通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

黄海平1,2,4,戴庭1,2,王汝传1,2,3,秦小麟4,陈九天1.基于(t, n)门限和划分树的可再生Hash链构造方案[J].通信学报,2013,(4):70~81

基于(t, n)门限和划分树的可再生Hash链构造方案

Novel self-renewal hash chain scheme based on (t, n) threshold and division tree

投稿时间： 2012-07-09

DOI：10.3969/j.issn.1 000-436x.2013.04.008

中文关键词：划分树；可再生散列链；(t n)-Mignotte’s门限方案；中国剩余定理

英文关键词:division-tree; renewal hash chain; (t n)-Mignotte's threshold; Chinese remainder theorem

基金项目:国家自然科学基金资助项目(61170065, 61003039)；江苏省科技支撑计划（工业）基金资助项目(BE2012183)；江苏省属高校自然科学研究重大基金资助项目(12KJA520002)；国家博士后基金资助项目(2012M511753)；江苏省博士后基金资助项目(1101011B)；江苏高校科技创新计划基金资助项目(CXLX12-0486)；江苏高校优势学科建设工程基金资助项目(信息与通信工程, yx002001)

作者	单位
黄海平1,2,4，戴庭1,2，王汝传1,2,3，秦小麟4，陈九天1	1. 南京邮电大学 计算机学院，江苏 南京 210003；2. 江苏省无线传感网高技术研究重点实验室，江苏 南京 210003；3. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室，江苏 南京 210003；4. 南京航空航天大学 计算机科学与技术学院，江苏 南京 210016

摘要点击次数:**534**

全文下载次数:**364**

中文摘要:

针对可再生hash链解决了其资源受限的缺点，但现有构造方案在安全性和复杂性等方面存在缺陷这一问题，提出“重复”、“划分”和“划分树”的定义，以及基于(t, n)-Mignotte’s门限的中国剩余定理秘密共享方案，设计了一种新的可再生hash链构造方法。从明文空间、双重认证和可证明安全3方面论证了新构造方案能确保新链中种子值的安全再生并有效抵制中间人攻击。同时仿真实验表明新构造方案在通信、计算和存储开销等方面相比于传统方案具有相同甚至更佳的性能。

英文摘要:

The introduction of renewal hash chain overcame resource-constrained defect in traditional hash chains, but the existing renewable schemes had still held unsatisfactory performance especially on security and complexity. The definitions of repetition, division and division-tree was proposed, and then a novel self-renewable hash chain construction scheme was put forward based on division and (t, n)-Mignotte's threshold Chinese remainder theorem secret sharing scheme. From three aspects of key space, twice authentication and provable security, it theoretically proves that the proposed hash scheme could ensure the novel seed value regenerated safely and resisting the middle-man attack effectively. Simulation experiments demonstrate that the novel scheme obtains equal or more satisfactory performances on the costs of communication, computation and storage than typical schemes.

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：北京市丰台区成寿寺路11号邮电出版大厦8层 电话：010-81055478，81055479
81055480，81055482 电子邮件：xuebao@ptpress.com.cn
技术支持：北京勤云科技发展有限公司