**Searchable Symmetric Encryption with Forward Search Privacy**

**Abstract:**

Searchable symmetric encryption (SSE) has been widely applied in the encrypted database for queries in practice. Although SSE is powerful and feature-rich, it is always plagued by information leaks. Some recent attacks point out that forward privacy which disallows leakage from update operations, now becomes a basic requirement for any newly designed SSE schemes. However, the subsequent search operations can still leak a signiﬁcant amount of information. To further strengthen security, we extend the deﬁnition of forward privacy and propose the notion of “forward search privacy”. Intuitively, it requires search operations over newly added documents do not leak any information about past queries. The enhanced security notion poses new challenges to the design of SSE. We address the challenges by developing the hidden pointer technique (HPT) and propose a new SSE scheme called Khons, which satisﬁes our security notion (with the original forward privacy notion) and is also efﬁcient. We implemented Khons and our experiment results on large dataset (wikipedia) show that it is more efﬁcient than existing SSE schemes with forward privacy.

**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)