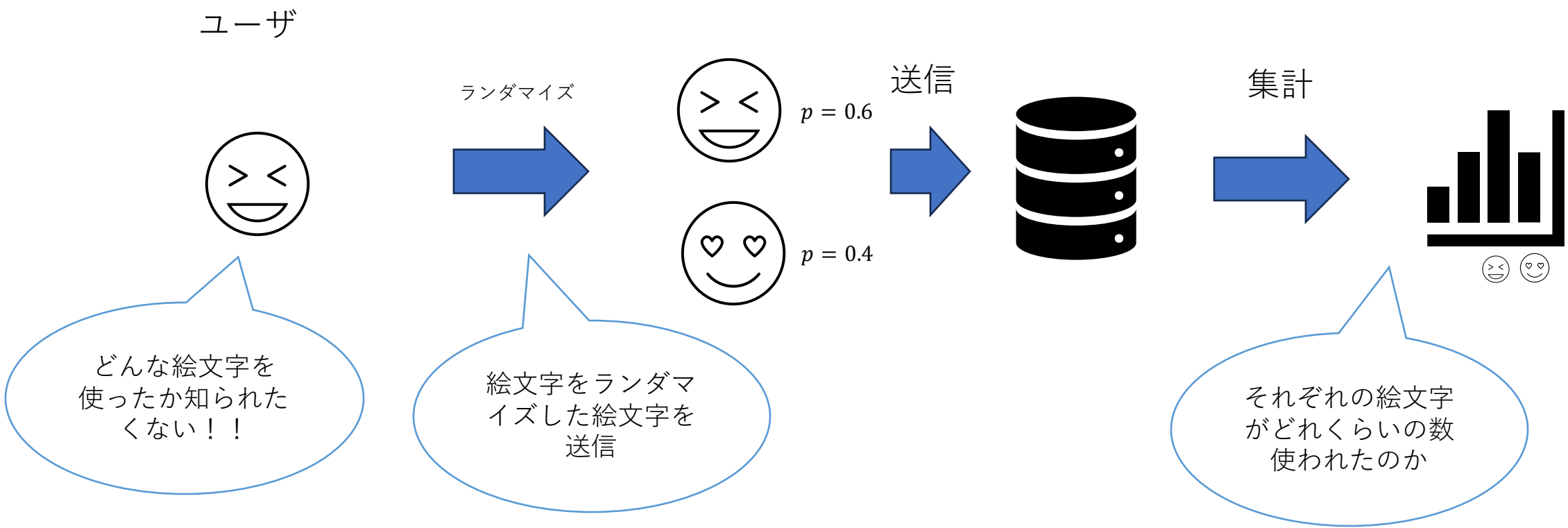
紛失通信とアダマール行列を用いてポイズニング安全性を強化したLDP方式の提案

清水正浩　菊池浩明

明治大学

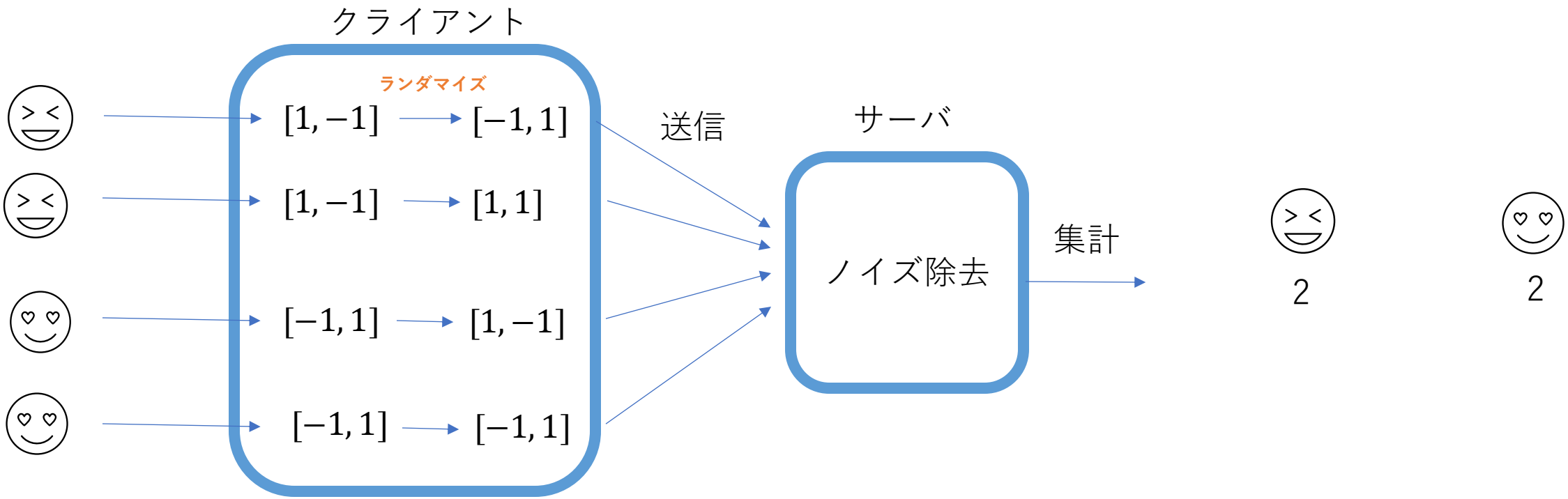
背景

- 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**

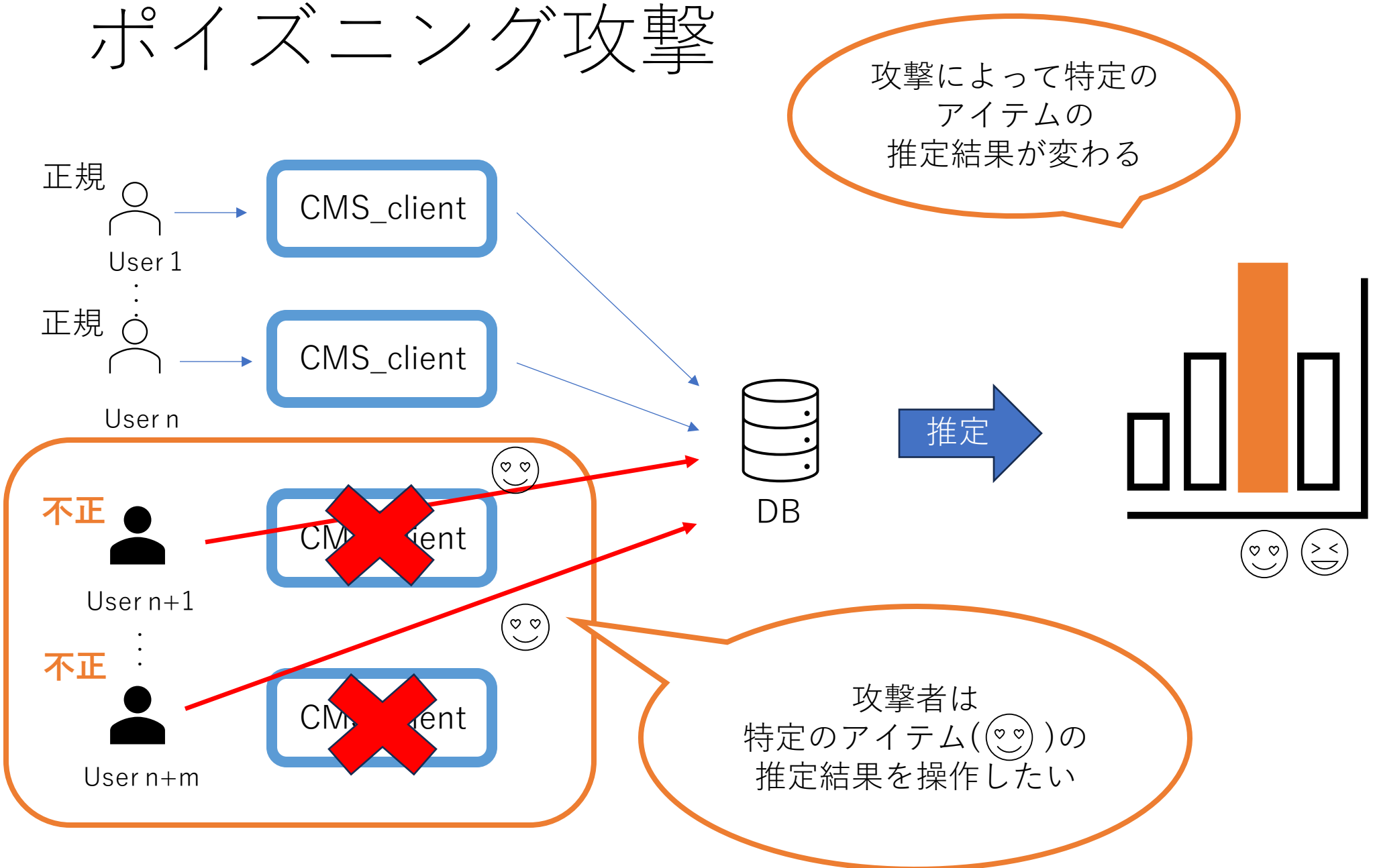


局所差分プライバシ CMS[Apple 2017]

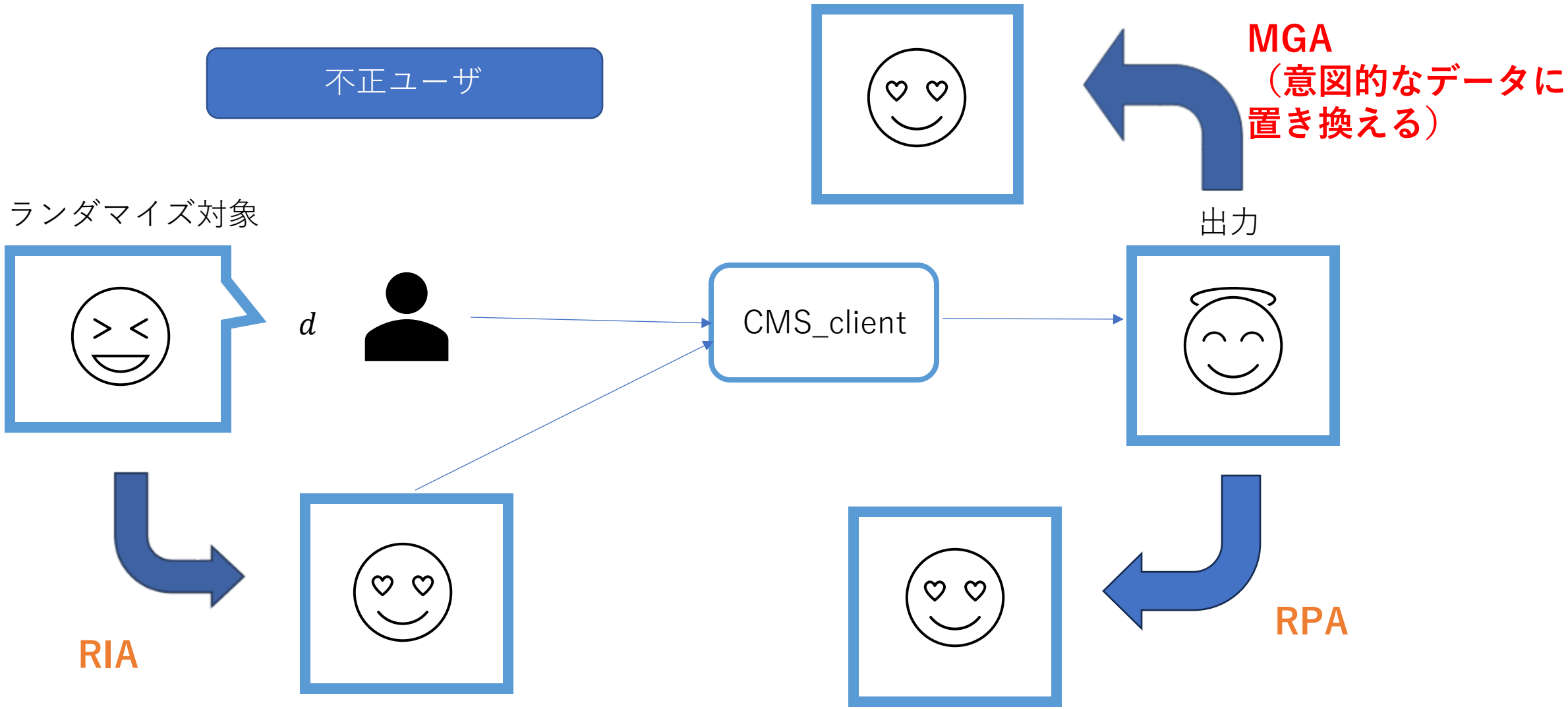
- データの収集者を信頼しないモデル
- ユーザ側でデータに**ランダマイズして**からサーバに送信。



ポイズニング攻撃


攻撃によって特定の
アイテムの
推定結果が変わる
正規
User 1
正規
User n
CMS_client
CMS_client
不正
User n+1
不正
User n+m
CMS_client
CMS_client
DB
推定
攻撃者は
特定のアイテム( )の
推定結果を操作したい

3つのポイズニング攻撃[Cao 2021]

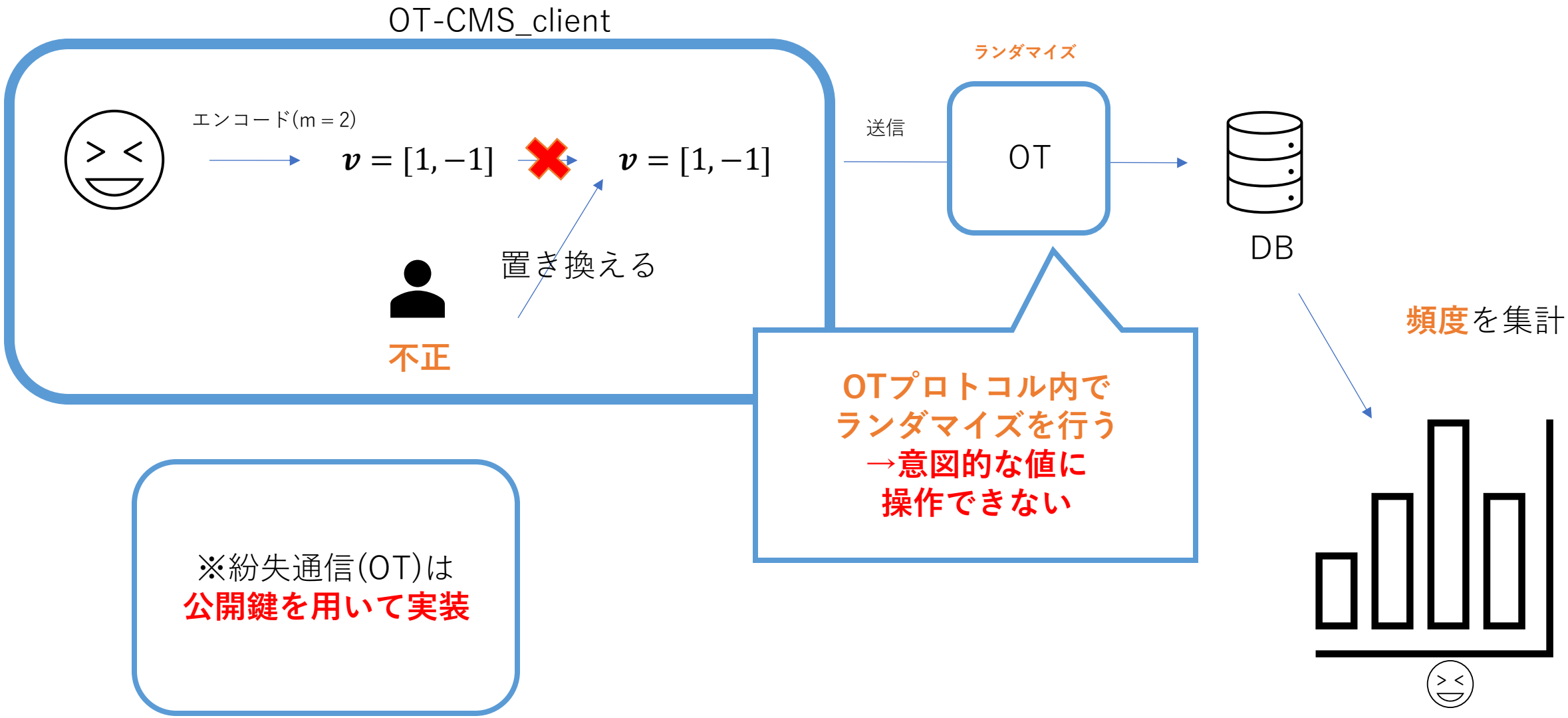


Caoらのポイズニング防止法

- Detecting Fake Users
  - サーバに送信されたユーザのデータを比較し、似たようなを不正ユーザとする探知法
  - 攻撃対象のアイテムが１つしかない場合、使用できない
- Conditional Probability based Detection
  - 攻撃対象のアイテムが１つしかない場合に使用する。
  - 攻撃対象のアイテムが外れ値のような振る舞いをすることを利用する。

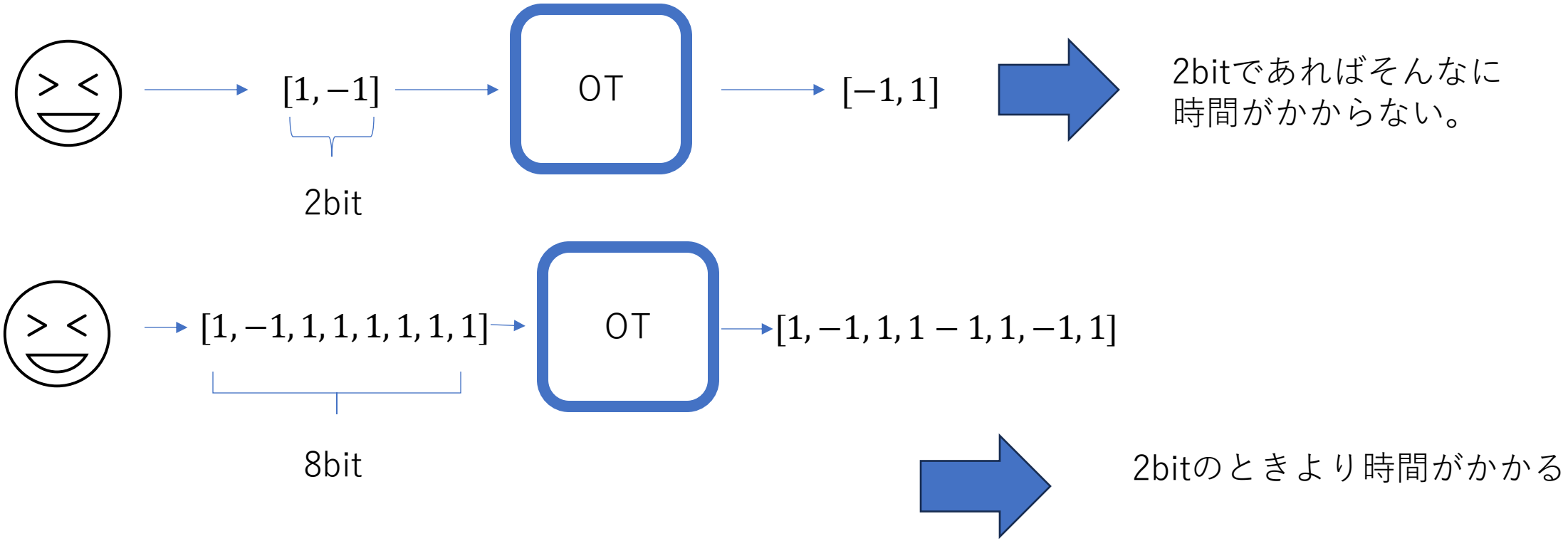
- →**どちらも不正ユーザの統計的な特徴をとらえる手法**

提案方式①　紛失通信（OT）の適用

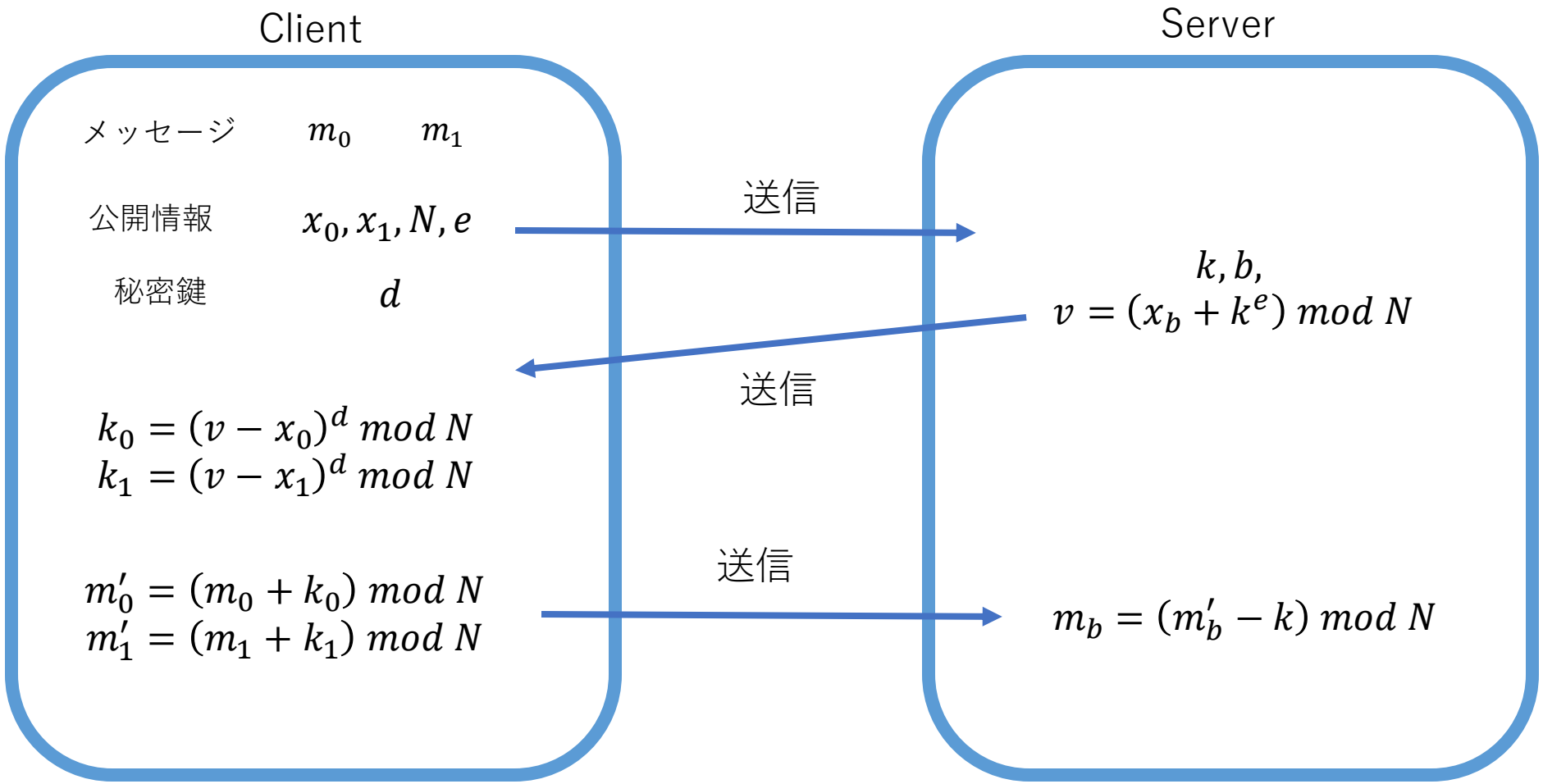


紛失通信の課題

- 各ビットごとに暗号化、復号するため、**ベクトル長**が大きくなると**通信コスト**が大きくなってしまう。
- 例えば、



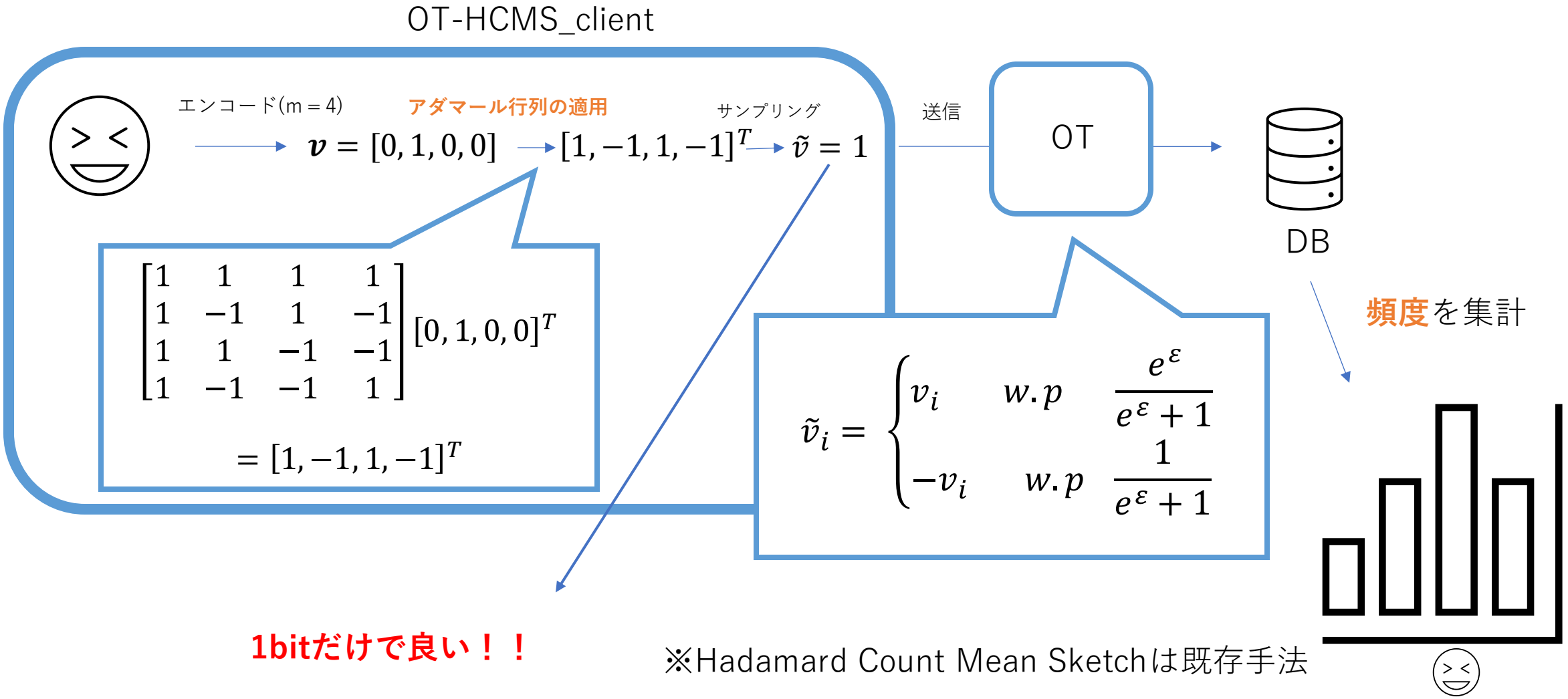
1-out-of-2 Oblivious Transfer(OT)



Clientはどちらの情報が知られたか知ることができない

Serverはどちらか一方の情報のみ復号できる

提案手法②　アダマール変換の適用



従来方式と提案方式の比較

	従来CMS	提案OT-HCMS
送信コスト	m	1
誤差	小	大
ポイズニング攻撃	脆弱	安全

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？

Q4. OT-CMSとOT-HCMSではどの程度、**処理時間**が変化するか？

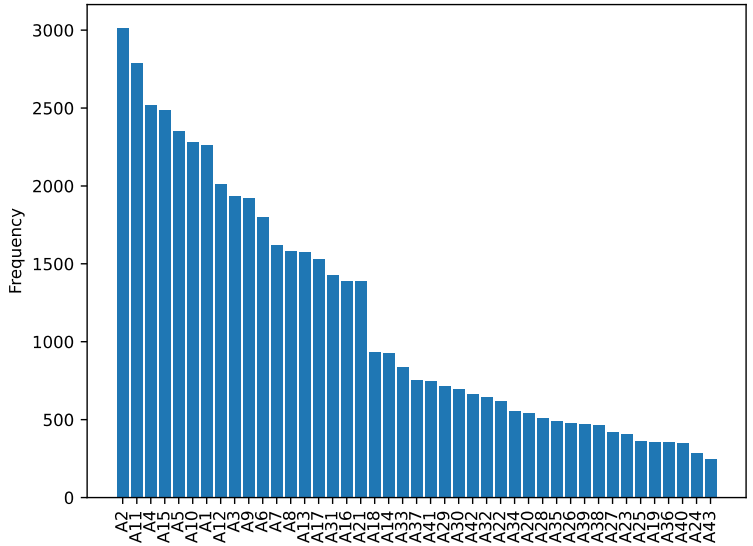
実験、評価指標

- 推定精度の評価指標：MSE
- 安全性の評価指標：Frequency Gain

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

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

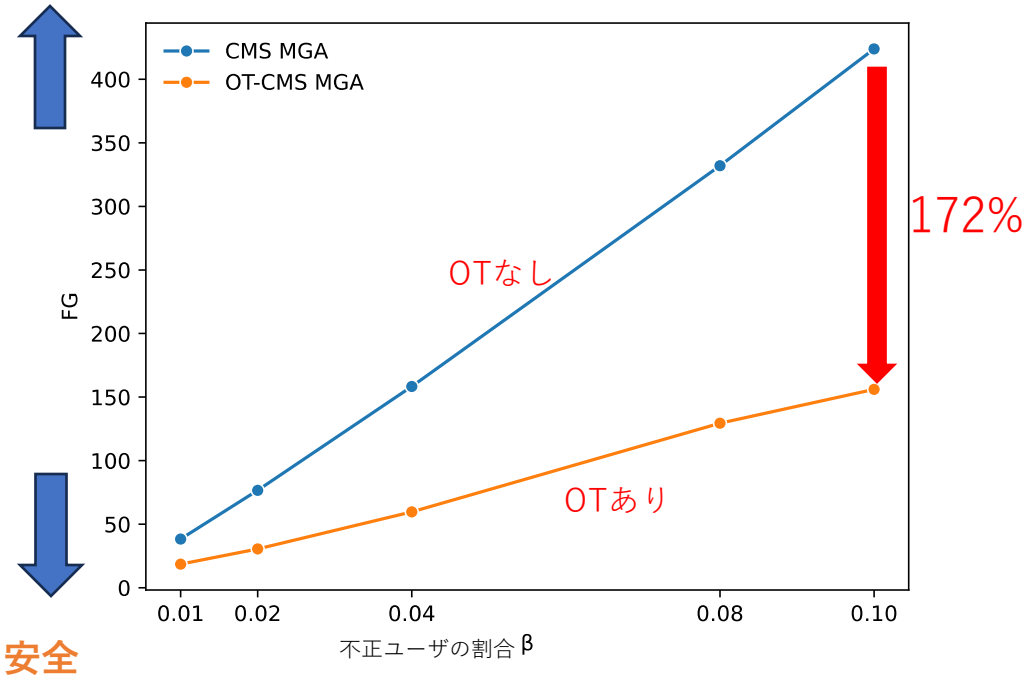
オンラインショッピングの購入頻度のデータ



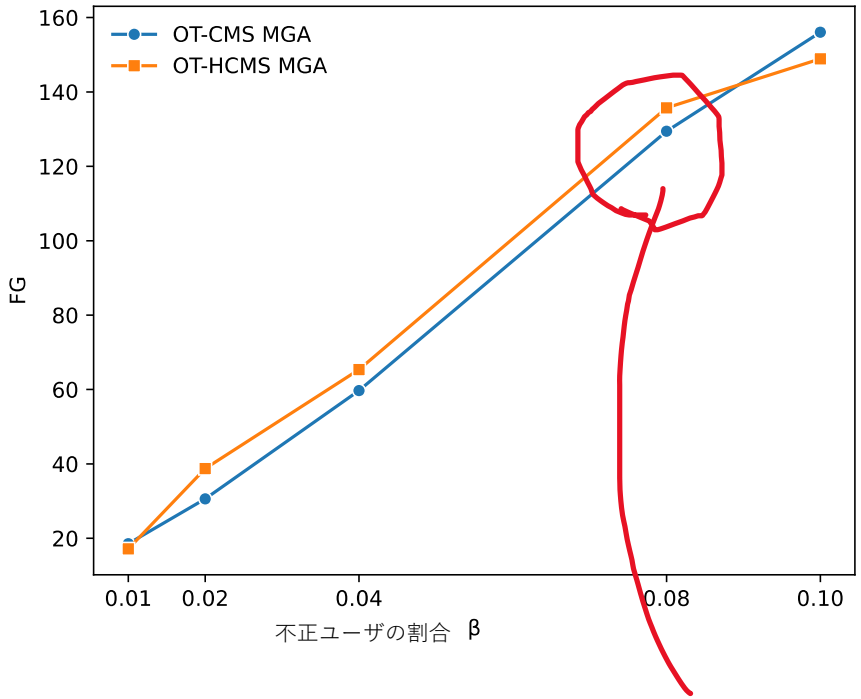
レコード数：49742　　アイテム数：43

実験結果①（提案方式の安全性）

リスク



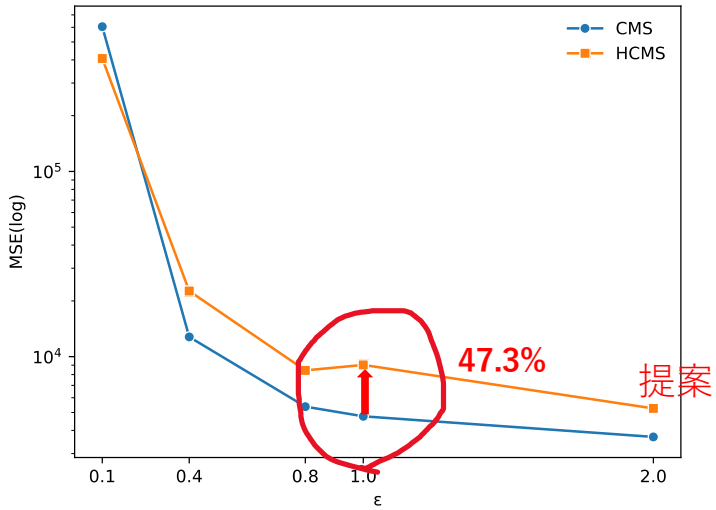
安全



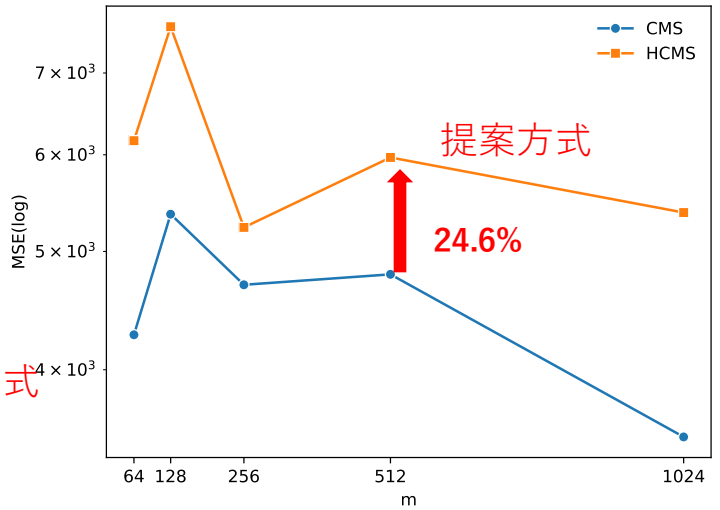
ほぼ変わらない

実験結果②（CMSとHCMSの推定精度）

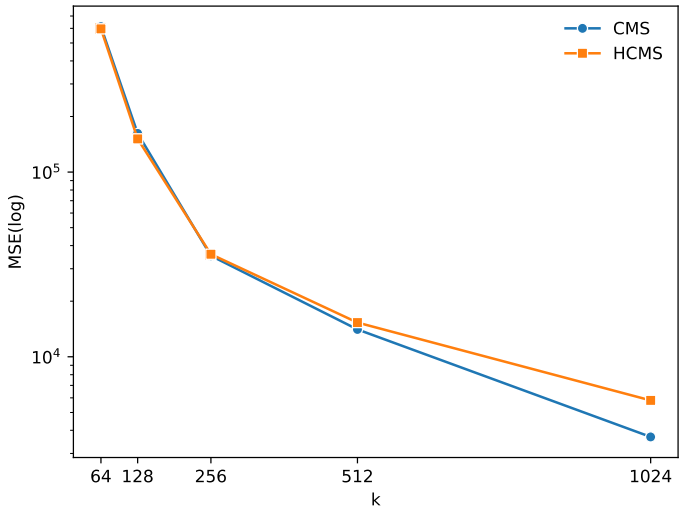
誤差



プライバシー予算



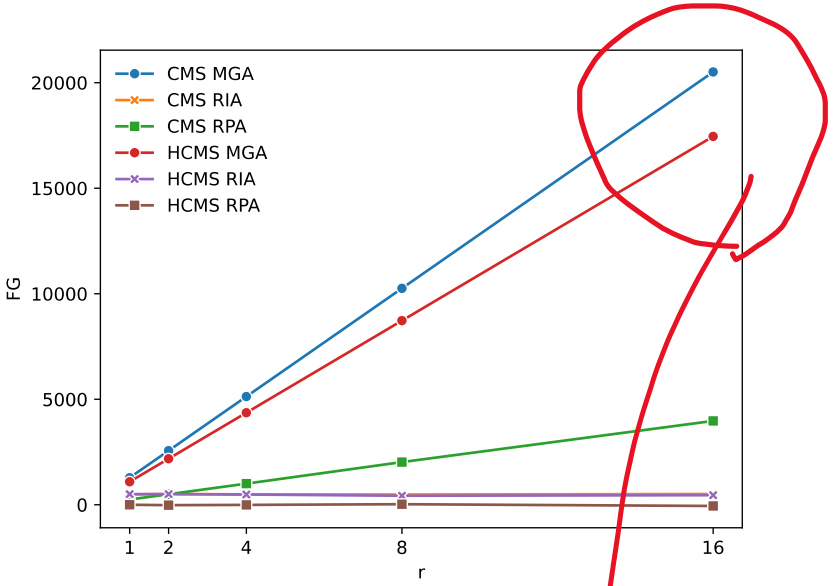
ドメイン長



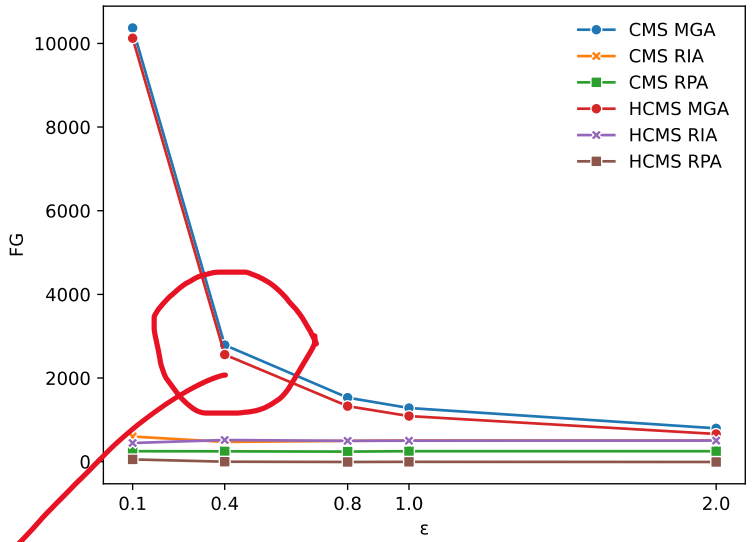
ハッシュ関数の数

全体としてHCMSの方が誤差が大きい!!
→アダマール変換を行うことによって誤差が大きくなる

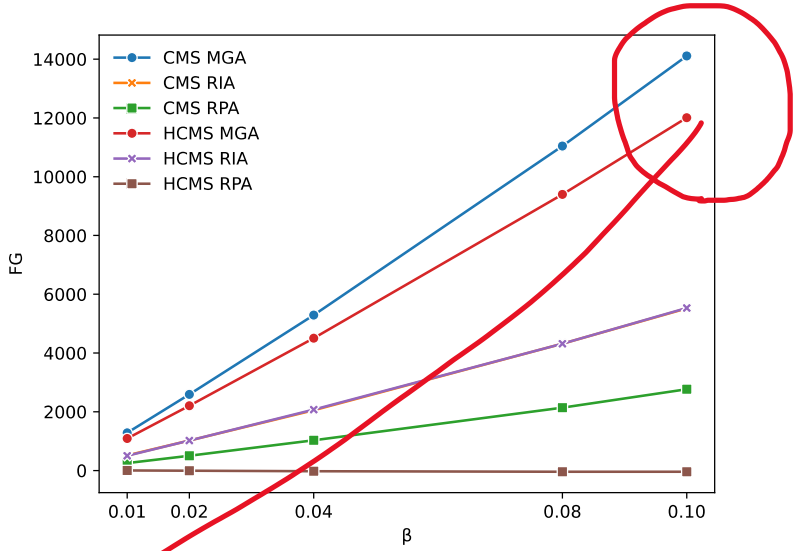
実験結果③（CMSとHCMSの安全性）



ターゲットアイテムの個数



プライバシー予算



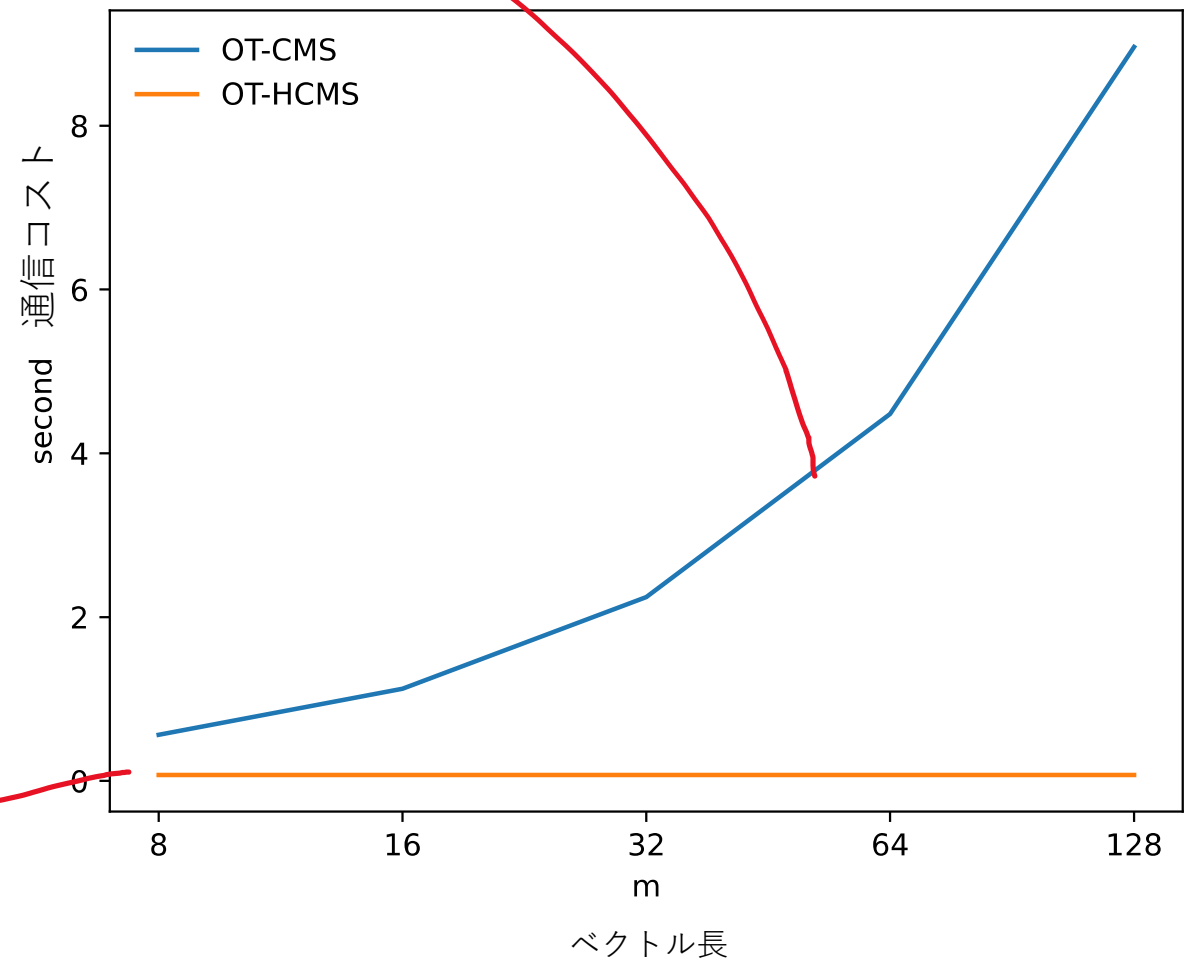
不正ユーザの割合

MGAは平均で16.0%CMSの方が脆弱！！

実験結果④　アダマール行列の適用

OT-CMSはベクトル長が増加するに従って、通信時間が**増加**する。

OT-HCMSはベクトル長が増加しても通信時間が**一定**



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**

まとめ

- 本研究では, LDPプロトコル CMSがポイズニング攻撃に対して脆弱であることを示し, 紛失通信を用いてロバストなOT-CMSを提案した.
- OT-CMSにアダマール行列を適用して送信時間を削減したOT-HCMSを提案した.
- 提案手法は従来手法よりMGAに対して最大で172%安全であることがわかった.
- 提案手法は本来のLDPの考え方と反している。