格子問題に基づく zk-SNARK の検討
Study on Lattice-based zkSNARK

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 are essential for privacy-preserving applications but often rely on discrete logarithm assumptions, which are vulnerable to quantum attacks. Lattice-based zk-SNARKs offer quantum resistance but suffer from large proof sizes. This study explores lattice-based commitments and inner-product arguments to improve efficiency. We aim to reduce proof sizes while maintaining security, enabling practical applications such as electronic auctions.

研究背景

従来の暗号技術は古典安全性に基づいていおり, 量子安全性がない.

古典安全性: 離散対数問題, 素因数分解
量子安全性: 格子問題, 同種写像問題, 符号問題
検討: 格子問題に基づいた zk-SNARK

格子問題

格子とは,n 個の線形独立なベクトルの整数係数の線形結合の集合.

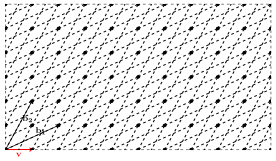

図 1: 格子の例

格子問題: 最短ベクトル問題, 最近ベクトル問題

格子問題の欠点としては, パラメータサイズが大きくなってしまう事である.

格子問題に基づいた zk-SNARK の紹介

- ゼロ知識証明とは, 命題が真である証拠を明かさずにその情報が真であることを相手に納得させる暗号技術.
- zk-SNARK とは, 多項式コミットメントを用いた証明長の短いゼロ知識証明であり, 計算の正当性をゼロ知識で検証できる.
- コミットメントとは, 秘匿性と束縛性を満たす値である.
  秘匿性: コミットした値のいかなる情報も漏れない
  束縛性: コミットした値とは, 異なる値で開示できない
  多項式コミットメントに用いられるコミットメントの例
  離散対数ベースのコミットメント: Pedersen コミットメント
  $\mathbb{G}$: 素数位数 p の群,x: メッセージ,r: ランダムス,G, $H \xleftarrow{\$} \mathbb{G}$

$$Com(x; r) = xG + rH$$

  格子ベースのコミットメント: Ajtai コミットメント
  $R := \mathbb{Z}/\langle X^d + 1\rangle$,$\boldsymbol{A}_1 \xleftarrow{\$} R_q^{\mu\times(\mu+\nu)}$,$\boldsymbol{A}_2 \xleftarrow{\$} R_q^{\mu\times\ell}$,$\boldsymbol{x}$: メッセージ,$\boldsymbol{r}$: ランダムス

$$Com(x; r) = \boldsymbol{A}_1\boldsymbol{r} + \boldsymbol{A}_2\boldsymbol{x}$$

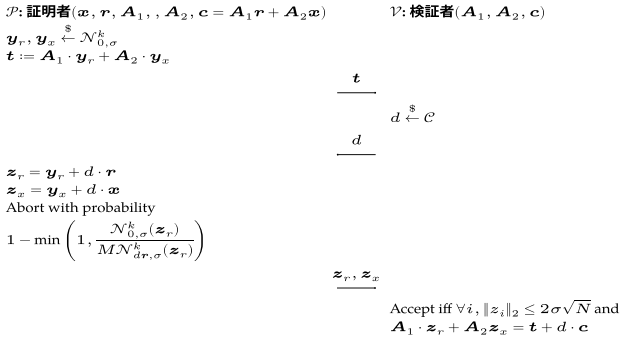

図 2: Ajtai コミットメントを用いた zk-SNARK の例

- 離散対数ベースの zk-SNARK として効率的なものがある
- 格子ベースの zk-SNARK としてはパラメータサイズが大きいので効率的なものがまだない.

今後の展望

格子ベースの zk-SNARK のパラメータサイズを削減し効率化を図る. かつ, 内積証明を活用したゼロ知識範囲証明を導入し, 電子オークションなどの実用的な応用を目指す.

参考文献

[BS22] Ward Beullens and Gregor Seiler. LaBRADOR: Compact proofs for R1CS from module-SIS. Cryptology ePrint Archive, Paper 2022/1341, 2022.
[HSS24] Intak Hwang, Jinyeong Seo, and Yongsoo Song. Concretely efficient lattice-based polynomial commitment from standard assumptions. In *Advances in Cryptology – CRYPTO 2024: 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18 – 22, 2024, Proceedings, Part X*, pages 414–448, Berlin, Heidelberg, 2024. Springer-Verlag.