**Towards Thwarting Template Side-channel Attacks in Secure Cloud Deduplications**

**Abstract:**

 As one of a few critical technologies to cloud storage service, deduplication allows cloud servers to save storage space by deleting redundant ﬁle copies. However, it often leaks side channel information regarding whether an uploading ﬁle gets deduplicated or not. Exploiting this information, adversaries can easily launch a template side-channel attack and severely harm cloud users’ privacy. To thwart this kind of attack, we resort to the k-anonymity privacy concept to design secure threshold deduplication protocols. Speciﬁcally, we have devised a novel cryptographic primitive called “dispersed convergent encryption” (DCE) scheme, and proposed two different constructions of it. With these DCE schemes, we successfully construct secure threshold deduplication protocols that do not rely on any trusted thirdparty.Ourprotocolsnotonlysupportconﬁdentialityprotections and ownership veriﬁcations, but also enjoy formal security guarantee against template side-channel attacks even when the cloud server could be a “covert adversary” who may violate the predeﬁned threshold and perform deduplication covertly. Experimental evaluations show our protocols enjoy very good performance in practice

**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)