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

倍ブロック長圧縮関数の量子衝突計算困難性について
A Note on Quantum Collision Resistance of Double-Block-Length Compression Functions

廣瀬勝一 * 桑門秀典 †
Shoichi Hirose Hidenori Kuwakado

キーワード ハッシュ関数, 圧縮関数, 衝突計算困難性, 量子アルゴリズム

あらまし

2005 年に Nandi は $h^\pi(x) := (h(x), h(\pi(x)))$ と定義される倍ブロック長圧縮関数のクラスを示した。ここで，h は出力長 n ビットのランダムオラクルであり，π は置換である。 Nandi は，π が不動点を持たないとき，h^π の衝突計算困難性が最適であることを示した。 本稿では $h^\pi(x)$ の量子衝突計算困難性について考察する。 最初に，π がインボリューションのとき，Grover 探索を用いることにより，$O(2^{n/2})$ 回の反復で h^π の衝突入力組を見つけることができることを示す。 次に，h^π の量子衝突計算困難性が最適となるための π に関する十分条件を示す。

* 福井大学, 〒 910-8507 福井市文京 3-9-1, University of Fukui, Fukui 910-8507, Japan
† 関西大学, 〒 569-1095 大阪府高槻市霊仙寺町 2-1-1, Kansai University, Osaka 569-1095, Japan