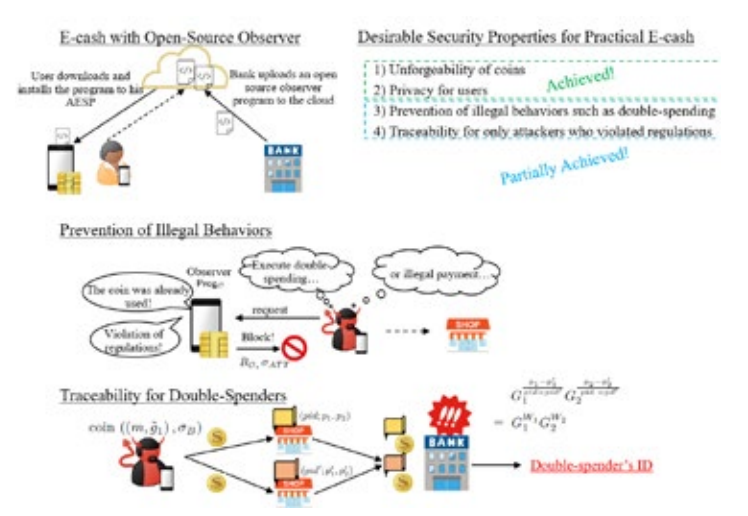


*Fully Homomorphic Encryption, Zero-Knowledge Proofs,
Deep Learning, Attention, Adversarial Examples,
Cyber Reasoning Systems, RoP/DoP, Cyberrange, ...*

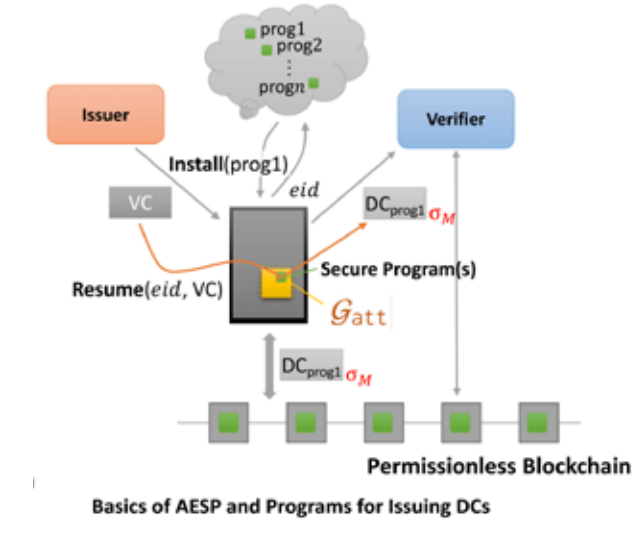
OTSUKA LABORATORY

大塚研究室

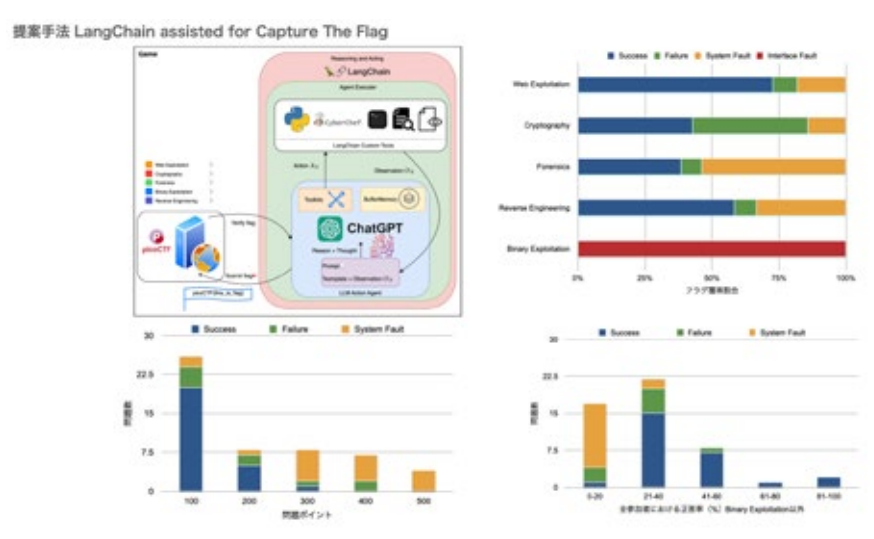
Blockchain X AI Security



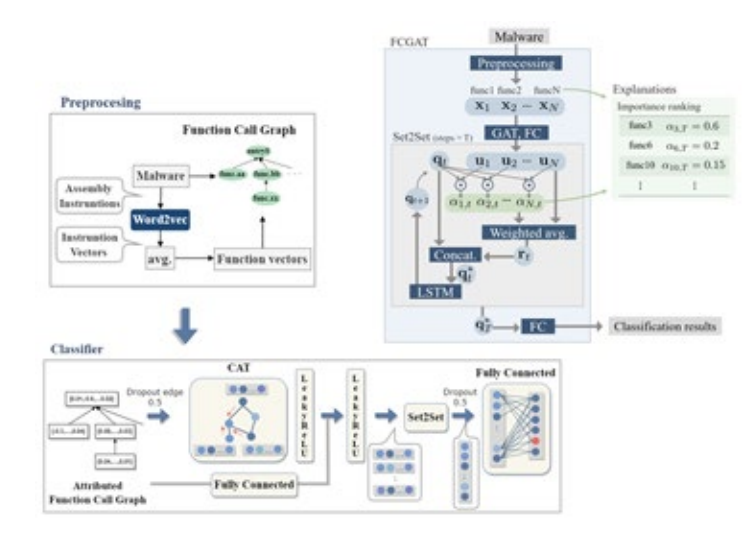
Taiishi Higuchi, Akira Otsuka, "Open-Cash: Electronic Cash with Open-Source Observers," Financial Cryptography and Data Security, FC 2023 International Workshops.



Koichi Moriyama, Akira Otsuka, Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors (IEEE Blockchain-2022).



佐竹達也, 大塚玲, "大規模言語モデルを用いた自律サイバー推論システムに関する研究" 人工知能学会全国大会論文集, 2023.



Mlnami Someya, Yuhei Otsubo, Akira Otsuka, "FCGAT: Interpretable Malware Classification Method using Function Call Graph and Attention Mechanism," Proceedings of NDSS Workshop on Binary Analysis Research (BAR2023).

研究例

- VeloCash: Anonymous decentralized probabilistic micropayments with transferability
- Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors
- 耐タンパー仮定に基づくオフライン・スマートコントラクトの研究
- AI-based Stable Coinの研究
- オーバーレイネットワーク情報を活用した暗号通貨追跡手法の研究
- Attack graphを用いたサイバーレンジシナリオの自動生成
- 自律サイバー推論システムにおけるBERTモデル導入による状態推定の強化
- 部分観測マルコフ決定過程によるニューラルエージェント強化学習を使用した自律型SQLインジェクション攻撃手法
- Theoretical Security against adversarial examples on Gaussian Processes
- 関数呼び出しグラフと関数埋め込みに基づくマルウェア分類手法

教授紹介 大塚 玲

1991年大阪大学工学研究科博士前期課程修了。
同年より野村総合研究所。2002年東京大学大学院工学系研究科電子情報工学専攻博士課程修了。博士(工学)。2005年4月より2017年3月まで産業技術総合研究所。2017年4月より情報セキュリティ大学院大学教授。
2006-2010産業技術総合研究所情報セキュリティ研究センター・セキュリティ基盤技術研究チーム長。2007-2014中央大学研究開発機構教授。
東京理科大学大学院工学研究科非常勤講師(2009-2011), 城西大学理学部数学科非常勤講師(2015-2022), 北陸先端科学技術大学院大学情報科学研究科非常勤講師(2016)。大阪大学大学院工学研究科非常勤講師(2022)。日本銀行金融研究所客員研究員(2020-2021)。
電子情報通信学会, 情報処理学会, IEEE, IACR, IFCA各会員。電子情報通信学会バイオメトリクス研究専門委員会顧問, 電子情報通信学会ISEC研究専門委員会委員。
情報処理学会論文誌編集委員。SCIS 2022プログラム委員長。人工知能学会 安全性とセキュリティ研究会(SIG-SEC)主幹事。
JNSAサイバーセキュリティ産学連携協議会代表。



Contact: otsuka@iisec.ac.jp