abtechchennai@gmail.com
www.abtechnologies.in
9840511458

ACCOUNTABLE PROXY RE-ENCRYPTION FOR SECURE DATA SHARING

ABSTRACT

Proxy re-encryption (PRE) provides a promising solution for encrypted data sharing in public cloud. When data owner Alice is going to share her encrypted data with data consumer Bob, Alice generates a re-encryption key and sends it to the cloud server (proxy); by using it, the proxy can transform Alice's ciphertexts into Bob's without learning anything about the underlying plaintexts. Despite that existing PRE schemes can prevent the proxy from recovering Alice's secret key by collusion attacks with Bob, due to the inherent functionality of PRE, it is inevitable that the proxy and Bob together are capable to gain and distribute Alices decryption capabilities. Even worse, the malicious proxy can deny that it has leaked the decryption capabilities and has very little risk of getting caught. To tackle this problem, we introduce the concept of Accountable Proxy Re-Encryption (APRE), whereby if the proxy is accused to abuse the re-encryption key for distributing Alice's decryption capability, a judge algorithm can decide whether it is innocent or not. We then present a non-interactive APRE scheme and prove its CPA security and accountability under DBDH assumption in the standard model. Finally, we show how to extend it to a CCA secure one.