Computer Security Symposium 2020
26 - 29 October 2020

差分プライバシと準同型暗号の組合せに関する研究動向調査

牛山 翔二郎 [1,*]　工藤 雅士 [1]　髙橋 翼 [2]
井上 紘太朗 [1]　鈴木 拓也 [1]　山名 早人 [1]

概要：近年，クラウドコンピューティングが新たなネットワークサービスとして注目を集めている．しかし，データ保管やデータ処理の過程において，クラウド上のサーバやデータ解析者へのプライバシ漏洩が懸念されている．プライバシ漏洩への対策として，本稿では 2 つの手法に注目した．1 つは，データにノイズを加えることで，データ提供者の元データの値が推測されることを防ぐ差分プライバシである．もう 1 つは，暗号化した状態のままの演算を可能にする準同型暗号である．差分プライバシと準同型暗号を組み合わせることで，計算結果の出力値に対するプライバシ保護と，データの通信や保管および計算過程における秘匿性の両方を達成するシステムを構築することができる．本稿では，差分プライバシと準同型暗号を組み合わせたプライバシ保護手法に関する研究調査を行い，近年の傾向についてまとめる．具体的には，データの収集方法やノイズを加えるタイミングなどに焦点を当て，特に差分プライバシと準同型暗号の組み合わせ方とユースケースについてそれぞれ分類し，今後の研究動向について考察する．

キーワード：差分プライバシ，準同型暗号，秘匿計算，プライバシ保護データマイニング

Survey on the Combination of Differential Privacy and Homomorphic Encryption

Shojiro Ushiyama[1,*]　Masashi Kudo[1]　Tsubasa Takahashi[2]
Kotaro Inoue[1]　Takuya Suzuki[1]　Hayato Yamana[1]

Abstract: In recent years, cloud computing has been attracting attention as a new network service; however, privacy leakage to cloud servers or data analysts becomes a serious concern. In this paper, we focus on two techniques to prevent privacy leakage. One is differential privacy that prevents guessing at the original values of data providers by adding noise to the data. The other is homomorphic encryption that enables arithmetic operations over its encrypted data. By combining differential privacy and homomorphic encryption, we can construct a system that preserves the privacy leakage from the computation output that will be revealed to the analysts as a plain data besides preserving it during communications, computing processes, and storing. In this paper, we investigate privacy preservation techniques that combine differential privacy and homomorphic encryption. We also summarize recent research trends. Specifically, we focus on the data collection methods and the timing of adding the noise. Then, we classify these methods depending on how they combine differential privacy and homomorphic encryption and how the use case is, and discuss the future research trends.

Keywords: Differential Privacy，Homomorphic Encryption，Secure Computation，Privacy-Preserving Data Mining

1. はじめに

近年，機械学習やデータ解析といった複雑な計算を代行するサービスである Machine Learning as a Service (MLaaS) が注目を集めている．MLaaS は，通常，クラウドコンピューティング型であり，機械学習やデータ解析を実行する計算ツールをクラウド上で提供する．クラウドコンピューティングでは，機密性の高いデータを取り扱う際に，データの保管や処理の過程において，クラウドサーバやデータ解析者へのプライバシ漏洩が懸念されている．本稿では，プライバシ保護手法の中でも，特に「差分プライバシ」と「準同型暗号」の２種類の手法に焦点を当てる．

差分プライバシ[1]とは，データ提供者が提供する元データや計算結果の出力値にノイズの加算を行うことにより，元データを推定することを困難にする，数学的根拠に基づいたプライバシ保護手法である．差分プライバシは，クラウドサーバ上に保管されるデータや計算結果の出力値に対してプライバシ保護を提供する．一方で，データの有用性を向上させるためには，加算するノイズ量を制限する必要があり，プライバシ強度が低下する．

準同型暗号とは，暗号化した状態のままでの演算を可能とする性質を持った暗号の総称である．準同型暗号をクラウドコンピューティングで使用することで，クラウドサーバ上で復号を行わずに演算を行うことを可能とし，クラウドサーバに対する秘匿性を提供する．一方で，準同型暗号を単体で使用した場合では，秘密鍵（復号鍵）を持つ出力

1 早稲田大学
Waseda University
2 LINE 株式会社
LINE Corporation.
* s-ushiyama@yama.info.waseda.ac.jp

結果の受信者に，出力結果を復号して得られる値から元データの値を推測される懸念がある．

両手法には一長一短がある．差分プライバシは元データにノイズを加えるため，元データを復元できないという利点があるものの，一旦ノイズが加わったデータに対する処理には制限がある．例えば，ノイズを含むデータに対してなんらかの演算を行う場合，その結果の正確性が問題となる．一方，準同型暗号は暗号化したまま演算が可能であるものの，秘密鍵によって復号化できる．このため，最終的に得られた結果がプライバシを侵害するような内容である場合，これを復号者から守る術がない．

こうした問題に対応するため，差分プライバシと準同型暗号を組み合わせることで，計算結果の出力値から元データを推測されることを防ぎ，かつ，データを保管や処理する過程でデータの秘匿性を保証するプライバシ保護手法を構築する研究が行われている．本稿では，差分プライバシと準同型暗号を組み合わせたプライバシ保護手法に関する研究動向の調査を行う．また，差分プライバシにおけるノイズを加えるタイミングに焦点を当て，差分プライバシと準同型暗号の組み合わせ方と，ユースケースについて，それぞれ 3 つのパターンに分類する．

本稿の貢献は以下の通りである．

1. 差分プライバシと準同型暗号を組み合わせたプライバシ保護手法に関する論文を，著者，著者の拠点，出版年，使用した差分プライバシの種類，使用した準同型暗号の種類，差分プライバシと準同型暗号の組み合わせ方，ユースケースの観点から表としてまとめる．これは，プライバシ保護手法を模索する研究者や開発者の助けとなる．
2. 差分プライバシと準同型暗号を組み合わせた研究に対して，差分プライバシにおけるノイズを加算するタイミングとユースケースの観点から分類を行い，研究が盛んに行われている組み合わせ方のパターンを示す．これは，今後の差分プライバシと準同型暗号を組み合わせた研究を深める上での助けとなる．

本稿の構成は以下の通りである．2 節では背景知識となる差分プライバシと準同型暗号について説明する．次に，3 節では実施した調査についての報告を行う．そして，4 節では行った調査に対して議論をする．最後に，5 節で結論を示す．

2. 背景知識

本節では，本稿の主要な背景知識である，差分プライバシと準同型暗号について説明する．

2.1 差分プライバシ

差分プライバシは Dwork ら[1]によって，2006 年に提案され，近年盛んに研究されているプライバシ保護手法である．差分プライバシは，元データの出力にノイズを加算することで，元データに対するプライバシ保護を提供する．また，差分プライバシは任意の背景知識を持つ攻撃者に対して有効であるとされている[2]．通常，差分プライバシにおけるプライバシ保護強度とデータの有用性はトレードオフである．具体的には，ノイズを多く加算すると，元データの値を推測することがより困難になるが，出力される統計値と真の値との差が大きくなり，計算結果の出力値の有用性が低下する．ノイズは平均 0 の確率分布に従いサンプリングされるため，データを多数集めると，統計的性質が復元される．

差分プライバシは，数学的根拠に基づいたプライバシ保護手法であり，以下の定義 1 を満たすことを，「あるメカニズムmはϵ-差分プライバシを満たす」と言う．定義 1 において，メカニズムとは，ノイズの付加等によって差分プライバシを満たすランダム性を持つ計算機構である．代表的なメカニズムとして，ラプラスメカニズム[1]，ガウシアンメカニズム[3]が挙げられる．また，$d(D, D')$は，2 つのデータベースDおよびD'において，同一ではないレコードの数を表す．具体的には，$d(D, D') = 1$とは，2 つのデータベースDおよびD'が 1 つのレコードを除いて，残りのレコードが全く同じデータベースであることを意味する．ϵは 0 より大きい任意の値であり，この値の大きさでプライバシ強度を調節することができる．具体的には，ϵが小さいほど保証されるプライバシの強度は強くなる．

定義 1([4]より引用)：

クエリqにおいて，$d(D, D') = 1$なる任意のデータベースの組D, D'，およびクエリ応答の出力の部分集合Sについて，

$$\frac{\Pr\left(m(q, D) \in S\right)}{\Pr\left(m(q, D') \in S\right)} \leq \exp(\epsilon) \quad (1)$$

ここで $\epsilon > 0$ である．また，$\Pr(a)$は，ある事象aが起こる確率を表す．

差分プライバシは，ノイズを加算するタイミングによって，下記の 2 種類に分類することができる．

1. セントラル差分プライバシ（グローバル差分プライバシとも呼ばれる）(以降, CDP)
2. ローカル差分プライバシ (以降, LDP)

CDP では，クラウドサーバが信頼できるサーバであることを仮定し，サーバが保持しているデータを使用した計算結果の出力値に対してノイズの加算を行う．一方, LDP では，クラウドサーバが信頼できないことを仮定し，データ収集時に元データに対してノイズの加算を行う. CDP と LDP の比較を図 1 に示す．図 1 において，「データ提供者」は必要なデータを提供するエンティティを示し，「データ利用者」はデータ解析者やサービス提供者といった，出力される統計値を使用するエンティティを示す.「データ提供者」と「データ利用者」はともに，エンティティが単一の場合とエンティティが複数の場合が存在する．クラウドサーバについ

ては，CDP では「信頼できるサーバ」と表記しており，クラウドサーバが信頼できるサーバであることを仮定している．一方で，LDP では「信頼できないサーバ」と表記しており，クラウドサーバに対する信頼を必要としない．

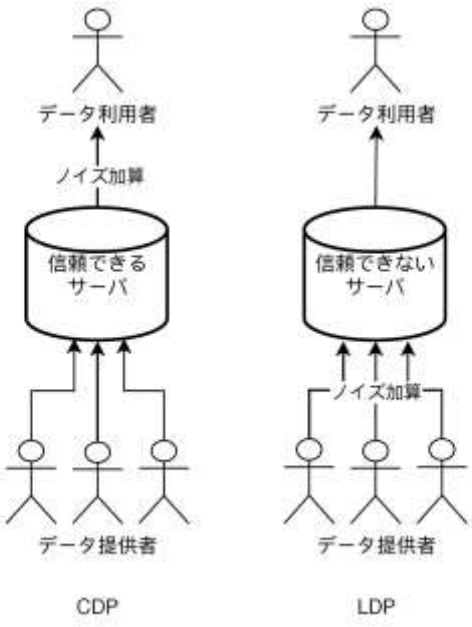

図 1　CDP（左）と LDP（右）の比較

CDP は，データに加えるノイズの量を，LDP と比べて小さくすることができる一方で，クラウドサーバを信頼しなければならないという制約がある．LDP は，信頼できるサーバを必要としない一方で，全ての出力の可能性がある範囲に差分プライバシを保証する必要があるため，$d(D, D') = 1$ の変化にのみ差分プライバシを保証する CDP と比べて加算するノイズの量が大きくなり，統計値の有用性が低下するという欠点がある．

2.2 準同型暗号

準同型暗号とは，暗号化した状態のままでの演算を可能とする性質を持った暗号の総称である．準同型暗号を使用することで，演算を行う者に対しても，データに含まれる秘密を保護することができる．一方で，準同型暗号には，計算コストが大きくなるという欠点がある．

暗号文上で準同型暗号を用いて行われる加算を準同型加算，乗法を準同型乗算と呼ぶ．準同型加算の性質を式(2)に，準同型乗算の性質を式(3)に示す．式(2)，(3)において，Encは暗号アルゴリズム，Decは復号アルゴリズムであり，aとbは平文を表す．

$$Dec\big(Enc(a) + Enc(b)\big) = a + b \quad (2)$$

$$Dec(Enc(a) \times Enc(b)) = a \times b \quad (3)$$

特に，準同型加算のみを実行できる準同型暗号を加法準同型暗号，準同型乗算のみを実行できる準同型暗号を乗法準同型暗号と呼ぶ．また，任意回数の準同型加算と準同型乗算を実行可能とする完全準同型暗号[5]は，近年盛んに研究されている．しかし，完全準同型暗号は，その膨大な計算コストにより，現時点では実用的ではないものの，発表から 10 年を経てその計算速度は大きく改善している．

より実用的な準同型暗号として，実用上充分な回数の加算と数回の乗算を許容する Somewhat 準同型暗号や，実用上充分な回数の加算と定められた回数の乗算を許容する Leveled 準同型暗号がある．なお，準同型乗算は，一般的に準同型加算と比べてより多くの計算コストを必要とする．

3. 調査

本節では，実施した調査の詳細を報告する．差分プライバシと準同型暗号を組み合わせたプライバシ保護手法に関する論文を選定する．選定した論文に対して，著者，著者の拠点，出版年，使用した差分プライバシの種類，使用した準同型暗号の種類，差分プライバシと準同型暗号の組み合わせ方，ユースケースの観点から表としてまとめる．

3.1 調査方法

以下の 4 つの手順にて調査を行った．

3.1.1. 調査目的の設定

本調査では，差分プライバシと準同型暗号を組み合わせた手法に関する研究に注目し，下記の 2 点を目的とした．

1. 近年の研究動向について調査すること
2. 今後の研究課題について調査すること

3.1.2. 論文の検索

差分プライバシと準同型暗号を組み合わせた手法に関する研究調査として，近年に発表された論文についての調査を実施した．本調査では，論文データベースとして Scopus[a]を採用した．以下の検索条件を用いて，2020 年 7 月 9 日に検索を行った．

- キーワード：“Differential Privacy”
  AND “Homomorphic Encryption”
- 検索範囲：論文タイトル，抄録，キーワード
- 出版年：2015 年～2020 年
- 論文種別：Conference Paper および Article

3.1.3. 論文の選定

3.1.2 で得られた論文に対して，論文の選定を実施し,本調査の対象とする論文の選定を行った.選定方法としては,各論文の抄録と結論を読み，その内容から本調査の対象である差分プライバシと準同型暗号を組み合わせた手法であるか否かの判断を行なった．

3.1.4. 論文の分類

選定した論文に対する分類を行う．論文の分類は，差分プライバシと準同型暗号の組み合わせ方に焦点を当てて行う．準同型暗号を使用する意義は，クラウドサーバやデー

a) https://www.scopus.com/

タ収集者といった仲介エンティティに対してデータの秘匿性を保証することである．準同型暗号の使用方法については，データ収集時に暗号化を行い，統計値を必要とするエンティティで復号化されるというパターンが主要である．今回選定した全ての論文においても，この主要なパターンが使用されており，準同型暗号の使用方法に違いは見られない．そこで，使用する差分プライバシの種類とノイズを加算するタイミングに基づいて分類を行い，下記の 3 つのパターンに分類する．

1. パターンⅠ：データ提供者による元データの暗号化前，かつ，データ提供者によるクラウドサーバへのデータ送信前に，データ提供者が各自の元データにノイズを加算する．LDP に分類される．
2. パターンⅡ：データ提供者による元データの暗号化後，かつ，データ提供者によるクラウドサーバへのデータ送信後に，クラウドサーバが暗号化されたデータにノイズを準同型加算する．LDP に分類される．
3. パターンⅢ：暗号化された状態のノイズを含まないデータをデータ提供者がクラウドサーバへ送信し，クラウドサーバが行う統計値計算後，クラウドサーバが計算結果の出力値にノイズを加算する．CDP に分類される．

3.2 調査結果

本項では，論文調査の結果を報告する．論文検索の段階で，54 本の論文が該当した．そして，論文の選定を行ったところ，20 本の論文を選定した．選定した 20 本に関して，出版年別の分布図を図 2 に示す．

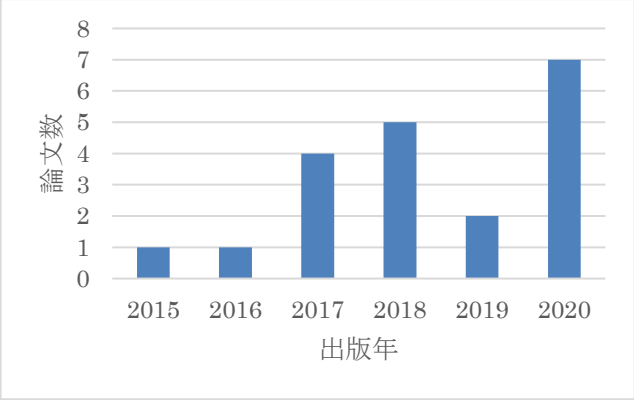

図 2　年ごとの論文数の推移

図 2 より，差分プライバシと準同型加算の組み合わせた手法に関する近年の研究は，2019 年を除き増加傾向にあることがわかる．

次に，選定した論文について，表 1 にまとめる．表 1 の項目について，説明する．

- 著者：著者名を記載する．
- 拠点：著者が所属している機関名を記載する．
- 論文種別：国際会議論文を「会議」，論文誌を「論文」と記載する．
- 会議・論文誌：国際会議または論文誌の略称を記載する．
- 出版年：各論文が出版された年を西暦で記載する．
- 差分プライバシの種類：各論文取り扱われている差分プライバシの種類を記載する．
  - CDP：CDP が使用されていることを示す．
  - LDP：LDP が使用されていることを示す．
- 準同型暗号の種類：各論文中で取り扱われている準同型暗号の種類を記載する．
- 組み合わせパターン：各論文が使用している差分プライバシと準同型暗号の組み合わせ方を示す．表記方法は 3.1.4 に基づく．
- ユースケース：各論文が想定しているユースケースを示す．
  - N：具体的なサービスへの適応を想定せず，プライバシ保護システムの構造を議論している論文．
  - N*：具体的なサービスを想定しないユースケース N において，特に，連合学習（英：Federated Learning[b]）または連合学習に類似する手法を，差分プライバシと準同型暗号を組み合わせたプライバシ保護手法に統合した手法を議論している論文．
  - A：医療ネットワークやモバイル広告といった既存の具体的なサービスに対して適応させたシステムについて議論している論文．また，具体的なユースケース名も合わせて示す．

以後，連合学習または連合学習に類似する手法を「分散型機械学習手法」とする．分散型機械学習手法は，データ提供者がそれぞれ独立して学習を行い，クラウドサーバでパラメータの更新を行うことで，参加者のデータのプライバシを保護する機械学習の総称を表す．

4. 議論

本節では，実施した調査に対しての議論を行う．まず，使用されている準同型暗号の種類と論文数の観点から議論を行う．次に，使用されている差分プライバシの種類と論文数の観点から議論を行い，更に分散型機械学習手法を考慮して議論する．最後に，組み合わせパターンとユースケースの観点から議論を行う．

4.1 使用する準同型暗号の種類について

表 1 から，20 本中 14 本の論文では準同型暗号として，加法準同型暗号が採用されていることがわかる．加法準同型暗号を採用する理由としては，計算量の問題から準同型加

b McMahan, B. and Ramage, D.: Federated learning: Collaborative machine learning without centralized training data, Google AI Blog (2017)

表 1　選定した論文のリスト(その 1)

著者	拠点	論文種別	会議・論文誌	出版年	差分プライバシの種類	準同型暗号の種類	組み合わせパターン	ユースケース
Christopher Buckley ら[6]	● カリフォルニア大学	会議	ICCCN	2015	LDP	加法準同型暗号(Elaine Shi らによる暗号方式[7])	I	A(広告配信)
Shujun Li ら[8]	● 塩城師範学院	論文	EURASIP J Wirel. Commun. Netw.	2016	LDP	加法準同型暗号(Paillier 暗号[9])	I	A(WiFi)
Vincent Bindschaedler ら[10]	● パロアルト研究所	会議	CODASPY	2017	LDP	加法準同型暗号(Paillier 暗号)	I	N
Abbas Acar ら[11]	● フロリダ国際大学 ● ペンシルベニア州立大学	会議	IEEE PAC	2017	LDP	完全準同型暗号(BGV[12])	I	N
Carlo Brunetta ら[13]	● チャルマース工科大学	会議	ISC	2017	LDP	完全準同型暗号(整数準同型暗号[14])	II	N
Yoshinori Aono ら[15]	● 情報通信研究機構 ● 神戸大学	会議	IEICE Trans. Inf. & Syst.	2017	CDP	加法準同型暗号(LWE-based 暗号[16])	III	N
Jean Louis Raisaro ら[17]	● ローザンヌ工科大学 ● ローザンヌ大学病院	論文	IEEE/ACM Trans. Comput. Biol. Bioinform.	2018	CDP	Somewhat 準同型暗号(FV[18])	III	A(医療)
Saket Komawar ら[19]	● プネー大学	会議	ICCUBEA	2018	CDP	加法準同型暗号(Paillier 暗号)	III	N
Jin Li ら[20]	● 広州大学 ● 北京交通大学 ● バージニア工科大学 ● ニューブラウンズウィック大学	会議	ESORICS	2018	LDP	加法準同型暗号(Paillier 暗号)	II	N
Ping Li ら[21]	● 広州大学 ● 南海大学 ● 北京交通大学 ● 西安電子科技大学 ● ディーキン大学	論文	Future Gener. Comput. Syst.	2018	LDP	加法準同型暗号(二重復号アルゴリズム[21])	II	N
Jinbo Xiong ら[22]	● 福建師範大学 ● 貴州大学 ● ジョージアサザン大学	論文	Wirel. Commun. and Mobile Comput.	2018	LDP	完全準同型暗号(BGV)	I	N
Jean Louis Raisaro ら[23]	● スイス連邦工科大学 ● ローザンヌ大学病院	論文	IEEE/ACM Trans. Comput. Biol. Bioinform.	2019	CDP	加法準同型暗号(楕円曲線エルガマル暗号)	III	A(医療)
Meng Hao ら[24]	● 電子科技大学 ● CETC ビッグデータ研究所 ● 通信セキュリティ科学技術研究所	会議	ICC	2019	LDP	加法準同型暗号(PPMD[25])	I	N*

表 1　選定した論文のリスト(その 2)

著者	拠点	論文種別	会議・論文誌	出版年	差分プライバシの種類	準同型暗号の種類	組み合わせパターン	ユースケース
Amrita Roy Chowdhury ら[26]	● ウィスコンシン大学 ● デューク大学 ● ウォータールー大学	会議	SIGMOD	2020	CDP	Somewhat 準同型暗号 (Labeled 準同型暗号[27])	Ⅲ	N
David Froelicher ら[28]	● スイス連邦工科大学	論文	IEEE Trans. Inf. Forensics Secur.	2020	CDP	加法準同型暗号 (楕円曲線エルガマル暗号)	Ⅲ	N
Miran Kim ら[29]	● テキサス大学 ● 蔚山科学技術大学 ● カリフォルニア大学	論文	IEEE Trans. Inf. Forensics Secur.	2020	LDP	Leveled 準同型暗号 (HEAAN[30])	I	N*
Maoguo Gong ら[31]	● 西安電子科技大学	論文	Neural Networks	2020	LDP	加法準同型暗号 (Paillier 暗号)	I	N*
Yu Xie ら[32]	● 西安電子科技大学	論文	Knowledge-Based Systems	2020	LDP	加法準同型暗号 (Paillier 暗号)	I	N*
David Froelicher ら[33]	● スイス連邦工科大学 ● ローザンヌ大学病院	会議	Stud. Health. Technol. Inform.	2020	CDP	加法準同型暗号 (楕円曲線エルガマル暗号)	Ⅲ	A (医療)
Muhammad Asad ら[34]	● 名古屋工業大学 ● ザガジグ大学	論文	Applied Sciences	2020	LDP	加法準同型暗号 (Paillier 暗号)	I	N*

算を使用している[20，23，24，31，34]ことや，総和や標準偏差を求めるユースケースでは準同型乗算を必要としない[6，8，10, 28]ことが挙げられる．

一方で，差分プライバシと準同型暗号を組み合わせたプライバシ保護手法において，完全準同型暗号や Somewhat 準同型暗号，Leveled 準同型暗号といった，準同型乗算を可能にする準同型暗号を組み合わせた論文は，20 本中 6 本と数が少ない． 準同型乗算は，幅広いユースケースに対応するときの解決策の 1 つになる．したがって，今後の研究課題として，差分プライバシに完全準同型暗号や Somewhat 準同型暗号, Leveled 準同型暗号といった乗算を可能にする準同型暗号を組み合わせることで，準同型加算と準同型乗算の両方に対応可能なシステムを構築することが挙げられる．また，準同型加算と準同型乗算の両方に対応可能なシステムを構築する上で，準同型乗算の計算量的問題は，解決するべき課題となるため，準同型乗算を軽量化することが必要となる．

4.2　使用する差分プライバシの種類について

次に，使用されている差分プライバシの種類について，年代別に論文数をまとめたグラフを図 3 に示す．

図 3 より，差分プライバシと準同型暗号を組み合わせた手法において，CDP を採用する手法と LDP を採用する手法は共に，2019 年を除き増加傾向にあることがわかる．

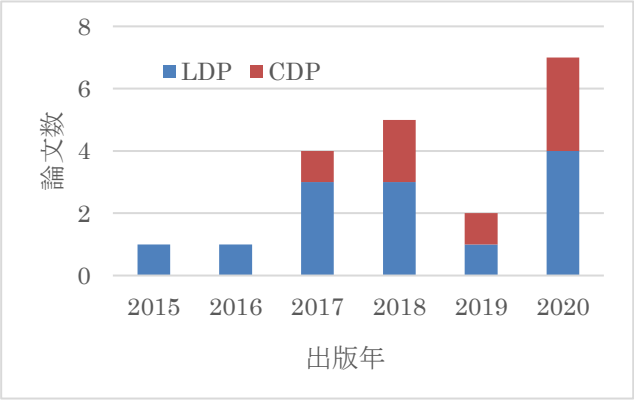

図 3　使用される差分プライバシの論文数推移

4.3　分散型機械学習手法と使用される差分プライバシの種類について

図 3 の条件に加えて，特に分散型機械学習手法を想定している論文，つまり，表 1 中のユースケース N*である論文に注目して分類を行い，図 4 に示す．具体的には以下の 4 つで分類する．

- 分散型機械学習手法(CDP):ユースケース N*, かつ, CDP を使用している論文
- 分散型機械学習手法(LDP):ユースケース N*, かつ, LDP を使用している論文
- その他(CDP):ユースケース N もしくは A, かつ, CDP を使用している論文
- その他(LDP):ユースケース N もしくは A, かつ, LDP を使用している論文

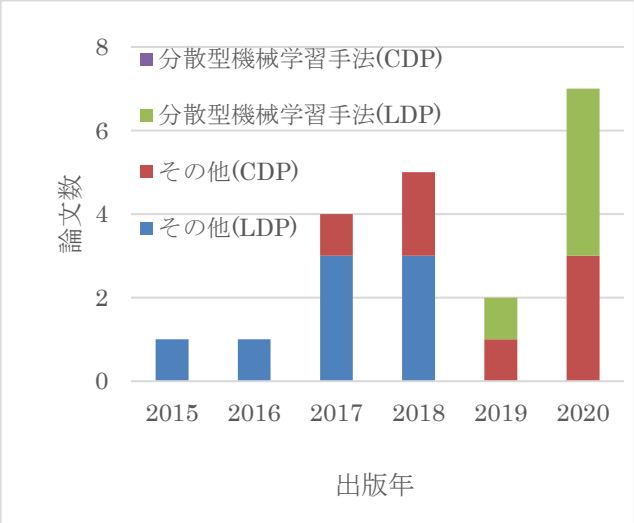

図 4　分散型機械学習手法と使用される差分プライバシの論文数推移

図 4 より，近年の研究動向に関して，分散型機械学習手法を除くユースケースにおける CDP と準同型暗号を統合する研究が増加傾向にあることと，分散型機械学習手法に LDP と準同型暗号を統合する研究が増加傾向にあることがわかる．一方で，分散型機械学習手法を除くユースケースにおいて，LDP と準同型暗号を組み合わせるケースは減少傾向にある．また， 分散型機械学習手法に CDP と準同型暗号を統合する研究に該当する論文数が 0 本であった．分散型機械学習手法をユースケースとする全ての論文で，LDP が採用されている．

4.4 組み合わせパターンとユースケースについて

表 1 における組み合わせパターンとユースケースに対して，それぞれのパターンの組み合わせの論文数と論文を投稿した研究グループ数（以下,拠点数）を表 2 に示す．研究グループ数の数え方は以下の通りである．

- 1 つの論文において，著者らの拠点が複数あった場合でも，1 つの研究グループとして数える．
- 異なる複数の論文において，同一著者が含まれる場合は，同一の研究グループとして数える．

表 2 より，差分プライバシにおけるノイズを加算するタイミングでの分類とユースケースの組み合わせにおいて，盛んに研究が行われている組み合わせを読み取ることができる．具体的には，ユースケースの N*である分散型機械学習手法に適応させる場合は，組み合わせパターンのパターン I でのみ研究が行われている． また，組み合わせパターンⅡの研究は，論文数が少なく，そのユースケースは具体的なサービスを想定しない N に限られている．ユースケース A の論文数は 5 本であるが，拠点数は 3 であった．

表 2　組み合わせパターンとユースケースのそれぞれの組合せの論文数（()内の値は拠点数を示す）

		ユースケース		
		N	N*	A
組み合わせパターン	I	3 (3)	5 (4)	2 (2)
	Ⅱ	3 (2)	0 (0)	0 (0)
	Ⅲ	4 (4)	0 (0)	3 (1)

4.5 議論のまとめ

近年の研究動向として，差分プライバシと準同型暗号を組み合わせるプライバシ保護負傷において，加法準同型暗号を採用する傾向がある．一方で，完全準同型暗号や Somewhat 準同型暗号，Leveled 準同型暗号といった，準同型乗算を可能にする準同型暗号を差分プライバシに組み合わせた論文数は少ない．

分散型機械学習手法を除くユースケースにおける CDP を使用する手法と，分散型機械学習手法における LDP を使用する手法が盛んに研究されている．一方で，CDP を分散型機械学習手法に対して適用した研究例は見つからなかった．

組み合わせパターンの観点からは，データ収集時における暗号化前に元データにノイズを加算する，組み合わせパターン I が最も盛んに研究されている．ユースケースの観点からは，特定のアプリケーションを想定せずその構造を議論する研究（ユースケース X1）が多い．

5. おわりに

本稿では，クラウドコンピューティングにおけるプライバシ保護手法として，差分プライバシと準同型暗号を組み合わせた手法に関する近年の研究動向を調査した．本稿の貢献は，差分プライバシと準同型暗号を組み合わせたプライバシ保護手法に関する論文について表にまとめると共に，研究が盛んに行われている組み合わせ方のパターンを示した点である．近年の研究動向として，（1）加法準同型暗号を採用する傾向があること，（2）CDP と準同型暗号を組み合わせる手法に関する研究と，分散型機械学習手法に適応させる研究の，2 種類の研究が増加傾向にあることがわかった．一方で，分散型機械学習手法に対して，差分プライバシと準同型暗号を組み合わせた手法を適応させる際に，CDP を採用するケースは確認できなかった．

今後の研究課題を 2 つ挙げる．1 つは，複雑なユースケースに対応するために，完全準同型暗号や Somewhat 準同

型暗号, Leveled 準同型暗号といった準同型乗算を可能にする準同型暗号を差分プライバシに組み合わせることで，準同型加算と準同型乗算の両方に対応可能なシステムを構築することである．もう 1 つは，分散型機械学習手法において，CDP と準同型暗号を組み合わせて使用することで，データの有用性を高めて学習処理を行えるようにすることである．

謝辞　本研究の一部は，2020 年度国立情報学研究所 CRIS 委託研究の助成を受けています．

参考文献

[1] Dwork, C., McSherry, F., Nissin, K. and Smith, A.: Calibrating Noise to Sensitivity in Private Data Analysis, Proc. TCC 2006, pp.265-284 (2006)
[2] 佐久間淳: データ解析におけるプライバシー保護, pp.85-111, 株式会社 講談社 (2016)
[3] Rastogi, V. and Nath, S.: Differentially private aggregation of distributed time-series with transformation and encryption, Proc. SIGMOD 2010, pp. 735–746. (2010)
[4] Dwork, C.: Differential Privacy, Proc. of 33rd ICALP 2006, LNCS, Vol.4052, pp.1-12 (2006)
[5] Gentry, S.: Fully Homomorphic Encryption Using Ideal Lattices, Proc. of the 41st annual STOC 2009, pp.169-178 (2009)
[6] Buckley, C., Pathak, H. P., Das, K. A., Chuah, C. and Mohapatra, P.: AnonAD: Privacy-aware Micro-targeted Mobile Advertisements without Proxies, Proc. of ICCCN 2015, pp.1-8 (2015)
[7] Shi, E., Chan, H. T.-H., Rieffel, E., Chow, R. and Song, D.: Privacy-Preserving Aggregation of Time-Series Data, Proc. of NDSS 2011, Vol.2, pp.3-19 (2011)
[8] Li, S., Li, H. and Sun, L.: Privacy-preserving Crowdsourced Site Survey in WiFi Fingerprint-based Localization, EURASIP J Wirel. Commun. Netw., Vol.2016, Article number 123 (2016)
[9] Paillier, P.: Public-key Cryptosystems Based on Composite Degree Residuosity Classes, EUROCRYPTO 1999, LNCS, Vol.1592. pp.223-238 (1999)
[10] Bindschaedler, V., Rane, S., Brito, A., Rao, V. and Uzun, E.: Achieving Differential Privacy in Secure Multiparty Data Aggregation Protocols on Star Networks, Proc. of 7th CODASPY 2017, pp.115-125 (2017)
[11] Acar, A., Celik, B. Z., Aksu, H., Uluagac, A. S. and McDaniel, P.: Achieving Secure and Differentially Private Computations in Multiparty Settings, Proc. of 1st PAC 2017, pp.49-59 (2017)
[12] Brakerski, Z., Gentry C. and Vaikuntanathan, V.: Fully Homomorphic Encryption without Bootstrapping, ITCS 2012, pp.309-325 (2012)
[13] Brunetta, C., Dimitrakakis, C., Liang, B. and Mitrokotsa, A.: A Differentially Private Encryption Scheme, ISC 2017, LNCS, Vol.10599, pp.309-326 (2017)
[14] Dirk, V. M., Gentry, C., Halevi, S. and Vaikuntanathan, V.: Fully Homomorphic Encryption over the Integers, Eurocrypt 2010, LNCS, Vol.6110, pp.24-43 (2010)
[15] Aono, Y., Hayashi, T., Phong, T. L. and Wang, L.: Input and Output Privacy-Preserving Linear Regression, IEICE Trans. Inf. & Syst., Vol.E100D, pp.2339-2347 (2017)
[16] Lindner, R. and Peikert C.: Better Key Sizes (and Attacks) for LWE-Based Encryption, CT-RSA 2011, LNCS, Vol.6558, pp.319-339 (2011)
[17] Raisaro, L. J., Choi, G., Pradervand, S., Colsenet, R., Jacquemont, N., Rosat, N., Mooser, V. and Hubaux, J.: Protecting Privacy and Security of Genomic Data in i2b2 with Homomorphic Encryption and Differential Privacy, IEEE/ACM Trans. Comput. Biol. Bioinform., Vol.15, No.5, pp.1413-1426 (2018)
[18] Fan, V. and Vercauteren, F.: Somewhat Practical Fully Homomorphic Encryption, IACR Cryptology ePrint Archive, Vol.2012, Article number 144 (2012)
[19] Komawar, S., Batwal, M., Shah, S., Shahani, S. and Abraham, J.: Privacy Preserving Data Aggregation on Secure Cloud, Proc. of ICCUBEA 2018, pp.1-5 (2018)
[20] Li, J., Ye H., Wang, W., Lou, W., Hou, Y. T., Liu, J. and Li, R.: Efficient and Secure Outsourcing of Differentially Private Data Publication, ESORICS 2018, LNCS, Vol.11099, pp.187-206 (2018)
[21] Li, P., Li, Y., Ye, H., Li, J., Chen, X. and Xiang, Y.: Privacy-preserving machine learning with multiple data providers, Future Gener. Comput. Syst., Vol.87, pp.341-350 (2018)
[22] Xiong, J., Ma, R., Chen, L., Tian, Y., Lin, L. and Jin, B.: Achieving Incentive, Security, and Scalable Privacy Protection in Mobile Crowdsensing Services, Wirel. Commun. and Mobile Comput., Vol.2018, Article number 8959635 (2018)
[23] Raisaro, L. J., Troncoso-Pastroriza, R. J., Misbach, M., Sousa, S. J., Pradevanb, S., Missiaglia, E., Michielin, O., Ford, B. and Hubaux, J.: MEDCO: Enabling Secure and Privacy-Preserving Exploration of Distributed Clinical and Genomic Data, IEEE/ACM Trans. Comput. Biol. Bioinform., Vol.16, No.4, pp.1328-1341 (2019)
[24] Hao, M., Li, H., Xu, G., Liu, S. and Yang, H.: Towards Efficient and Privacy-preserving Federated Deep Learning, Proc. of ICC 2019, pp.1-6 (2019)
[25] Jun, Z., Zhenfu, C., Xiaolei, D. and Xiaodong, L.: PPDM: A Privacy-Preserving Protocol for Cloud-Assisted E-Healthcare Systems, JSTSP, Vol. 9, No.7, pp.1332–1344 (2015).
[26] Chowdhury, A. R., Wang, C., He, X., Machanavajjhala, A. and Jha, S.: Cryptɛ: Crypto-Assisted Differential Privacy on Untrusted Servers, Proc. of SIGMOD 2020, pp.603-619 (2020)
[27] Barbosa, M., Catalano, D. and Fiore, D.: Labeled Homomorphic Encryption: Scalable and Privacy-Preserving Processing of Outsourced Data. ESORICS 2017, LNCS, Vol.10492, pp.146-166 (2017)
[28] Froelicher, D., Troncoso-Pastroriza, R. J., Sousa, S. J. and Hubaux J: Drynx: Decentralized, Secure, Verifiable System for Statistical Queries and Machine Learning on Distributed Datasets, IEEE Trans. Inf. Forensics Secur., Vol.15, pp.3035-3050 (2020)
[29] Kim, M., Lee, J., Ohno-Machado, L. and Jiang, X.: Secure and Differentially Private Logistic Regression for Horizontally Distributed Data, IEEE Trans. Inf. Forensics Secur., Vol.15, pp.695-710 (2020)
[30] Cheon, H. J., Kim, A., Kim, M. and Song, Y.: Homomorphic Encryption for Arithmetic of Approximate Numbers, ASIACRYPT 2017, LNCS, Vol.10624. pp.409-437 (2017)
[31] Gong, M., Feng, J. and Xie, Y.: Privacy-enhanced multi-party deep learning, Neural Networks, Vol.121, pp.484-496 (2020)
[32] Xie, Y., Wang, H., Yu, B. and Zhang, C.: Secure collaborative few-shot learning, Knowledge-Based Systems, Vol.203, Article number 106157 (2020)
[33] Froelicher, D., Misbach, M., Troncoso-Pastoriza, R. J. Raisaro, L. J. and Hubaux, J.: MedCo2: Privacy-Preserving Cohort Exploration and Analysis, Stud. Health. Technol. Inform., Vol.270, pp.317-321 (2020)
[34] Asada, M., Moustafa, A. and Ito, T.: FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning, Applied Science, Vol.10, No.8, Article number 2864 (2020)