**SCIS 2022** 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

# メッセージ長を拡張する耐量子コミットメント方式
# Message-restriction-free commitment scheme based on lattice assumption

宮地　秀至 *　　王　イントウ †　　宮地　充子 *†
Hideaki Miyaji　　Yuntao Wang　　Atsuko Miyaji

**キーワード** コミットメント方式，ハッシュ関数，LWE，ナップザック問題

## あらまし

コミットメント方式はゼロ知識証明などの基本的な暗号作業に不可欠な要素である．近年，格子暗号は耐量子暗号として実用化に向けた研究が行われている．その一つに格子暗号を用いたコミットメント方式の研究が行われている．コミットメント方式では，短いメッセージだけでなく任意のメッセージを出力する必要がある．大きなメッセージを送信するためには，メッセージ文字列のサイズを大きくすることがコミットメント方式の重要な課題の一つである．メッセージ文字列のサイズを大きくするためにBaumらは，2018年に大きなメッセージサイズの送信を可能にするコミットメント方式を構築した．しかし，入力の部分にメッセージだけでなくメッセージ以外の目的で利用される空間が適用されており，メッセージに適用可能な空間はより大きくできる余地がある．本提案では，Baumらが提案したコミットメント方式のメッセージ空間をより大きくするコミットメント方式を提案し，その安全性である束縛性と秘匿性を証明する．さらに，本提案の安全なパラメータをそれぞれ提案する．

## 1　研究背景

メッセージ長を拡大したコミットメント方式の作成は近年盛んに行われている．2015年には， Benhamoudaらがメッセージ空間に制限のないコミットメント方式を作成し [1]．2018年にbaumらが [1] のコミットメント方式をベースにしたコミットメント方式を作成した [2]．[2] のコミットメント方式では，コミットメント方式の安全性である束縛性と秘匿性に関して，統計的秘匿性と計算量的束縛性が成立することを示し，さらに統計的束縛性と計算量的秘匿性も満たすことができることを示した．

しかし [2] のコミットメント方式では，入力部分に0が追加されており，挿入できるメッセージ空間の割合としては，[1] のコミットメント方式よりも小さくなる．

## 2　本提案のコミットメント方式

Baumらよって提案されたLWEベースのコミットメント方式は多項式環 $A_1 \in R_q^{n\times k}$，$A_2 \in R_q^{l\times k}$，メッセージ値 $x \in R_q^l$，乱数多項式ベクトル $r \in S_\beta^k$（$S_\beta : \ell_\infty$ ノルムが $\beta$ である多項式環 $R$）を用いて以下のように構成される．

$$Com(x;r) \quad = \quad \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot r + \begin{bmatrix} 0^n \\ x \end{bmatrix}$$

本提案のコミットメント方式は，コミットメント方式の入力を $\begin{bmatrix} x^{n+l} \end{bmatrix}$ と拡大したコミットメント方式を提案する．

また，提案方式の計算量的束縛性が Approximation-SVP 問題に，計算量的秘匿性が DKS 問題に帰着することを示す．さらに本提案のコミットメント方式の統計的秘匿性と計算量的束縛性を満たすことも示す．

## 参考文献

[1] F. Benhamouda, S. Krenn, V. Lyubashevsky, and K. Pietrzak, “Efficient zero-knowledge proofs for commitments from learning with errors over rings,” 2015.

[2] C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner, and C. Peikert, “More efficient commitments from structured lattice assumptions,” 2018.

* 大阪大学大学院， 大阪府吹田市山田丘 1-1, 〒 565-0871
† 北陸先端科学技術大学院大学，石川県能美市旭台１丁目１, 〒 923-1211