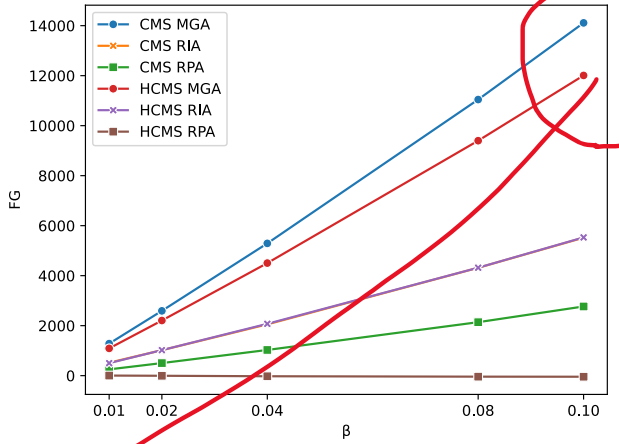
実験結果（脆弱さ）



ターゲットアイテムの個数



プライバシー予算



不正ユーザの割合

MGAは平均で16.0%CMSの方が脆弱！！

提案手法の限界

- 局所差分プライバシ方式はデータの収集者を信頼しないモデルであるが、OT-CMSとOT-HCMSはサーバを信頼することによって成り立つモデルである。

- 本来の局所差分プライバシ方式の考えに矛盾している。

- **実際の局所差分プライバシの運用環境によって変えるべき**

Research Question

Q1. **OTを適用した方式は既存の方式より安全にすることができるか？**

→できる

Q2. HCMSではどれ位、**推定精度**が落ちるのか？

→CMSに比べ、最大で89.7%低い。

Q3. CMSとHCMSではどちらの方がポイズニング攻撃に対して**脆弱**なのか？

→CMSの方が16.0%脆弱