计算机应用 2008, 28(8) 1907-0911 DOI: ISSN: 1001-9081 CN: 51-1307/TP

论文

可信计算平台模块密码机制研究

罗捷 严飞 余发江 张焕国

摘要：

可信计算已经成为世界信息安全领域的新潮流。介绍了可信计算平台模块(TPM)的基本体系，分析了它的密码机制，指出了其密码机制上的特色与不足。针对现有可信计算组织（TCG）规范中密钥管理授权机制比较复杂的缺点，结合OIAP与OSAP的思想，给出了一种授权复用的技术方案与授权协议，并给出了协议的安全性证明。

关键词： 密码 密钥管理 可信计算平台模块(TPM) 可信计算

Research on cryptology mechanism of trusted computing platform module

Abstract:

Trusted computing is a new tendency in the field of data security. The basic architecture of trusted computing platform module was introduced, and its cryptology mechanism was discussed. Through analyzing the cryptology mechanism of TCG, the advantages and disadvantages was pointed out. Aiming at the problem that the key management and authentication of TCG specifications were very complicated, a scheme of multiusing authentication data and a authentication protocol were proposed, which colligated OIAP and OSAP, and the security proof of this protocol was given.

Keywords: cryptology key management trusted computing module trusted computing

收稿日期 2008-04-25 修回日期 1900-01-01 网络版发布日期

DOI:

基金项目:

通讯作者: 罗捷

作者简介:

参考文献：

本刊中的类似文章

1．王玲玲 张国印 马春光.一种基于双线性对的可验证无证书环签密方案[J]. 计算机应用, 2007,27(9): 2167-2169

2．彭长根;李祥;罗文俊.可转换签密的几种改进方案[J]. 计算机应用, 2006,26(5): 1068-1070

3．李士达 胡玥 王兴秋 于真.一种基于ECC的SIP认证方案的提出与实现[J]. 计算机应用, 2007,27(2): 311-313

4．赵洋 蓝天 马新新 张凤荔 .基于加同态公钥密码体制的两方安全议价协议[J]. 计算机应用, 2006,26(11): 2576-2577

5．杨帆 沙瀛 程学旗.一个P2P分布式数字签名系统[J]. 计算机应用, 2007,27(2): 308-310

6．赵宇 王亚弟 韩继红 范钰丹 赵琦.一种基于问题求解理论的密码协议形式模型[J]. 计算机应用, 2007,27(2): 303-307
7．张艳霞 王劲林.一种P2P网络鲁棒访问控制协议[J]. 计算机应用, 2007,27(3): 538-540
8．李志军 耿技 王佳昊 秦志光 .传感器网络的多重单向散列随机密钥预分配协议[J]. 计算机应用, 2006,26(8): 1802-1806
9．冯国柱 李超 .基于视觉密码的身份认证方案[J]. 计算机应用, 2006,26(10): 2318-2319
10． 刘宏伟 卫国斌 .可信计算在VPN中的应用[J]. 计算机应用, 2006,26(12): 2935-2937
11．石峰 戴冠中 刘航 苗胜 李美峰 .基于门限方案的智能卡密钥管理系统的设计与实现[J]. 计算机应用, 2006,26(9): 2156-2159
12．赵宇 袁霖 王亚弟 韩继红 .一种改进的Woo-Lam密码协议模型[J]. 计算机应用, 2006,26(9): 2116-2120
13．肖政 韩英 叶蓬 侯紫峰 .基于可信计算平台的体系结构研究与应用[J]. 计算机应用, 2006,26(8): 1807-1809
14．刘军龙 王彩芬 .基于身份的可截取门限签名方案[J]. 计算机应用, 2006,26(8): 1817-1820
15．石润华 黄刘生 .一种简单的可验证秘密共享方案[J]. 计算机应用, 2006,26(8): 1821-1823
16．章静; 许 力; 林志伟.自组网中基于簇的混合密钥管理策略[J]. 计算机应用, 2006,26(6): 1328-1330
17．宣文霞.一种适合大型动态多播的密钥管理方案[J]. 计算机应用, 2006,26(6): 1334-1336
18．文静华; 张梅; 李祥.一种新的密码协议分析方法及其应用[J]. 计算机应用, 2006,26(5): 1087-1089
19．商建伟 李锋 张燕燕.一种入侵容忍的广播通讯KDC方案[J]. 计算机应用, 2007,27(5): 1038-1040
20．谭良 周明天.一种新的用户登录可信认证方案的设计与实现[J]. 计算机应用, 2007,27(5): 1070-1072
21．谭利平 李方伟.移动通信系统中的认证与密钥协商协议[J]. 计算机应用, 2007,27(6): 1343-1344
22．李明 秦宝东 李大兴.Koblitz曲线密码体制中一种可抵抗边带信道攻击的标量乘算法[J]. 计算机应用, 2007,27(8): 1926-1928
23．杨春 简丽 何军 .基于BB84与椭圆曲线的数字签名方案[J]. 计算机应用, 2007,27(10): 2475-2477
24．钟黔川 朱清新.Blowfish密码系统分析[J]. 计算机应用, 2007,(12): 2940-2941
25．张学军.一种完整的非对称公钥叛逆者追踪方案的密码学分析与改进[J]. 计算机应用, 2008,28(11): 2808-2810
26．张忠 向涛.一种基于Smart Card的远程用户身份验证方案的安全性讨论[J]. 计算机应用, 2008,28(11): 2811-2813
27．杨先文 李峥.一种GF(2m)上椭圆曲线点运算的混合坐标系[J]. 计算机应用, 2007,(12): 2962-2964
28．张波 向阳.语义网中基于本体的语义信任计算研究[J]. 计算机应用, 2008,28(2): 267-271
29．夏琦 许春香 高建彬.对一种代理签名方案的密码学分析和改进[J]. 计算机应用, 2009,29(2): 353-354
30．向新银.可认证的无证书密钥协商协议[J]. 计算机应用, 2008,28(12): 3165-3167
31．方燕萍 章晓芳 张广泉.串空间模型及其认证测试方法的一种扩展与应用[J]. 计算机应用, 2008,28(12): 3205-3207
32．李莉 曾国荪 陈波.开放网络环境下的属性远程证明[J]. 计算机应用, 2008,28(1): 77-79
33．张学峰 姜皇普 王永栓.基于矩阵格的传感器网络密钥预配置方案[J]. 计算机应用, 2008,28(1): 85-87
34．殷新春 侯红祥 谢立.一种基于加法链的快速标量乘算法[J]. 计算机应用, 2008,28(1): 56-58,6
35．曾玮妮 林亚平 卢秋英.无线传感器网络中基于簇协作的分布式组密钥管理方案[J]. 计算机应用, 2009,29(3): 638-842
36．熊光泽 常政威 桑楠.可信计算发展综述[J]. 计算机应用, 2009,29(4): 915-919,
37．马新强 Huang Yi 李丹宁.可信计算发展研究[J]. 计算机应用, 2009,29(4): 920-923
38．高洁 袁家斌 徐涛 齐艳珂.一种基于混合反馈的混沌图像加密算法[J]. 计算机应用, 2008,28(2): 434-436
39．彭长艳 张权 唐朝京.基于IBC的TLS握手协议设计与分析[J]. 计算机应用, 2009,29(3): 633-637
40．谢松 郭忠文 曲海鹏 吕广鹏.基于多密钥空间的无线传感器网络密钥管理方案[J]. 计算机应用, 2009,29(4): 932-934,
41．袁益民 盛利元 尚芳.基于TD-ERCS混沌系统的图像加密方法[J]. 计算机应用, 2008,28(4): 906-909
42．汪丽 邢伟 徐光忠.基于四元整数的ElGamal公钥密码体制[J]. 计算机应用, 2008,28(5): 1156-1157
43．陈联俊 赵云 张焕国.一种基于演化计算的序列密码分析方法[J]. 计算机应用, 2008,28(8): 1912-1915
44．丁晓宇 刘建伟 邵定蓉 刘淳.基于CPK的高效移动Ad Hoc网络密钥管理方案[J]. 计算机应用, 2008,28(8): 1916-1919
45．田野 厉树忠.随机混沌动力系统组及序列加密算法[J]. 计算机应用, 2008,28(7): 1779-1780

46. quietloner.高效的动态安全组播密钥协商方案[J]. 计算机应用, 2008,28(8): 1943-1945

47. 吕宁 孙广明 张宇.基于多混沌系统的图像分组密码设计[J]. 计算机应用, 2008,28(9): 2263-2266

48. 殷新春 赵荣 侯红祥 谢立.基于折半运算的快速双基数标量乘算法 [J]. 计算机应用, 2009,29(05): 1285-1292

文章评论 (请注意:本站实行文责自负, 请不要发表与学术无关的内容!评论内容不代表本站观点.)

反馈人		邮箱地址	
反馈标题		验证码	8944