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

準同型暗号に基づく秘密計算の能動的攻撃者に対する秘匿性について
On Privacy against Malicious Adversaries for Secure Computation Based on Homomorphic Encryption

縫田 光司 *†
Koji Nuida

キーワード 秘密計算、準同型暗号、能動的攻撃者、不正な暗号文

あらまし

準同型暗号に基づき、クライアントが鍵生成を行いサーバは暗号化されたデータのみを取り扱う種類の秘密計算プロトコルにおいて、Akavia と Vald [1] は暗号化方式が IND-CPA 安全であっても malicious なサーバに対する情報の秘匿性が成り立たない具体例を示し、秘匿性を保証するための充分条件を提示した。本論文では、Akavia らの議論では malicious なサーバがクライアントに送るクエリ中に不正な暗号文が含まれる可能性が考慮されていないことを指摘し、Akavia らの充分条件では秘匿性が必ずしも保証されない具体例を示すとともに、不正な暗号文の取り扱いも考慮した秘匿性のための充分条件を提示する。

参考文献

[1] A. Akavia, M. Vald, “On the Privacy of Protocols based on CPA-Secure Homomorphic Encryption”, IACR Cryptology ePrint Archive, Report 2021/803, 2021, Version 20210616:092806 (accessed on November 22, 2021)

* 九州大学マス・フォア・インダストリ研究所, 福岡県福岡市 Institute of Mathematics for Industry (IMI), Kyushu University, Fukuoka, Japan nuida@imi.kyushu-u.ac.jp
† 産業技術総合研究所, National Institute of Advanced Industrial Science and Technology (AIST)