Cryptology ePrint Archive: Report 2011/208

Direct Constructions of Bidirectional Proxy Re-Encryption with Alleviated Trust in Proxy

Jian Weng and Yunlei Zhao

Abstract: In this work, we study (the direct constructions of) bidirectional proxy re-encryption (PRE) with alleviated trust in the proxy, specifically the master secret security (MSS) and the non-transitivity (NT) security, in the standard model, and achieve the following:

1. A multi-hop MSS-secure bidirectional PRE scheme with security against chosen plaintext attacks (CPA) in the standard model, where the ciphertext remains constant size regardless of how many times it has been re-encrypted. To the best of our knowledge, there exists previously no MSS-secure multi-hop bidirectional PRE scheme with constant size of ciphertexts (whether in the random oracle model or not).

2. A single-hop MSS-secure and non-transitive bidirectional PRE scheme with security against chosen ciphertext attacks (CCA) in the standard model. The CCA-secure scheme is based on the CPA-secure scheme, and particularly employs a new re-encryption key (REK) generation mechanism to which each user makes equal contributions, where a \emph{single} REK is used in both directions with the same proxy computation. Single-hop non-transitive bidirectional PRE schemes also enjoy better fine-grained delegate right control (against malicious proxy).

The security analysis uses Coron's technique [Coron, Crypto 2000], which particularly allows adaptive secret key corruption. Along the way, we also refine and clarify the security models for bidirectional PRE.

Category / Keywords: public-key cryptography / public key cryptography

Date: received 1 May 2011, last revised 8 May 2011

Contact author: cryptjweng at gmail com