基于 CPK 的可信平台用户登录认证方案

马宇驰,赵 远,邓依群,李益发
MA Yu-chi,ZHAO Yuan,DENG Yi-qun,LI Yi-fa

解放军信息工程大学 信息工程学院 应用数学系,郑州 450002
Department of Applied Mathematics,Information Engineering Institute,PLA Information Engineering University,Zhengzhou 450002,China
E-mail:mayuchi9111027@hotmail.com

MA Yu-chi,ZHAO Yuan,DENG Yi-qun,et al.Trusted computing platform login authentication scheme based on CPK. Computer Engineering and Applications,2010,46(1):90-94.

Abstract: Identity authentication for user login is very important to the operation system,and is the basis for building the trusted computing environment.The related technology of authentication is discussed.The theory of CPK(Combination of Public Key) is introduced.In addition,according to the standards of the Trusted Computing Group(TCG),using CPK and dynamic authentication code technology,a trusted computing platform login authentication scheme based on CPK is proposed.The scheme is double ingredient,separates authentication and warrant strictly.This paper not only shows a heuristic analysis about the characteristic and security of the scheme,but also,in strand space model,proves the security of the scheme,which indicates the scheme is more secure than the corresponding scheme presented in TCG standard.

Key words: trusted computing;Combination of Public Key(CPK);identity authentication;trusted login;strand space model

摘 要: 用户登录身份认证是建立操作系统可信性的一个非常重要的环节,是建立可信计算环境的基础。首先讨论了认证的相关技术,介绍了 CPK(组合公钥)原理,然后根据可信计算组织的规范,利用 CPK 算法和动态验证码的技术,提出了一种基于 CPK 的可信平台用户登录认证方案,该方案属于双因素认证方案,将认证和授权严格分开,并启发式分析了方案的特色和安全,最后在串空间模型下证明了方案的安全性,取得了比 TCG 标准中引用的方案更好的性能。

关键词: 可信计算;组合公钥(CPK);身份认证;可信登录;串空间模型
DOI: 10.3778/j.issn.1002-8331.2010.01.029 **文章编号:** 1002-8331(2010)01-0090-04 **文献标识码:** A **中图分类号:** TP311

1 前言

认证(authentication)是开放式信息系统中的一个重要概念,它是建立信任的基础,在信息安全领域占有极为重要的位置。熟知,在 Internet 上的交换信息过程,经常要用到认证;在金融、商务等重要的票据交换部门,认证系统一直是建立交易信任的基础;而在政府部门的保密信息系统中,敏感信息在接受访问之前必须要进行严格的身份认证。用户在需要使用计算机时,首先要进行的必须是用户身份的鉴别,这样才能保证用户行为的可信,计算机也才能够为其提供可信的服务。用户只有通过了身份认证,成为系统的合法用户后,才可以使用主机的相关资源。因此,用户登录身份认证是极为重要的,是操作系统中最基本的服务,其他的安全服务都要依赖于它。一旦身份认证系统出现问题,那么操作系统的所有安全措施将形同虚设。

认证系统的核心是建立签名机制[1],签名机制又依靠合理的密钥管理来实现,因此,密钥管理技术是签名机制和认证机制的基础。认证系统的密钥管理需要解决两个问题:一是密钥管理的规模化,二是基于标识的密钥分发。目前的解决方案主要有三种:一种是基于PKI 技术构建的认证系统,另一种是基于 IBC 技术构建的认证系统,最后一种是基于 CPK 技术构建的认证系统。

随着人们对认证技术的不断应用和理解,PKI 认证系统暴露出很多缺点:一是 PKI 体系结构中,CA 必须动态处理与认证相关的所有细节,PKI 依靠运行层次化的 CA 机构来扩大密钥管理的规模,导致了成本代价高(包括 CA 的建设成本、CA 的日常维护成本、用户证书的生产成本、RA 的运营成本等),随着用户数量的不断增大,造成了机构的膨胀和通信量的加大,其运行效率也在逐步降低;二是采用第三方证明的方式关联标识和密钥,采用在线证书库的证明方式,证书属性是公钥证书。IBC 虽然取消了第三方证明的机制,且证书属性是 ID 证书,但还需要在线目录库的支持,密钥空间的大小与密钥量成线性关系,双线性映射的计算比较困难,导致运行效率不高;同时,IBC 的安全性还没有得到很好的分析和确认。

具有我国自主知识产权的基于身份标识的 CPK(Combination of Public Key)组合公钥算法[2]是一种具有独特优势的新

基金项目: 国家重点基础研究发展规划(973)子课题(the National Grand Fundamental Research 973 Program of China under Grant No.2007CB311100)。
作者简介: 马宇驰(1982-),男,硕士研究生,研究方向为信息安全、密码学;赵远(1979-),男,硕士研究生,研究方向为信息安全、密码学;邓依群(1966-),女,副教授,研究方向为信息安全技术及其应用;李益发(1964-),男,副教授,硕士研究生导师,研究方向为密码学与信息安全。
收稿日期: 2008-07-10 **修回日期:** 2008-11-10

技术,能很好地解决密钥管理的两个问题,而且满足验证的简便性和管理的有效性[1],其安全性基于离散对数的难解性,可信度高,证书属性是 ID 证书,是完全基于身份标识的公钥算法,不需要第三方的证明,不需要在线数据库的支持,只要很少的参数就能管理大量的密钥,整个认证过程可以在芯片级实现,极大地提高了运行的效率,并降低了成本。

CPK 标识认证体系建立在 CPK 可信逻辑基础上,并通过 CPK 密钥算法实现。CPK 可信逻辑采用"条件满足性"的证明方法,由主体可信性、客体可信性、内容可信性、行为可信性四个方面证明,大大超出了相信逻辑的形式化推理证明,从而为构造超大规模、适用广泛的可信认证系统奠定了坚实的理论基础。

2005 年 6 月 3 日,北京市科委邀请国内知名信息安全专家对 CPK 算法进行了评议,一致认为"CPK 密钥管理算法是我国具有自主知识产权的密钥管理算法,经过多年的研究和实践,奠定了坚实的工作基础,具有重大创新意义和广泛的应用前景"。

作为构建可信世界的技术基础,CPK 可以应用于所有需要逻辑证明的领域,如:

(1)可信计算:以单台计算机为基础,将通信部分剥离(由可信连接处理),用 CPK 技术使软件产品标签化、验证技术通用化、CPK 认证模块控制非授权软件,特别是恶意软件的加载和执行,达到可信计算环境。特别,在可信登录方面 CPK 也有独特优势。

(2)可信连接:用 CPK 标识认证算法,对通信标识进行认证和验证,提供真实性证明,将多次交互过程简化为一次或两次过程,直接实现任何两端的可信连接。

(3)可信交易:用 CPK 标识认证算法,对用户身份标识和印章标识进行认证。

2　CPK 原理

CPK 是指组合公钥,是由我国著名信息安全专家南湘浩先生提出的一种新的集中式公钥管理模式[2]。它的基本思想是,管理中心首先生成很多密钥因子,由密钥因子可组合成很多公、私钥对,公钥全都存贮在一个安全的芯片中,私钥则由中心直接发放给用户。

以下是一个基于椭圆曲线的组合公钥的例子。

设 f 是适当选择的一个椭圆曲线,E 是 f 上的有理点构成的加法群,阶为 n(适当选择意味着 n 足够大),G 是基点(即加法群的生成元)。适当选择 $s\times t$ 个整数 r_{ij} 作为私钥因子,并用矩阵 ***SSK*** 表示,称为私钥种子矩阵。由私钥因子又可以得到相应的公钥因子:$g_{ij}=r_{ij}G$,从而可得相应的公钥种子矩阵 ***PSK***,即

$$\boldsymbol{SSK}=\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1t} \\ r_{21} & r_{22} & \cdots & r_{2t} \\ \vdots & \vdots & & \vdots \\ r_{s1} & r_{s2} & \cdots & r_{st} \end{pmatrix},\quad \boldsymbol{PSK}=\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1t} \\ g_{21} & g_{22} & \cdots & g_{2t} \\ \vdots & \vdots & & \vdots \\ g_{s1} & g_{s2} & \cdots & g_{st} \end{pmatrix}$$

文献[9]中指出,在 ***PSK*** 中的每列中取一个因子,其和构成一个公钥。如此可构成 $s^t<n$ 个不同的公钥。适当选择 s 和 t,可形成一个巨大的密钥空间。

SSK 由管理中心统一生成并保管。用户私钥是 t 个私钥因子的和,由管理中心利用适当选择的函数 φ 作为映射算法(公钥查询函数),根据用户名(要求用户不能重名)先确定 ***PSK*** 中的因子,继而查找 ***SSK*** 中的相应因子,并将诸因子之和即用户私钥面对面或通过专门的秘密通道发放给用户。公钥查询函数 φ 通常取单向函数或单向陷门函数,以用户名作为输入(用户名的使用要规范化)。任一用户验证其他用户的公钥时,可先访问管理中心的黑名单列表,然后利用公钥查询函数 φ 查找 ***PSK*** 即可。

例如,取 φ 为输出值足够长的 Hash 函数,将用户名(通常包含用户的姓名、单位等基本信息)作为输入,将输出的 φ 函数值作为参数,第一个 k 位($2^k\geqslant t$)确定第一列应取哪一行,第二个 k 位确定第二列应取哪一行,依此类推。实际应用时,函数 φ 是保密的,内置于芯片中,用户可以使用 φ,但并不知道 φ 的内部运行状态,这样有利于整个系统的安全。

使用时,由于每个用户有自己的私钥,可用于解密、签名或身份认证。而当验证其他用户的签名时,可以直接输入该用户名,利用 φ 在 ***PSK*** 中查找其公钥即可。

CPK 详细的内容可参见文献[2],其中对组合公钥的思想及相关算法作了详尽的介绍,并给出了更多的变换,以满足各种不同环境下的需求。

3　基于 CPK 的用户登录认证方案

该方案适用于封闭式环境,在此环境中的每台可信主机的 TPM[3](身份标识为 ID_{TPM})中都已经嵌入了相同的 CPK 系统模块,每个合法用户 U 也持有嵌入了相同的 CPK 系统模块的 U-KEY,身份标识为 ID_{U-KEY},每个 ID_{TPM} 和 ID_{U-KEY} 都唯一对应 CPK 系统模块中的一个公钥,TPM 和 U-KEY 中的 CPK 系统模块都分别存储有自己的私钥 SK_{TPM} 和 SK_{U-KEY},并且要求所有用户记住自己的口令 PW,该 U-KEY 除完成基本的密码运算和产生随机数外,还要存储认证参数,包括 U-KEY 持有者口令 PW 的 HASH 值 $Y=H(PW)$和动态验证码 AC。每台可信主机的 TPM 中也存储有平台主人口令的 HASH 值 Y_0 和平台主人的动态验证码 AC_0。TPM 和其主人 U-KEY 中的动态验证码初始值一致,由网络运营商随机选定。U-KEY 中的数据是受保护不可读取的。方案中的主机/TPM 含有的 CPK 模块的公私钥就是各自的 EK 公私钥。

3.1　该文方案

可信主机加电启动后,等待用户登录,接着用户将 U-KEY 插入其 USB 接口,然后进行下面的步骤:

(1)TPM→U-KEY:D_1,R_1,ID_{TPM}

(2)U-KEY→TPM:$D_2,ID_{U-KEY},[R_1,ID_{U-KEY}]SK_{U-KEY},\{R_2\}PK_{TPM}$

(3)TPM→U-KEY:$D_3,PK_{AIK},PCR,H(ID_{TPM},PK_{AIK},R_2),[ID_{TPM},D_3,PCR]SK_{AIK}$

(4)U→TPM:PW

U-KEY→TPM:$\{R_1,AC,ID_{U-KEY},Y\}PK_{TPM}$

(5)TPM→U-KEY:$\{R_2,D_4,AC_1\}PK_{U-KEY}$

(6)U-KEY→TPM:D_5

说明:

(1)TPM 产生随机数 R_1,将询问请求 D_1、R_1 和自己的身份标识一同发给 U-KEY,询问 U-KEY 是否要求登录;

(2)U-KEY 产生随机数 R_2,由 ID_{TPM} 在 CPK 系统中查找到 TPM 的公钥 PK_{TPM},产生加密项$\{R_2\}PK_{TPM}$,再利用自身的私钥产生签名项$[R_1,ID_{U-KEY}]SK_{U-KEY}$,最后将登录请求 D_2、自己的身份标识 ID_{U-KEY}、$[R_1,ID_{U-KEY}]SK_{U-KEY}$ 和$\{R_2\}PK_{TPM}$ 发送给 TPM;其中,$\{M\}K$ 表示用密钥 K 加密数据 M,$[M]K$ 表示用密钥 K 签名数据 M,而 A,B 表示 A 和 B 级连,$H(M)$表示对 M 进行 HASH 运算;

(3)TPM 收到(2)中的消息后,读取 ID_{U-KEY},而后在 CPK 系统中查找 ID_{U-KEY} 对应的公钥 PK_{U-KEY},并利用 PK_{U-KEY} 验证签名 $[R_1,ID_{U-KEY}]SK_{U-KEY}$,若签名为假,退出并终止登录;若签名为真,则用自己的私钥解密 $\{R_2\}PK_{TPM}$ 得到 R_2,这时产生身份证明密钥(Attestation Identity Key,AIK),将 AIK 公钥 PK_{AIK}、ID_{TPM} 和 R_2 一同 HASH 得到 $H(ID_{TPM},PK_{AIK},R_2)$,然后再用 AIK 私钥产生签名项 $[ID_{TPM},D_3,PCR]SK_{AIK}$,最后将操作事务记录 D_3、PK_{AIK}、平台配置寄存器的值 PCR、$H(ID_{TPM},PK_{AIK},R_2)$ 和 $[ID_{TPM},D_3,PCR]SK_{AIK}$ 发给 U-KEY;

(4)U-KEY 收到(3)中的消息后,利用 ID_{TPM}、PK_{AIK} 和自己保留的 R_2,计算它们的 HASH 值,并与收到的 $H(ID_{TPM},PK_{AIK},R_2)$ 比较,若不等,则退出并终止登录;若相等,则用 PK_{AIK} 验证签名 $[ID_{TPM},D_3,PCR]SK_{AIK}$,若签名为真,且 PCR 值表明平台可信,U-KEY 会提示用户主机当前状态可信,可以输入口令,于是用户在键盘输入自己的口令 PW,同时,U-KEY 产生并发送用 PK_{TPM} 加密的数据 $\{R_1,AC,ID_{U-KEY},Y\}PK_{TPM}$;否则,表明当前状态不可信,U-KEY 触发可信启动过程重新启动平台;

(5)TPM 收到(4)中的消息后,读取 PW,利用自己的私钥 SK_{TPM} 解密 $\{R_1,AC,ID_{U-KEY},Y\}PK_{TPM}$ 得到 Y、AC,并利用 R_1 检验消息的新鲜性,若通过,接着 TPM 进行如下的操作:

①将 PW 进行 HASH 运算得到 $H(PW)$,并与 Y 比对,若相等,转到②;若不等,退出并终止登录;

②比较 Y 和 Y_0,若相等,初步判定为平台主人,并转到③;若不等,确认为普通合法用户,TPM 通过主机 LCD 提示用户可以使用可信平台;注:此时,步骤(5)和(6)无需进行;

③比较 AC 和 AC_0,若相等,确认为平台主人,接着产生新的动态验证码 AC_1,并计算 $\{R_2,D_4,AC_1\}PK_{U-KEY}$ 后发送给 U-KEY,其中 D_4 为 TPM 将用户确认为平台主人的认证结果;若不等,通过主机 LCD 提醒用户存在非法登录,接着退出并终止登录;

(6)U-KEY 收到(5)中的消息后,解密得到 D_4 和 AC_1,并利用 R_2 检验消息的新鲜性,查看确认为平台主人的认证结果 D_4,用 AC_1 更新 U-KEY 中的动态验证码,同时向 TPM 发送一个确认消息 D_5。

TPM 收到确认消息 D_5 后,用 AC_1 更新自己的动态验证码。这时平台提示完全开启成功,平台主人可以使用。

3.2 方案的特色和分析

3.2.1 方案特色

(1)利用 CPK 技术,实现了平台、U-KEY 和用户之间的双向认证,体现了 CPK 基于身份标识、信任度高等优点。

(2)用户需要使用可信平台时,先要确定平台的状态,只有平台是可信的时候,用户才输入自己的口令,防止不可信或恶意的平台窃取用户的敏感信息。

(3)对平台主人的身份认证增加了动态验证码的比对,该过程使用静态口令和动态验证码相结合的认证技术,比 U-KEY 加口令认证方案多了一个动态验证,进一步加强了对平台主人身份认证的强度,平台主人每成功登录一次动态验证码就发生变化,故假使所有认证信息都被非法用户取得并登录过,则只要平台主人再次登录就会发现问题,可以把损失控制在比较小的范围内,而单纯使用静态口令,只要不同时登录,很难发现有非法用户冒用的存在,因而大大提高了安全性。

(4)当用户利用自己的 U-KEY 使用他人的平台时,用户的真实身份不会被平台记录,可以防止被追踪和隐私外泄。

(5)将认证和授权过程严格分开,严格区分不同用户的使用权限。

(6)计算量少,执行效率比较高,数字签名运算是最复杂的运算,其他运算是数据的加解密、产生随机数和 HASH 运算。

3.2.2 启发式分析

表 1 给出了 TCG 标准授权方案[3]、TCG 改进方案[4]在安全特性方面的详细比较,表中√、×和-分别表示方案具备、不具备和不涉及某个安全特性。

表 1 该文方案和其他方案的比较

安全特性	TCG 标准方案	TCG 改进方案	该文方案
多因素认证	单因素	双因素	双因素
需要智能卡	×	√	√
采用的密码机制	基于口令的单钥	口令和单钥	CPK、口令、动态验证码
U-KEY 鉴别用户	×	√	√
用户鉴别 U-KEY	-	×	√
用户鉴别平台	×	×	√
平台鉴别用户	√	√	√
平台鉴别 U-KEY	-	√	√
U-KEY 鉴别平台	-	√	√
口令的机密性和完整性	×	×	√
对平台状态验证	×	×	√
非法登录检查	×	×	√
多用户认证和授权控制	×	×	√
抗重放攻击	√	√	√
减少 U-KEY 丢失危害	-	√	√
用户身份隐私性	×	×	√
安全级别	低	中	高
执行效率	高	较高	较高

在该文方案的执行过程中,使用了随机数来保证数据的新鲜性,以防止重放攻击。其中,步骤(1)、(2)、(3)实现 U-KEY 和平台之间的双向身份验证,U-KEY 签名 TPM 产生的随机数,只有和声明身份一致的主体才拥有私钥,才能产生相应的签名,并且验证方利用 CPK 基于身份标识的特性,由身份标识极其方便地查找其公钥,来验证签名,此种方法属于标识认证[5],其安全性可依靠签名体制的安全性。重要的是,TPM 的 CPK 私钥(即是 EK 私钥)没有用于签名,只用于解密 $\{R_2\}PK_{TPM}$,且还在 TPM 中进行,很好地保护了 EK 私钥的安全性。因为只有 TPM 能够解密得到 R_2,同时再由 HASH 的单向性保证,所以通过 $H(ID_{TPM}PK_{AIK}R_2)$ 的比较就能够确信 TPM 与声称的身份一致,又很好地保证了 R_2 的机密性。步骤(4)中,由于 TPM 和 U-KEY 不直接存储用户原始口令,且是在用户先确认平台可信的情况下才输入口令的,口令自身的机密性、完整性、真实性和新鲜性得到了保证,自身安全性在通信和计算过程中都大大提高。U-KEY 中的口令模板和动态验证码加密传送,保证了口令模板和动态验证码的机密性,此处安全性可归结为加密机制的安全性。

步骤(5)中,匹配算法①、②和③是一个层级验证的过程,验证强度逐渐增大。首先,匹配算法①验证用户的合法性,这就实现了 U-KEY 对用户的认证,若验证通过,用户也可以根据结果来证实自己持有的 U-KEY 是合法的,从而实现了用户对 U-KEY 的验证;由于只有合法的 U-KEY 才可以提供用户的口令模板 Y 和动态验证码 AC,在通过了说明中①、②匹配算法后,TPM 可鉴别该 U-KEY 为合法用户所有,从而实现了 TPM

对用户身份的鉴别。匹配算法③是对平台主人的进一步强化认证,平台主人可以依靠它来判断前一次以平台主人身份进行登录的用户合法性,能够及时地发现问题,减少损失。匹配算法②和③将认证结果和新的动态验证码加密传送,实现了它们的机密性,此处安全性可归结为加密体制的安全性。当 U-KEY 和 TPM 均成功完成验证算法后,用户可根据 LCD 的提示来隐性地确认平台及 U-KEY 的合法性。在平台主人登录时,平台的成功开启是在更新完动态验证码之后进行的,这样就确保了 TPM 和 U-KEY 中动态验证码的及时更新,也为下一次的登录做好了准备。

4　在串空间模型下的安全性分析

串空间模型(SSM)是由 Fabrega、Herzog 和 Guttman 在文献[6]中提出,将安全协议的形式化分析技术推向一个新的高度。串空间模型是一种结合定理证明和协议迹的混合方法,由于它具有高效、严谨、直观、简洁等特点,受到研究人员的广泛关注。它不仅可以用于证明安全协议的正确性,还可以用于构造攻击,揭示安全协议的内在缺陷。

Gavin Lowe 研究了一系列认证特性[7],串空间模型非常适用于陈述和验证他提出的一致性。

一致性:若当一个协议主体 B 作为响应者使用 x 与他所认为的 A 作为发起者完成一轮协议时,确实存在一轮协议执行,其中,A 作为发起者也使用 x,并且认为他的响应者是 B。

秘密性:在串空间中,不存在节点 n,无论是正常节点还是入侵者节点,曾经把 x 未加保护地作为它的项。

Guttman 和 Fabrege 在文献[8]中提出了一种在串空间中简单有效的认证测试方法。该方法基于一个新的值的加密形式的改变,形成了认证测试边。主要通过两类认证测试,出测试和入测试,结合这两类测试,再加上自发测试和相关方法检验秘密性和认证属性。这种方法在很多安全协议中都成功测试。

输入认证测试:新数据 M 以一种加密形式被接收,那么只有一个诚实主体能够把 M 加密成这种形式。输出认证测试:新数据 M 以加密形式发送,那么只有一个诚实主体能够从这种形式中提取出它。自发测试:新数据 M 被接收,那么有主体能够发送它。

4.1　预备知识

给出一些项集合的含义:ID 为身份标识集合;R 为随机数集合;K 为协议使用的密钥集合,Key_P 表示入侵者掌握的密钥;D 为协议执行过程中主体传递的其他数据。其中,$K\cap(ID\cup R\cup D)=\emptyset$,$ID\cap R=\emptyset$,设 $T=ID\cup R\cup D$。

定理 1　假设 C 是 Σ 上的一个丛。$S\subseteq T\cup K$,$k\subseteq K$,且 $K\subseteq S\cup k^{-1}$,那么 $I_k[S]$是诚实的。

有关串空间模型的理论详见文献[6,8-9],这里不再赘述。下面给出在串空间模型下的该文方案的安全性证明。

4.2　该文方案的串空间模型

定义 1　(1)$TPM[D_1,D_2,D_3,D_4,D_5,ID_{TPM},ID_{U-KEY},R_1,R_2,PCR,Y,PW,AC,AC_1]$是串 $s\in\Sigma$ 的集合,且 s 具有迹$<+D_1R_1ID_{TPM}$,$-D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}$,$+D_3PK_{AIK}PC-RH(ID_{TPM}PK_{AIK}R_2)[ID_{TPM}D_3PCR]SK_{AIK}$,$-PW$,$-\{R_1ACID_{U-KEY}Y\}PK_{TPM}$,$+\{R_2D_4AC_1\}PK_{U-KEY}$,$-D_5>$,协议参与者中属于上述集合的是 TPM;

(2)$U-KEY[D_1,D_2,D_3,D_4,D_5,ID_{TPM},ID_{U-KEY},R_1,R_2,PCR,Y,AC,AC_1]$是一些串 $s\in\Sigma$ 的集合,且 s 具有迹$<-D_1R_1ID_{TPM}$,$+D_2ID_{U-KEY}[R_1ID_{U-KEY}]-SK_{U-KEY}\{R_2\}PK_{TPM}$,$-D_3PK_{AIK}PCRH(ID_{TPM}PK_{AIK}R_2)[ID_{TPM},D_3,PCR]SK_{AIK}$,$+\{R_1ACID_{U-KEY}Y\}PK_{TPM}$,$-\{R_2D_4AC_1\}PK_{U-KEY}$,$+D_5>$,协议参与者中属于上述集合的是 U-KEY;

(3)$U[PW]$是一些串的集合,且该串具有迹$<+PW>$,协议参与者中属于 U。

引理 1　集合 TPM、$U-KEY$ 和 U 是两两不相交的。

证明　因为 TPM 和 $U-KEY$ 这两个集合中元素迹的首项符号不同,所以 TPM 和 $U-KEY$ 是不相交的。TPM 和 $UTPM$ 不相交,$U-KEY$ 和 U 不相交是显然的。

定义 2　设入侵者串为 P,则方案的串空间 $\Sigma=Init\cup Serv\cup P$。

4.3　认证属性分析

下面利用认证测试的方法说明方案中的认证属性。

命题 1　C 是串空间 Σ 上的一个丛,s 是属于 $TPM[D_1,D_2,D_3,D_4,D_5,ID_{TPM},ID_{U-KEY},R_1,R_2,PCR,Y,PW,AC,AC_1]$的高为 2 的串,假设 $SK_{U-KEY}\notin Key_P$,R_1 唯一最初生成,则存在高至少为 2 的串 $s'\in U-KEY[D_1,D_2,D_3',D_4',D_5',ID_{TPM}',ID_{U-KEY},R_1,R_2',PCR',Y',AC',AC_1']$。

证明　首先指出 $TPM[D_1,D_2,D_3,D_4,D_5,ID_{TPM},ID_{U-KEY},R_1,R_2,PCR,Y,PW,AC,AC_1]$上的边$+D_1R_1ID_{TPM}\Rightarrow -D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}$ 是 $D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}$ 中 R_1 的入测试,其中 $SK_{U-KEY}\notin Key_P$。$D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}$ 是$<s,1>$中 R_1 的测试成分,因为它包含 R_1,且没有任何正常节点有这种类型的项作为真子项。根据文献[8]中入测试定理,存在正常节点 $m',m''\in C$,满足 $D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}$ 是节点 m''的成分,且边 $m'\Rightarrow m''$是 R_1 的转换边。

因为节点 m''是正的正常节点并且 $term(m'')=D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}$,所以对于某个 $s'\in U-KEY[D_1',D_2',D_3',D_4',D_5',ID_{TPM}',ID_{U-KEY}',R_1',R_2',PCR',Y',AC',AC_1'],m''=<s',2>$。因为 $term(<s',2>)=D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}$,所以得到 $D_1=D_1'$,$D_2=D_2'$,$ID_{U-KEY}=ID_{U-KEY}'$,$R_1=R_1'$。又因为在 C 中,$<s',1>\Rightarrow<s',2>$是转换边,所以 s'的高度至少是 2。

命题 2　C 是串空间 Σ 上的一个丛,s 是属于 $U-KEY[D_1,D_2,D_3,D_4,D_5,ID_{TPM},ID_{U-KEY},R_1,R_2,PCR,Y,AC,AC_1]$的高为 3 的串,假设 $SK_{TPM}\notin Key_P$,R_2 唯一最初生成,则存在高至少为 3 的串 $s'\in TPM[D_1,D_2,D_3,D_4',D_5',ID_{TPM},ID_{U-KEY},R_1,R_2,PCR,Y',PW',AC',AC_1']$。

证明　可以看到,边$+D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}\Rightarrow -D_3PK_{AIK}PCRH(ID_{TPM}PK_{AIK}R_2)$是 $D_2ID_{U-KEY}[R_1ID_{U-KEY}]SK_{U-KEY}\{R_2\}PK_{TPM}$ 中 R_2 的出测试,因此根据文献[8]中出测试定理,其他过程与命题 1 类似,就可得到命题结论。

同样类似,根据自发测试定理,很容易知道 $U-KEY$ 和 U 是相互认证的。又因为 $U-KEY$ 和 TPM 是相互认证的,所以 U 和 TPM 也是相互认证的。

4.4　秘密性和新鲜性分析

命题 3　C 是串空间 Σ 上的一个丛,R_1、AC 和 Y 均是唯一最初生成的,$SK_{TPM}\notin Key_P$,则 AC 和 Y 是秘密的和新鲜的。

证明　在丛 C 中,令 $S=\{R_1,AC,Y,SK_{TPM}\}$,$k=K\backslash PK_{TPM}$,则 $S\subseteq T\cup K$,$k\subseteq K$,$K\subseteq S\cup k^{-1}$,满足定理 1 的条件,即 $I_k[S]$是诚实的,不存在正常节点 $n\in C$,n 是理想 $I_k[S]$的入口点。于是,对于任何节点 $n\in C$,可得 $term(n)\notin S$,这样就保证了 AC 和 Y 的秘密性。

对于节点$-\{R_1ACID_{U-KEY}Y\}PK_{TPM}$,由自发测试定理知道,存在正常节点$+\{R_1ACID_{U-KEY}Y\}PK_{TPM}\in C$,又 R_1 唯一最初生成于正

常节点,易知存在正常节点$+D_1R_1ID_{TPM}$和$-\{R_1ACID_{U-KEY}Y\}PK_{TPM}$,满足$+D_1R_1ID_{TPM}\Rightarrow{}^{+}-\{R_1ACID_{U-KEY}Y\}PK_{TPM}$和$+D_1R_1ID_{TPM}\leq+\{R_1ACID_{U-KEY}Y\}PK_{TPM}\leq-\{R_1ACID_{U-KEY}Y\}PK_{TPM}$,所以由文献[9]新鲜性定义,项$\{R_1ACID_{U-KEY}Y\}PK_{TPM}$是新近的,即$AC$和$Y$是新鲜的。

与命题3的证明方法类似,也可以得出AC_1是秘密的和新鲜的。

至此,方案在串空间模型下的安全性得到了证明。

5 结论

由该文方案可知,基于身份标识的CPK组合公钥算法能很好地解决密钥管理的两个关键问题,与数字签名协议共同构成规模化标识认证算法。标识认证是新一代信息安全的"纲",在可信计算、可信交易、可信连接等领域中起着基础作用。CPK是一种具有独特优势的新技术,其私钥由中心统一生成发放,是一种直接的信任,用于可信计算时,可以确保高信任度,这对可信计算来说十分重要。该文根据可信计算组织的规范,利用CPK算法的诸多优势,使用静态口令和动态验证码相结合的方式,提出了一种基于CPK的可信平台用户登录认证方案,将认证和授权严格分开,并在串空间模型下证明了方案的安全性,结果表明该方案可以很好地解决可信平台的身份认证问题,为进一步建立可信计算环境提供了基础。

参考文献:

[1] 南相浩.CPK算法与标识认证[J].信息安全与通信保密,2006(9):12-16.
[2] 南湘浩,陈中.网络安全技术概论[M].北京:国防工业出版社,2003.
[3] Trusted Computing Group.TPM main specification version 1.2[EB/OL].(2007-08-08).http://www.trustedcomputinggroup.org.
[4] George P.User authentication with smart cards in trusted computing architecture[C]//Proceedings of the International Conference on Security and Management,Las Vegas,Nevada,USA,2004:25-31.
[5] 南相浩."认证"有关问题的讨论[J].计算机安全,2006(9):34.
[6] Thayer F,Herzog J C,Guttman J D.Strand space:Why is a security protocol correct?[C]//Proceedings of 1998 IEEE Symposium on Security and Privacy.Oakland:IEEE Computer Society Press,1998:160-171.
[7] Lowe G.A hierarchy of authentication specification[C]//Proceedings of 10th Computer Security Foundations Workshop.[S.l.]:IEEE Computer Society Press,1997:31-43.
[8] Guttman J D,Thayer F J.Authentication tests[C]//Proceedings of IEEE Symposium on Security and Privacy,Oakland CA,2000:96-109.
[9] Guttman J D.Security protocol design via authentication tests[C]//Proceedings of the 15th IEEE Computer Security Foundations Workshop.[S.l.]:IEEE Computer Society Press,2002:92-103.
[10] Trusted Computing Group.TCG specification architecture overview[EB/OL].(2007-08-08).http://www.trustedcomputinggroup.org/groups/TCG_1_2_Architecture_Overview.pdf.
[11] Oppliger R,Rytz R.Does trusted computing remedy computer security problems[J].Security & Privacy Magazine(IEEE),2005,3(2):16-19.
[12] 郑宇,何大可,何明星.基于可信计算的移动终端用户认证方案[J].计算机学报,2006,29(8):1255-1264.

(上接20页)

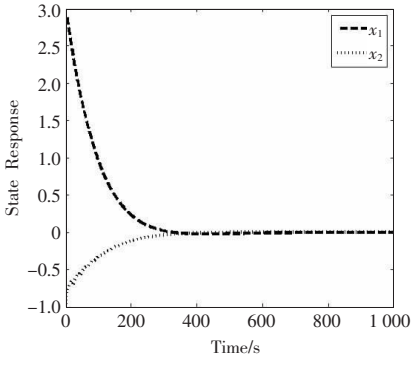

图2 系统的状态响应

知闭环系统(3)是指数稳定的。文献[10]研究了控制输入为$\boldsymbol{u}(t)=\boldsymbol{K}\boldsymbol{x}(t-\tau(k))$形式下、事先给定$H_\infty$范数上界$\gamma$情况下的$H_\infty$控制器设计问题。但并未给$H_\infty$范数上界$\gamma$该如何估计。由注4可知,$H_\infty$范数上界$\gamma$只需满足$\boldsymbol{B}_w-\gamma^2\boldsymbol{I}<0$即可。事实上,给定$\gamma=0.346\,4$,利用式(7),可解得控制器反馈增益为:$\boldsymbol{K}_1=[-0.800\,0,-3.206\,9]$,$\boldsymbol{K}_2=[1.196\,8,3.542\,4]$此时系统的状态反应如图2所示,由图2可知闭环系统(3)也是指数稳定的。然而当$\gamma=0.346\,4$时,文献[10]所给算法是失效的。这表明结果具有更弱的保守性。

5 结论

通过建立新的差分不等式,构造了一个新的Lyapunov函数,给出了一个改进的H_∞控制器设计算法。该算法克服了以往算法不能直接进行控制器求解、需要求解逆矩阵以及无法估计H_∞范数上界γ的缺点。仿真例子表明新算法是有效的。

参考文献:

[1] Zhang W,Michael S B,Stephen M P.Stability of networked control systems[J].IEEE Control Systems Magazine,2001,21(2):84-99.
[2] 赵虹,吴敏,刘国平.带时变时延的网络化控制系统控制器设计方法[J].信息与控制,2006,35(3):325-329.
[3] 张玉泉,钟秋海.时延和丢包网络控制系统的观测器设计[J].微计算机信息,2009,25(4):108-110.
[4] 孔德明,方华京.网络化控制系统连续动态输出反馈控制器设计[J].湖南大学学报,2007,34(12):35-40.
[5] 戴建国.时滞系统方法的网络控制系统的研究[J].计算机工程与应用,2009,45(20):13-15.
[6] 夏红伟,凌明祥,王常虹.不确定网络化控制系统保性能控制器设计[J].吉林大学学报,2008,38(1):173-177.
[7] 张玉泉,钟秋海,王林.具有时滞和丢包的网络化控制系统稳定性分析[J].北京理工大学学报,2008,28(4):329-333.
[8] 孙海义,李宁.随机网络控制系统的H_∞控制[J].沈阳建筑大学学报,2008,25(4):35-38.
[9] 彭晨,岳东,彭丽萍.网络控制中基于LMI的次优化允许等价时滞界研究[J].系统仿真学报,2007,19(2):369-387.
[10] 戴建国.时滞系统方法的网络化H_∞控制[J].计算机工程与应用,2009,45(19):1-5.
[11] Lee T,Radovic U.General decentralized stabilization of large-scale linear continuous and discrete time-delay systems[J].International Journal of Control,1987,46:2127-2140.