A General Dynamic Secret Sharing Algorithm in Distributed System

[1] Li Xiaoxin, [2] Guo Qingping, Zhang Feng
School of Computer Science and Technology, Wuhan University of Technology, Yujiatou Campus, Wuhan 430063, China.
Email: liwonder@sina.com[1] qpguo@mail.whut.edu.cn[2]

ABSTRACT

In order to produce, manage and protect distributed key more safely, especially for the private key of the CA center, Country's military secret and so on, a General Dynamic Secret Sharing Algorithm has been proposed, which based on the study of a Proactive Secret Sharing Algorithm **错误！未找到引用源。** and a General Verifiable Secret Sharing protocol **错误！未找到引用源。**. The algorithm makes Secret Sharing more practical and more applicable. And some new conception has been presented, such as Virtual Shares, Increased Shares and Working Shares. A scheme of dynamic renewing each minimal authorized subset has also been presented and realized, which makes adversary don't know how to attack and makes the Secret Sharing system more safely.

Key Words: secret sharing; general dynamic secret sharing; access structure; minimal authorized subset; virtual shares.