

明治大学外国人研究者招聘制度 報告書

<招聘教授・研究員の情報 / Guest Professor・Guest Scholar>

氏 名	Chih-Hsun Lin
Name	
所属機関(派遣元)	National Yang Ming Chiao Tung University
Affiliation (Home Organization)	
現在の職名	Ph.D. Student
Position	
研究期間(日本への入国日から出国日)	2024/9/1～2025/8/31
Period of Stay (from the date of entry to departure)	
専攻	Department of Computer Science
Field of Research	
ホスト教員氏名と所属学部研究科等	菊池浩明, 総合数理学部先端メディアサイエンス学科
Name of host teacher and affiliation at Meiji University	

<外国人研究者からの報告 / Foreign Researcher Report>

①研究課題 / Research Theme
Differential Private Machine Learning Algorithms
②研究概要 / Outline of Research
本研究では、台湾・国立陽明交通大学の博士課程学生、Chih-Hsun Lin氏を招聘し、「差分プライバシー機械学習アルゴリズム」をテーマとして、1年間にわたり共同研究を行った。Lin氏は、差分プライバシー、深層学習、プライバシー保護型AIに関する深い知識を有しており、当研究室で進めているビッグデータの安全な二次利用を目指す差分プライバシーの研究との融合により、新たなセキュリティモデルの構築に取り組んだ。 研究活動は週1回の定例ミーティングを中心に進められ、大学院ゼミにも継続的に参加いただいた。特に、局所差分プライバシーに対するポイズニングの研究においては、大学院生の研究成果に対し、理論面・技術面において多くの有益なコメントを提供いただき、研究の質の向上に大きく貢献された。本研究は、その後、情報セキュリティに関する国際会議 ESORICS 2025にて採択され、大きな研究性と繋がった。 また、滞在期間中に、先端数理科学研究科とスウェーデンの大学院生支援プログラムWallenberg AI, Autonomous Systems and Software Program (WASP) (Knut and Alice Wallenberg基金による研究支援プログラム) との共同ワークショップが2024年10月7日に中野キャンパスで開催され、Lin氏は “Differentially Private Synthesis for Time-Series Data” と題したポスター発表を行った。本研究は、Lin氏が予めから進めている差分プライバシーを満たした合成データ生成アルゴリズムに関するものであり、スウェーデンの博士課程学生との間で有益な議論が交わされた。 本共同研究は、データプライバシーと機械学習を融合した先進的なセキュリティ・プライバシー保護手法の設計と実証に大きく寄与し、今後の国際共同研究の基盤形成において重要な成果となった。
③招聘期間中の研究活動の実績 / The research results as Guest Professor・Guest Scholar
本共同研究の成果を、“Data Poisoning Attacks to Locally Differentially Private Range Query Protocols” としてまとめ、情報セキュリティに関する国際会議に投稿し、査読中である。

HP掲載等のために、研究活動写真を2枚、ご提供下さい。
Please submit some photos of your research activities for the university website.

