Cryptology ePrint Archive: Report 2013/040

An Effi cient CCA2-Secure Variant of the McEliece Cryptosystem in the Standard Model

Roohallah Rastaghi

Abstract: Recently, a few CCA2-secure (IND-CCA2) variant of the McEliece cryptosystem in the standard model were introduced. All these schemes are based on Rosrn-Segev approach and lossy trapdoor function and utilize k-repetition paradigm. The main drawback of these chemes is that they are need additional encryption and have large key size compared to the original scheme, which intricate the public-key size problem in the code-based cryptosystem. Furthermore, full CCA2-security of these schemes achieved by using a strongly unforgeable one-time signature scheme, and so, the resulting scheme need separate encryption. Therefore, these schemes are completely impractical.

In this manuscript, we propose a new and efficient IND-CCA2 variant of the McEliece cryptosystem in the standard model. The main novelty is that, unlike previous approaches, our approach is a generic ransformation and can be applied to any code-based one-way cryptosystem (both the McEliece and the Niederreiter cryptosystems). Our approach also leads to the elimination of the encryption repetition and using strongly unforgeable one-time signature scheme. This novel approach is more efficient, the publick/secret keys are as in the original scheme and the encryption/decryption complexity are comparable to the original scheme. CCA2-security of the proposed scheme can be reduced in the standard model to the McEliece assumptions. To the best of our knowledge, this is the first variant of the code-based cryptosystem that is IND-CCA2 in the standard model without using k-repetition paradigm and strongly unforgeable one-time signature scheme.

Category / Keywords: Post-quantum cryptography, McEliece cryptosystem, IND-CCA2, Permutation algorithm, Standard model.

Publication Info: This is a preliminary version of the paper that submits to the PQ-crypto’2013.‎

Date: received 26 Jan 2013, last revised 30 Jan 2013

Contact author: r(dot) rastaghi59(at)gmail com