**Authenticated Medical Documents Releasing with Privacy Protection and Release Control**

**Abstract:**

In the context of Information Societies, a tremendous amount of information is daily exchanged or released. Among various information-release cases, medical document release has gained signiﬁcant attention for its potential in improvinghealthcareservicequalityandefﬁcacy.However,integrityandoriginauthenticationofreleasedmedicaldocuments is the priority in subsequent applications. Moreover, sensitive nature of much of this information also gives rise to a serious privacy threat when medical documents are uncontrollably made available to untrusted third parties. Redactable signatures allow any party to delete pieces of an authenticated document while guaranteeing the origin and integrity authentication of the resulting (released) subdocument. Nevertheless, most of existing redactable signature schemes (RSSs) are vulnerable to dishonest redactors or illegal redaction detection. To address the above issues, we propose two distinct RSSs with ﬂexible release control (RSSs-FRC). We also analyse the performance of our constructions in terms of security, efﬁciency and functionality. The analysis results show that the performance of our construction has signiﬁcant advantages over others, from the aspects of security and efﬁciency.

**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)