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

Quantum Resistance on Modes of Operation in Block Ciphers

Jeeun Lee*

Keywords: quantum adversaries; quantum security; block ciphers; modes of operation

Abstract

In this research, as one of the most widely used cryptographic primitives, the quantum security of confidentiality modes of operation in block ciphers are examined: CBC, IGE, CFB, OFB, and CTR. First, quantum adversaries are classified as Q0, Q1, and Q2 depending on their ability to perform quantum computation. The corresponding new quantum proof techniques are also presented. Then the underlying block ciphers are assumed as pseudorandom functions which are Q0, Q1, and Q2 secure. Also, modes of operation to be investigated are represented in the quantum circuit. Next, our desired security notions are considered in terms of quantum version of indistinguishability (IND) and chosen-plaintext attack (CPA): IND under quantum CPA (IND-qCPA), weak-quantum IND under quantum CPA (wqIND-qCPA), and quantum IND under quantum CPA (qIND-qCPA). In conclusion, the security of each mode in Q0-, Q1-, or Q2-secure block ciphers is analysed and compared in these various quantum security game scenarios.

* Korea Institute for Advanced Study, Seoul 02455, South Korea.