Proxy re-encryption with unforgeable re-encryption keys.


Summary: Proxy re-encryption (PRE) provides nice solutions to the delegation of decryption rights. In proxy re-encryption, the delegator Alice generates re-encryption keys for a semi-trusted proxy, with which the proxy can translate a ciphertext intended for Alice into a ciphertext for the delegatee Bob of the same plaintext. Existing PRE schemes have considered the security that the collusion attacks among the proxy and the delegatees cannot expose the delegator’s secret key. But almost all the schemes, as far as we know, failed to provide the security that the proxy and the delegatees cannot collude to generate new re-encryption keys from the delegator to any other user who has not been authorized by the delegator. In this paper, we first define the notion of the unforgeability of re-encryption keys to capture the above attacks. Then, we present a non-interactive CPA secure PRE scheme, which is resistant to collusion attacks in forging re-encryption keys. Both the size of the ciphertext and the re-encryption key are constant. Finally, we extend the CPA construction to a CCA secure scheme.

doi:10.1007/978-3-319-12280-9_2