

プライバシーに配慮したデータ処理技術の研究動向 (EDBT 2014 参加報告)

川本 淳平^{1,a)}

概要: 毎年欧州にて開催されるデータベース分野におけるトップ会議の一つである International Conference on Extending Database Technology (EDBT) への参加報告として、本会議並びに関連ワークショップにて発表された、プライバシーに配慮したデータ処理技術の研究動向を報告する。

1. はじめに

International Conference on Extending Database Technology (EDBT) は、毎年欧州にて開催されるデータベース分野におけるトップ会議の一つである。2009 年より、データベース理論を扱う国際会議 International Conference on Database Theory (ICDT) と併催している。また、プライバシー研究に関する併設ワークショップとして Privacy and Anonymity in the Information Society (PAIS) が開催されている。今年度は、ギリシアのアテネにて開催された。

今年からの取り組みとして、プロシーディングスとプレゼンテーションスライドのオープン化があり、プロシーディングスは <http://openproceedings.org/>、プレゼンテーションスライドは <http://www.edbticdt2014.gr/index.php/detailed-program> より入手できる。

プライバシー分野において特筆すべきは、今年度の Test of Time Award に、2004 年の EDBT にて発表された Agarwal らの [1] が選ばれたことである。本論文は、プライバシー保護データマイニングに関するもので、多次元データに対する匿名化フレームワークを提案している。受賞理由として、10 年経過した現在においても多く引用されていることなどが挙げられていたが、プライバシー保護がデータベース研究において重要な課題の一つと見なされていることも理由であると考えられる。

2. 会議報告

本会議では、プライバシー関連の発表は 2 セッション、

Privacy-Aware Data Processing と Privacy in Networks、
合計 7 件であった。以下にその概要を紹介する。

2.1 Privacy-Aware Data Processing セッション

Li らの [2] では、高次元データに対して差分プライバシー [3] を満足するプライバシー保護データ出版手法を提案している。通常、高次元データに対して差分プライバシーを保証する場合、付加されるノイズが大きくなり、出版データの利便性が低くなってしまふ。Li らの提案手法 DPCopula では、コピュラを用いて差分プライバシーを満足する多次元データの合成を行っている。

To らの [4] は、センサーデータに関するプライバシー保護のため、センサーから得られたデータを一か所にて管理するのではなく、分散管理する仕組みについての研究である。そして、分散環境において、プライバシーを考慮した問合せ処理のためのプロトコルを提案している。個々のデータを秘匿した状態での問合せ実行では、結合や集約演算の実行が課題である。To らは、honest-but-curious 攻撃者のもとで安全な問合せ処理を実現している。

Zhu らの [5] では、時系列データの比較問題を取り扱っている。二つのデータベースがそれぞれ時系列データを持っており、他方のデータベースに時系列データそのものを公開することなく二つの時系列データの距離を計算するプロトコルを提案している。提案手法は、Dynamic Time Warping と Discrete Fréchet Distance を用いた距離計算を準同型暗号を基にしたプロトコルにて実現している。

2.2 Privacy in Networks セッション

Tassa らの [6] では、ソーシャルネットワークなどにおけるロコミ伝搬に関するデータ解析を行う場合におけるプライバシー保護を議論している。ここでは、秘密計算を用い

¹ 九州大学大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering,
Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-
0395, Japan

^{a)} kawamoto@inf.kyushu-u.ac.jp

てソーシャルネットワークにおける影響を計算する方法を提案している。

Jorgensen らの [7] では、ソーシャルネットワークデータを基にしたパーソナライズされた推薦を行う場合におけるプライバシー保護技術を提案している。差分プライバシー [3] を基にした既存手法の多くは、付加するノイズが多く、推薦制度が低いという問題があった。彼らの提案手法は、クラスタリングとソーシャルネットワークにおけるコミュニティの構造データを持ちることで、付加すべきノイズ量を削減している。

Nobari らの [8] は、グラフデータのプライバシー保護出版についての研究である。彼らは、link disclosure 攻撃を防ぐための新しいプライバシー定義である L-opacity を提案している。Zhang らの [9] も同様にグラフデータのプライバシー保護出版についての研究であり、特にソーシャルグラフデータのプライバシー保護出版における新たな攻撃手法についての研究である。通常、ソーシャルグラフデータは非同次のグラフデータである。そのため、その非同次性のうち、いくつかの特徴を用いた攻撃が多く提案されてきた。Zhang らは、非同次性から情報を抽出することで、従来よりも強力な攻撃手法を提案している。

3. おわりに

本稿では、国際会議 EDBT への参加報告としてプライバシー研究に関する発表の紹介を行った。なお、2015 年の EDBT は、ベルギーのブリュッセルにて開催予定である。

参考文献

- [1] Aggarwal, C. C. and Yu, P. S.: A Condensation Approach to Privacy Preserving Data Mining, *Proc. of 9th International Conference on Extending Database Technology*, Springer, pp. 183–199 (2004).
- [2] Li, H., Xiong, L. and Jiang, X.: Differentially Private Synthesization of Multi-Dimensional Data using Copula Functions, *Proc. of the 17th International Conference on Extending Database Technology*, No. c, OpenProceedings.org, pp. 475–486 (2014).
- [3] Dwork, C., Mcsherry, F., Nissim, K. and Smith, A.: Calibrating Noise to Sensitivity in Private Data Analysis, *Proc. of the Third Theory of Cryptography Conference*, Springer, pp. 265–284 (2006).
- [4] To, Q.-c., Nguyen, B. and Pucheral, P.: Privacy-Preserving Query Execution using a Decentralized Architecture and Tamper Resistant Hardware, *Proc. of the 17th International Conference on Extending Database Technology*, OpenProceedings.org, pp. 487–498 (2014).
- [5] Zhu, H., Meng, X. and Kollios, G.: Privacy Preserving Similarity Evaluation of Time Series Data Preserving Privacy in Databases, *Proc. of the 17th International Conference on Extending Database Technology*, OpenProceedings.org, pp. 499–510 (2014).
- [6] Tassa, T. and Bonchi, F.: Privacy Preserving Estimation of Social Influence, *Proc. of the 17th International*

Conference on Extending Database Technology, OpenProceedings.org, pp. 559–570 (2014).

- [7] Jorgensen, Z. and Yu, T.: A Privacy-Preserving Framework for Personalized, Social Recommendations, *Proc. of the 17th International Conference on Extending Database Technology*, No. c, OpenProceedings.org, pp. 571–582 (2014).
- [8] Nobari, S., Karras, P., Pang, H. and Bressan, S.: L-opacity : Linkage-Aware Graph Anonymization, *Proc. of the 17th International Conference on Extending Database Technology*, No. c, OpenProceedings.org, pp. 583–594 (2014).
- [9] Zhang, A., Xie, X., Chang, K. C.-C., Gunter, C. A., Han, J. and Wang, X.: Privacy Risk in Anonymized Heterogeneous Information Networks, *Proc. of the 17th International Conference on Extending Database Technology*, No. c, OpenProceedings.org, pp. 595–606 (2014).