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

A Quantum Search-to-Decision Reduction for the LPN Problem

Kyohei Sudo * Masayuki Tezuka * Keisuke Hara * † Yusuke Yoshida *
Keisuke Tanaka *

Keywords: LPN problem, Quantum reduction, Search-to-Decision, Goldreich-Levin theorem

Abstract

The learning parity with noise (LPN) problem has found many cryptographic applications as the hardness assumption. There are two variants of the problem, decisional LPN problem and search LPN problem. It is known that the decisional LPN problem is polynomially equivalent to the search LPN problem. The most recent proposed reduction is the one proposed by Katz and Shin [1].

In this work, we propose a quantum reduction from the search LPN problem to the decisional LPN problem. Our reduction is inspired by the quantum Goldreich-Levin theorem by Adcock and Cleve [2]. Specifically, we construct a predicator which predicates inner product $a \cdot s$, where a is its input and s is the secret string of the LPN problem, using the distinguisher of the decisional LPN problem. In a similar way to the discussion of the quantum Goldreich-Levin theorem, this predicator can be used to construct a solver of the search LPN problem. The efficiency of our reduction is incomparable to the classical one by Katz and Shin. Then, we investigate the conditions under which our reduction works more efficiently than the classical one.

References

[1] Jonathan Katz and Ji Sun Shin, "Parallel and Concurrent Security of the HB and HB$^+$ Protocols," EUROCRYPT, 2006.

[2] Mark Adcock and Richard Cleve, "A Quantum Goldreich-Levin Theorem with Cryptographic Applications," STACS, 2002.

* Tokyo Institute of Technology, Tokyo, 152-8552 Japan. A part of this work was supported by iJST OPERA JPMJOP1612, JST CREST JPMJCR14D6, JPMJCR2113, JSPS KAKENHI JP16H01705, JP17H01695, JP19J22363, JP20J14338, 21H04879.

† National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan.