Cryptology ePrint Archive: Report 2013/106

URDP: General Framework for Direct CCA2 Security from any Lattice-Based PKE Scheme

Roohallah Rastaghi

Abstract: Design efficient Lattice-based cryptosystem secure against adaptive chosen ciphertext attack (IND-CCA2) is a challenge problem. To the date, full CCA2-security of all proposed Lattice-based PKE schemes achieved by using a generic transformations such as either strongly unforgeable one-time signature schemes (SU-OT-SS), or a message authentication code (MAC) and weak form of commitment. The drawback of these schemes is that encryption requires "separate encryption". Therefore, the resulting encryption scheme is not sufficiently efficient to be used in practice and it is inappropriate for many applications such as small ubiquitous computing devices with limited resources such as smart cards, active RFID tags, wireless sensor networks and other embedded devices.

In this work, for the first time, we introduce an efficient universal random data padding (URDP) scheme, and show how it can be used to construct a "direct" CCA2-secure encryption scheme from "any" worst-case hardness problems in (ideal) lattice in the standard model, resolving a problem that has remained open till date. This novel approach is a "black-box" construction and leads to the elimination of separate encryption, as it avoids using general transformation from CPA-secure scheme to a CCA2-secure one. IND-CCA2 security of this scheme can be tightly reduced in the standard model to the assumption that the underlying primitive is an one-way trapdoor function.

Category / Keywords: public-key cryptography / Post-quantum cryptography, Lattice-based PKE scheme, Universal random data padding, CCA2-security, Standard model

Date: received 24 Feb 2013, last revised 1 Mar 2013, withdrawn 3 Mar 2013

Contact author: r rastaghi59 at gmail com

Available formats: (-- withdrawn --)

Version: 20130304:025809 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]