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

HQC暗号を応用した秘匿内積計算プロトコル（III）
A Secure Computation Protocal of Inner Product Using HQC Cryptosystem (III)

中山 太雅 * 廣友 雅徳 † 福田 洋治 ‡ 毛利 公美 §
Taiga Nakayama Masanori Hirotomo Youji Fukuta Masami Mohri
白石 善明 ¶
Yoshiaki Shiraishi

キーワード 秘匿計算，内積，HQC 暗号，耐量子性

あらまし

ビックデータ解析，データマイニングでは扱うデータに個人情報などの秘密情報が含まれるため，プライバシーを保護したまま計算できる秘匿計算が注目されている．それらの秘匿計算プロトコルは，素因数分解や離散対数問題などの数論ベースの問題の困難性を利用した公開鍵暗号を応用して設計されている．しかし，これらの問題は量子計算機によって容易に解けることが知られており，実用的な量子計算機が実現した場合，秘匿計算プロトコルの安全性は保てなくなる．このような問題に対し，耐量子を有する暗号として符号ベース暗号方式がいくつか提案されている．Gaborit らは準巡回シンドローム復号問題に基づいた公開鍵暗号方式 HQC[1][2] を NIST のポスト量子暗号標準化コンペティションへ提案している．筆者らは，HQC 暗号を応用し，耐量子性を有する秘匿内積計算プロトコル [3][4] を提案している．このプロトコルは，HQC 暗号を二者間の秘匿内積計算に応用し，準巡回シンドローム復号問題に基づくことで耐量子性を有している．また，このプロトコルでは，長さ 2 または 3 のベクトルの内積計算が可能であった．

本稿では，計算可能なベクトルの長さを拡大した秘匿内積計算プロトコルを提案する．この提案プロトコルでは，シンプレックス符号の構成をアルゴリズムに用いることで計算を行うベクトル長の拡大を可能にしている．さらに，提案プロトコルの安全性の評価を行い，セキュリティレベルとパラメータの関係を示し，既存の攻撃手法に対する安全性を考察する．

参考文献

[1] HQC, https://pqc-hqc.org/.

[2] C. Aguilar-Melchor, O. Blazy, J.-C. Deneuville, P. Gaborit, and Gilles Zémor, “Efficient encryption from random quasi-cyclic codes,” IEEE Trans. Inf. Theory, vol.64, no.5, pp.3927–4943, May 2018.

[3] 中山太雅，廣友雅徳，福田洋治，毛利公美，白石善明，“HQC 暗号を応用した秘匿内積計算プロトコル，” 信学技報，Sept. 2020.

[4] 中山太雅，廣友雅徳，福田洋治，毛利公美，白石善明，“HQC 暗号を応用した秘匿内積計算プロトコル (II)，” コンピュータセキュリティシンポジウム 2020（CSS2020），Oct. 2020.

* 佐賀大学大学院理工学研究科 Graduate of Science and Engineering, Saga University (nakayamt@ma.is.saga-u.ac.jp)
† 佐賀大学理工学部 Faculty of Science and Engineering, Saga University
‡ 近畿大学理工学部 Faculty of Science and Engineering, Kindai University
§ 岐阜大学工学部 Faculty of Engineering, Gifu University
¶ 神戸大学大学院工学研究科 Graduate School of Engineering, Kobe University