

第二回 留学報告書

2025 年 6 月

高橋秀明

2024 年夏より Columbia University, Department of Computer Science, Ph.D.課程に進学しました、高橋秀明です。第二回目となる本報告書では、博士課程に進学してから二つ目のセメスターのなんやかんやを報告させていただきます。

1. 授業

今学期は、暗号の入門的な授業である「Introduction to Cryptography」とブロックチェーンの理論面を学ぶ「The Science of Blockchains」を受講しました。Introduction to Cryptography は、意外と整数論や楕円関数に関する話題の比率はそこまで高くなく、様々な Security Game (CCA, CPA, 疑似乱数、一方向関数、耐衝突ハッシュ関数など)がどのように帰着・関係しているかを学ぶことに重きが置かれているように感じました。評価は宿題と試験に加え、計算機を用いない暗号アルゴリズムを設計するというチームプロジェクトによって行われており、そこまで難しくはなかったです。The Science of Blockchains は、ブロックチェーンに関する様々なアルゴリズムやプロトコルの理論を学ぶ授業でした。授業を担当していた教授がコンセンサスプロトコルの専門家ということもあり、授業のかなりの部分が Tendermint や Longest Chain Consensus などの解説および証明に費やされていました。チームプロジェクトでは Data Availability Sampling という、「ブロックに含まれているトランザクションデータがネットワーク上にきちんと公開されており利用可能である」ことを効率的に検証する手法についてのサーベイを行いました。実際に Data Availability に取り組んでいるいくつかの会社のエンジニアや研究者の方々にインタビューしたり、自分たちでアルゴリズムを一から実装して実験してみたりと、多くの新しい知見を得ることができました。

2. 研究

研究では、前回の報告書でも述べた「ゼロ知識証明の回路の実装に脆弱性がないかをテスト

する」というプロジェクトに取り組んでいます。ゼロ知識証明とは、入力 x に対して出力 y を返すようなプログラム P があるとき、「私は P の出力が y となるような入力 x を知っている」ということを、入力 x を公開することなく、高速に検証・証明する技術です。効率的な証明を実現するためには、証明者がプログラム P を適切な多項式制約として定義する必要があります。この時、制約が不十分だったりもしくは過剰であった場合、適切な証明を生成できなくなったり、悪意のある証明者が不正な証明を生成できてしまう可能性が発生します。既存研究の多くはパターンマッチングや形式検証を用いていますが、脆弱性がないにもかかわらず脆弱性があると誤検知してしまったり、バグのパターンの一部しかサポートしておらず多くの脆弱性を見逃すこともあり、さらに大きな回路に対しては極めて低速であるなど様々な問題を抱えています。これらの問題を解決するために、我々は Program Mutation と Fuzzing とよばれる動的な手法でバグの検知を試みています。具体的には、入力 x から出力 y を導く計算プログラム P とそれに対応する回路制約 C に着目し、まずは P をランダムな入力 x の下で実行して出力 y を得ます。もしこの (x, y) が制約 C を満たさないのであれば、これは正当な入出力が制約 C を満たさないことを意味するので、 C が過剰であると判断できます。さらに、我々のツールはプログラム P をわずかに改変した変異プログラム P' を作り、同じ入力 x の下で P' を実行してその出力 y' を得ます。もし y と y' が異なり、かつ (x, y) および (x, y') の両者が制約 C を満たすのであれば、これは制約 C が出力を一意に定めることができないことを意味するので、 C が不十分であると言えます。現在の実装は、Circom というゼロ知識証明の回路を実装するツールとして最も人気のある言語をサポートしており、現在までに 50 個以上の脆弱性を様々なプロジェクトで検知することができました。論文化も進めており、すでに arXiv に投稿済みです。年内にどこかの国際会議で採択されることを目指しています。

論文: Takahashi, Hideaki, et al. "zkFuzz: Foundation and Framework for Effective Fuzzing of Zero-Knowledge Circuits." arXiv preprint arXiv:2504.11961 (2025).

実装: <https://github.com/Koukyosyumei/zkFuzz>

3. 最後に

改めまして、留学を支援していただいている船井情報科学振興財団の皆様に感謝申し上げます。ご期待に応えることができるよう、より一層努力を重ねたいと思います。