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

Bernstein-Vazirani 量子アルゴリズムに基づく ランダムブール関数の隠れシフト問題の求解について

Solving Boolean Hidden Shift Problem based on Bernstein-Vazirani Quantum Algorithm

八藤後 彬 * 米山 一樹 *
Akira Yatougo Kazuki Yoneyama

キーワード 量子，共通鍵暗号，隠れシフト問題，ランダムブール関数, Bernstein-Vazirani の量子アルゴリズム，Simon の量子アルゴリズム

あらまし

隠れシフト問題は，2 つの関数 $f_0, f_1 : \{0,1\}^m \to \{0,1\}^n$ について，$\forall x\ f_0(x) = f_1(x \oplus s)$ を満たす唯一の秘密情報 s を発見する問題である．求解により同種写像問題に基づく耐量子公開鍵暗号系や，ある種の共通鍵暗号系への攻撃に応用できることが知られており，量子優位性を示す問題のひとつとして，理論的にも重要である．

隠れシフト問題における f_0, f_1 に対して，$F(b,x) = f_b(x)$ と定義すると，関数 $F : \{0,1\} \times \{0,1\}^m \to \{0,1\}^n$ は $\forall x\ F(b,x) = F(b \oplus 1, x \oplus s)$ を満たし，$(1,s)$ を周期に持つ周期関数となる．

周期発見問題を解くアルゴリズムとして知られる Simon の量子アルゴリズムを関数 F に適用することにより，古典計算では指数時間要するのに対し，量子計算では多項式時間で周期 $(1,s)$ を導出できることが知られている．また，Gavinsky らは量子サンプリングに基づく周期発見によって，隠れシフト問題を解く手法を提案した．

一方，近年 Bernstein-Vazirani（BV）量子アルゴリズムに基づく周期発見が提案された．BV 量子アルゴリズムに基づく周期発見は，Simon の量子アルゴリズムに基づく場合に対して，幾つかの暗号方式への適用において量子ビット数や実行時間の効率の良さが示されている．

本稿では，隠れシフト問題の特殊形として，ランダムブール関数 $f_0, f_1 : \{0,1\}^m \to \{0,1\}$ に着目し，BV 量子アルゴリズムに基づく周期発見により隠れシフト問題を解くアルゴリズムを提案する．また，提案手法の優位性を示すため，Simon の量子アルゴリズム，および量子サンプリングに基づく周期発見と提案手法について，仮定を揃えた上で量子回路を Python フレームワーク Cirq 上で構成・シミュレーションを行い，サブルーチンの呼出回数および実行時間の観点から比較する．

その結果，各手法におけるサブルーチンの呼出回数および実行時間は表 1 の通りとなり，BV 量子アルゴリズムに基づく提案手法は Simon の量子アルゴリズムに基づく場合と比較してサブルーチンの呼出回数，量子サンプリングに基づく場合と比較して実行時間でそれぞれ優位性を持ち，ランダムブール関数の隠れシフト問題の求解において有効であることを示す．

* 茨城大学大学院 理工学研究科 情報工学専攻， 〒 316–0033 日立市中成沢町 4–12–1, Major in Computer and Information Sci. , Graduate School of Sci. and Eng. , Ibaraki University, 4–12–1 Nakanarusawa, Hitachi, Ibaraki, 316–0033 Japan

表 1: **各方式実行結果 ($\bar{Q}$: 平均呼出回数, $\bar{T}$: 平均実行時間)**

入力ビット数 (b,x)	Simon($\bar{Q}$)	Simon($\bar{T}$)	BV($\bar{Q}$)	BV($\bar{T}$)	Sampling($\bar{Q}$)	Sampling($\bar{T}$)
3	6.673	0.016	3.331	0.008	3.327	0.011
4	15.748	0.063	7.882	0.030	7.868	0.050
5	27.031	0.204	13.538	0.094	13.540	0.164
6	36.455	0.521	18.213	0.250	18.202	0.444
7	45.884	1.335	23.042	0.638	23.095	1.211