ACE 署名攻撃評価報告書概要

概要
本報告では、簡略化した ACE 署名に対して、以下の 2 つの観点から評価を行った.

(1) Strong RSA 仮定および汎用一方向性ハッシュ関数の存在を仮定した上での、適応的選択文書攻撃に対する安全性.

(2) 公開鍵に含まれる RSA 型の合成数 n の素因数分解問題に対する安全性.

(1) については、ACE 署名は適応的選択文書攻撃に対して安全であることがが検証できた. (2) については、合成数 n は数体ふるい法および $p-1$ 法に対して安全である事が示されたが、$p+1$ 法に対しては安全性を保証できないため問題が生じる可能性がある. 但し、この問題は鍵生成時に、$p+1$ 法に対する安全性の条件を付け加えることにより回避できる.

Abstract
In this report,we evaluate simplified version of ACE Sign from the following two points of view:

(1) The security against adaptive chosen message attack, under the strong RSA assumption and the assumption that exsit universal one-way family of hash function.

(2) The security of RSA type composite number n that is the part of public key against factorization.

For (1) we verificate that ACE Sign is secure agsinst adaptive chosen message attack . For (2) the composite number n is secure against number field sieve and $p-1$ method,but probably its security is not guaranted against $p+1$ method. We can avoid this problem by adding the condition as to $p+1$ method in the key generation step.