

2024 年度年次報告書

数学・数理科学と情報科学の連携・融合による情報活用基盤の創出と社会課題解決に向けた展開

2020 年度採択研究代表者

末永 幸平

京都大学 大学院情報学研究科  
准教授

AI 集約的サイバーフィジカルシステムの形式的解析設計手法

主たる共同研究者:

岸田 昌子 (情報・システム研究機構 国立情報学研究所 准教授)

## 研究成果の概要

理論基盤構築では、時間制約と未知パラメータを含むハイパー論理「Hyper parametric timed CTL」を提案し、複数実行パス間の関係性を形式的に表現可能にした。この成果はトップ国際会議 EMSOFT 2024 で発表され、自動運転システムなど安全クリティカルなシステムの検証に貢献している。監視技術では、完全準同型暗号を用いた秘匿モニタリング手法を RV 2024 で発表。プライバシーを保護しながら数値的安全性測定の監視を可能にし、企業との共同研究として産業応用も進めている。基盤技術として、既存技術より 72~179 倍高速な暗号コンパイラ「HEIR」をセキュリティ国際会議 NDSS 2024 で発表した。制御手法では、機械学習を活用したイベントトリガ型モデル予測制御を IEEE Transactions on Cybernetics に、交通信号最適化のための「信号時空間論理」アプローチを IEEE Transactions on Intelligent Transportation Systems に掲載した。また、自動運転の「安全性と目標達成の両立」を実現する「ゴール認識型 RSS」を国際会議 IV 2024 で発表した。さらに、未整備環境での自律走行のためのカメラ画像を用いたオンライン経路制御や、歩行者空間での安全走行のための注意機構を組み込んだ制御手法を研究し、実験による有効性検証も行った。

### 【代表的な原著論文情報】

- 1) Masaki Waga, Étienne André: Hyper Parametric Timed CTL. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.
- 2) Masaki Waga, Kotaro Matsuoka, Takashi Suwa, Naoki Matsumoto, Ryotaro Banno, Song Bian, Kohei Suenaga: Oblivious Monitoring for Discrete-Time STL via Fully Homomorphic Encryption. Proceedings of the 24th International Conference on Runtime Verification (RV 2024), 59-69.
- 3) Song Bian, Zian Zhao, Zhou Zhang, Ran Mao, Kohei Suenaga, Yier Jin, Zhenyu Guan, Jianwei Liu: HEIR: A Unified Representation for Cross-Scheme Compilation of Fully Homomorphic Computation. Proc. of the 31st Annual Network and Distributed System Security Symposium (NDSS).
- 4) Kazumune Hashimoto, Yuga Onoue, Akifumi Wachi, Xun Shen: Learning-based Event-triggered MPC with Gaussian processes under terminal constraints, IEEE Transactions on Cybernetics (accepted, 2025) DOI: 10.1109/TCYB.2025.3536606
- 5) Sagar V Patil, Kazumune Hashimoto, Masako Kishida, “A Robust Traffic Flow Control Using Connected Vehicle Technology: Signal Spatio-Temporal Logic-Based Approach”, IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 12, pp. 19658-19674, 2024