A Study on Design and Security Analysis of Modes of Operation for Symmetric-key Cryptography

Soichi Furuya

January 2004

Abstract

With the development of information society, transmitted information became valuable and advanced. Due to these social phenomenon, social effort in order to protect information has been needed, represented in Digital Signature Act and Privacy Act.

Cryptography is the fundamental technology of such information security, and the realization of a secure efficient encryption method is one of social demands.

Symmetric-key cryptography is the indispensable technology to realize encryption mechanism to hide secret information between entities secretly sharing a secret key (common key). Also symmetric-key cryptography is usable for message-authentication mechanism to detect an unauthorized data manipulation.

In the area of symmetric-key cryptography, studies on cryptographic primitives used for the security of cryptographic mechanisms are important. In the meantime, the research on modes of operation is important, that is the way to use the cryptographic primitives including how one should use the cryptographic primitives in order to achieve expected functions. In order to realize encryption and message-authentication mechanisms, we need not only secure cryptographic primitives but also theories which prove the security of such mechanisms used in a modelized setting. In the setting, a number of assumptions are typically set; some are obviously recognized and the others are implicit or unrecognized. We, therefore, have issues to be solved such as if these assumptions are realistic, what kind of security can be achieved by the mode, and if the achievable method is efficient.

This paper proposes a new mode of encryption with message authenticity, and gives the proof based on the modern theory of the provable-security setting. We also study one aspect of operational issues regarding mechanisms based on symmetric-key cryptography, and analyze the relation to the security of such mechanisms.