耐量子安全なゼロ知識サムチェックプロトコルの構成に関する研究

A Study on Construction of Quantum-Secure Zero-Knowledge Sumcheck Protocols

氏名: 水上昌大, システム分科会, 情報セキュリティ大学院大学

zk-SNARKs enable succinct and privacy-preserving verification of computations, but most practical constructions rely on discrete-logarithm assumptions and are vulnerable to quantum attacks. This work studies a post-quantum approach based on lattice problems and proposes a lattice-based polynomial commitment with a trapdoor. Using this commitment, we construct a zero-knowledge sumcheck protocol that achieves evaluation hiding under the MSIS assumption. The proposed protocol preserves succinctness and quantum resistance, and can be used as a building block for post-quantum zk-SNARK constructions.

はじめに

zk-SNARK(zero-knowledge Succinct Non-Interactive Argument Knowledge):簡潔なゼロ知識証明

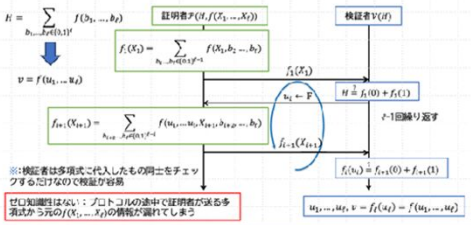
研究背景:
- 近年,暗号資産の取引やプライバシーの保護の観点からzk-SNARKが注目されている.
- 近年のzk-SNARKは検証者の計算負担を軽減するためにサムチェックプロトコルが用いられている.
- zk-SNARKを構成するためにサムチェックプロトコルのゼロ知識化が重要である.

研究目的:
- 離散対数ベースの,サムチェックプロトコルを用いたzk-SNARKは多く提案されているが,離散対数ベースでは,量子計算機に解かれてしまう.

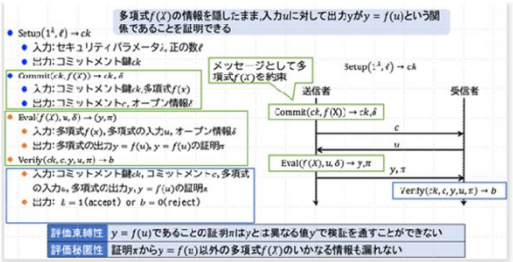
研究の貢献:
- zk-SNARKに耐量子性を持たせるために格子ベースの多項式コミットメントを用いたゼロ知識サムチェックプロトコルを提案する.
- 提案プロトコルをzk-SNARKの部品とすることで,耐量子性を付与することを可能にする.

サムチェックプロトコル

$\mathbb{F}$ を有限体とする.



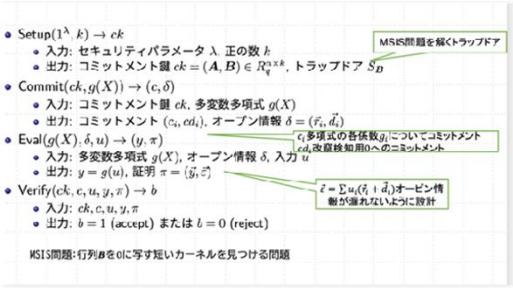
多項式コミットメントスキーム



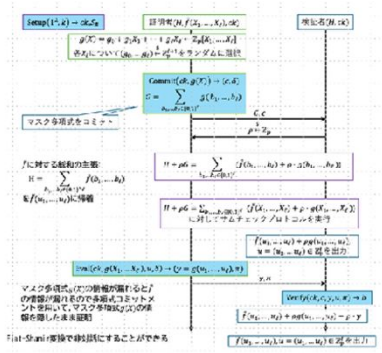
関連研究:Xie らの研究

- タイトル:Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation
- 著　者:Tiancheng Xie,Jiaheng Zhang,Yupeng Zhang,Charalampos Papamanthou,Dawn Song
- 学会:Crypto 2019
- 概要:
  離散対数ベースの多項式コミットメントを用いてサムチェックプロトコルのゼロ知識化
- 課題: 離散対数だと量子計算機に解かれてしまう.

格子ベースの多項式コミットメント



ゼロ知識サムチェックプロトコル



- 健全性: サムチェックプロトコルの健全性と評価束縛性から導かれる.
- ゼロ知識性: 多項式コミットメントの評価秘匿性を用いれば, 構成可能

評価

命題の多項式のサイズ $O(2^\ell)$ に対して通信量, 検証時間ともに $poly(\lambda + \log 2^\ell)$