（ 続紙 1 ）

京都大学	博士（情報学）	氏名	劉 上（LIU SHANG）
論文題目	A Study on Crypto-Assisted Differentially Private Graph Analysis (暗号支援による差分プライバシーのグラフ分析に関する研究)		

（論文内容の要旨）

Graph data analysis has become highly popular across various domains, including social networks, transportation systems, and protein forecasting, due to its widespread applicability. Standard graph analytics encompass degree distribution, subgraph counting (e.g., k-star counting, triangle counting), and others. Nevertheless, most graph analytics are performed on sensitive data, posing a risk of data compromise through the analytical results. Thus, developing methods that enable these graph analytics while ensuring individual privacy is of paramount importance.

Differential privacy (DP) has been widely used to provide formal privacy protection. It safeguards individual privacy against adversaries with arbitrary background knowledge and has emerged as the gold standard for private graph analytics. However, DP ensures privacy by adding noise to sensitive information, which can impact overall utility. Conversely, cryptography has long been the foundation for secure communication in the presence of adversarial behavior. It ensures data confidentiality, integrity, and authenticity across various digital platforms and communications. Nevertheless, cryptography does not offer a formal privacy guarantee like DP. In the literature of private graph analysis, DP and cryptography have typically been studied separately. Combining these two approaches holds promise for improving the trade-off between utility and privacy in differentially private graph analytics.

This dissertation presents three works on exploiting crypto-assisted differentially private graph analytics. First, it introduces an approach that demonstrates how cryptography can enable high utility in publishing differentially private degree distribution under node-local differential privacy. Second, it presents CARGO, a crypto-assisted differentially private triangle counting system that achieves high-utility triangle counting of a central model without relying on a trusted server, akin to a local model. Finally, it introduces FEAT, a federated graph analytic framework that achieves an optimal tradeoff between utility and privacy by integrating cryptography into differential privacy. Specifically, this thesis addresses the following three research topics:

Topic 1: Crypto-assisted differentially private degree distribution.
This thesis proposes an algorithm to publish the degree distribution with Node-LDP by exploring how to select the graph projection parameter in the local setting. Specifically, it designs a crypto-assisted local projection method based on cryptographic primitives, achieving higher accuracy than the baseline pureLDP local projection method.

Topic 2: Crypto-assisted differentially private triangle counting.
This thesis proposes a crypto-assisted differentially private triangle

counting system, named CARGO, leveraging cryptographic building blocks to improve the effectiveness of differentially private triangle counting without the assumption of trusted servers. It achieves high utility similar to the central model but without the need for a trusted server, akin to the local model.

Topic 3: Crypto-assisted differentially private federated graph analytics. This thesis proposes a federated graph analytic framework, named FEAT, which enables arbitrary downstream common graph statistics while preserving individual privacy. it designs a differentially private set union (DPSU) algorithm, which ensures that sensitive information is reported only once and the output global graph is protected under differential privacy.

In summary, Chapter 2 to Chapter 4 of this thesis correspond to the three presented research topics. In Chapter 2, it demonstrates how cryptography can enable high utility in publishing differentially private degree distributions under node-local differential privacy. In Chapter 3, it introduces a crypto-assisted differentially private triangle counting system that achieves high-utility triangle counting comparable to a central model without requiring a trusted server, similar to a local model. In Chapter 4, it presents a federated graph analytics framework that balances utility and privacy by integrating cryptography into differential privacy. Finally, Chapter 5 summarizes the thesis and discusses potential future research directions.

（続紙 ２ ）

（論文審査の結果の要旨）

グラフ分析は、さまざまな種類のグラフデータにおいて有意義な洞察を得るための強力なツールでソーシャルネットワーク、交通システム、タンパク質予測など、様々な領域で応用されている。しかし、グラフ統計を直接公開することは、個人に関する機密情報を漏洩する可能性がある。そのため、グラフ内の個人のプライバシーを保護しながらこれらのグラフ特性を分析するソリューションを開発する必要がある。本論文は、暗号技術を利用して差分プライバシーのグラフ分析の有用性を向上させる方法を探ることを目的とし、グラフ分析の精度を向上させるための3つの新しいアルゴリズムを提案している。詳細は以下に示す。

まず、本論文では信頼できるサーバに依存しないノード局所差分プライバシー（Node-LDP）の下でプライバシーを保護された次数分布の問題を研究している。ローカルでプライバシーを保護しながらグラフ投影を実行することで、高い有用性を維持できる次数分布のアルゴリズムを提案している。

次に、本論文は信頼されるサーバを前提としない暗号技術を用いた差分プライバシーによる三角形カウントの統計アルゴリズムを提案している。このアルゴリズムは、暗号技術を用いることで、信頼できるサーバがない状況下でも高い有用性を実現している。ここでは提案された方法の包括的な理論的および実証的分析を提供している。

最後に、本論文は、組織間でのグラフデータの直接的な共有を避けながら分散的グラフ分析を行う「連合グラフ分析」を提案している。既存研究には、差分プライバシーによるグラフ分析がよく研究されているが、組織間でデータが分散したシナリオでは、組織間でのグラフデータが重複する問題があるため、有用性とプライバシーのトレードオフをうまく達成できていない。本論文は、この問題を解決するため、Private Set Unionを用いた連合グラフ分析フレームワーク「FEAT」を提案し、その有効性を示している。

本論文は、以上のように、暗号技術と差分プライバシーを組み合わせることで、グラフデータ分析の有用性とプライバシーのトレードオフを改善する手法を示している。これらの研究成果は、学術的および実用的に大きな貢献を果たしている。よって、本論文は博士（情報学）の学位論文として価値あるものと認める。また、令和6年7月18日、論文内容とそれに関連した事項について試問を行った結果、合格と認めた。さらに、本論文のインターネットでの全文公表についても支障がないことを確認した。