明治大学大学院　先端数理科学研究科

2022 年度

修士学位請求論文

EM アルゴリズムを用いた Key-Value データについての局所差分プライバシプロトコルの提案

学位請求者　先端メディアサイエンス専攻

堀込　光

目 次

第 1 章　序論 **1**
1.1 研究背景 1
1.2 研究の対象と研究目的 1
1.3 研究方法 2
1.4 新規性と貢献 2
1.5 本稿の構成 3

第 2 章　基本定義と従来研究 **5**
2.1 基本定義 5
2.2 局所差分プライバシ 5
2.3 Randomized Response(RR) 6
2.4 Harmony 7
2.5 PrivKV 8
2.5.1 摂動化 8
2.5.2 統計値推定 9
2.5.3 PrivKVM 10
2.6 局所差分プライバシへのポイズニング攻撃 10
2.6.1 M2GA 12
2.6.2 RMA 12
2.6.3 RKVA 13

第 3 章　EM アルゴリズムを用いた局所差分プライバシプロトコルの提案 **14**
3.1 基本 EM アルゴリズム 14
3.2 提案手法 emPrivKV 14
3.2.1 数値例 15

第 4 章　評価実験 **18**
4.1 目的 18
4.2 データセット 18
4.3 評価方法 18
4.3.1 推定精度 18
4.3.2 ポイズニング攻撃に対する強度 19
4.4 結果 19

4.4.1 推定精度 19
4.4.2 ポイズニング攻撃に対する強度 21
4.5 考察 24
4.6 提案手法の限界と解決方法 25

第 5 章 まとめ **29**

参考文献 **29**

謝辞 **32**

研究業績 **33**

第1章　序論

1.1　研究背景

スマートデバイスの大幅な普及により，サービス事業者はユーザのあらゆる行動を分析して利活用することができるようになった．例えば，スマートデバイスの日々の使用データを収集することで，バッテリー管理の最適化や，パーソナライズされたサービスおよびデジタルコンテンツの配信などに利用することができる．しかし，日々の使用データは非常に機密性の高いデータであり，多くの人が事業者に個人データをアクセスされることに抵抗を持っている．2020 年の総務省の調査では，日本人の 78% が自身のパーソナルデータを提供することに不安を感じていると回答した [12]．そのため，機密性の高いデータをより安全に取り扱い，利活用していくシステムの構築が必要となる．

局所差分プライバシ [1] は，機密性の高いデータを安全に収集する技術である．信頼性の低い事業者に自身の情報を送信する前に自身のデバイス内でランダマイズすることで，事業者に対して情報を秘匿化する．局所差分プライバシの保障のある安全性から Google[8] や Apple[23]，Microsoft[9] などのサービス企業は独自の局所差分プライバシプロトコルを用いて，ユーザの情報を収集している．

離散値と連続値の代表的な局所差分プライバシアルゴリズムとしてそれぞれ，Warner らによる Randomized Response(RR)[2] と Nguyên らによる Harmony[3] が知られている．Ye らは，key-value データの key に対して RR を value に対して Harmony を組み合わせて適用することで，局所差分プライバシを満たす局所差分プライバシプロトコル PrivKV[7] とその対話型プロトコル PrivKVM[7] を提案した．これにより，2 次元データである key-value データの key に対する頻度と value に対する平均値の相関を維持して推定することができる．

PrivKV のような多くの局所差分プライバシプロトコルでは，ランダマイズされたデータから最尤推定法を用いて統計情報を推定する [2, 3, 7]．しかし，最尤推定法では，データの頻度が小さすぎたり大きすぎる key では，推定精度を欠く場合がある．これは，多くのビックデータで一般に生じ得る条件であり，局所差分プライバシを用いる場合に避けられない課題である．また，局所差分プライバシプロトコルは，悪意のあるユーザが特定の情報を収集者に送信することで，不正を検知されずに分析結果を操作するポイズニング攻撃のような操作に対して脆弱であることが指摘されている [4]．

1.2　研究の対象と研究目的

key-value データは，多くのアプリケーションで使用されるデータ構造である．例えば，$\{\langle \mathrm{YouTube}, 0.5\rangle, \langle \mathrm{Twitter}, 0.1\rangle, \langle \mathrm{Instagram}, 0.2\rangle\}$ のような離散値 (アプリケーション名など) と連続値 (使用時間など) の組み合わせデータである．各ユーザは，複数のアイテム（key）とそれに対応する評価値 (value) を保持している．収集者は，評価数が多く評価値の高いアイテムをおすすめとして提供することなどを

目的として，全てのユーザから key-value データを収集し，各アイテムの評価数（頻度）と平均評価値を分析している．そのようなデータの利活用を促すために局所差分プライバシプロトコルを用いて，可変長である key-value データを安全に収集し，高精度に統計値を推定することが本研究の目的である．

また近年，Amazon のような推薦システムを用いているサイトでは，高評価のレビュー数を水増しして高評価のアイテムを装う不正操作が問題となっている．ユーザ自身がデータをランダマイズする局所差分プライバシでは，いくつかの不正操作が考えられる．そのため，複数の不正操作を想定し，不正操作が統計値へ与える影響を調査する必要がある．

1.3 研究方法

本研究では，EM(Expectation Maximization) アルゴリズム [6] に着目し，新しい局所差分プライバシプロトコル emPrivKV を提案する．EM アルゴリズムは，反復手法であり，ベイズの定理を用いて収集したランダマイズデータから事後確率を推定する．推定値の算出を反復することで，頻度が極端な key に対しても高い精度で推定することができる．

PrivKV の摂動対象の値域は連続値 $[-1, 1]$ であるところに困難がある．そこで，PrivKV の入力 v を直接推定する代わりに，2 値にランダマイズされた $v^* \in \{-1, 1\}$ に注目する．中間状態 v^* の集合 $X = \{\langle 1, 1\rangle, \langle 1, -1\rangle, \langle 0, 1\rangle, \langle 0, -1\rangle\}$ の事後確率を推定すれば，v の平均値も推定できるからである．こうして，PrivKV 特有の EM アルゴリズムを提案して，value の統計値の推定精度を向上することを試みる．

EM アルゴリズムに基づく提案方式は，局所差分プライバシプロトコルの潜在的な課題であるポイズニング攻撃 [4] に対しても効果がある．なぜならば，ポイズニング攻撃により歪んだ確率分布からの統計値推定の影響が小さいからである．本研究では，提案方式がポイズニング攻撃に頑強であることを Wu らが提案した 3 種類のポイズニング攻撃手法，Maximal Gain Attack(M2GA)，Random Message Attack(RMA)，Random Key-Value pair Attack(RKVA)[5] に対する耐性があることを実験的に示す．

1.4 新規性と貢献

Erlingsson らは，Randomized Aggregatable Privacy-Preserving Ordinal Response（RAPPOR）[8] を提案した．RAPPOR では，Bloom Filter を用いてエンコーディングされたデータの各ビットに対して RR[2] を適用し，ランダマイズを行う．さらに，各ユーザから収集したランダマイズデータに対して，最尤推定法を適用することで，アイテムの頻度を推定する．長谷川らは，RAPPOR によりランダマイズされたデータから入力集合の周辺確率を推定することで，EM アルゴリズムを適用し，推定精度を改善する手法を提案した [15]．Fant らの手法 [14] では，多次元データに対して各属性ごと独立に Bloom Filter を用いて RAPPOR を適用し，ランダマイズデータから EM アルゴリズムを用いて，入力ベクトルの組み合わせごとの同時確率を推定する．Ren らが提案した LoPub[13] では，各ビットの頻度を EM アルゴリズムと Lasso 回帰をハイブリットに適用しすることで，属性間の同時

確率を推定する．しかし，これらを本研究の対象である可変長の Key-Value データに直接適用することはできない．key-value データにおける統計値推定の精度を改善する手法として，エンコーディングに Padding-and-Sampling[16] を用いる PCKV[17] や Harmony を改良し，連続値の 2 値化区間を操作する PrivKVM* [18] などが提案されている．

局所差分プライバシの従来の手法と提案手法の比較を表 1.1 に整理する．Fant ら [14] や Ren ら [13] は局所差分プライバシプロトコルへの EM アルゴリズム適用手法を提案している．Fant らや Ren らは，国勢調査のように 1 ユーザの持つ記録レコードが固定長である多次元データに対して，多次元 Bloom Filter を用いた RAPPOR[8] を適用し，EM アルゴリズムや Rasso 回帰を用いて，属性間の同時確率を推定する．一方，提案手法では，購買履歴のようにあるユーザの key（離散値）と value（連続値）の複数レコードからなる可変長の 2 次元データ (key-value データ) を対象としている．連続値を含む 2 次元符号化したデータに対しての EM アルゴリズムは自明ではなく，我々の調査する限り初めての研究である．

また，本研究の貢献は以下の 3 つである．

- 局所差分プライバシプロトコル PrivKV でランダマイズされた key-value データから key の頻度と value の平均値を推定する新しい局所差分プライバシプロトコルを提案すること．
- ガウス分布，べき分布，線形分布のような既知の合成データや Movie Lens，Clothing Datasets のようなオープンデータセットを用いた実験において，データサイズやプライバシ費用 ϵ に関わらず精度の改善を示したこと．
- 提案手法のポイズニング攻撃に対する強度を調査したこと．

表 1.1: 先行研究との比較

	Fant ら [14]	Ren ら [13]	本提案方式
符号化	多次元 Bloom Filter, RAPPOR[8]	多次元 Bloom Filter, RAPPOR[8]	2 次元符号化, PrivKV[7]
推定	EM アルゴリズム	EM アルゴリズム, Lasso 回帰	EM アルゴリズム
対象	連続値を含む多次元データ	連続値を含む多次元データ	key（離散値） value（連続値）
ユーザのレコード	固定長	固定長	可変長
ポイズニング攻撃	未調査	未調査	本研究

1.5 本稿の構成

本稿の構成と，各章の概要は以下の通りである．

- 2 章：本稿の基本定義と従来研究を述べる．

- 3 章：Key-Value データにおける EM アルゴリズムを用いた局所差分プライバシプロトコルを説明する.
- 4 章：統計値の推定精度とポイズニング攻撃に対する強度を評価する.
- 5 章：本稿のまとめを行う.

第2章　基本定義と従来研究

2.1　基本定義

局所差分プライバシプロトコルでは，各ユーザが自身のデータに対してノイズを付与し，そのデータを収集者へ送信する．収集者は，各ユーザから得られたデータを集計し，度数や平均値を推定する．n 人のユーザの集合を $U = \{u_1, u_2, ..., u_n\}$ とする．各ユーザは離散値，連続値，または key-value データを保持している．取扱う d 種類の離散値の集合を $K = \{k_1, k_2, ..., k_d\}$，連続値 $[-1, 1]$ の集合を V とする．プライバシ費用を ϵ とし，ある入力を t に対するランダムアルゴリズム M を $M(t, \epsilon)$ と記述する．

2.2　局所差分プライバシ

局所差分プライバシ [1] の概要を図 2.1 に示す．局所差分プライバシは，機密性の高いデータを安全に収集する技術である．信頼性の低い事業者に自身の情報を送信する前に自身のデバイス内でランダマイズすることで，事業者に対して情報を秘匿化する．局所差分プライバシでは，任意の異なる 2 つの入力に対して，ランダムアルゴリズム M の出力が同一になる確率の比が十分に小さいことを保証している．これにより，出力からそのユーザの正確な入力を特定することができず，ユーザのプライバシーを保証する．ランダムアルゴリズム M についての局所差分プライバシは以下のように定義される．

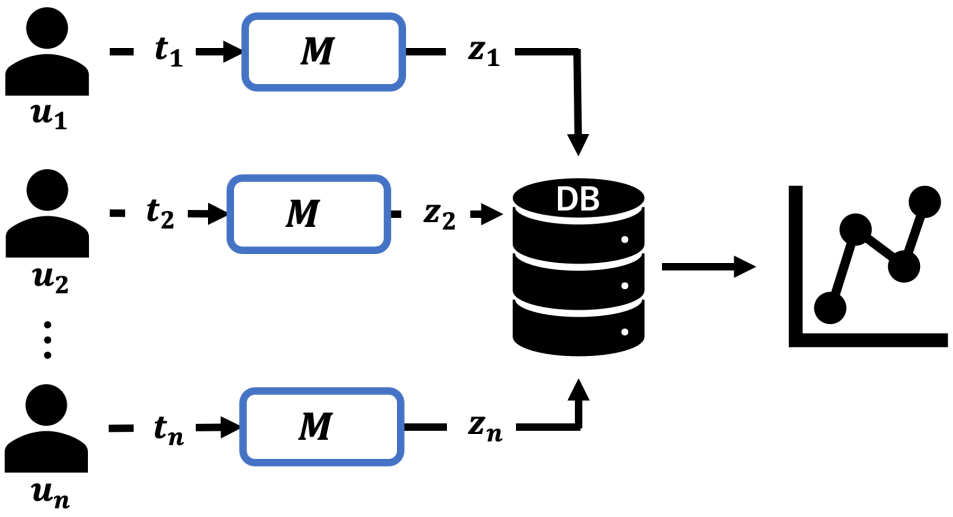


図 2.1: 局所差分プライバシの概要

定義 1. 局所差分プライバシ [1]

D を入力の集合，Z を出力の集合とする．M を入力 $t \in D$ に対して $z \in Z$ を出力するランダムアルゴリズムとする．任意の 2 つの入力 $t, t' \in D$ と任意の出力 $z \in Z$ に対して，

$$\frac{Pr[M(t,\epsilon) = z]}{Pr[M(t',\epsilon) = z]} \leq e^{\epsilon}$$

が成立するとき，ランダムアルゴリズム M は ϵ-局所差分プライバシを満たすという．

2.3 Randomized Response(RR)

離散値データの局所差分プライバシアルゴリズムに Randomized Response(RR)[2] がある．RR では，確率 p で真の値を出力し，それ以外の確率 q で偽の値を出力することで，プライバシを保護する．収集者は全ユーザの出力 $k^* \in K$ から各離散値の度数を推定する．

入力 d 種類の離散値の集合 K 中からユーザが保有する値 $k \in K$ を入力とする．

摂動 確率 p で真の値 k を出力し，確率 q で K の中から k 以外の値 $k' \in K - \{k\}$ を出力する．すなわち，

$$k^* = \begin{cases} k & w/p \quad p, \\ k' & w/p \quad q \end{cases}$$

となる．

定理 1. Randomized Response[21]

維持確率 p，遷移確率 q が以下のとき，局所差分プライバシを満たす．

$$\begin{cases} p = \frac{e^{\epsilon}}{e^{\epsilon}+d-1}, \\ q = \frac{1}{e^{\epsilon}+d-1}. \end{cases}$$

証明. 異なる 2 つの入力 $k, \hat{k} \in K$ に対して，同一の出力 k^* となるとき，入力に対する出力の確率比の最大は，

$$\begin{aligned} \frac{Pr[RR(k,\epsilon) = k^*]}{Pr[RR(\hat{k},\epsilon) = k^*]} &\leq \frac{Pr[RR(k,\epsilon) = k]}{Pr[RR(\hat{k},\epsilon) = k]} \\ &= \frac{p}{\frac{1-p}{d-1}} \\ &= \frac{p}{q} \\ &= e^{\epsilon} \end{aligned}$$

となる． □

集計 n 人のユーザから出力を収集し，各 $k_i \in K$ の度数を推定する．収集した出力の中で k_i の度数を f_i' とし，k_i の真の度数を f_i とする．最尤推定法では，k_i を保有する平均 $f_i p$ のユーザが k_i を出力し，k_i 以外を保有する平均 $(1 - f_i)q$ のユーザが k_i を出力するため f_i' の期待値は，

$$f_i' = f_i p + (1 - f_i)q$$

となる．上式から真の度数 f_i の最尤値は，

$$L[f_i] = \frac{f_i' - q}{p - q} = \frac{f_i' - 1 + p}{2p - 1} \tag{2.1}$$

となる．

2.4 Harmony

Nguyên らは連続データの局所差分プライバシアルゴリズムに Harmony[3] を提案している．Harmony では，連続値 $v \in V$ を 2 値化することで，RR の適用を可能にしている．また，RR を適用した値を定数倍することで，期待値を v として出力する．

入力 ユーザの保有する連続値 $v \in V(= [-1, 1])$ を入力とする．

摂動 Harmony の摂動工程を Value Perturbation Primitive(VPP) と呼ぶ．VPP には，連続値 v を 2 値化する工程と 2 値化された値 v^* に対して RR を適用する工程がある．

・2 値化 入力 v に対して，v に依存する確率で 2 値化された値を $v^*(\in \{-1, 1\})$ とする．

$$v^* = \begin{cases} 1 & w/p \quad \frac{1+v}{2}, \\ -1 & w/p \quad \frac{1-v}{2}. \end{cases}$$

・Randomized Response 2 値化された v^* に対して $RR(v^*, \epsilon)$ を適用する．

$$v^+ = \begin{cases} v^* & w/p \quad p = \frac{e^\epsilon}{e^\epsilon + 1}, \\ -v^* & w/p \quad q = \frac{1}{e^\epsilon + 1}. \end{cases}$$

Harmony では，VPP で得られた値に対して，定数倍した $\hat{v}$ を出力とする．

$$\hat{v} = v^+ \frac{e^\epsilon + 1}{e^\epsilon - 1}$$

定理 2. VPP，Harmony[3]

ランダムアルゴリズム VPP と Harmony は局所差分プライバシを満たす．

証明. 2 つの異なる入力 $v, v' \in V$ に対して同一の出力 $v^+ = 1$ となるとき，入力に対する出力の確率比は，

$$\begin{aligned} \frac{Pr[VPP(v, \epsilon) = 1]}{Pr[VPP(v', \epsilon) = 1]} &= \frac{\frac{1+v}{2}p + \frac{1-v}{2}q}{\frac{1+v'}{2}p + \frac{1-v'}{2}q} \\ &\leq \frac{\max_v\{v(e^\epsilon - 1) + e^\epsilon + 1\}}{\min_{v'}\{v'(e^\epsilon - 1) + e^\epsilon + 1\}} \\ &= e^\epsilon \end{aligned}$$

となる．$v^+ = -1$ についても同様に成立し，ϵ-局所差分プライバシを満たす．また，Harmony は VPP で得られた値を定数倍しているので，異なる 2 つの入力に対する出力の比は VPP と同様であり，ϵ-局所差分プライバシを満たす． □

このとき，入力 v に対する出力 $\hat{v}(=\{-\frac{e^\epsilon+1}{e^\epsilon-1}, \frac{e^\epsilon+1}{e^\epsilon-1}\})$ の期待値は，

$$\begin{aligned} E(\hat{v}) &= \frac{e^\epsilon+1}{e^\epsilon-1}(\frac{1+v}{2}p + \frac{1-v}{2}q) - \frac{e^\epsilon+1}{e^\epsilon-1}(\frac{1+v}{2}q + \frac{1-v}{2}p) \\ &= \frac{e^\epsilon+1}{e^\epsilon-1}(vp - vq) \\ &= v\frac{e^\epsilon+1}{e^\epsilon-1}\frac{e^\epsilon-1}{e^\epsilon+1} \\ &= v \end{aligned}$$

となる．

集計 Harmony では，n のユーザから出力を収集し，平均値 m を推定する．収集した出力の中で，$\hat{v} = \frac{e^\epsilon+1}{e^\epsilon-1}$ の度数を m_1，$\hat{v} = -\frac{e^\epsilon+1}{e^\epsilon-1}$ の度数を $m_2(= 1 - m_1)$ とする．平均値 $\hat{m}$ は以下のように推定される．

$$\hat{m} = \frac{m_1 - m_2}{n} \tag{2.2}$$

2.5 PrivKV

Ye らは離散値と連続値の 2 次元データである key-value データについての局所差分プライバシアルゴリズム PrivKV[7] を提案した．PrivKV では，離散値のランダマイズに依存した確率で連続値を同時にランダマイズすることで，離散値と連続値の相関を維持する．PrivKV は，$k_i \in K$ に対する頻度と $v_i \in V$ に対する平均値の推定を目的とする．本節では，PrivKV のランダマイズ方式と統計値 (度数，平均値) の推定方式を説明する．

2.5.1 摂動化

入力 i 番目のユーザ u_i が持つ ℓ_i 個の key-value 対の入力集合を $S_i = \{\langle k_j, v_j\rangle | 1 \le j \le \ell_i, k_j \in K, v_j \in V\}$ とする．S_i を key-vlaue 集合，S_i の h 番目の $\langle k_h, v_h\rangle$ を key-value データと呼ぶ．

符号化 d 種類の key-value データの収集を考える．S_i の符号化ベクトルを $S_i' = (\langle k_1', v_1'\rangle, \cdots, \langle k_d', v_d'\rangle)$ とする．ここで，$\langle k_j, v_j\rangle \in S_i$ について，

$$\langle k_s', v_s'\rangle = \begin{cases} \langle 1, v_j\rangle \text{ if } \langle k_j, *\rangle \in S_i, \\ \langle 0, 0\rangle \text{ otherwise} \end{cases}$$

と符号化する．例えば，$\ell = 3, d = 5$ の入力集合 $S_i = \{\langle k_1, v_1\rangle, \langle k_4, v_4\rangle, \langle k_5, v_5\rangle\}$ の符号化ベクトル S_i' は，

$$S_i' = (\langle 1, v_1\rangle, \langle 0, 0\rangle, \langle 0, 0\rangle, \langle 1, v_4\rangle, \langle 1, v_5\rangle)$$

である．

摂動 key-value データの摂動には，value を摂動する工程と key を摂動する工程がある．key と value のランダマイズにはそれぞれ ϵ_1，ϵ_2 を割り当てる．長さ d の符号化ベクトル S_i' からランダムに 1 つの key-value データ $\langle k_a', v_a'\rangle \in S_i'$ を選択する．

・**value の摂動** $k'_a = 0$ の場合，v'_a を $[-1, 1]$ からランダムに選択する．まず，value の値を v'_a に依存する確率で，

$$v^*_a = \begin{cases} 1 & w/p \quad \frac{1+v'_a}{2}, \\ -1 & w/p \quad \frac{1-v'_a}{2} \end{cases}$$

と v^*_a に 2 値化する．次に v^*_a を

$$v^+_a = \begin{cases} v^*_a & w/p \quad p_2 = \frac{e^{\epsilon_2}}{1+e^{\epsilon_2}}, \\ -v^*_a & w/p \quad q_2 = \frac{1}{1+e^{\epsilon_2}} \end{cases}$$

でランダマイズし，v^+_a とする．

・**key の摂動** PrivKV では，key が遷移するとき value も同時に変化させる．key のランダマイズは

$k'_a = 1$ の場合，

$$\langle k^*_a, v^+_a \rangle = \begin{cases} \langle 1, v^+_a \rangle & w/p \quad p_1 = \frac{e^{\epsilon_1}}{1+e^{\epsilon_1}}, \\ \langle 0, 0 \rangle & w/p \quad q_1 = \frac{1}{1+e^{\epsilon_1}} \end{cases}$$

$k'_a = 0$ の場合，

$$\langle k^*_a, v^+_a \rangle = \begin{cases} \langle 0, 0 \rangle & w/p \quad p_1 = \frac{e^{\epsilon_1}}{1+e^{\epsilon_1}}, \\ \langle 1, v^+_a \rangle & w/p \quad q_1 = \frac{1}{1+e^{\epsilon_1}}, \end{cases}$$

とする．摂動化 $\langle k^*_a, v^+_a \rangle$ と選択した key-value データのインデックス a を送信する．

差分プライバシの合成定理により，差分プライバシを満たす複数のランダムアルゴリズムを多重に適用したアルゴリズムは全てのプライバシー費用 ϵ_i の和について差分プライバシを満たすことが知られている [22]．局所差分プライバシも同様であり，その際，全体のプライバシー費用 ϵ を求めることができる．

定理 3. 連続的な局所差分プライバシアルゴリズムの組み合わせによるプライバシ費用 [22]

b 個のランダムアルゴリズムが累積した合成アルゴリズムを $\hat{M}$ とし，b 個のランダムアルゴリズムの集合を $M^* = \{M_1, M_2, ..., M_b\}$ とする．M^* のそれぞれのランダムアルゴリズム $M^*{}_i$ が ϵ_i-局所差分プライバシを満たすとき，b 個のランダムアルゴリズムが累積した合成アルゴリズム $\hat{M}$ は局所差分プライバシを満たし，全体の $\epsilon_{\hat{M}}$ は，

$$\epsilon_{\hat{M}} = \epsilon_{M^*{}_1} + \epsilon_{M^*{}_1} + \ldots + \epsilon_{M^*{}_b}$$

について $\epsilon_{\hat{M}}$-局所差分プライバシを満たす．

定理 3 の証明は，[22] を参照されたい．ランダムアルゴリズム VPP と RR を組み合わせた PrivKV 全体のプライバシ費用 ϵ は $\epsilon = \epsilon_1 + \epsilon_2$ となり，本稿では，$\epsilon_1 = \epsilon_2 = \frac{\epsilon}{2}$ と仮定する．

2.5.2 統計値推定

頻度推定 収集した key-value データ $\langle k^*_a, v^+_a \rangle$ の中で，$k_i = 1$ の度数を f'_i とし，k_i の真の度数を f_i とする．k_i の度数の最尤値 $\hat{f}_i$ は，

$$\hat{f}_i = \frac{p_1 - 1 + f'_i}{2p_1 - 1} \tag{2.3}$$

と推定される．ここで，$p_1 = \frac{e^{\epsilon_1}}{1+e^{\epsilon_1}}$ である．

平均値推定 収集したkey-valueデータ $\langle k_a^*, v_a^+ \rangle$ の中で，$\langle k_i, v_i \rangle = \langle 1, 1 \rangle$ の度数を n'_{1i}，$\langle k_i, v_i \rangle = \langle 1, -1 \rangle$ の度数を n'_{2i} とする．$\langle k_i, v_i \rangle = \langle 1, 1 \rangle$ の推定度数 $\hat{n}_{1i}$ と $\langle k_i, v_i \rangle = \langle 1, -1 \rangle$ の推定度数 $\hat{n}_{2i}$ は，

$$\begin{aligned} \hat{n}_{1i} &= \frac{N(p_2 - 1) + n'_{1i}}{2p_2 - 1}, \\ \hat{n}_{2i} &= \frac{N(p_2 - 1) + n'_{2i}}{2p_2 - 1} \end{aligned}$$

となる．ここで，$N = n'_{1i} + n'_{2i}$，$p_2 = \frac{e^{\epsilon_2}}{1+e^{\epsilon_2}}$ となり，平均値 $\hat{m}_i$ は，

$$\hat{m}_i = \frac{\hat{n}_{1i} - \hat{n}_{2i}}{N} \tag{2.4}$$

と推定される．

2.5.3 PrivKVM

PrivKV のランダマイズでは，key-value データのサンプリングで $\langle k'_a, v'_a \rangle \in S'_i = \langle 0, 0 \rangle$ が選択された場合，v'_a は $[-1, 1]$ からランダムに値が付与される．度数の少ない key では，v'_a がランダムに付与される割合が大きいため，平均値は 0 に近づく．そこで Ye らは，PrivKV の対話型アルゴリズム PrivKVM[7] と PrivKVM*[18] を提案した．PrivKVM では，算出した平均値をユーザに送り返し，2 回目以降の摂動で，$\langle k'_a, v'_a \rangle \in S'_i = \langle 0, 0 \rangle$ のとき，$v'_a = \hat{m}_a$ とすることでこの問題を解決している．

ユーザとの対話回数を $c(\geq 2)$ とし，c 回目の推定度数，推定平均値をそれぞれ $\hat{f}_i^{(c)}$，$\hat{m}_i^{(c)}$ とする．また，key のランダマイズと value のランダマイズで対話ごとに割り振る ϵ をそれぞれ，$\epsilon_{11}, \epsilon_{12}, ..., \epsilon_{1c}$ と $\epsilon_{21}, \epsilon_{22}, ..., \epsilon_{2c}$ とする．1 回目の収集では，PrivKV を用いて推定値 $\hat{f}_i^{(1)}, \hat{m}_i^{(1)} = PrivKV(S'_i, (\epsilon_{11} + \epsilon_{21}))$ を算出する．2 回目以降の収集では，$\langle k'_a, v'_a \rangle \in S'_i = \langle 0, 0 \rangle$ の場合，$v'_a = {m_i}^{(c-1)}$ とする．c 回の対話のあと，$\hat{f}_i^{(1)}$，$\hat{m}_i^{(c)}$ を推定値とする．[7] では，

$$\begin{cases} \epsilon_1 = \epsilon_2 = \frac{\epsilon}{2}, \\ \epsilon_{11} = \epsilon_1, \quad \epsilon_{12} = \epsilon_{13} = \cdots = \epsilon_{1c} = 0, \\ \epsilon_{21} = \epsilon_{22} = \cdots = \epsilon_{1c} = \frac{\epsilon_2}{c} \end{cases}$$

のように，ϵ を割り振っている．またこのとき，$\epsilon_1 = \epsilon_{11} + \epsilon_{12} + \cdots + \epsilon_{1c}$，$\epsilon_2 = \epsilon_{21} + \epsilon_{22} + \cdots + \epsilon_{2c}$ となる．本稿でも同様の大きさで ϵ を割り振る．このとき，key のランダマイズのプライバシ費用は PrivKV と同じであるため，PrivKVM での推定度数 $\hat{f}_i$ は PrivKV と同じである．

2.6 局所差分プライバシへのポイズニング攻撃

局所差分プライバシにおいてポイズニング攻撃とは，攻撃者がある key に対して特定の情報をサーバに送信することで，その key の推定値を操作する攻撃である．局所差分プライバシでは，ユーザが自身の情報をランダマイズし送信情報を作成するため，サーバに気づかれずにポイズニングを自在にできる．

攻撃者は，局所差分プライバシプロトコルを参照でき，システム上で m 人の偽ユーザを容易に作成し，偽ユーザから特定の情報を送信する．偽ユーザの集合を $U_m = \{u_{n+1}, u_{n+2}, \cdots, u_{n+m}\}$ とす

る．また，偽ユーザ i の出力を y_i とし，その集合を $Y = \{y_{n+1}, y_{n+2}, \cdots, y_{n+m}\}$ とする．攻撃者が操作する r 個の key をターゲット key とし，その集合を $T = \{k_1, k_2, \cdots, k_r\}$ とする．サーバは，n 人の真ユーザと m 人の偽ユーザを合わせた $n+m$ 人の出力から統計値を推定する．

n 人の真ユーザの key k に対する推定度数を $\hat{f}_k$，偽ユーザを含めた $n+m$ 人の key k に対する推定度数を $\tilde{f}_k$ とする．ポイズニング攻撃による推定度数の変化量を $\Delta\hat{f}_k = \tilde{f}_k - \hat{f}_k$ とし，ターゲット key に対する平均変化量の総和を頻度利得 (frequency gain)[5]

$$G_f(Y) = \sum_{k \in T} \mathbb{E}[\Delta \hat{f}_k] \tag{2.5}$$

と呼ぶ．また，同様に n 人の真ユーザの key k に対する推定平均値を $\hat{m}_k$，偽ユーザを含めた $n+m$ 人の key k に対する推定平均値を $\tilde{m}_k$ とする．ポイズニング攻撃による推定平均値の変化量を $\Delta\hat{m}_k = \tilde{m}_k - \hat{m}_k$ とし，その平均変化量の総和を値利得 (mean gain)[5]

$$G_m(Y) = \sum_{k \in T} \mathbb{E}[\Delta \hat{m}_k] \tag{2.6}$$

とする．

本研究では，ポイズニング攻撃による統計値操作の影響を調査するために，Wu らが提案した以下の 3 つのポイズニング攻撃手法を取り扱う．各ポイズニング攻撃の構成図を図 2.2 に示す．

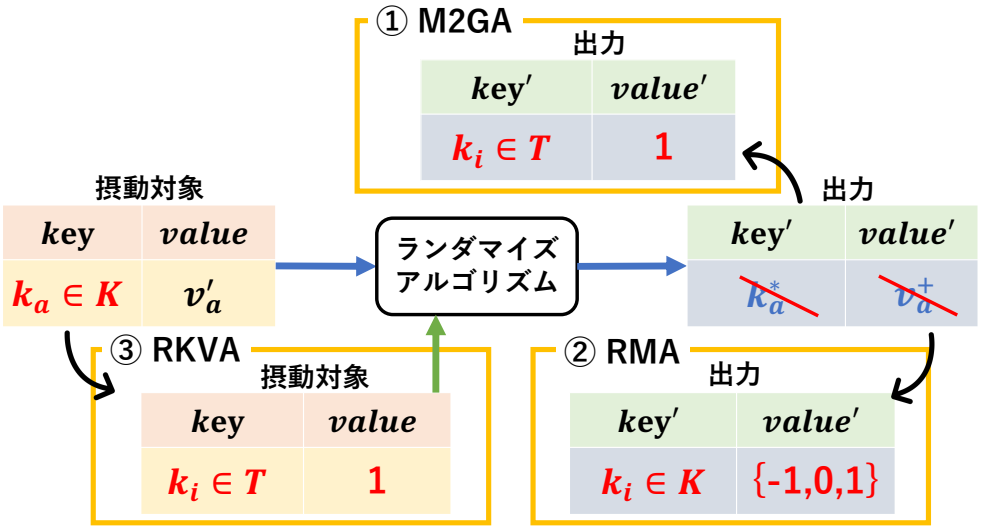


図 2.2: ポイズニング攻撃

・Maximal Gain Attack(M2GA) 摂動化後のデータを加工する．偽ユーザは，ターゲット key からインデックスを選択し，$\langle 1, 1\rangle$ を送信することで，ターゲット key の頻度利得と値利得の両方を最大にする．

・Random Message Attack(RMA) 摂動化データをランダムなものに置き換える．サーバに送信する key-value データを出力候補の中からランダムに選択し，そのインデックスを K からランダムに選択する．このとき，$\frac{1}{2}$ の確率で $\langle 0, 0\rangle$ を送信し，$\frac{1}{4}$ の確率で $\langle 1, 1\rangle$ か $\langle 1, -1\rangle$ を送信する．

・Random Key-Value pair Attack(RKVA) 摂動化前の符号化データを操作し，定められた摂動化を行う．偽ユーザは，ターゲット key からインデックスを選択し，$\langle 1,1\rangle$ を摂動対象として PrivKV を適用し，得られた出力を送信する．

2.6.1 M2GA

M2GA は，出力を操作する攻撃である．また，偽ユーザは頻度利得と値利得の両方が最大になるように出力を作成する．このとき，頻度利得と値利得は最尤推定法により算出されたものとする．n_1^k，n_{-1}^k をそれぞれ真のユーザの中で $\langle k,1\rangle$，$\langle k,-1\rangle$ を出力した人数とする．また，$\tilde{n}_1^k$，$\tilde{n}_{-1}^k$ をそれぞれ偽ユーザの中で $\langle k,1\rangle$，$\langle k,-1\rangle$ を出力した人数とする．PrivKV ではユーザは，1 つの key-value データとそのインデックスを出力する．

まず，頻度利得が最大になる条件を考える．頻度利得 $G_f(Y)$ は以下のように式変形できる．

$$\begin{aligned} G_f(Y) &= \sum_{k\in T}\mathbb{E}[\tilde{f}_k]-\mathbb{E}[\hat{f}_k] \\ &= \sum_{k\in T}\left\{\mathbb{E}\left[\frac{(n_1^k+n_{-1}^k+\tilde{n}_1^k+\tilde{n}_{-1}^k)/(n+m)-q_1}{p_1-q_1}\right]-\mathbb{E}\left[\frac{(n_1^k+n_{-1}^k)/n-q_1}{p_1-q_1}\right]\right\} \end{aligned}$$

なので，偽ユーザの出力の集合 Y は，$\sum_{k\in T}\mathbb{E}[\frac{\tilde{n}_1+\tilde{n}_{-1}}{(n+m)(p_1-q_1)}]$ に影響する．また，$(n+m)(p_1-q_1)$ は定数であるため，頻度利得 $G_f(Y)$ を最大にするためには，$\sum_{k\in T}\mathbb{E}[\tilde{n}_1+\tilde{n}_{-1}]$ を最大にする必要がある．偽ユーザの全てがターゲット key T から意図的に特定のインデックス k を選択し，$\langle 1,1\rangle$ か $\langle 1,-1\rangle$ を送信したとき，$\sum_{k\in T}(\mathbb{E}[\tilde{n}_1^k]+\mathbb{E}[\tilde{n}_{-1}^k])=m$ となり，頻度利得 $G_f(Y)$ が最大となる．

次に，同様に値利得が最大になる条件を考える．値利得 $G_m(Y)$ は以下のように式変形できる．

$$\begin{aligned} G_m(Y) &= \sum_{k\in T}\mathbb{E}[\tilde{m}_k]-\mathbb{E}[\hat{m}_k] \\ &= \sum_{k\in T}\left\{\mathbb{E}\left[\frac{n_1^k-n_{-1}^k+\tilde{n}_1^k-\tilde{n}_{-1}^k}{(p_2-q_2)(n_1^k+n_{-1}^k+\tilde{n}_1^k+\tilde{n}_{-1}^k)}\right]-\mathbb{E}\left[\frac{n_1^k+n_{-1}^k}{(p_2-q_2)(n_1^k+n_{-1}^k)}\right]\right\} \end{aligned}$$

$c_1^k=nf_k(p_2-q_2)m_k$，$c_2^k=nf_k$ とすると，値利得 $G_m(Y)$ を最大にするためには，$\sum_{k\in T}\frac{\mathbb{E}[\tilde{n}_1-\tilde{n}_{-1}]+c_1^k}{\mathbb{E}[\tilde{n}_1+\tilde{n}_{-1}]+c_2^k}$ を最大にする必要がある．なので，偽ユーザの全てがターゲット key T から意図的に特定のインデックス k を選択し，value= 1 を送信したとき，$\mathbb{E}[\tilde{n}_1^k]=\frac{m}{r}$，$\mathbb{E}[\tilde{n}_{-1}^k]=0$ となり，値利得 $G_m(Y)$ が最大となる．つまり，M2GA では，ターゲット key の頻度利得と値利得の両方を最大にするために，全偽ユーザはターゲット key を 1 つ任意に選択し，$\langle 1,1\rangle$ を送信する．

2.6.2 RMA

RMA は，出力をランダムに選択する攻撃である．RMA では偽ユーザは K から key を一つランダムに選択し，出力に関しても出力候補の中からランダムに選択する．つまり，$\frac{1}{2}$ の確率で，$\langle 0,0\rangle$ を送信し，$\frac{1}{4}$ の確率で，$\langle 1,1\rangle$ か $\langle 1,-1\rangle$ を送信する．このとき，偽ユーザは $\frac{1}{2d}$ の確率で，key k に対する推定値を操作する．つまり，$E[\tilde{n}_1^k]=E[\tilde{n}_{-1}^k]=\frac{m}{4d}$ となる．

2.6.3 RKVA

RKVA は，摂動対象を操作する攻撃である．RKVA では，偽ユーザはターゲット key$T$ から key を一つランダムに選択する．また，偽ユーザは，$\langle 1, 1\rangle$ を摂動対象として PrivKV を適用し，得られた出力を送信する．このとき，$\mathbb{E}[\tilde{n}^k_1] = \frac{me^{\epsilon_1}e^{\epsilon_2}}{r(e^{\epsilon_1}+1)(e^{\epsilon_2}+1)}$，$\mathbb{E}[\tilde{n}^k_{-1}] = \frac{me^{\epsilon_1}}{r(e^{\epsilon_1}+1)(e^{\epsilon_2}+1)}$ となる．

第3章　EMアルゴリズムを用いた局所差分プライバシプロトコルの提案

本節では，key-value データに対して EM アルゴリズムを適用した局所差分プライバシプロトコル emPrivKV を提案する．

3.1　基本 EM アルゴリズム

d 種類の入力の集合を $X = \{x_1, x_2..., x_d\}$，d' 種類の出力の集合を $Z = \{z_1, z_2..., z_{d'}\}$ とする．n 人のユーザがそれぞれ自身の持つ値 $x_i \in X$ を入力とし，ランダムアルゴリズムを適用し，出力 $z_j \in Z$ を送信する．反復回数を t として，出力の集計から d 個の入力について度数推定を行う．t 回目の x_i 推定値を $\theta^{(t)} = ({\theta_1}^{(t)}, {\theta_2}^{(t)}, \ldots, {\theta_d}^{(t)})$ とし，初期値を $\theta^{(0)} = (\frac{1}{d}, \frac{1}{d}, \ldots, \frac{1}{d})$ とする．ユーザ u の t 回目の X に対する推定値を $\hat{\theta}_u^{(t)} = (\hat{\theta}_{u,1}^{(t)}, \hat{\theta}_{u,2}^{(t)}, \ldots, \hat{\theta}_{u,d}^{(t)})$ とする．

入力 x_i に対して出力 z_j となる条件付き確率は，ベイズの定理より，

$$Pr[z_j|x_i] = \frac{Pr[z_j, x_i]}{Pr[x_i]}$$

となる．従って，出力 z_j で条件付けられたとき入力が x_i である事前確率は，

$$Pr[x_i|z_j] = \frac{Pr[z_j|x_i]Pr[x_i]}{\sum_{s=1}^{|X|} Pr[z_j|x_s]Pr[x_s]}$$

となり，$t-1$ 回目の推定出力 z_j に対する入力 x_i の t 回目の推定確率は，

$$\hat{\theta}_{u,i}^{(t)} = Pr[x_i|z_j] = \frac{Pr[z_j|x_i]{\theta_i}^{(t-1)}}{\sum_{s=1}^{|X|} Pr[z_j|x_s]{\theta_s}^{(t-1)}}$$

で更新される．$t-1$ 回目の推定値 $\theta^{(t-1)}$ を用いて，ユーザごとに $\hat{\theta}_u^{(t-1)}$ を計算し，$\hat{\theta}_u^{(t-1)}$ の平均値 $\theta^{(t)}$ を

$$\theta^{(t)} = \frac{1}{n}\sum_{u=1}^{n} \hat{\theta}_u^{(t-1)}$$

とする．これをあらかじめ定めた閾値 $\eta > 0$ に対して，$|{\theta_i}^{(t)} - {\theta_i}^{(t-1)}| \leq \eta$ となって ${\theta_i}^{(t)}$ が収束するまで繰り返す．

3.2　提案手法 emPrivKV

提案方式のアルゴリズムを Algorithm 1 に示す．出力 $\langle k_a^*, v_a^+ \rangle$ から摂動工程の中の VPP を適用し value を 2 値化した key-value データ $\langle k_a', v_a^* \rangle$ を推定する．このとき，$X = \{\langle 1, 1\rangle, \langle 1, -1\rangle, \langle 0, 1\rangle, \langle 0, -1\rangle\}$，

出力の集合 $Z = \{\langle 1,1\rangle, \langle 1,-1\rangle, \langle 0,0\rangle\}$ に対する入力 $X = \{\langle 1,1\rangle, \langle 1,-1\rangle, \langle 0,1\rangle, \langle 0,-1\rangle\}$ の事後確率は表 3.1 に従う．例えば，出力 $\langle k_a^*, v_a^+\rangle = \langle 1,1\rangle$ であったとき，$\langle k_a', v_a^*\rangle = \langle 1,-1\rangle$ である事後確率 $Pr[\langle 1,1\rangle|\langle 1,-1\rangle] = p_1 q_2$ となる．

n 人のユーザから出力 $\langle k_a^*, v_a^+\rangle \in Z$ を観測する．$k_a \in K$ について初期値は $\theta^{(0)} = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ とする．t 回の反復を行なった結果得られた入力 X の推定度数を $\theta^{(t)} = (\theta^{(t)}_{\langle 1,1\rangle}, \theta^{(t)}_{\langle 1,-1\rangle}, \theta^{(t)}_{\langle 0,1\rangle}, \theta^{(t)}_{\langle 0,-1\rangle})$ とする．

定理 4. 推定値

推定度数 $\hat{f}_a$ は，

$$\hat{f}_a = \theta^{(t)}{}_{\langle 1,1\rangle} + \theta^{(t)}{}_{\langle 1,-1\rangle} \tag{3.1}$$

となり，推定平均値 $\hat{m}_a$ は，

$$\hat{m}_a = \frac{\theta^{(t)}_{\langle 1,1\rangle} - \theta^{(t)}_{\langle 1,-1\rangle}}{\theta^{(t)}_{\langle 1,1\rangle} + \theta^{(t)}_{\langle 1,-1\rangle}} \tag{3.2}$$

となる．

証明. *2*値化データ $\langle k_a', v_a^*\rangle$ が $\langle 1,1\rangle$ や $\langle 1,-1\rangle$ であるのは，key k_a についてそのユーザが v_a の値を保有しているとき，およびそのときに限る．2 値化データ $\langle k_a', v_a^*\rangle = \langle 1,1\rangle$ の割合を $\theta_{\langle 1,1\rangle}$，$\langle k_a', v_a^*\rangle = \langle 1,-1\rangle$ の割合を $\theta_{\langle 1,-1\rangle}$ とする．長さ d の符号化ベクトル S_i' からランダムに 1 つの摂動対象データ $\langle k_a', v_a'\rangle$ を選択するとき，$k_a' = 1$ であるユーザの割合の期待値は，

$$\mathbb{E}[k_a' = 1] = \mathbb{E}[\theta_{\langle 1,1\rangle} + \theta_{\langle 1,-1\rangle}]$$

となる．ゆえに，k_a の値を保有するユーザの割合は，

$$\hat{f}_a = \theta_{\langle 1,1\rangle} + \theta_{\langle 1,-1\rangle}$$

となる．v_a の平均値 m_a の期待値は

$$\mathbb{E}[\hat{m}_a] = \mathbb{E}\left[\frac{\theta_{\langle 1,1\rangle} - \theta_{\langle 1,-1\rangle}}{\theta_{\langle 1,1\rangle} + \theta_{\langle 1,-1\rangle}}\right]$$

なので，平均値は，

$$\hat{m}_a = \frac{\theta^{(t)}_{\langle 1,1\rangle} - \theta^{(t)}_{\langle 1,-1\rangle}}{\theta^{(t)}_{\langle 1,1\rangle} + \theta^{(t)}_{\langle 1,-1\rangle}}$$

となる． □

3.2.1 数値例

k_a の度数 $\hat{f}_a$ と平均値 $\hat{m}_a$ を推定することを考える．ユーザ u の出力 $\langle k_a^*, v_a^+\rangle \in Z$ が $z_1 = \langle 1,1\rangle$ であったとする．度数を推定する key-value データ $X = (\langle 1,1\rangle, \langle 1,-1\rangle, \langle 0,1\rangle, \langle 0,-1\rangle)$ の度数初期値を

表 3.1: 出力 Z に対する X の事後確率 $Pr[Z|X]$

$X = \langle k'$	$, v^+\rangle$	$Z = \langle k^*$	$, v^*\rangle$	$Pr[z\|x]$
1	1	1	1	p_1p_2
1	1	1	-1	p_1q_2
1	1	0	0	$q_1(p_2+q_2)$
1	-1	1	1	p_1q_2
1	-1	1	-1	p_1p_2
1	-1	0	0	$q_1(p_2+q_2)$
0	1	1	1	q_1p_2
0	1	1	-1	q_1q_2
0	1	0	0	$p_1(p_2+q_2)$
0	-1	1	1	q_1q_2
0	-1	1	-1	q_1p_2
0	-1	0	0	$p_1(p_2+q_2)$

$\theta^{(0)} = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ とする．出力 $\langle k_a^*, v_a^+\rangle$ が $z_1 = \langle 1, 1\rangle$ であったとき，value を 2 値化した key-value データ $\langle k_a', v_a^*\rangle$ が $x_1 = \langle 1, 1\rangle$ である確率は，ベイズの定理を用いて，

$$
\begin{aligned}
Pr[x_1|z_1] &= \frac{Pr[z_1|x_1]Pr[x_1]}{\sum_{s=1}^{4} Pr[z_1|x_s]Pr[x_s]} \\
&= \frac{Pr[z_1|x_1]{\theta_1}^{(0)}}{\sum_{s=1}^{4} Pr[z_1|x_s]{\theta_s}^{(0)}} \\
&= \frac{\frac{1}{4}p_1p_2}{\frac{1}{4}p_1p_2 + \frac{1}{4}p_1q_2 + \frac{1}{4}q_1p_2 + \frac{1}{4}q_1q_2} \\
&= \frac{p_1p_2}{p_1(p_2+q_2) + q_1(p_2+q_2)} \\
&= p_1p_2 = \frac{e^{\epsilon_1}e^{\epsilon_2}}{(1+e^{\epsilon_1})(1+e^{\epsilon_2})}
\end{aligned}
$$

となる．$\epsilon = 1$，$\epsilon_1 = \epsilon_2 = \frac{\epsilon}{2}$ とすると，$\hat{\theta}_{1,u}^{(1)} \approx 0.387455$ となる．出力 z_1 に対する入力 x_2, x_3, x_4 の確率についても同様に計算し，全てのユーザの平均を $\theta^{(1)}$ として更新する．

Algorithm 1 EM algorithm for PrivKV

$S_1, \ldots, S_n \leftarrow$ key-value data for n responders.

for all $u \in [n]$ **do** sample a tuple $\langle k'_a, v'_a \rangle$ from a vector S'_i

$v_a^+ \leftarrow VPP(v'_a, \epsilon_2)$

$k_a^* \leftarrow RR(k'_a, \epsilon_1)$

outputs $\langle k^*, v_a^+ \rangle \in Z = \{\langle 1,1\rangle, \langle 1,-1\rangle, \langle 0,0\rangle\}$

end for

$\Theta^{(0)} \leftarrow$ a uniform probability for $X = \{\langle 1,1\rangle, \langle 1,-1\rangle, \langle 0,1\rangle, \langle 0,-1\rangle\}$.

repeat(E-step)

$t \leftarrow 1$

Estimate posterior probability $Pr[V_i = 1 | Z_i]$.

(M-step) Update marginal probability $\theta_i^{(t+1)}$.

until $|\theta_i^{(t+1)} - \theta_i^{(t)}| \leq \eta$

for all $a \in K$ **do** estimate

$\hat{f}_a \leftarrow \theta^{(t)}_{\langle 1,1\rangle} + \theta^{(t)}_{\langle 1,-1\rangle}$

$\hat{m}_a \leftarrow \frac{\theta^{(t)}_{\langle 1,1\rangle} - \theta^{(t)}_{\langle 1,-1\rangle}}{\theta^{(t)}_{\langle 1,1\rangle} + \theta^{(t)}_{\langle 1,-1\rangle}}$

end for return $\hat{f}_1, \hat{m}_1, \ldots, \hat{f}_d, \hat{m}_d$

第4章　評価実験

4.1　目的

本実験の目的は，提案手法の推定精度の向上をプライバシ費用 ϵ やユーザ数 n の観点から調査することである．また，提案手法のポイズニング攻撃に対する安全性についても調査する．いくつかの合成データとオープンデータセットを用いて，提案手法と PrivKV，PrivKVM(c=3) を比較する．

4.2　データセット

合成データの key と value は，ガウス分布 ($\mu = 0, \sigma = 10$)，べき分布 ($F(x) = (1 + 0.1x)^{-\frac{11}{10}}$)，線形分布 ($F(x) = x$) に従う．表 4.1 に，それぞれの合成データの頻度と平均値の平均と分散を示す．key 数は $d = 50$ でユーザ数は $n = 10^5$ である．

表 4.1: 合成データの統計量

distribution	$E(f_k/n)$	$Var(f_k/n)$	$E(m_k)$	$Var(m_k)$
Gaussian	0.49506	0.10926	−0.00987	0.43702
Power-low	0.20660	0.06290	−0.58681	0.25160
Linear	0.51	0.08330	0	0.34694

表 4.2 に 2 つのオープンデータセット MovieLens データセット [10] と Clothing データセット [11] の詳細を示す．また，データセットの例を表 4.3 に示す．これらのデータセットは，ユーザの評価データをもとに特定のアイテムをおすすめする推薦システムの評価に用いられる．どちらのデータセットにも，映画のタイトルや衣料品のブランドなど，多数のアイテムが含まれている．したがって，多くのアイテムに対する評価値は疎である．また，これらのデータセットの評価値は正規分布であり，アイテムの頻度はべき乗分布に従う．したがって，合成データは実際のオープンデータのモデルとなる．

これらのデータを用いて，アイテムの推薦に用いられる各アイテムの度数とその評価値を推定する．また，異なる分布のデータセットを用いることで，分布による推定値の精度を調査する．

4.3　評価方法

4.3.1　推定精度

n 人のユーザから出力された key-value データに対して，emPrivKV と PrivKV，PrivKVM(c=3) で key k の度数 $\hat{f}_k$ とその平均値 $\hat{m}_k$ を推定する．key の真の度数を f_k，value の真の度数を m_k とし，

表 4.2: オープンデータセット

item	MoveiLens[10]	Clothing[11]
# ratings	10,000,054	192,544
# users	69,877	9,657
# items	10,677	3,183
value range	0.5 – 5	1 – 10

表 4.3: データ例

User ID	Item ID	Rating
1	81	5
1	402	3
2	913	4
3	162	2
3	572	5
3	674	4
⋮	⋮	⋮

推定誤差を MSE(Mean Square Error) を

$$\begin{aligned} MSE_f &= \frac{1}{|K|}\sum_{i=1}^{|K|}\left(\hat{f}_i - f_i\right)^2, \\ MSE_m &= \frac{1}{|K|}\sum_{i=1}^{|K|}\left(\hat{m}_i - m_i\right)^2 \end{aligned}$$

で評価する．この試行を 10 回行い，評価値の平均を精度とする．

4.3.2 ポイズニング攻撃に対する強度

プライバシ費用 ϵ，真ユーザに対する偽ユーザの割合 $b = m/n$，ターゲット key 数 r を変化させ，頻度利得と値利得を算出し，攻撃に対する強度を求める．頻度利得，値利得が小さいほどポイズニング攻撃に対する変化量が小さく，ポイズニング攻撃に対して頑強である．パラメータの初期設定を $\epsilon = 1$，$b = 0.05$，$r = 1$，$n = 10^4$ とする．パラメータごとに 50 回の試行を行い，結果の平均を評価値とする．

4.4 結果

4.4.1 推定精度

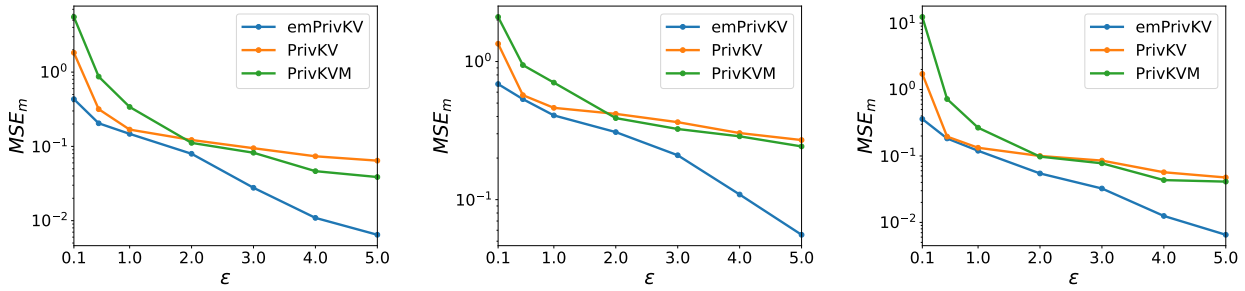
• ϵ による精度 ユーザ数 n=10^5，key 数 d=50 とし，ϵ についての推定精度を比較する．表 4.4 にガウス分布，べき分布，線形分布における度数の平均推定誤差 MSE_f を示す．3 つの分布において，提

案手法は，最尤推定を用いた PrivKV と PrivKVM に比べ，どの ϵ の場合でも最も精度が高い．特に $\epsilon = 0.1$ のとき，EM アルゴリズによる平均推定誤差 MSE_f は PrivKV に比べ，3 つの合成データの平均で 65.9% 改善されている．

表 4.4: ϵ による $MSE(f)(\times 10^{-4})$ の変化

	Gauss		Power-Law		Linear	
ϵ	EM	PrivKV，PrivKVM	EM	PrivKV，PrivKVM	EM	PrivKV，PrivKVM
0.1	756.68	1921.74	671.25	2170.25	602.84	1885.28
0.5	64.00	84.63	55.48	84.83	70.35	92.98
1	18.08	22.59	18.58	19.27	16.02	20.17
3	2.02	2.32	1.59	2.59	2.52	2.79
5	1.15	1.32	0.97	1.02	1.28	1.43

図 4.1a にガウス分布，図 4.1b にべき分布，図 4.1c に線形分布における平均値の平均推定誤差 MSE_m を示す．平均推定もどの ϵ の場合でも emPrivKV の精度が最も高い．emPrivKV では他手法に比べ，ϵ が大きくなるにつれて，より正確に推定される．特に $\epsilon = 5$ のとき，emPrivKV による平均推定誤差は PrivKV に比べ，3 つの合成データの平均で 85.2%，PrivKVM(c=3) に比べ 80.5% 改善されている．



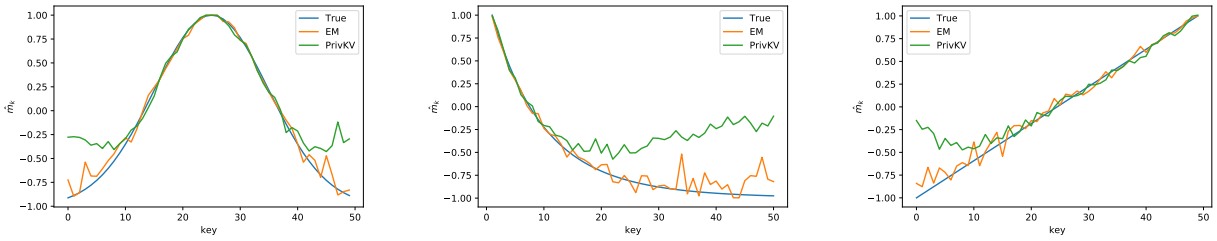
(a) Gaussian **(b)** Power-low **(c)** Linear

図 4.1: ϵ による平均値推定誤差 MSE_m

図 4.2 に $\epsilon = 4$ のときの key に対する推定平均値の分布を示す．PrivKV では度数の割合が 0.3 以下の小さい key に対して推定値の誤差が大きいのに対し，emPrivKV では，度数の割合が 0.1 の key まで小さな誤差で推定していることがわかる．

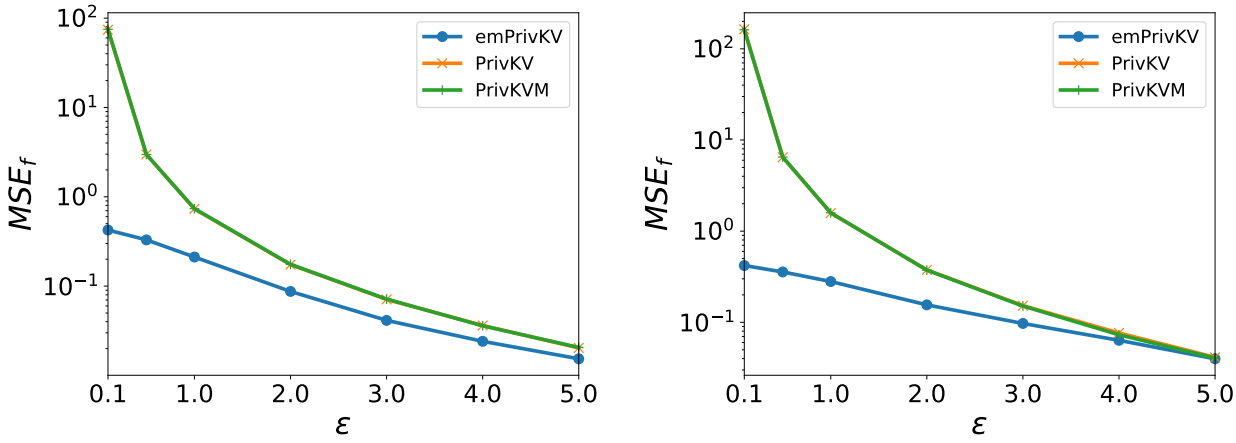
図 4.3a と図 4.3b，図 4.4a と図 4.4b にそれぞれ 2 つのオープンデータセットの度数と平均値の平均推定誤差を示す．オープンデータセットでは，度数と平均値で ϵ が小さいほど平均推定誤差の差が大きい傾向が見られた．どのオープンデータセットのもどの ϵ についても emPrivKV の精度が最も高い．特に $\epsilon = 0.1$ のとき，2 つのデータセットの平均で MSE_f と MSE_m はそれぞれ，PrivKV に比べ 95.2% と 98.6% 改善され，PrivKVM に比べ MSE_m は 99.8% 改善された．

・ユーザ数 n による精度 $\epsilon = 2$，key 数 d=50 とし，ユーザ数 n についての推定精度を比較する．表 4.5 に度数の平均推定誤差 MSE_f を示す．emPrivKV では，ユーザ数に関係なく推定誤差が小さかった．



(a) Gaussian **(b)** Power-low **(c)** Linear

図 4.2: key の平均値推定分布 ($\epsilon = 4$)



(a) MovieLens **(b)** Clothing

図 4.3: ϵ による度数推定誤差 MSE_f

特に，べき分布では，$n = 10^4$ のとき，PrivKV に比べ精度が 36.2% 改善された．

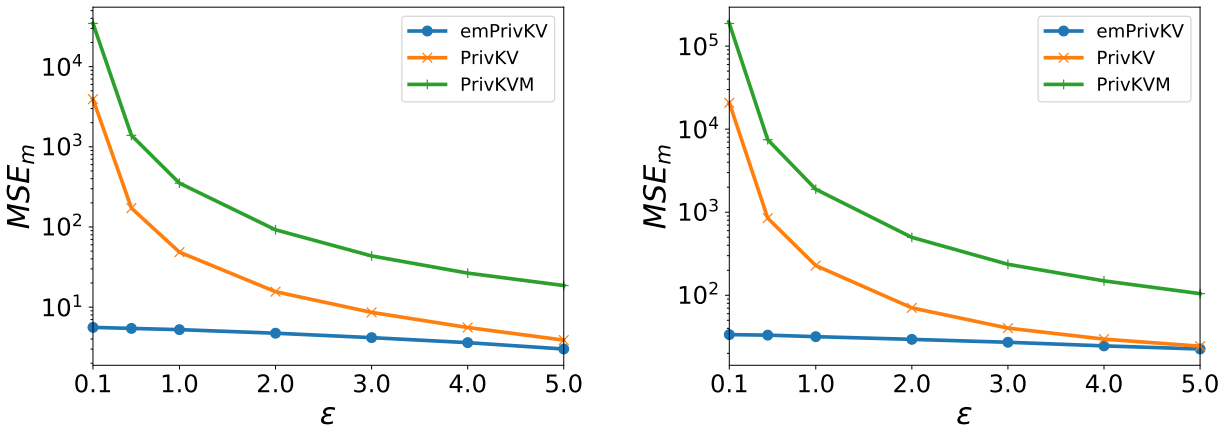
図 4.5a にガウス分布，図 4.5b にべき分布，図 4.5c に線形分布における度数の平均推定誤差 MSE_m を示す．$n \leq 5 \times 10^4$ のユーザ数の少ないときでは，emPrivKV は他手法との推定誤差の差は小さいが，ユーザ数が増えるにつれ推定誤差の差は大きくなり，推定精度が向上している．特に，度数の少ない key が多数存在するガウス分布では，$n = 5 \times 10^6$ のとき，PrivKV と比較して 31.6%，PrivKVM と比較して 26.5% の改善が見られた．

4.4.2 ポイズニング攻撃に対する強度

・頻度利得 図 4.6 から図 4.11 にガウス分布と MovieLens の 3 つのポイズニング攻撃による頻度利得を示す．上列，中央列，下列はそれぞれ偽ユーザの割合 b，プライバシ費用 ϵ，ターゲット key 数 r についての頻度利得である．

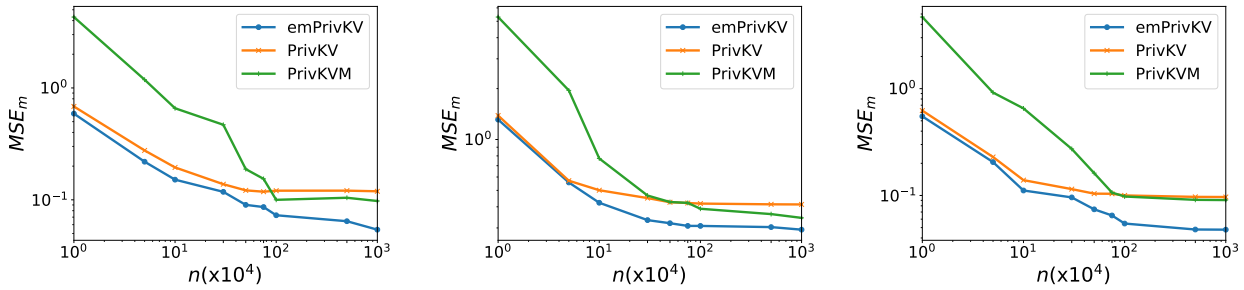
3 つのポイズニング攻撃手法を比較すると，ガウス分布（図 4.6 から図 4.8）では，M2GA がどのパラメータの組み合わせでも最も頻度利得が大きく，攻撃による影響が大きい．一方で MovieLens（図 4.9 から図 4.11）では M2GA と RKVA での攻撃による頻度利得に差は見られない．

図 4.6 から図 4.11 の emPrivKV と他手法を比較すると，M2GA と RKVA では，どのパラメータの組み合わせでも emPrivKV が他のプロトコルに比べ頻度利得が小さい．M2GA（図 4.6a と図 4.9a）で



(a) MovieLens **(b)** Clothing

図 4.4: ϵ による平均値推定誤差 MSE_m



(a) Gaussian **(b)** Power-low **(c)** Linear

図 4.5: ユーザ数 n による平均値の平均値推定誤差 MSE_m

は，偽ユーザの割合 b を増加させると，PrivKV と PrivKVM の頻度利得が増加するが，emPrivKV では $b \geq 0.01$ で頻度利得は一定で安定しており，偽ユーザ増加に対する耐性が高い．偽ユーザが増えるほど，emPrivKV と PrivKV の頻度利得の差は大きくなり，emPrivKV が $b = 0.2$ のときガウス分布では 70.3%，MovieLens では 85.6% 小さい．中央列の ϵ を変化させた結果，M2GA（図 4.6b と図 4.9b）ではどの ϵ でも他プロトコルに比べ emPrivKV の頻度利得が小さい．特に ϵ が小さいときにその差も大きく，$\epsilon = 0.1$ のときガウス分布では 92.3%，MovieLens では 95.8% 小さい．

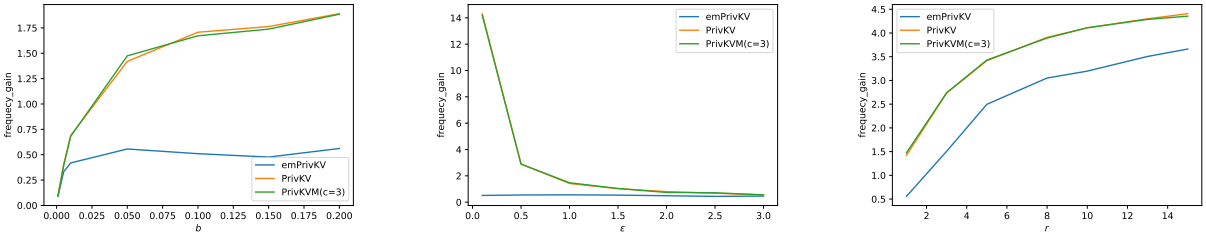
下列のターゲット key 数 r が増加すると M2GA（図 4.6c と図 4.9c）の頻度利得も単調に増加する．r の数にかかわらず，emPrivKV が他手法に比べの頻度利得が一定の割合で小さく，ガウス分布では平均で 17%，MovieLens では平均 24.6% 小さい．

・値利得 図 4.12 から図 4.17 にガウス分布と MovieLens の 3 つのポイズニング攻撃による値利得を示す．3 つのポイズニング攻撃手法を比較すると，ガウス分布（図 4.12 から図 4.14）では M2GA がどのパラメータの組み合わせでも最も値利得が大きく，攻撃による影響が大きい．一方で MovieLens（図 4.15 から図 4.17）では M2GA と RKVA での攻撃による頻度利得に差は見られない．

図 4.12 から図 4.17 で emPrivKV と他手法を比較すると，M2GA では，どのパラメータの組み合わせでも emPrivKV が他のプロトコルに比べ値利得が小さい．M2GA の上列（図 4.12a と図 4.15a）の偽ユーザの割合 b では，emPrivKV では $b \geq 0.005$ で値利得は一定で安定している．$b = 0.2$ のとき

表 4.5: ユーザ数 $n(\times 10^4)$ による $MSE_f(\times 10^{-4})$ の変化

	Gauss		Power-Law		Linear	
$n[10^4]$	EM	PrivKV, PrivKVM,	EM	PrivKV, PrivKVM	EM	PrivKV, PrivKVM
1	476.26	527.91	346.71	543.28	404.47	538.94
5	107.26	110.05	72.82	99.44	89.92	118.34
10	36.09	51.43	39.24	51.12	54.17	70.00
50	9.42	11.55	9.08	12.20	10.48	15.93
100	4.64	4.77	4.88	5.50	5.62	7.40
500	1.82	2.47	1.36	1.99	1.80	2.00
1000	1.41	1.60	0.76	1.18	0.97	1.49



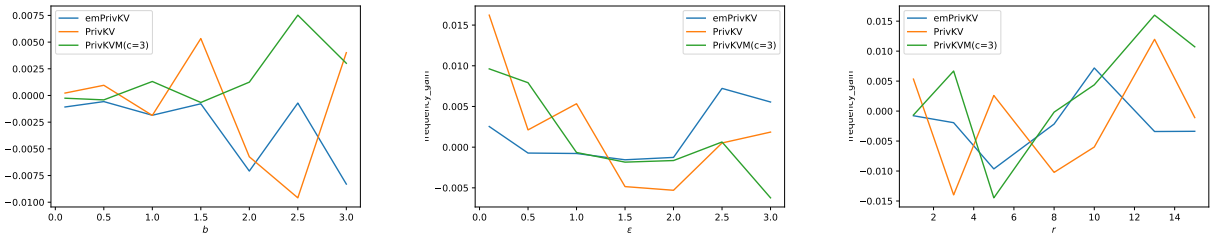
(a) 偽ユーザの割合 b **(b)** ϵ **(c)** ターゲット key 数 r

図 4.6: M2GA の頻度利得 (Gauss)

ガウス分布（図 4.12a）では PrivKV と比較して 75.0%，PrivKVM と比較して 91.5% 小さい．また，MovieLens（図 4.15a）では，PrivKV と比較して 89.2%，PrivKVM と比較して 97.7% 小さい．

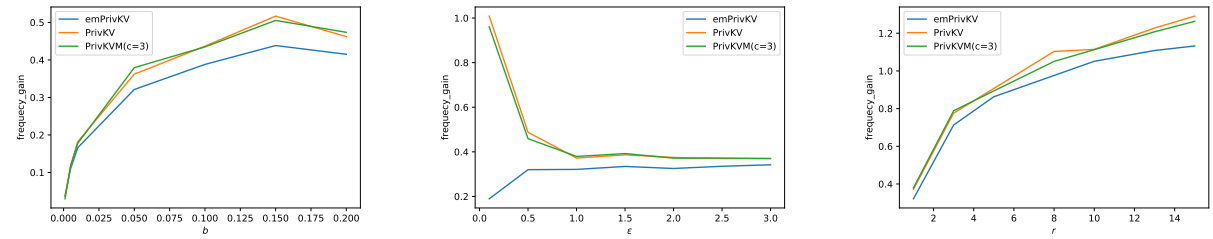
中央列の ϵ を変化させた結果，M2GA（図 4.12b と図 4.15b）では，どの ϵ でも他プロトコルに比べ emPrivKV の値利得が小さい．emPrivKV では，ϵ によらず値利得は一定であるのに対して，PrivKV や PrivKVM では，ϵ が小さいときに値利得が大きい．特に $\epsilon = 0.1$ のときの値利得は，ガウス分布では PrivKV と比較して 96.9%，PrivKVM と比較して 98.8% 小く，MovieLens では，PrivKV と比較して 98.9%，PrivKVM と比較して 99.3% 小さい．r の数にかかわらず，emPrivKV が他手法に比べの値利得が小さく，ガウス分布（図 4.12c）では平均で PrivKV の 24.5%，PrivKVM の 77.7% 小さく，MovieLens（図 4.15c）では，PrivKV と比較して 87.4%，PrivKVM と比較して 93.8% 小さい．一方で，ガウス分布と MovieLens ともにどの局所差分プライバシプロトコルも RMA（図 4.13b，図 4.16b）の影響は見られない．

RKVA のターゲット key 数 r（図 4.14c）について emPrivKV と PrivKV の値利得の差はないが，偽ユーザの割合 b(図 4.14a) が大きいときや ϵ(図 4.14b) が小さいときに値利得の差が大きく，emPrivKV は PrivKV と比較して $b = 0.2$ のとき 16.1%，$\epsilon = 0.1$ のとき 62.2% 小さい．



(a) 偽ユーザの割合 b　　**(b)** ϵ　　**(c)** ターゲット key 数 r

図 4.7: RMA の頻度利得 (Gauss)



(a) 偽ユーザの割合 b　　**(b)** ϵ　　**(c)** ターゲット key 数 r

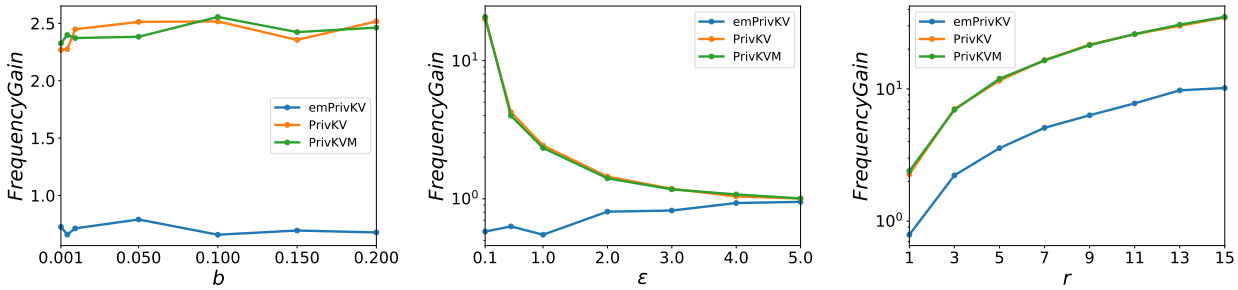
図 4.8: RKVA の頻度利得 (Gauss)

4.5　考察

4 章で示したように，提案手法では，図 4.5 の頻度の小さな key の平均値の推定精度が改善した．PrivKV では，出力 v_k^+ から $v'_k = 1$ と $v'_k = -1$ の推定を行っており，欠損値 $v'_k = 0$ の場合を考慮していないため，平均値は 0 に近似する．一方で，emPrivKV では，ベイズの定理を用いた反復手法であり，出力 $\langle 1, 1\rangle$ から摂動対象に $\langle 1, 1\rangle$ や $\langle 1, -1\rangle$ の割合だけでなく，欠損値 $\langle 0, 0\rangle$ の割合も考慮しているため，推定精度が改善した．

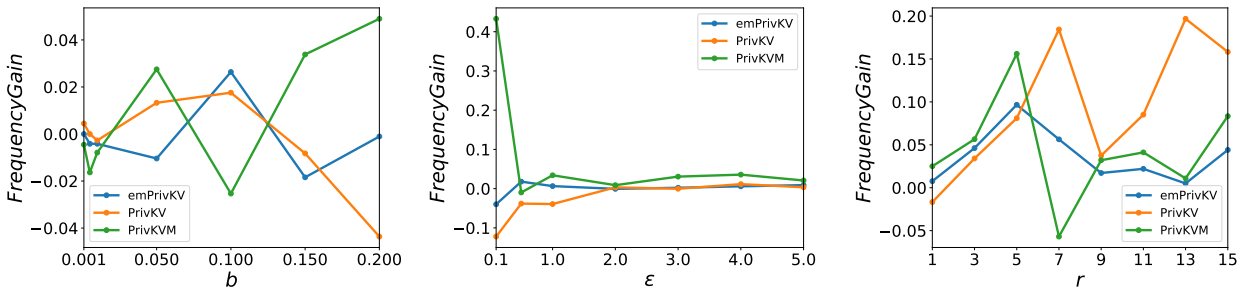
合成データでは，プライバシ費用 ϵ が大きくなるほど，従来手法に比べ精度が改善していくが，オープンデータセットでは，プライバシ費用 ϵ が小さいほど精度が改善している．このように異なる振る舞いとなったのは，アイテム数に対するユーザ数の割合が大きく異なるためであると考える．

実験結果から MovieLens データセットや Clothing データセットのような疎であるデータセットでは，より安全（小さなプライバシ費用 ϵ）に収集したデータに対して高精度な推定を行うことができる．



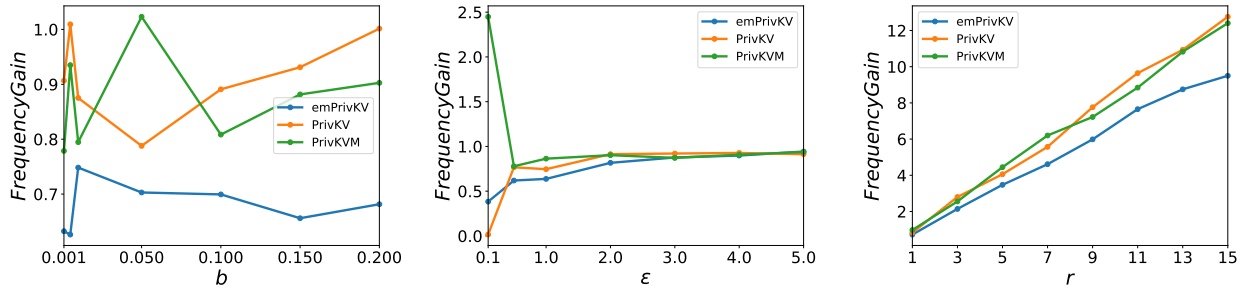
(a) 偽ユーザの割合 b　　**(b)** ϵ　　**(c)** ターゲット key 数 r

図 4.9: M2GA の頻度利得 (MoveiLens)



(a) 偽ユーザの割合 b **(b)** ϵ **(c)** ターゲット key 数 r

図 4.10: RMA の頻度利得 (MoveiLens)



(a) 偽ユーザの割合 b **(b)** ϵ **(c)** ターゲット key 数 r

図 4.11: RKVA の頻度利得 (MoveiLens)

ポイズニング攻撃についても，従来手法は，M2GA や RKVA のような攻撃は，出力 $v_k^+ = 1$ を増加させるため，推定値が大きく変化してしまう．提案手法の推定方式では，出力 $v_k^+ = 1$ の割合からは直接的に影響を受けづらいため，従来手法と比較して安全であると考えられる．

4.6 提案手法の限界と解決方法

提案手法の限界は以下の 3 つである．また，その解決策について説明する．

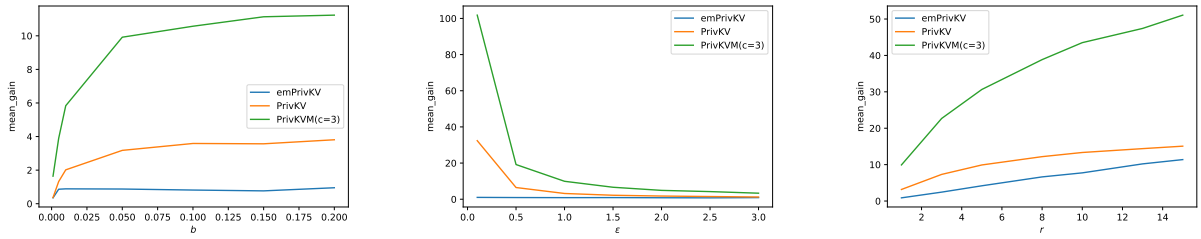
・計算量

提案手法における度数 f_m による収束までの反復回数 t を図 4.18 に示す．また，収束までの推定値 $\theta_{\langle 1,1\rangle}$ の変化を図 4.19 に示す．図 4.18 から度数が 0.5 付近のときや 0，1 などの極端に少ないときや大きいときでは，収束までの計算量が大幅に増加する傾向がある．また，図 4.19 から反復を繰り返すことで収束速度が遅くなることがわかる．

EM アルゴリズムに共役勾配法や準ニュートン法などの非線形最適化法を適用することで収束速度が改善することが知られている [24]．そのため，提案手法に対して非線形最適化法を適用することが計算量を削減する解決策である．

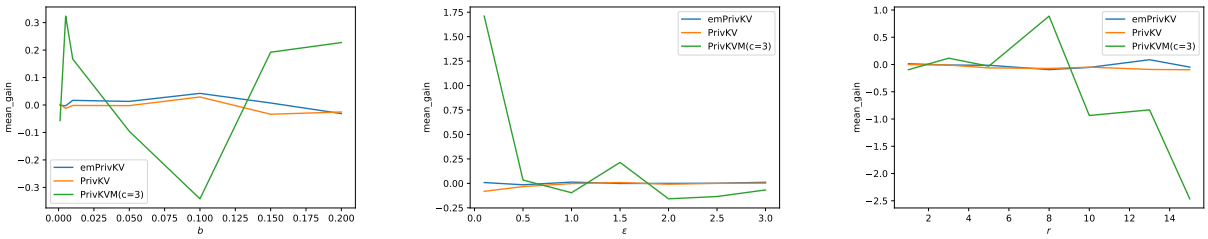
・ポイズニング攻撃の安全性

提案手法は PrivKV に比べ M2GA によるポイズニング攻撃に対して安全であったが，その安全性は十分ではない．出力結果を意図的に操作する M2GA のような攻撃に対しては，異常値検出のような対策を検討する必要がある．Wu ら [5] は，出力値のインデックスの分布を基にして外れ値を検出



(a) 偽ユーザの割合 b　　**(b)** ϵ　　**(c)** ターゲット key 数 r

図 4.12: M2GA の値利得 (Gauss)



(a) 偽ユーザの割合 b　　**(b)** ϵ　　**(c)** ターゲット key 数 r

図 4.13: RMA の値利得 (Gauss)

する異常検出による対策を提案している．しかし，この方法では，統計値を算出するための検出までの時間がかかる．より即応性の高い対策として次の解決策を提案する．

(1) 確率的な処理の証拠を示すコミットメントプロトコル [19]

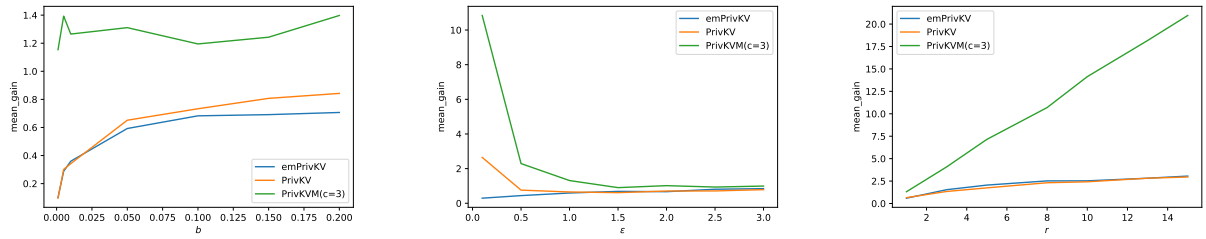
乱数の代わりにハッシュ関数などの一方向性を持つ暗号技術を用いて，意図なくランダマイズを正しく行なっていることを証明する．M2GA や RMVA に効果的と考える．

(2) サンプリングを紛失通信で実施する [20]

紛失通信では，d 個の符号化ベクトルの内の 1 つをサーバが選択する．ユーザが不正に意図的なデータを選ぶことを防止する．

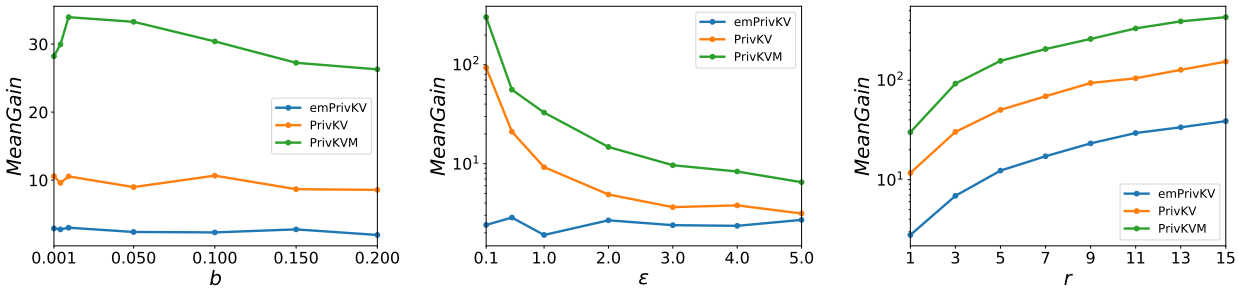
・推定精度の比較

本研究では，PrivKV のランダマイズデータに対して EM アルゴリズムを適用する手法を提案し，PrivKV や PrivKVM との推定精度を比較した．しかし，PrivKV の他にも key-value データについての局所差分プライバシプロトコルが提案されている [17, 18]．本研究では行なっていない，これらの局所差分プライバシプロトコルとの推定精度の比較が今後の課題である．



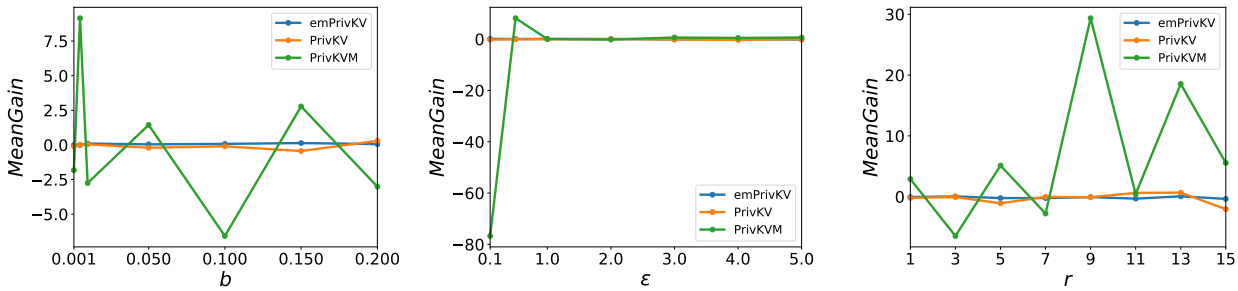
(a) 偽ユーザの割合 b **(b)** ϵ **(c)** ターゲット key 数 r

図 4.14: RKVA の値利得 (Gauss)



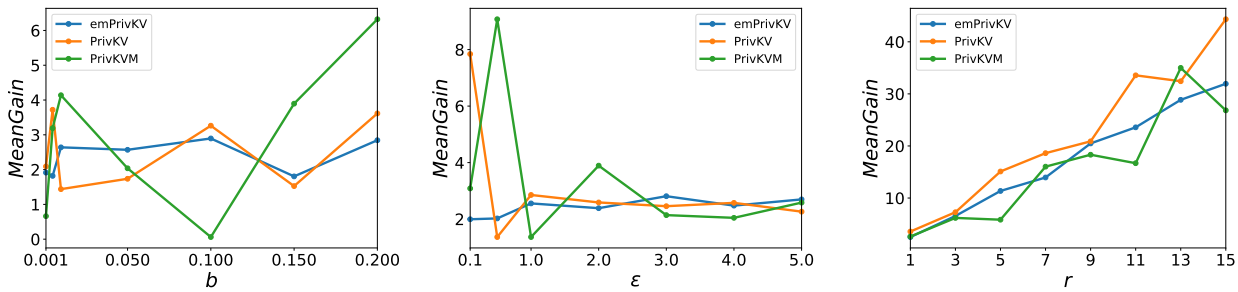
(a) 偽ユーザの割合 b **(b)** ϵ **(c)** ターゲット key 数 r

図 4.15: M2GA の値利得 (MovieLens)



(a) 偽ユーザの割合 b **(b)** ϵ **(c)** ターゲット key 数 r

図 4.16: RMA の値利得 (MovieLens)



(a) 偽ユーザの割合 b **(b)** ϵ **(c)** ターゲット key 数 r

図 4.17: RKVA の値利得 (MovieLens)

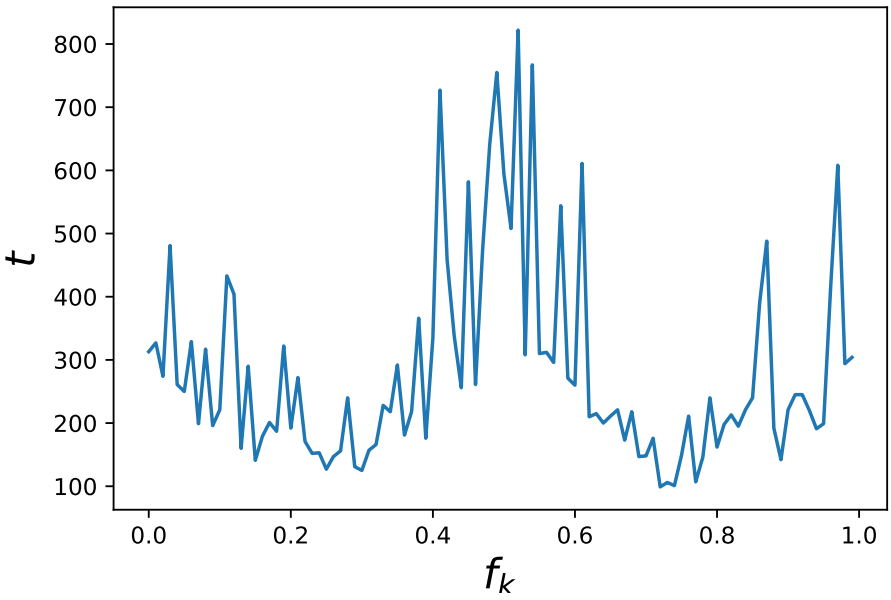


図 4.18: 度数 f_k による収束までの反復回数 t
$(n = 10^5,\ \epsilon = 1,\ \eta = 10^{-5})$

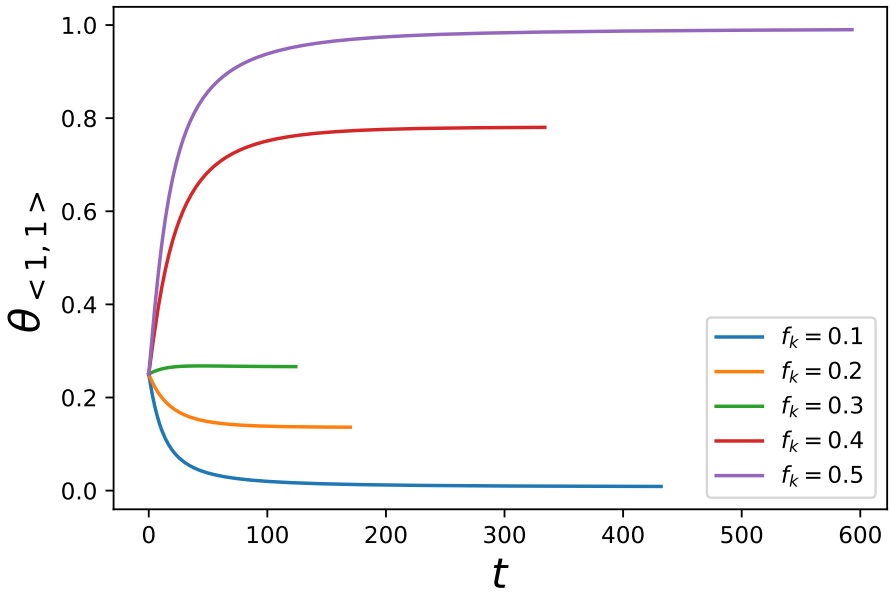


図 4.19: 反復回数 t と推定値 $\theta_{\langle 1,1\rangle}$ の変化
$(n = 10^5,\ \epsilon = 1,\ \eta = 10^{-5})$

第5章　まとめ

key-value データにおける局所差分プライバシプロトコル PrivKV は，ランダマイズされたデータに対して最尤推定法を用いることで統計情報を推定する．そのため，度数が極端に少ない key や大きい key の推定精度が低い問題がある．その問題を改善するために，本研究では，PrivKV と同様の手法で収集したデータに対して EM アルゴリズムを適用する手法を提案した．提案手法の有効性を検証するために，合成データとオープンデータセットを用いて評価を行った．その結果，特に PrivKV, PrivKVM では大きな誤差となった度数の小さな key について，EM アルゴリズムを用いることで，推定精度が改善した．度数推定では，ユーザ数 $n = 10^4$，$\epsilon = 0.1$ のとき，3 つの合成データの平均で約 69.5% の改善が見られた．また，平均値推定では，ユーザ数 $n = 10^4$，$\epsilon = 5$ のとき，平均で 85.2% の改善が見られた．特に度数の小さな key が比較的多いべき分布に従うデータの時に EM アルゴリズムを用いた手法が効果的であった．

また，提案手法に対するポイズニング攻撃の影響を調査した．その結果，3 種類のポイズニング攻撃手法の中で M2GA が最も大きく統計値を操作するリスクが高い．しかし，提案手法はポイズニング攻撃に対する耐性が高く，特に推定値に最も影響を与える M2GA でも，(偽ユーザの割合 b が 0.2) PrivKV と比較し頻度利得を 70.3%改善した．さらに，値利得は (偽ユーザの割合 b が 0.2)PrivKV と比較して 75%改善した．従って，提案手法は，一般的な利用ケースで有効である．

参考文献

[1] J. C. Duchi, M. I. Jordan, M. J. Wainwright, “Local privacy and statistical minimax rates”, Foundations of Computer Science, pp. 429-438, 2013.

[2] S. L. Warner, “Randomized response: A survey technique for eliminating evasive answer bias”, Journal of the American Statistical Association, pp. 63-69, 1965.

[3] T. T. Nguyên, X. Xiao, Y. Yang, S. C. Hui, H. Shin, J. Shin, “Collectiong and analyzing data from smart device users with local differential privacy”, arXiv:1606.05053, 2016.

[4] X. Cao, J. Jia, N. Z. Gong, “Data poisoning attacks to local differential privacy protocols”, USENIX Security Symposium, pp. 947-964, 2021.

[5] Y. Wu, X. Cao, J. Jia, N. Z. Gong, “Poisoning Attacks to Local Differential Privacy Protocols for Key-Value Data”, USENIX Security Symposium, pp. 519-536, 2022.

[6] 宮川雅巳, “EM アルゴリズムとその周辺”, 応用統計学, Vol. 16, No. 1, pp. 1-19, 1987.

[7] Q. Ye, H. Hu, X. Meng, H. Zheng, “PrivKV : Key-Value Data Collection with Local Differential Privacy”, IEEE Symposium on Security and Privacy , pp. 294-308, 2019.

[8] Ú. Erlingsson, V. Pihur, A. Korolova, “RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response”, ACM Conference on Computer and Communications Security, pp.1054-1067, 2014.

[9] B. Ding, J. Kulkarni, S. Yekhanin, “Collecting telemetry data privately”, Neural Information Processing Systems, pp.3574-3583, 2017.

[10] MovieLense 10M Dataset, `https://grouplens.org/datasets/movielens/` (accessed in 2022).

[11] Clothing Fit Dataset for Size Recommendation, `https://www.kaggle.com/datasets/rmisra/clothing-fit-dataset-for-size-recommendation`(accessed in 2022).

[12] 総務省, 情報通信白書令和 2 年版, `https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd133240.html`(accessed in 2022).

[13] X. Ren, C. Yu, W. Yu, S. Yang, X. Yang, J. A. McCann, P. S. Yu, “LoPub : high-dimensional crowdsourced data publication with local differential privacy”, IEEE Transactions on Information Forensics and Security, pp. 2151-2166, 2018.

[14] G. Fant, V. Pihur, Ú. Erlingsson, “Building a RAPPOR with the unknown : Privacy-preserving learning of associations and data dictionaries”, Proceedings on Privacy Enhancing Technologies, pp. 41-61, 2016.

[15] 長谷川聡, 三浦尭之, “一般化逐次ベイズ法を用いた局所差分プライベートな度数分布推定”, コンピュータセキュリティシンポジウム, pp. 199-206, 2020.

[16] G. Cormode, S. Jha, T. Kulkarni, N. Li, D. Srivastava, T. Wang, “Privacy at scale: Local differential privacy in practice”, International Conference on Management of Data, pp. 1655-1658, 2018.

[17] X. Gu, M. Li, Y. Cheng, L. Xiong, Y. Cao, “PCKV: Locally Differentially Private Correlated Key-Value Data Collection with Optimized Utility”, USENIX security symposium, pp. 967-984, 2020.

[18] Q. Ye, H. Hu, X. Meng, H. Zheng, K. Huang, C. Fang, J. Shi, “PrivKVM*: Revisiting Key-Value Statistics Estimation with Local Differential Privacy”, IEEE Transactions on Dependable and Secure Computing, 2021.

[19] M. V. Ferreira, S. M. Weinberg, “Credible, truthful, and two-round (optimal) auctions via cryptographic commitments”, ACM Conference on Economics and Computation, pp. 683-712, 2020.

[20] J. Kilian, “Founding crytpography on oblivious transfer”, In Proceedings of the twentieth annual ACM symposium on Theory of computing, pp. 20-31, 1988.

[21] P. Kairouz, S. Oh, P. Viswanat, “Extremal mechanisms for local differential privacy”, Neural Information Processing Systems, pp. 2879-2887, 2014.

[22] F. McSherry, “Privacy integrated queries: an eztensible platform for privacy-preserving data analysis”, International Conference on Management of Data, pp. 19-30, 2009.

[23] B. Ding, J. Kulkarni, S. Yekhanin, “Collecting telemetry data privately”, Neural Information Processing Systems, pp. 3571-3580, 2017.

[24] M. Jamshidian, R. I. Rennrich, “Acceleration of the EM algorithm by using quasi − Newton methods”, Journal of the Royal Statistical Society: Series B, Vol. 59, No. 3, pp. 569-587, 1997.

謝辞

本論文は筆者が明治大学大学院先端数理科学研究科先端メディアサイエンス専攻博士前期課程に在学中の研究成果をまとめたものである．本研究を遂行するにあたり多くの方々から多大なる御指導と御援助を賜りました．

特に，明治大学総合数理学部先端メディアサイエンス学科の菊池浩明教授には，研究テーマに関する御指導をはじめ，国際会議や PWSCUP などへの参加に関する多くの御援助を賜り，本論文を完成に導いていただいただけでなく，研究活動を通して大きく成長する機会を与えていただきました．深く感謝申し上げます．

明治大学総合数理学部先端メディアサイエンス学科の斉藤裕樹教授，中村聡史教授，荒川薫教授には本論文の執筆に関して有益なご教示を賜りました．深く感謝申し上げます．

Department of Information Management and Finance，National Yang Ming Chiao Tung University の Chia-Mu Yu 准教授には本論文に有益な御助言を賜りました．心から感謝申し上げます．

合同研究を通して，御援助や研究者としての姿勢をご教授いただいた，三菱電機株式会社の藤田正浩様，山中忠和様，松田規様，吉村礼子様，清水りな様に心から感謝申し上げます．

さらに，多くの貴重な御助言をいただいた明治大学菊池研究室の皆様に感謝致します．

最後に，博士前期課程に進学する機会を与えていただき，学生生活を支えてくださった家族に厚く感謝致します．

研究業績

研究業績

国際会議論文（査読あり）

1. Hikaru Horigome，Hiroaki Kikuchi，“Improvement of Estimate Distribution with Local Differential Privacy”，Modeling Decisions for Artificial Intelligence 2022，pp．68-79，2022.

2. Hikaru Horigome，Hiroaki Kikuchi，Chia-Mu Yu，“Expectation-Maximization Estimation for Key-Value Data Randomized with Local Differential Privacy”，Advanced Information Networking and Applications 2023，2023．(採録済み)

国内研究会

1. 堀込光，菊池浩明，Chia-Mu Yu，“Key-Value データにおける曲処分プライバシアルゴリズム PrivKV の改良”，マルチメディア，分散，協調とモバイルシンポジウム 2022，pp．1209-1216，2022.

2. 堀込光，菊池浩明，Chia-Mu Yu，“ポイズニング攻撃に対してロバストな EM アルゴリズムを用いた key-value データにおける LDP プロトコル”，コンピュータセキュリティシンポジウム 2022，pp．129-136，2022.

3. 藤田正浩，山中忠和，松田規，吉村礼子，堀込光，伊藤聡志，菊池浩明，“個人情報保護システム要件一覧抽出ツールの実現”，研究報告コンピュータセキュリティ，pp．1-8，2022.