ACE 暗号攻撃評価報告書 概要

概要

Advanced Cryptographic Engine に含まれる公開鍵暗号方式 (以下, ACE 暗号) に対する安全性の評価を行った. 暗号スキームの安全性証明の検証の結果, ACE 暗号は, 汎用一方向性ハッシュ関数と, 擬似ランダム性を持つ擬似乱数生成器の存在, および決定性 Diffie-Hellman 問題の困難性を前提として適応的選択暗号文攻撃に対して強秘匿性 (または頑強性) を持つことがわかった. また, 推奨パラメータ長での決定性 Diffie-Hellman 問題の困難性を評価した結果, 離散対数問題への攻撃において, 指数計算法に対して耐性を持つよう適切にパラメータを選択するならば安全性には問題がないことがわかった.

Abstract

We estimated the security of the public key encryption scheme pertained to the Advanced Cryptographic Engine (ACE). As a result of the verification of the proof of security of ACE scheme, it turned out that this scheme is semantically secure against the adaptive chosen ciphertext attack under the assumptions of the existence of universal one-way functions and "pseudo-random" bit generator and the difficulty of the decisional Diffie-Hellman problem. Moreover, the lengths of parameters are secure enough as long as those are selected so that the index calculus methods for the discrete logarithm problem are unadaptable.