Siguna Müller
Some remarks on Williams' public-key crypto functions,
Fibonacci Quart. **44** (2006), no. 3, 224–234.

Abstract

In 1984, H.C. Williams introduced a public key cryptosystem whose security is as intractable as factorization. That is, the system is provably as difficult to break as it is to find the factors of the modulus $n = pq$. By utilizing properties of the Lucas functions, this proposal is the only factorization equivalent scheme that is known which does not impose any restrictions on the primes used in the modulus.

However, Williams anticipates several restrictions on the messages without further analyzing if these are always fulfilled. By investigating simple numerical examples we found that any message not meeting these criteria cannot be encrypted and most likely directly exposes a factor of the modulus during the encryption process.

We analyze this problem encountered in the original scheme and establish the exact number of such 'dangerous' messages. Moreover, we provide a simple modification of the Williams' system which minimizes these difficulties. The modification does not complicate the system in any way. Evaluation of the proposed system can be obtained in exactly the same number of steps as in the original system. The results obtained will demonstrate that the possible lack of security due to the 'dangerous' messages is negligibly small for large moduli.