电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

首页 | 期刊介绍 | 编 委 会 | 投稿指南 | 期刊订阅 | 联系我们 | 留言板 | English

电子与信息学报 » 2011, Vol. 33 » Issue (12) :2916-2921   DOI: 10.3724/SP.J.1146.2011.00406

论文   最新目录 | 下期目录 | 过刊浏览 | 高级检索   << Previous Articles | Next Articles >>

高效的在线/离线代理重签名方案

杨小东* 王彩芬*

西北师范大学数学与信息科学学院 兰州 730070

Efficient On-line/Off-line Proxy Re-signature Schemes

Yang Xiao-dong Wang Cai-fen*

College of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070, China

摘要 | 参考文献 | 相关文章

Download: PDF (231KB) HTML 1KB Export: BibTeX or EndNote (RIS) Supporting Info

摘要 为了改善代理重签名的性能，该文提出在线/离线代理重签名方案。其基本思想是将重签名算法分成离线阶段和在线阶段。在签名消息到来之前，离线阶段进行重签名的大部分计算，并将这些运算结果保存起来；在签名消息到来时，利用离线阶段保存的数据能在很短的时间内生成消息的在线重签名。文中给出了在线/离线代理重签名方案形式化定义，在此基础上构造了具体实现的方案，并在随机预言模型下给出其安全性证明。该方案可将任意一个代理重签名方案转换为一个高效的在线/离线代理重签名方案。分析结果表明，新方案在效率上优于已有的代理重签名方案，在线重签名算法仅需要1次模减法运算和1次模乘法运算。

关键词： 代理重签名 在线/离线 变色龙哈希函数 随机预言模型

Abstract: To improve the performance of proxy re-signature schemes, the schemes of on-line/off-line proxy re-signature are proposed in this paper. The main idea is to split the re-signing procedure into two phases: the off-line and on-line phases. Most of the computations are performed in the off-line phase before seeing the message to be re-signed. The results of this precomputation are saved and then used in the on-line phase when the message must be re-signed. On-line/off-line proxy re-signature schemes are used in a particular scenario where the proxy must respond quickly once the message to be re-signed is presented. Based on the formal definition of on-line/off-line proxy re-signatures, an efficient construction of on-line/off-line proxy re-signature is presented. It can convert any proxy re-signature scheme into a highly efficient on-line/off-line one. Security is proved in the random oracle model. Compared wirh the existing proxy re-signature schemes, the new scheme is more efficient in the communication cost and the computational cost. It needs one modular subtraction computation and one modular multiplication computation in the on-line re-signing generation algorithm.

Keywords: Proxy re-signature On-line/off-line Chameleon hash function Random oracle model

Received 2011-04-27;

本文基金:

国家自然科学基金(61063041)和西北师范大学青年教师科研能力提升计划(NWNU-LKQN-10-22)资助课题

通讯作者: 杨小东 Email: y200888@163.com

Service
把本文推荐给朋友
加入我的书架
加入引用管理器
Email Alert
RSS
作者相关文章
杨小东
王彩芬

引用本文:

杨小东, 王彩芬.高效的在线/离线代理重签名方案[J] 电子与信息学报, 2011,V33(12): 2916-2921

Yang Xiao-Dong, Wang Cai-Fen.Efficient On-line/Off-line Proxy Re-signature Schemes[J] , 2011,V33(12): 2916-2921

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2011.00406 或 http://jeit.ie.ac.cn/CN/Y2011/V33/I12/2916