**Secure Channel Free Certificate-Based Searchable Encryption Withstanding Outside and Inside Keyword Guessing Attacks**

**Abstract:**

Searchable public key encryption (SPKE) is a useful public key cryptographic primitive that allows a user to perform keyword searches over publicly encrypted messages on an untrusted storage server while guaranteeing the privacy of the original messages as well as the search keywords. However, most of the previously proposed SPKE frameworks suffer from the security vulnerability caused by the keyword guessing attack and some other weaknesses. Inspired by the ideas of certificatebased cryptography and signcryption, we present a new SPKE framework called certificate-based searchable encryption. The new framework not only provides resistance to the existing known types of keyword guessing attacks, but also enjoys some appealing merits, such as implicit authentication, no key escrow and no secure channel. Under this new framework, we devise a concrete searchable certificate-based encryption scheme. In the random oracle model, it is proven to meet the keyword ciphertext indistinguishability, the keyword ciphertext unforgeability and the keyword trapdoor indistinguishability under the adaptive chosen-keyword attack. The comparisons indicate that it is secure and practicable.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/UBUNTU.
* Implementation : NS2
* NS2 Version : 2.28
* Front End : OTCL (Object Oriented Tool Command  Language)
* Tool : Cygwin (To simulate in Windows OS)