CORR 2000-05

On the Security of a Williams Based Public Key Encryption Scheme

Siguna Müller*

Abstract Motivated by some strong and interesting cryptographic properties of the intrinsic structure of Williams' encryption scheme [36], we present a practical modification thereof that can be proven secure against adaptive chosen-ciphertext attacks. While our proof applies a notion of security closely related to the strong concept of 'plaintext-awareness' [4], we do not require the use of random oracles. To this end, we introduce a comparable notion and prove the security without relying on the ROM. In particular, our underlying intractability assumptions are the factorization problem of any large integer $n = pq$, and a concept similar to the "oracle hashing" paradigm introduced in [11]. The main advantage of our system is that we do not rely on any special form of the modulus $n = pq$, nor do we require any specific values of the primes p and q. Furthermore, we do not rely on "truly random" has functions. The assumptions that we make are both well-defined and reasonable.

Keywords Chosen Ciphertext Security, Message Awareness, Factorization Intractability, Oracle Hashing, Williams' Encryption Scheme