

# 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。

- 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

- Setup( $1^\lambda, k$ )  $\rightarrow ck$ 
  - 入力: セキュリティパラメータ  $\lambda$ , 正の数  $k$
  - 出力: コミットメント鍵  $ck = (A, B) \in \mathbb{R}_q^{k \times k}$ , トラップドア  $S_B$
- Commit( $ck, g(X)$ )  $\rightarrow (c, \delta)$ 
  - 入力: コミットメント鍵  $ck$ , 多変数多項式  $g(X)$
  - 出力: コミットメント  $c = (r_1, \dots, r_k)$ , オープン情報  $\delta = (r_1, \dots, r_k)$
- Eval( $g(X), \delta, u$ )  $\rightarrow (y, \pi)$ 
  - 入力: 多変数多項式  $g(X)$ , オープン情報  $\delta$ , 入力  $u$
  - 出力:  $y = g(u)$ , 証明  $\pi = (\tilde{y}, \tilde{\pi})$
- Verify( $ck, c, u, y, \pi$ )  $\rightarrow b$ 
  - 入力:  $ck, c, u, y, \pi$
  - 出力:  $b = 1$  (accept) または  $0$  (reject)

MSIS問題:行列  $B$  に与えられたベクトル  $v$  を見つける問題

### サムチェックプロトコル

$\mathbb{F}$  を有限体とする。

証明者  $P(f, (f_1, \dots, f_k))$  と検証者  $V(f)$  のやり取り:

- 証明者は  $f(x) = \sum_{i=1}^k f_i(x_i)$  をコミットする。
- 検証者は  $u = (u_1, \dots, u_k)$  を入力し、 $H = f(u) + f_1(u_1)$  を計算する。
- 証明者は  $f_1(x_1)$  をコミットする。
- 検証者は  $u_1 = r_1$  を入力し、 $H = f_1(r_1) + f_2(u_2)$  を計算する。
- このプロセスを  $k$  回繰り返す。
- 最終的に  $H = f_k(u_k)$  が得られる。

※: 検証者は多項式を代入したもののサムチェックするのではなく、検証者が多項式  $f_1(x_1)$  の情報を漏れさせない。

### ゼロ知識サムチェックプロトコル

Setup( $1^\lambda, k$ )  $\rightarrow ck$  (MSIS問題)

Commit( $ck, f(X)$ )  $\rightarrow (c, \delta)$

Eval( $g(X), \delta, u$ )  $\rightarrow (y, \pi)$

Verify( $ck, c, u, y, \pi$ )  $\rightarrow b$

MSIS問題:行列  $B$  に与えられたベクトル  $v$  を見つける問題

### 多項式コミットメントスキーム

- Setup( $1^\lambda, k$ )  $\rightarrow ck$ 
  - 入力: セキュリティパラメータ  $\lambda$ , 正の数  $k$
  - 出力: コミットメント鍵  $ck$
- Commit( $ck, f(X)$ )  $\rightarrow (c, \delta)$ 
  - 入力: コミットメント鍵  $ck$ , 多項式  $f(x)$
  - 出力: コミットメント  $c$ , オープン情報  $\delta$
- Eval( $g(X), \delta, u$ )  $\rightarrow (y, \pi)$ 
  - 入力: 多項式  $g(x)$ , 多項式の入力, オープン情報
  - 出力: 多項式の出力  $y = f(u)$ ,  $y = f(u)$  の証明  $\pi$
- Verify( $ck, c, u, y, \pi$ )  $\rightarrow b$ 
  - 入力: コミットメント鍵  $ck$ , コミットメント  $c$ , 多項式の入力, 多項式の出力  $y = f(u)$  の証明  $\pi$
  - 出力:  $b = 1$  (accept) or  $b = 0$  (reject)

評価独立性:  $y = f(u)$  であることの証明  $\pi$  は  $y$  と異なる値  $y'$  で検証を通すことができない

評価秘密性: 証明  $\pi$  が  $y = f(u)$  以外の多項式  $f'(x)$  のいかなる情報も漏れない

- 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密性を用いれば、構成可能

### 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

### 評価

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