局所差分プライバシにおけるパラメータの秘匿について

高木　駿†　曹　洋†　吉川　正俊†

† 京都大学情報学研究科　〒 606–8501 京都府京都市左京区吉田本町 36-1
E-mail: †takagi.shun.45a@st.kyoto-u.ac.jp, ††{yang,yoshikawa}@i.kyoto-u.ac.jp

あらまし　近年，データ分析技術の発達とその利用により人々の生活が豊かになっているが，その反面，プライバシ漏洩が問題視されている．そのことから，個人のプライバシを保護しつつデータ分析をすることが重要な課題になっている．様々なプライバシ保護技術が研究されてきたが，データ提供の際に提供者が自身のデータに雑音を加えてデータを提供する方法の基準である局所差分プライバシを用いる方法が特に注目されている．局所差分プライバシではプライバシパラメータによってプライバシ保護の強度を調整することができるが，データ提供者がプライバシパラメータを公開する前提でプライバシ保護の強度が定義されている．しかし，プライバシパラメータを公開しない場合の理論的なプライバシ保護の強度は研究されていない．この論文では，個人がプライバシパラメータを調整し，秘匿にする場合のプライバシ保護の強度の厳密な定義 Parameter Blending Privacy(PBP) を提案する．さらに，応用先の一つとして，プライバシを保護したカテゴリデータの収集と頻度推定の枠組みを提案する．プライバシパラメータを公開する場合と秘匿にする場合の頻度推定の精度を同じプライバシ保護の強度で比較して，秘匿にする場合の方が頻度推定の精度がよくなる場合があることを示した．

キーワード　差分プライバシ，局所差分プライバシ

1 はじめに

近年，様々なデータが電子的に収集され，活用されている．その中には個人のプライバシに関わる情報が含まれているものがあるため，活用や収集ができないことがある．そのために，プライバシ保護をしながらそういったデータの活用や収集する方法が必要とされており，研究が盛んになっている [1] [2] [3]．中でも，差分プライバシ [4] と呼ばれるプライバシ基準を用いる方法が厳密なプライバシ保護をしていると注目されている [5]．もし計算機構が ϵ-差分プライバシを満たす場合，入力に対する計算機構による出力が公開されたとしても，ϵ で示される程度に入力に含まれる個人のプライバシが保護される．直感的には，出力を見たとしても出力に加わった乱数に基づく雑音のために，データセットに任意の個人の情報が含まれていたかが推測が難しくなることが保証される．しかし，差分プライバシでは，信頼できるデータ収集者が正しく差分プライバシを満たす計算機構を使用することを前提としているため，データ収集者が信頼できない場合成立しない．そこで，そういったデータ収集者を必要としない局所差分プライバシ [6] が提案された．局所差分プライバシでは，データ収集者も攻撃者になり得ると考え，データ提供者がデータを提供する前にデータに雑音を加えることで自身のプライバシを保護する．そのため，データ提供者は雑音の大きさ（以降パラメータと呼ぶ）を調整することで，個人が望むプライバシ保護が可能である．しかし，ほとんどの局所差分プライバシの応用 [1] [1] は個人がパラメータの調整はせずに共有している一つのパラメータを使用する．この論文では，個人がパラメータを調整し，その値を秘匿とする場合の理論的なプライバシ保護の保証を考える．

ここではまず，パラメータを秘匿にする場合に，局所差分プライバシの二つの不十分さを例を挙げて説明する．

例 1 (*Plausible deniability* による不十分さ)．データ提供者 A は何らかの局所差分プライバシを満たす計算機構をパラメータ θ_0 で使うとする．局所差分プライバシの考え方では関数 E によって $E(\theta_0)$ というプライバシ保護の強度（以降プライバシ強度と呼ぶ）が計算される．次にデータ提供者 B が同じ計算機構をパラメータ θ_1 で使うとする．同様の考えでプライバシ強度は $E(\theta_1)$ となる．これは各データ提供者が使用したパラメータを公開した場合である．もし，A と B がパラメータを秘匿とする場合はどうなるだろうか．局所差分プライバシでは，パラメータを秘匿にすることによる厳密なプライバシ強度は定義されていなく，その強度は同じく $E(\theta_0)$ と $E(\theta_1)$ と考えるしかない．しかし，データ収集者（攻撃者）は収集したデータがどのパラメータから出力されたものかわからないため，より推測が難しくなっていると考えられる．例えば，答えのドメインが $\mathcal{X} = \{$”はい”,”いいえ”$\}$ であるデータを収集するとし，パラメータ θ_0 は正直に答える，θ_1 は同確率で”はい”か”いいえ”を無作為に答えるとする．この場合，局所差分プライバシに基づくと，各パラメータが秘匿にされていたとしても，A のプライバシ強度は $E(\theta_0) = 0$（最高）で B のプライバシ保護の度合いは $E(\theta_1) = \infty$（最低:全くプライバシ保護がされていない.）となる．しかし，攻撃者から見ると，二つのデータのどちらが B のデータかがわからないため，実際は B のプライバシも保護されている．

例 2 (ベイズの定理に基づく解釈の不十分さ)．局所差分プライ

1：https://machinelearning.apple.com/2017/12/06/learning-with-privacy-at-scale.html

バシはベイズの定理に基づいてその性質が解釈される．まず，例 *1* と同じ設定で説明する．ここでは，データ $d, d' \in \mathcal{X}$ とパラメータ θ を確率変数として考える．d が与えられたときの事後分布はベイズの定理より，$\Pr(o|d) = \sum_\theta \Pr(o|d,\theta)\Pr(\theta)$ と考えることができる．そして，計算機構が ϵ-差分プライバシを満たすとは，$\forall d, d \in \mathcal{X}, o \in Y, |\log \Pr(o|d)/\Pr(o|d')| \leqq \epsilon$ を満たすことと同値である．ここで，取り得る応答値の集合を Y とおいた．この解釈に基づくと，ϵ の値（つまり，プライバシ強度）が θ に依存しなくなったが，それは，A と B は同じプライバシ保護の度合い（つまり，$E(\theta_0) = E(\theta_1)$）であることを意味する．決定的に自らの意思で θ_0 を用いた A のプライバシは一切漏洩してないはずであるから，この局所差分プライバシの考え方は不適切であると考えられる．

例 1 はパラメータを秘匿にした場合，”B は θ_0 を用いた可能性がある”ということを局所差分プライバシでは考慮できないことが原因である．この考えは *Plausible deniability* と呼ばれており，差分プライバシの原理でもある．例 2 はパラメータを確率変数として扱っており，パラメータを決定的に選択する場合を局所差分プライバシでは考慮できないことが原因にある．これらを考慮したプライバシ定義はまだ提案されていない．そこで，この論文では，パラメータを決定的に選択し，秘匿にすることで得られる *Plausible deniability* を考慮したプライバシの考え方 Parameter Blending Privacy (PBP) を提案する．

この論文ではデータ提供者の用いるパラメータとデータに相関がないと仮定する．この仮定は Jorgensen ら [7] が述べるように現実的であると信じている．この場合，データ提供者はデータ収集に参加する前に自身の持つデータではなく各自の趣向によってパラメータを選択する．しかし，この論文では触れないが，相関がある場合は，パラメータ情報が漏洩することによるデータプライバシの漏洩を考慮する必要がある．この場合のパラメータ秘匿下でのプライバシ保証も重要な課題であり，今後の研究の展望の一つである．

パラメータを秘匿にすることで，新たな *Plausible deniability* が生じプライバシ強度が高くなるが，本来のデータの推定にパラメータが使えなくなるため，データ分析の質の低下が生じるだろう．この論文では最後にそのプライバシ強度とデータの推定の質のトレードオフを実験的に示す．その方法として，パラメータを秘匿にする場合と公開する場合で，同じプライバシ強度になるように二つの計算機構を構築する．そして、パラメータを秘匿にする場合はパラメータを使わずに推定を行い，公開する場合はパラメータを用いて推定を行う．これらの推定の精度を比較する．

データ収集のシミュレーションを行い，実際にデータ収集と分析を行なって比較した結果，パラメータを秘匿にする場合の方が同じプライバシ強度でデータ分析の質が良い場合があることが示された．まとめるとこの論文の貢献は以下のようになる．

- パラメータを秘匿にする場合のプライバシ定義 Parameter Blending Privacy(PBP) を提案する．
- PBP を用いた一つのデータ収集とデータ分析の枠組みを提案する．
- パラメータを秘匿にすることで，同じプライバシ強度で，公開する場合よりもデータ分析の精度がよくなる場合があることを実験的に示した．

2 準　　備

この章では，差分プライバシと局所差分プライバシと関連研究，問題設定を述べる．

2.1 ϵ-差分プライバシ

ここではこの論文の基礎である Dwork [4] の差分プライバシを説明する．差分プライバシはデータベースにおける個人のデータのプライバシ保護を目的としたプライバシ基準である．あるデータベースから母集団に関する統計的な知識を提供する目的で統計量が公開されたとする．実はこのとき，個人の情報を知りたい攻撃者にこの統計量を見られると，個人の情報が高い精度で推測されてしまう恐れがある．例えば，ある疾患に関する調査のデータベースがあったときに，”個人が疾患にかかっているかどうか”という情報は個人が知られたくない情報である．そこで，”全国の 30 代で疾患を持つ人の人数”・”東京都在住で疾患を持つ人の人数”・”東京都在住の 30 代で疾患を持つ人の人数”という三つのクエリを発行したとする．このとき，東京都在住の 30 代の A さんが疾患を持つかどうかを攻撃者は推測できてしまうのだろうか．それは，データベースの内容に依ってできる可能性もあるし，できない可能性もあるとしか言えなく，プライバシが保護されている保証はない状態なのである．そこで，Dwork は差分プライバシと呼ばれるデータベースから個人のプライバシを保護するために満たされるべき基準を提案し，今やその基準はあらゆる攻撃者やデータベースに対してプライバシの保護ができる，強力な基準であることが広く認められている．

2.1.1 定　　義

ここではその定義を述べる．そのためにまず記法を導入する．X をレコードのドメイン，レコード $x \in X$ を個人の情報を含むデータ，レコードの集合をデータベース $D = \{x_i\}_{i=1}^n$ とする．データベース $D \in \mathcal{D}$ に対するランダムな応答値 $y \in Y$ を返す計算機構を m と置く．ここで取りうるデータベースの集合を $\mathcal{D}$，クエリ応答値に雑音を加えた結果得られる値の集合を Y とした．2 つの同じサイズのデータベース D, D' において，同一でないレコードが一つである場合，D, D' は隣接しているという．このとき，$\epsilon \in \mathbb{R}^+$ について差分プライバシは以下のように定義される．

定義 1. *ϵ-差分プライバシ任意の隣接データベースの組 $D, D' \in \mathcal{D}$，および任意の出力の部分集合 $S \subseteq Y$ について，*

$$\left|\log \frac{Pr(m(D) \in S)}{Pr(m(D') \in S)}\right| \leqq \epsilon \tag{1}$$

ならば，計算機構 m は ϵ-差分プライバシを満たすという．

直感的には，m が ϵ-差分プライバシを満たすとき，$m(D)$

を観測されたとしても，隣接するデータベースに対する出力 $m(D')$ が似ていることが保証されており，任意の隣接データベース D' と識別ができないため，任意の一つのレコード，すなわち個人のレコードが何であるかを推測が難しいことを表している．

2.2 ϵ-局所差分プライバシ

この節では局所差分プライバシについて説明する．差分プライバシはデータ所持者が統計量を公開する際に，隣接データベースの識別不能性を保証することで個人のプライバシを保護する．その場合，信頼できるデータ所持者が正しく差分プライバシを満たす計算機構を使用する必要がある．つまり，信頼できる第三者を必要とする．局所差分プライバシは，信頼できる第三者を仮定できない場合に用いられる．具体的にはデータ提供者が提供の前に自身のデータに雑音を加えることでプライバシを保護する．この場合，各個人が一つのデータで構成されるデータベースを所持しており，データそのものという統計量を公開すると捉えることもできる．その場合，隣接データベースはドメイン上の任意のデータであり，差分プライバシと同様に任意の隣接データベースとの識別不能性を保証することでプライバシは保護することができると考える．$\epsilon \in \mathbb{R}^+$ について局所差分プライバシは以下のように定義される．

定義 2. ϵ-局所差分プライバシ　以下を満たすとき，計算機構 m は ϵ-局所差分プライバシを満たすという．

$$\forall d, d' \in \mathcal{X}, o \in Y, \quad \left| \log \frac{Pr(m(d) = o)}{Pr(m(d') = o)} \right| \leqq \epsilon \tag{2}$$

直感的には計算機構 m に d を入力として出力しても，任意のデータ d' を入力とした場合の出力と識別することができないため，本来のデータが何であったかが推測できないことを保証している．Zhang [3] らと Wang [2] らはこの論文と同じようにパラメータ秘匿下での頻度推定の枠組みを提案しているが，そのプライバシ強度は局所差分プライバシを基礎としており，パラメータを秘匿にすることによる厳密なプライバシ強度は考慮していない．この論文では，パラメータを秘匿することにより得られる *Plausible deniability* を考慮した新たなプライバシ定義を考える．

2.3 頻度推定

この論文では提案したプライバシ定義の一つの応用先として，頻度推定を目的としたデータ収集を行う．データ d はカテゴリデータであり，そのドメインは $\mathcal{X} = \{d_0, d_1, ..., d_r\}$ であるとする．データ提供者はプライバシ保護のために雑音を加えて提供する．このような設定での頻度推定の枠組みとしては Rappor [1] が有名であるが，この論文ではパラメータを秘匿にすることで得られる *Plausible deniability* とデータ分析の質の低下のトレードオフを検証するために，Wang らの簡単な設定 [8] を用いる．これは，雑音を加えるというより，データ提供者がデータのドメインからデータを確率的に選択することでプライバシ保護を行う．評価は以下のように各データの割合の推定値と実際の割合の二乗誤差の平均を用いる．

$$\frac{1}{r-1} \sum_{i=0}^{r-1} \left(\frac{n_{d_i}}{n} - \hat{\pi}_{d_i} \right)^2 \tag{3}$$

ここで n は収集したデータの総数，n_{d_i} は提供データのうちのデータ d_i の総数，$\hat{\pi}_{d_i}$ は n_{d_i}/n の推定値である．

2.4 問題設定

この論文では，一章で述べたようにパラメータとデータには相関がなく，独立であると仮定する．図 1 にデータ収集の流れを示す．まず，データ提供者は確率的ではなく決定的にパラメータを選択する．そして，VPN などによる匿名化などの手法で各提供者がどの割合でパラメータを使ったかを収集する．つまり，各データ提供者がどのパラメータを使ったかは秘匿情報であるが，パラメータの頻度 $\Pr(\theta) = n_\theta/n$ は公開情報であると仮定する．また，パラメータはデータと独立であると仮定ため，パラメータの匿名化による収集はデータのプライバシ漏洩に関わらない．攻撃者は Honest but Curious モデルを採用する．つまり，攻撃者は個人のプライバシに関わる情報を推定しようとするが，プロトコルに背いた行動はしないと仮定する．この論文で使われる記号の意味を表 1 にまとめた．

表 1　記号の意味

記号	意味
d	収集するデータ.
z	乱数に基づく雑音が入ったデータ
Z	収集したデータ $Z = \{z_1, ..., z_n\}$
m	d を入力とし，z を確率的に出力する計算機構.
θ	計算機構 m のパラメータ. 離散値を想定している.
n	データ収集への参加者数
n_θ	パラメータ θ を用いた人の人数
n_d	収集したデータのうちのデータ d の総数
$\Pr(\theta)$	θ を用いた人の頻度の全体に対する割合 $= n_\theta$/n
$\mathcal{X}$	d のドメイン
Θ	θ のドメイン $= supp(\Pr(\theta))$
λ_d	Z のうちの d の割合
π_d	収集したデータのうちの d の割合 $= n_d/n$
$\hat{\pi}_d$	π_dの推定値
E	プライバシ強度関数 $E : \Theta \to \mathbb{R}$

3 パラメータ秘匿下でのプライバシ強度: Parameter Blending Privacy

本章では新しいプライバシの考え方である Parameter Blending Privacy(PBP) を提案する．PBP は局所差分プライバシの考え方に基づいた，パラメータを秘匿にすることにより得られる *Plausible deniability* を考慮したプライバシ強度である．PBP を導出するために，まず計算機構 m をパラメータを選択して使用した際のプライバシの漏洩（以降プライバシ損失と呼ぶ）について考える．

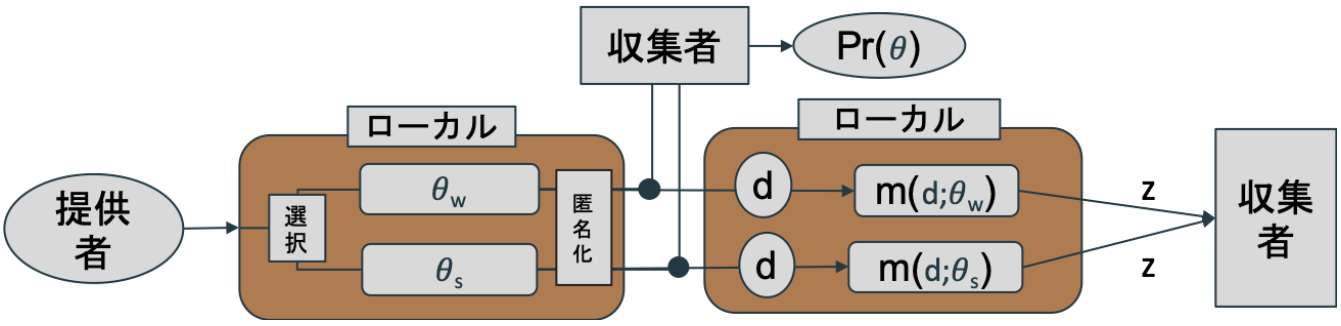

図 1　パラメータを秘匿にする場合のデータ収集の流れ.

3.1　プライバシ損失

ここでは，n 人のデータ提供者が，各々がローカルでパラメータを選択して計算機構 m を用いて提供する場合のプライバシ損失について考える．また，2.4 節で述べたように，各パラメータ $\theta \in \Theta$ が選ばれた割合 $\Pr(\theta)$ は公開情報であると仮定する．ここで，プライバシ強度というのは，計算機構 m の出力 $o = m(d;\theta)$ が与えられたときの入力 $d \in \mathcal{X}$ が何であったかの識別可能性の低さと言える．これは差分プライバシの原理である．パラメータ θ を使った場合の d とパラメータ $\theta'\Theta$ を使った場合の $d' \in \mathcal{X}$ の識別可能性（プライバシ損失と言う）は以下のように定式化できる．

$$L^o((d,\theta),(d',\theta')) = \left|\log \frac{\Pr(\theta)\Pr(m(d;\theta)=o))}{\Pr(\theta')\Pr(m(d';\theta')=o)}\right| \qquad (4)$$

右辺の分子は，d を所持しているデータ提供者がパラメータ θ を用いて o を出力する確率で，分母は d' を所持しているデータ提供者がパラメータ θ' を用いて o を出力する確率である．直感的には，プライバシ損失 $L^o((d,\theta),(d',\theta'))$ が小さいというのは，o を出力する確率が，d を用いた場合と d' を用いた場合で似ているため，o を攻撃者が見たとしても，入力が d か d' のどちらか識別できない状態を表している．逆にプライバシ損失が大きい場合，確率の差が大きいため，攻撃者が o を見た場合に，入力が d であるか d' かを識別できる状態であると言える．

3.2　パラメータ秘匿下でのプライバシ定義

前の節では，プライバシ損失をデータ d, d' の識別可能性として定義した．ここではこのプライバシ損失の考え方を用いて，局所差分プライバシを拡張することを考える．

局所差分プライバシに基づくと，任意のデータ $d \in \mathcal{X}$ を入力として計算機構 m を用いて応答値 $o \in Y$ を出力した場合に，任意のデータ $d' \in \mathcal{X}$ と識別できない（つまり，プライバシ損失が小さい）ことが保証されている場合に，プライバシは保護されていると言う．パラメータが秘匿とされている場合，プライバシ損失は (4) 式のように書ける．局所差分プライバシと同様に，任意のデータの組に対してこのプライバシ損失が低いことが保証されている場合，プライバシは保護されていると言える．これを Parameter Blending Privacy(PBP) として以下のように定式化する．

定義 3. *E-Parameter Blending Privacy* プライバシ強度関数 E に対して以下を満たすとき，計算機構 m は *E-parameter blending privacy* を満たすという．

$$\begin{aligned}&\forall\theta \in \Theta, d, d' \in \mathcal{X}, o \in Y, \exists\theta' \in \Theta\\ &L^o((d,\theta),(d',\theta')) \leqq E(\theta)\end{aligned} \qquad (5)$$

ここでプライバシ強度関数は $E : \Theta \to \mathbb{R}$ はパラメータから定数へ写す関数である．これは，パラメータ θ 用いる場合のプライバシ強度は $E(\theta)$ であることを意味する．直感的に，*E-PBP* は全てのパラメータ θ について，任意の二つのデータの組 d, d' と出力 o に対するプライバシ損失が $E(\theta)$ 以下になるパラメータ θ' が存在することを保証している．言い換えれば，*E-PBP* を満たす計算機構 m を用いて，θ を選択して d に対する応答値 $o = m(d;\theta)$ を出力したとしても，任意の他のデータ d' と $E(\theta)$ で示される程度に識別できないことが保証されている．

また，*(4)* 式を見てわかるように，パラメータの頻度 $\Pr(\theta)$ が $E(\theta)$ の値に依存する．つまり，データ提供者の選択したパラメータの割合 $\Pr(\theta)$ によって，そのプライバシ強度が変化する．*4* 章でその一例を示す．注意が必要なのが，$\Pr(\theta)$ の値はデータ提供者が各々が決定的に選択するものであるため，データ収集者側で操作することができないことである．この論文ではパラメータを秘匿にすることによる効果を検証するのが目的のため触れないが，得られたパラメータの割合 $\Pr(\theta)$ でプライバシ強度が最大になるように最適な計算機構を構築するという *PBP* を活用する方法が考えられる．

3.3　ベイズの定理に基づく解釈

ここでは *PBP* のベイズの定理に基づく解釈を説明する．計算機構 m が *E-PBP* を満たす時，d, d', θ, θ' を確率変数であると仮定し，ベイズの定理を用いると，*(5)* 式より以下が導かれる．

$$\begin{aligned}&\forall\theta \in \Theta, d, d' \in \mathcal{X}, o \in Y, \exists\theta' \in \Theta\\ &\left|\log \frac{\Pr(d,\theta|o)}{\Pr(d',\theta'|o)} - \log \frac{\Pr(d)}{\Pr(d')}\right| \leqq E(\theta)\end{aligned} \qquad (6)$$

今，左辺の第二項はデータ d と d' の事前の識別可能性を表す定数であり，第一項が出力 o が与えられた時の，パラメータ θ を用いて d を曖昧化したのか，パラメータ θ' を用いて d' を曖昧化したのかの事後の識別可能性であると言える．つまり，*PBP* はこの事前の識別可能性と事後の識別可能性の差が $E(\theta)$ 以下になる θ' が存在することを保証している解釈することができる．

3.4 局所差分プライバシとの関係

ここでは局所差分プライバシと *PBP* の関係を示す．プライバシ強度関数 E が与えられたとき，局所差分プライバシとの関係として以下の定理が成り立つ．

定理 1. 計算機構 m が全ての $\theta \in \Theta$ について $E(\theta)$-局所差分プライバシを満たすとき，以下を満たすプライバシ強度関数 E' に対して，計算機構 m は E'-*PBP* を満たす．

$$\forall \theta \in \Theta, E'(\theta) \leqq E(\theta) \tag{7}$$

Proof. 計算機構 m は全ての $\theta \in \Theta$ に対して E-局所差分プライバシを満たすため，(2) 式より，以下が成り立つ．

$$\begin{aligned} &\forall \theta \in \Theta, d, d' \in \mathcal{X}, o \in Y, \\ &L^o((d,\theta),(d',\theta)) \leqq E(\theta) \end{aligned} \tag{8}$$

よって，(5) 式より，$\forall \theta \in \Theta, E(\theta) = E'(\theta)$ に関して，E'-PBP を満たす．つまり，$E'(\theta) \leqq E(\theta)$ である．Q.E.D. □

なお，$E(\theta) < E(\theta)$ を満たすかは，θ や計算機構，$\Pr(\theta)$ に依存するが，*4* 章でそれを満たす場合があることを示す．この定理は，全ての既存の局所差分プライバシを満たす計算機構について，パラメータを秘匿にすることでプライバシ強度が下がることはなく，プライバシ強度が高くなる場合があることを示している．また，計算機構が全ての θ に対して $E(\theta)$-局所差分プライバシを満たすなら，E-*PBP* を満たすことを示している．つまり，*PBP* は局所差分プライバシを一般化した定義であることがわかる．また，パラメータ θ_p を公開するというのは $\Pr(\theta_p) = 1$ であると解釈することもできる．つまり，$supp(\Pr(\theta)) = \Theta = \{\theta_p\}$ であり，その場合，*PBP* の定義は局所差分プライバシと等しくなる．

3.5 複数回の出力

今まで，計算機構を一回のみ用いる場合を考えていた．この場合，例えば，継続して複数回データ収集をする場合を考えることができない．ここでは，パラメータを変えずに複数回の出力をした場合のプライバシ強度について考える．計算機構 $m_1, \ldots, m_i, \ldots, m_r$ がそれぞれ，パラメータを公開した場合に E_i-*PBP* を満たすとする．つまり，全ての $\theta \in \Theta$ について $E_i(\theta)$-局所差分プライバシを満たすとする．これらの計算機構を続けて用いて出力する計算機構を M とする．つまり，$m_i : \mathcal{X} \times Y_1 \times \cdots \times Y_{i-1} \to Y_i$ と書くことができる．Y_i を m_i の出力のドメインとした．この時，以下の定理が成り立つ．

定理 2. 計算機構 M は以下を満たす E について E-*PBP* を満たす．

$$\forall \theta \in \Theta, E(\theta) \leqq \sum_i^r E_i(\theta) \tag{9}$$

Proof. 計算機構 m_i は全ての $\theta \in \Theta$ に対して E-局所差分プライバシを満たすため，(2) 式より，以下が成り立つ．

$$\begin{aligned} &\forall \theta \in \Theta, d, d' \in \mathcal{X}, o \in Y, \\ &L^o((d,\theta),(d',\theta)) \leqq E(\theta) \end{aligned} \tag{10}$$

また，差分プライバシの合成定理 [4] より，以下が成り立つ．

$$\left| \log \frac{\Pr(\theta)\Pr(M(d;\theta) = o)}{\Pr(\theta)\Pr(M(d';\theta) = o)} \right| \leqq \sum_i^r E_i(\theta) \tag{11}$$

よって，(5) 式より，$\forall \theta \in \Theta, E(\theta) = \sum_i^r E_i(\theta)$ を満たす E に関して，E-PBP を満たす．つまり，$E'(\theta) \leqq E(\theta)$ である．Q.E.D. □

つまり，複数回の出力においても，パラメータを秘匿にすることで局所差分プライバシよりもプライバシ強度が低くなることはなく，高くなっている場合がある．

4 実　　験

ここでは *PBP* を使った一つの例として，*PBP* を満たす頻度推定を簡単な設定で示す．局所差分プライバシの枠組みとの違いはパラメータが秘匿とされることである．

4.1 設　　定

4.1.1 データ提供者

データ提供者はデータ $d \in \mathcal{X} = \{d_0, d_1\}$ を所持しており，$\Theta = \{\theta_w, \theta_s\}$ からパラメータを選択する．計算機構として，*Randomized Response [9]* を使用する．*Randomized Response* では以下のような確率行列 P で表される確率に従ってデータを選択する．

$$\mathbf{P} = \begin{pmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{pmatrix} \tag{12}$$

ここで $p_{yx} = \Pr(d = d_y | d = d_x)$ は d_x を入力とした時の d_y を出力する確率を示す．パラメータによって確率行列を変更することでプライバシ強度を調整することができる．

4.1.2 計 算 機 構

上で述べたように，今回用いる計算機構はデータとパラメータを入力されたとき，確率的にデータを選択し出力する．ここでは $m(d;\theta_s)$，$m(d;\theta_w)$ は以下の確率行列で表される計算機構であるとする．

$$\mathbf{P}_{\theta_s} = \begin{pmatrix} 0.6 & 0.4 \\ 0.4 & 0.6 \end{pmatrix} \tag{13}$$

$$\mathbf{P}_{\theta_w} = \begin{pmatrix} 0.8 & 0.2 \\ 0.2 & 0.8 \end{pmatrix} \tag{14}$$

この場合，例えば，$\Pr(\theta_w) = \Pr(\theta_s) = 0.5$ であった場合，$E'(\theta_s) = \log 1.5$，$E'(\theta_w) = \log 3$ である E' について計算機構は E'-*PBP* を満たす．パラメータを公開する場合，$E(\theta_s) = \log 1.5$，$E(\theta_w) = \log 4$ である E について，E-*PBP*（局所差分プライバシ）を満たす．

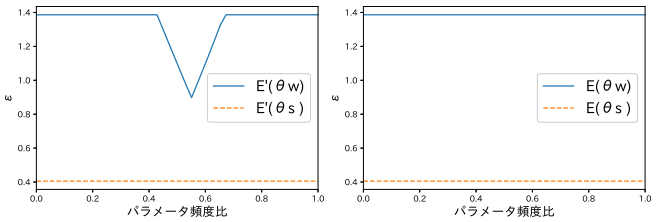

図 2　パラメータ頻度比 $\Pr(\theta_w)$ とプライバシ強度の関係．左はパラメータを秘匿にする場合 (PBP) で右はパラメータを公開する場合 (局所差分プライバシ)．

このように，$E'(\theta_w) < E(\theta_w)$ であり，パラメータを秘匿することにより，新たな *Plausible deniability* が生じたため，プライバシ強度が高くなっていることがわかる．

4.2　パラメータの頻度とプライバシ強度の関係

3.2 節で述べたように，パラメータはデータ提供者が決定的に選択するため，データ収集者が $\Pr(\theta)$ を操作することはできない．そこで，$\Pr(\theta)$ が *PBP* とどのような関係にあるのかが重要である．それを調べるため，前節で導入した二つの計算機構を用いて実験を行なった．$\Pr(\theta_w)$ を変えて，プライバシ強度 $E'(\theta_w)$ と $E'(\theta_s)$ を計算した．図 *2* がその結果を表したグラフである．図 *2* の左はパラメータを秘匿にする場合 *(PBP)* で，右がパラメータを公開する場合 *(*局所差分プライバシ*)* である．$\Pr(\theta_w)$ が変化することで，ある一定の範囲でプライバシ強度が変わっていることがわかる．逆に，そのほかの範囲ではパラメータを秘匿にした場合でも，プライバシ強度が変わっていない．このように，*PBP* ではデータ提供者が選んだパラメータの割合 $\Pr(\theta_w)$ によって，プライバシ強度が変化する．$E'(\theta_s)$ で変化が見られないのは，θ_w を使った場合との識別不能性よりも，θ_s を使った場合との識別不能性が高いためである．このように，基本的には弱いプライバシ強度（つまり，単体では識別不能性が低い）のパラメータが強いプライバシ強度のパラメータとの識別が難しくなるため，プライバシ強度が高くなる．

図 *2* の極値は計算機構によって変化する．つまり，これはこの論文の範囲を超えるが，データ収集者はこの極値が $\Pr(\theta_w)$ になるように計算機構を構築すれば，パラメータを秘匿にすることによる効果が最大限得られると考えられる．また，効果が得られないことがわかれば，パラメータを秘匿にしても公開してもプライバシ強度が変わらないため，データ提供者がパラメータを公開すれば良いと考えられる．

4.3　パラメータの頻度と有用性の関係

前節では $\Pr(\theta_w)$ によって，プライバシ強度がどのように変化するかを見た．ここでは，$\Pr(\theta_w)$ が変化した場合に，有用性がどのように変化するかを実験的に示す．まず，この仮想的なデータ収集は π_{d_0} を推定することが目的である．つまり，収集したデータ Z の有用性は π_{d_0} の推定値 $\hat{\pi}_{d_0}$ の誤差の大きさと考えることができる．言い換えると，$\hat{\pi}_{d_0}$ の誤差が小さい場合に，収集したデータの有用性が高いと考えられる．ここではまず，推定値の求め方について説明する．ここで注意が必要なのはパラメータが秘匿の場合と公開の場合で推定の方法が変わるということである．この実験では，それぞれについて対数尤度最大化と不偏推定量による二通り，計四通りの推定を行なった．

4.3.1　対数尤度最大化

対数尤度を微分して極値を求めることで尤度を最大にする $\hat{\pi}_{d_0}$ を求める．

a）　パラメータが秘匿の場合

対数尤度はパラメータが秘匿の場合，以下のように表される．

$$\ln \Pr(Z) = \sum_i^n \sum_\theta \ln(\Pr(\theta)(2\Pr(m(d_0;\theta) = z_i)\pi_{d_0} - \pi_{d_0} + \Pr(m(d_0;\theta) = z_i) + 1) \tag{15}$$

b）　パラメータが公開の場合

対数尤度はパラメータが公開されている場合，以下のようになる．

$$\ln \Pr(Z) = \sum_i^n \ln(2\Pr(m(d_0;\theta_i) = z_i)\pi_{d_0} - \pi_{d_0} + \Pr(m(d_0) = z_i;\theta_i) + 1) \tag{16}$$

4.3.2　不偏推定量

二つ目の方法が不偏推定量を用いる方法である．収集したデータ Z のうち，実際に観測した d_0 の割合を λ_{d_0} と書くとき，π_{d_0} の不偏推定量 $\hat{\pi}_{d_0}$ は以下のように導出される．

$$\hat{\pi}_{d_0} = \frac{p_{00} - 1}{2p_{00} - 1} + \frac{\lambda_{d_0}}{2p_{00} - 1} \tag{17}$$

a）　パラメータが秘匿の場合

パラメータが秘匿の場合，

$$p_{00} = \sum_\theta \Pr(\theta)\Pr(m(d_0;\theta) = d_0) \tag{18}$$

と表すことができる．これを *(17)* 式に代入することで，推定値 $\hat{\pi}_{d_0}$ を得る．

b）　パラメータが公開の場合

パラメータが公開されている場合，Z の中からデータをパラメータによって選ぶことで三種類の p_{00}（つまり，$\mathbf{P}_{\theta_\mathbf{w}}[\mathbf{0},\mathbf{0}]$，$\mathbf{P}_{\theta_\mathbf{s}}[\mathbf{0},\mathbf{0}]$，秘匿の場合と同じ p_{00}）を考えることができるため，三種類の不偏推定量が導出することができ，それらの中で最も分散が小さいものを選べば良い．$\hat{\pi}_{d_0}$ の分散は以下のように導出される．

$$\frac{\hat{\pi}_{d_0}(1 - \hat{\pi}_{d_0})}{n-1} + \frac{1}{n-1}\left(\frac{1}{16(p_{00} - 0.5)^2} - \frac{1}{4}\right) \tag{19}$$

4.3.3　パラメータの頻度と有用性の関係

ここでは，上で説明した四通りの推定値の誤差（有用性）とパラメータの頻度の関係を示す．なお，公開する場合と秘匿にする場合で公平にするために $E(\theta_w)$ の値が一定になるように計算機構を調整した．パラメータを秘匿にすることの効果が見られた範囲で 10000 回のシミュレートを行い，四通りの推定値の誤差を計算した．その結果が図 *3* である．縦軸が推定値の誤差で横軸が $\Pr(\theta_w)$ である．全てプライバシ強度が一定である

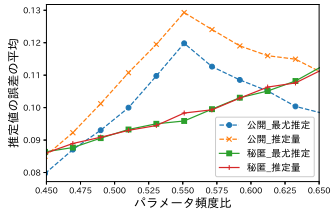

図 3　パラメータの頻度と有用性の関係．$n = 100$，$\pi_0 = 0.5$ の時の結果．

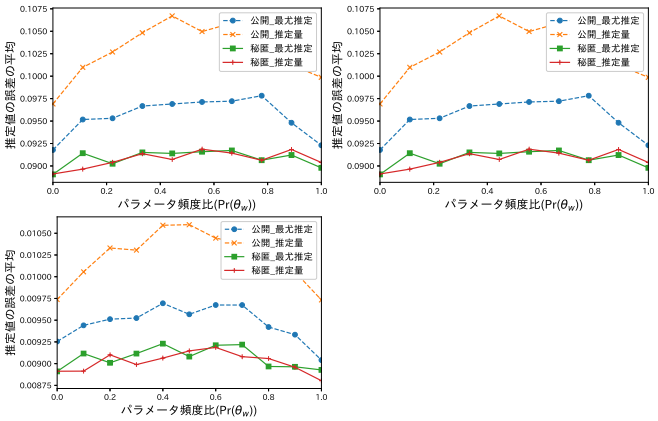

図 4　母数 n =100(左上)，1000（右上），10000（左下）でデータ頻度を $[0, 1]$ の範囲で変えてシミューレションを 10000 回繰り返した時の推定値の誤差の平均．

ため，より下側にある場合，プライバシと有用性の良いトレードオフが達成できていると言える．この結果を見ると，一部の範囲で秘匿にすることでそれが達成できていることがわかる．ただし，一部の範囲でそのトレードオフは悪くなっている．これは，図 *2* の公開する場合との変化が少ししか見られない部分である．パラメータを公開する場合よりもプライバシ強度がある程度以上高くなった場合に，プライバシ・有用性トレードオフの向上が見られることがわかる．

つまり，$\Pr(\theta_w)$ が与えられた時に，図 *2* の極値の部分が $\Pr(\theta_w)$ になるように計算機構を調整することでプライバシ・有用性のトレードオフの向上を達成できると考えられる．

4.4　母数とデータの頻度比と有用性の関係

ここまで，パラメータの頻度がどのようにプライバシ強度に影響するかを見てきた．ここでは，パラメータの頻度を $\Pr(\theta_w) = 0.5$ に固定して，母数 n とデータの頻度 π_{d_0} が有用性にどのように影響を与えるかを，パラメータを秘匿にする場合と公開する場合について比較しながら示す．なお，公平に比較するために，パラメータを秘匿にする場合と公開する場合について，$E(\theta_s) = \log 1.5$, $E(\theta_w) = \log 3$ について *E-PBP* を満たすように計算機構を構築した．データの頻度 π_{d_0} は $[0, 1]$ の範囲で，母数 n は 100,1000,10000 の三つで変えて，10000 回のシミュレートを行い四通りの推定値 $\hat{\pi}_{d_0}$ の誤差の平均をとった．図 *4.4* がその結果である．

全て同じプライバシ保護の度合いであり，より下側が誤差が小さく有用性が高いと言える．つまり，パラメータを秘匿にする場合の方がより良いデータ分析ができていることがわかる．

5　結　　論

この論文では，パラメータを秘匿にする場合のプライバシ保護の保証を局所差分プライバシを拡張することで理論的に考えた．提案した新しいプライバシの考え方 *PBP* に基づくと，パラメータを秘匿にすることで，プライバシ強度が実際に高くなる場合があることを示した．*PBP* を用いた一つのデータ収集の枠組みを提案し，実際にシミュレートすることで，パラメータを公開する場合に比べて，パラメータを秘匿にする場合の方が同じプライバシ強度の時にデータ分析の質がよくなる場合があることが示された．これはつまり，パラメータを秘匿にすることでプライバシ・有用性のトレードオフが向上する場合があることを示している．

今回は簡単なデータ収集の枠組みを用いたが，実際に用いられているようなデータ収集の枠組み（例えば，*RAPPOR*）に *PBP* を適用した場合にも，その効果が見られるかは未知である．また，$\Pr(\theta)$ が与えられた時に，最適な計算機構を構築することが可能かどうかも未知である．また，データとパラメータが依存関係にある場合の理論的なプライバシ保証も重要な課題である．今後はこれらの課題を解決していきたい．

6　謝　　辞

文　　献

[1] *Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In* Proceedings of the 2014 ACM SIGSAC conference on computer and communications security, *pp. 1054–1067. ACM, 2014.*

[2] *Shaowei Wang, Liusheng Huang, Miaomiao Tian, Wei Yang, Hongli Xu, and Hansong Guo. Personalized privacy-preserving data aggregation for histogram estimation. In* 2015 IEEE Global Communications Conference (GLOBECOM), *pp. 1–6. IEEE, 2015.*

[3] *Xin-Yuan Zhang, Liu-Sheng Huang, Shao-Wei Wang, Zhen-Yu Zhu, and Hong-Li Xu. Personalized differential privacy preserving data aggregation for smart homes. In* 3rd International Conference on Wireless Communication and Sensor Networks (WCSN 2016). *Atlantis Press, 2016.*

[4] *Cynthia Dwork. Differential privacy.* Encyclopedia of Cryptography and Security, *pp. 338–340, 2011.*

[5] *Cynthia Dwork. A firm foundation for private data analysis.* Communications of the ACM, *Vol. 54, No. 1, pp. 86–95, 2011.*

[6] *Shiva Prasad Kasiviswanathan, Homin K Lee, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. What can we learn privately?* SIAM Journal on Computing, *Vol. 40, No. 3, pp. 793–826, 2011.*

[7] *Zach Jorgensen, Ting Yu, and Graham Cormode. Conservative or liberal? personalized differential privacy. In* 2015 IEEE 31St international conference on data engineering, *pp. 1023–1034. IEEE, 2015.*

[8] *Yue Wang, Xintao Wu, and Donghui Hu. Using randomized response for differential privacy preserving data collection. In* EDBT/ICDT Workshops, *Vol. 1558, 2016.*

[9] *Stanley L Warner. Randomized response: A survey tech-*

nique for eliminating evasive answer bias. Journal of the American Statistical Association, *Vol. 60, No. 309, pp. 63–69, 1965.*