# 格子問題に基づいた zk-SNARK

# Study on Lattice-based zkSNARK

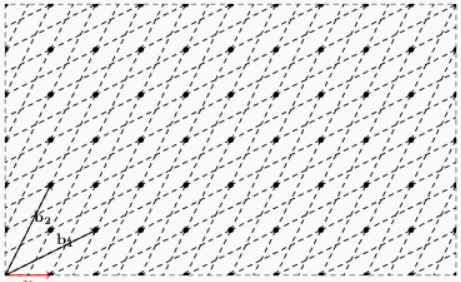
水上昌大・システム分科会・情報セキュリティ大学院大学

## 研究背景

現在,zk-SNARK について離散対数ベースのものは効率的なものがあるが, 耐量子の安全性に基づいた zk-SNARK については効率的なものがない. なので, 効率的な zk-SNARK の検討を行う.

## 格子問題

格子という線型独立なベクトルの線型結合で表せる網目上の模様の中で, 織りなされる数学的困難な問題で, 量子耐性があると仮定されている.




## 格子問題に基づく zk-SNARK の先行研究

格子問題に基づく zk-SNARK のほとんどが以下で示される Ajtai コミットメントに基づいている.

$R := \mathbb{Z}/\langle X^d + 1\rangle, \boldsymbol{A}_1 \xleftarrow{\$} R_q^{\mu\times(\mu+\nu)}, \boldsymbol{A}_2 \xleftarrow{\$} R_q^{\mu\times\ell}$, $\boldsymbol{x}$: メッセージ, $\boldsymbol{r}$: ランダムス

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

**今後の方針**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.