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

範囲証明つき準同型暗号とその対話的プロトコル
Homomorphic Encryption with range proof and its interactive protocol

光成滋生 *
Mitsunari Shigeo

キーワード 準同型暗号, 範囲証明, ブラインド範囲証明, 暗号文変換対話プロトコル

あらまし

準同型暗号は復号することなく暗号文を使った計算が可能な暗号方式であり，電子投票や機械学習の推論などへの応用が研究されている．準同型暗号を用いて複数のクライアントが生成した暗号文を集計する場合，それぞれの暗号文の入力値の範囲に制約を与えたい場合がある．その場合，入力値の平文がある範囲にあることを保証するゼロ知識証明 ZKRP(Zero Knowledge Range Proofs) を利用することが多い．

集計を階層的に行いたい場合，複数の暗号文は準同型暗号により 1 個の暗号文に変換されるが，従来のゼロ知識証明の方式は証明を集約できない．そのため集約後の暗号文が，ある範囲に入っていることを確認するには集約前の個別の ZKRP を確認しなければならない．本論文では，範囲証明付き暗号文を集約した暗号文に対して新しい ZKRP を付与する方法を考察する．

まず，与えられた暗号文に対して対応する平文を知ること無く範囲証明をつける対話的ブラインド ZKRP を提案する．そして SCIS2020 で提案した対話的暗号文変換プロトコルと組み合わせて集約後の暗号文から ZKRP つきの暗号文を生成する対話プロトコルを提案する．

* サイボウズ・ラボ株式会社, 東京都中央区日本橋 2-7-1 東京日本橋タワー 27F, Cybozu Labs, Inc., Tokyo Nihombashi Tower 27F, 2-7-1 Nihombashi, Chuo-ku, Tokyo 103-6028, herumi@nifty.com