

石润华, 黄刘生, 杨威, 仲红. 新型有效的秘密共享方案[J]. 通信学报, 2012, (1):10~16

## 新型有效的秘密共享方案

DOI:

中文关键词:

英文关键词:

基金项目:

作者

单位

[石润华, 黄刘生, 杨威, 仲红](#)

摘要点击次数: 179

全文下载次数: 103

中文摘要:

提出了一种新的秘密共享方案。该方案分两层实现: 上层, 基于Stern-Brocot树把一个大的秘密拆分为t个小整数(子秘密); 底层, 借鉴一维元胞自动机模型中的进化方法, 把上层的t个子秘密作为初始状态, 动态生成各参与者的共享。特别地, 该方案能够动态扩展参与者, 动态调整门限值, 动态更新秘密和共享。另外, 还具有计算简单, 各参与者共享份额短的优点。分析结果表明, 该方案安全、有效。

英文摘要:

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

[关闭](#)

版权所有: 通信学报

地址: 北京东城区广渠门内大街80号通正国际大厦6层602室 电话: 010-67110006-869/878/881 电子邮件: xuebao@ptpress.com.cn  
技术支持: 北京勤云科技发展有限公司