Cryptology ePrint Archive: Report 2011/361

Compact CCA-Secure Encryption with Ciphertext Verifiability

S.Sree Vivek and S.Sharmila Deva Selvi and C.Pandu Rangan

Abstract: While CCA secure encryption schemes that provide ciphertext indistinguishability offer strongest form of message secrecy, the integrity of the ciphertext is often overlooked. In most of the practical applications it is required that the ciphertext should be verifiable with respect to the decrypted message in order to check whether the ciphertext components are intact after traveling through insecure channels. In this work, we first point out that all the existing schemes with compact ciphertext provide ciphertext indistinguishability but do not provide ciphertext verification during the decryption process. Thus, while the adversary does not gain any knowledge about the message, he is capable of altering the ciphertext into another ciphertext which will decrypt to an arbitrary message. Next, we propose three schemes where our first scheme provides compact ciphertext for messages of size greater than λ (where λ is a parameter such that any computation involving 2^λ or more steps is considered infeasible in practice), the second scheme is for messages of any size $(m\geq 1)$ and the third one is a stateful encryption scheme. All these three schemes provide ciphertext verifiability with the same ciphertext overhead of the existing schemes that do not offer ciphertext verifiability. We prove the security of our schemes in the random oracle model.

Category / Keywords: public-key cryptography / Adaptive Chosen Ciphertext Secure (CCA), Provable Security, CCA with Ciphertext Indistinguishability, CCA with Ciphertext Verification, Practicality of CCA secure schemes, Random Oracle model

Date: received 4 Jul 2011

Contact author: ssreevivek at gmail com,sharmioshin@gmail com

Available formats: PDF | BibTeX Citation

Version: 20110706:025754 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]