

**Strong Key-Exposure Resilient Auditing for Secure Cloud Storage**

**Abstract:**

Key exposure is one serious security problem for cloud storage auditing. In order to deal with this problem, cloud storage auditing scheme with key-exposure resilience has been proposed. However, in such a scheme, the malicious cloud might still forge valid authenticators later than the key-exposure time period if it obtains the current secret key of data owner. In this paper, we innovatively propose a paradigm named strong key-exposure resilient auditing for secure cloud storage, in which the security of cloud storage auditing not only earlier than but also later than the key exposure can be preserved. We formalize the definition and the security model of this new kind of cloud storage auditing and design a concrete scheme. In our proposed scheme, the key exposure in one time period doesn’t affect the security of cloud storage auditing in other time periods. The rigorous security proof and the experimental results demonstrate that our proposed scheme achieves desirable security and efficiency.