DOI:10.13229/j.cnki.jdxlgxb2009.03.047
第39卷 第3期 吉林大学学报(工学版) Vol.39 No.3
2009年5月 Journal of Jilin University (Engineering and Technology Edition) May 2009

基于信任服务的IBE系统

胡 亮[1],初剑峰[1],林 宇[1],王首道[2],金 哲[1]

(1.吉林大学 计算机科学与技术学院,长春 130012;2.北京工业大学 计算机科学与技术学院,北京 100124)

摘 要:针对现有的基于身份的加密(Identity Based Encryption,IBE)系统缺少标识管理、权限管理、密钥管理,没有解决域间互操作的问题。通过在现有的IBE系统上增加4个管理机制完善系统。设计了基于信任服务的IBE系统。介绍了该方案的系统架构和工作原理,并将该方案与PKI系统进行对比,对比结果证明了其高安全性、高效率、低成本的优势。

关键词:计算机系统结构;数据安全;基于身份的加密;信任服务;密钥管理

中图分类号:TP309.2 文献标识码:A 文章编号:1671-5497(2009)03-0737-06

IBE system based on trust service

HU Liang[1], CHU Jian-feng[1], LIN Yu[1], WANG Shou-dao[2], JIN Zhe[1]

(1. *College of Computer Science and Technology, Jilin University, Changchun* 130022, *China*; 2. *College of Computer Science and Technology, Beijing University of Technology, Beijing* 100124, *China*)

Abstract: The existing IBE system can avoid the problems of PKI, but in practical application it is lacking of identity management, authority management and key management, while it can not resolve the cross-domain interoperability. In this paper, we designed a new scheme: IBE system based on trust service, through add four mechanisms to the existing system to complete the system. The architecture and mechanism of the new scheme is introduced. This scheme validates the superiority of high security, high efficiency and low cost compared with PKI.

Key words: computer systems organization; data security; identity based encryption (IBE); trust service; key management

可信认证技术是现代信息安全的核心,当前两种主要的认证技术分别是PKI(Public Key Infrastructure,公钥基础设施)和IBE[1](Identity Based Encryption,基于身份加密)。可信认证技术是电子商务、电子政务、电子军务等电子交易活动建立信任的基础。PKI分散式的密钥产生方式使其更适用于密钥持有者的经济利益与密钥安全性具有直接关系的电子商务领域。IBE集中式的密钥产生方式使其更适用于要求基于公钥体系下的数据报可以定时销毁的电子政务和电子军务领域。

现有的IBE系统并不具有集中的密钥管理、标识管理、权限管理机制,这导致了IBE域内的用户不区分信任等级,所有用户可以无限制地使用系统全部服务,系统无法实现定时更换全部密钥等问题。现有的IBE系统也没有解决域间互操作问题,这导致了IBE无法解决可信身份移动和跨域授权等问题。因此现有的IBE系统难以实际部署在电子政务和电子军务中。作者提出了一个基于信任服务的IBE系统来解决这些问题,

收稿日期:2008-05-27.

基金项目:国家自然科学基金项目(60473099);教育部新世纪优秀人才支持计划基金项目(NCET-06-0300).

作者简介:胡亮(1968-),男,教授,博士生导师.研究方向:网格计算与网络安全.E-mail:hul@mail.jlu.edu.cn

通过在现有 IBE 系统上增加四个管理机制来完善系统,使其具有更强的实用性和安全性。

1 IBE 系统与 PKI 系统对比

PKI 系统与 IBE 系统的本质区别在于密钥产生方式。PKI[2] 属于分散式产生方式,私钥由用户自己生成,公钥随机计算生成,需第三方权威机构 CA(Certification Authority,认证中心)认证并公布,通讯双方通过 CA 利用数字证书进行身份认证,即认证的过程必须建立在对第三方的共同信任的基础之上。因此 PKI 更适用于密钥的持有者的经济利益与密钥安全性具有直接关系的电子商务领域。PKI 系统在证书管理恰当、用户私钥保存妥善的情况下,可以起到很好的身份认证功能,但是当需要互相安全通信的机构的数量急剧增长时,PKI 信任域之间的互连互通问题将成为 PKI 建设的瓶颈[3]。

IBE 属于集中式产生方式,IBE[4] 是 Shamir 在 1984 年最早提出来的,其初衷是简化电子邮件系统中的证书管理。IBE 系统是一种将用户公开的字符串信息(例如邮件地址、电话号码等)用作公钥的加密方式。它使得任何一对用户之间能够安全地通信以及在不需要交换私钥和公钥的情况下验证每一个人的签名,并且不需要保存密钥目录及第三方服务。IBE 系统中用户的私钥可由一个被称为 PKG (Private Key Generator,私钥生成器)的可信机构生成。

与 PKI 相比 IBE 具有以下优势:①IBE 系统将用户标识用作公钥,直接将安全策略同加密和授权方法绑定,认证过程无需经过证书交换,因此省去了一系列对证书的操作,避免了建设运行 CA 的困难[5];②IBE 的用户私钥由 PKG 生成,系统主密钥 s 改变,所有用户私钥随之改变($d_{ID}=sD_{ID}$)。因此 IBE 的密钥可以统一定时更换,并可规定私钥有效期限,系统安全性更高,危机后恢复更快[6];③IBE 采用了比 PKI 的 RSA 加密算法更优越的 ECC 加密算法。ECC 在与 RSA 同等长度的密钥下具有计算量小、储存空间少、带宽低、曲线资源丰富等优势[7]。

由于与 PKI 相比,IBE 更换系统全部密钥成本低、时间短、系统结构简单、安全性高,并且在更换密钥时系统可维持正常工作,因此 IBE 更适用于具有严格权限等级、要求基于公钥体系下的服务及数据报可以定时销毁的电子政务和电子军务领域。

2 基于信任服务的 IBE 系统

尽管 IBE 与 PKI 相比更适于电子政务、电子军务领域,但是要将现有的 IBE 实际部署在电子政务、电子军务系统中还存在很多问题有待解决[8]。针对现有的 IBE 系统存在的问题,本文设计了一个基于信任服务的 IBE 系统。这个系统具有集中式的信任服务,人们可以通过它安全、方便、透明地使用系统所支撑的具体服务。

基于信任服务的 IBE 系统由 4 个部分组成:定时更换的密钥管理机制、统一身份的标识管理机制、集中审计的权限管理机制、域间互连模块的管理机制。这 4 个机制彼此相互信任,四者之间的关系具体如图 1 所示。

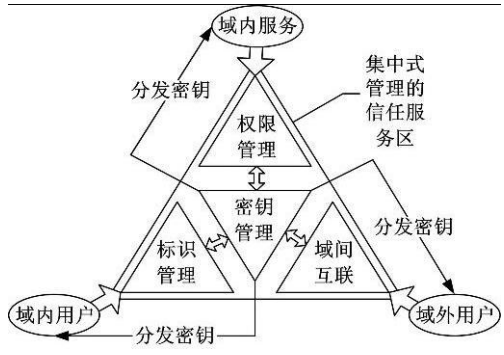

图 1 基于信任服务的 IBE 模型

Fig. 1 Model of IBE system based on trust service

标识管理是域内用户进入系统使用服务的入口。请求服务的域内用户首先向标识管理模块发送申请密钥的请求,标识管理机制对该用户进行认证,将通过认证的合法用户的请求报文用数字签名和数字信封进行封装,并发送给密钥管理模块。密钥管理模块只向标识管理模块认证为合法的用户发放私钥。

数字签名保证了请求报文来自正确的标识管理模块,数字信封保证了请求报文发给正确的密钥管理模块。数字签名和数字信封是系统中 4 个机制间相互信任的保障,是基于信任服务的 IBE 系统的核心算法。数字签名算法的签名步骤为:

(1)设 k 是一个安全参数,G 是定义在 F_p 上的椭圆曲线的基点,选择临时密钥对(k, R),并且满足 $R=kG=(p, q)$。

(2)n 为椭圆曲线系统参数,令 $r=p \bmod n$,如果 $r=0$,返回步骤(1)。

(3)计算待签报文 M 的 Hash 值 $H=Hash(M)$，并 H 将转换成整数 e。

(4)使用标识管理的当前私钥 d_{ID}，计算 $s\equiv k^{-1}(e+d_{ID})(\mathrm{mod}n)$，如果 $s=0$，返回步骤(1)。

(5)输出数字签名为 $S=(r,s)$。

数字签名算法的验证过程如下：

(1)如果 $r,s\notin[1,n-1]$，验证失败。

(2)计算待验证报文 M 的 Hash 值 $H=Hash(M)$，并将 H 转换成整数 e。

(3)计算 $u_1\equiv es^{-1}(\mathrm{mod}n)$，$u_2\equiv rs^{-1}(\mathrm{mod}n)$。

(4)计算 $R=E(p,q)=u_1G+u_2Q_{ID}$，如果 $R=0$，验证失败。

(5)令 $v=p\mathrm{mod}n$，如果 $v=r$ 验证成功，否则验证失败。

数字信封技术是把分组密码算法和非对称加密算法结合起来的混合密码机制。同时运用它们的优点是使加密传输安全可靠，工具有很高的效率。

2.1　定时更换的密钥管理机制

该机制的主要目的是实现一个自动的、安全的、定时的更换密钥的管理机制。该机制不仅为用户生成私钥，也为该系统所支持的服务、该系统的四个管理模块生成私钥。以实现用户与服务、用户与管理模块及四个管理模块之间的安全通信。该机制主要由三个部分构成，分别是：①以 EPOLL 为核心的 PKG 前置，用来实现高性能的服务端，满足高并发量的需求；②以 ECC 为核心的 PKG 后台，用来生成所有与用户标识对应的私钥列表；③随机数产生器，用来产生伪随机数。该机器在数据库中保存两张密钥列表，在其中一张使用的同时，另一张密钥列表生成新密钥。新密钥生成工作完成以后，可以随时或定时切换两张密钥列表，以此来实现系统全部用户密钥的瞬时更新。实现密钥管理机制的核心算法有两个，分别是私钥生成算法和随机数生成算法。私钥生成算法的具体流程如下：

初始化算法：初始化 PKG，生成通用的系统参数和主密钥 。

(1)设 k 是一个安全参数，选择一个 k-bit 并且满足 $p=2\mathrm{mod}3$，$p=6q-1$ 的素数(q 为一个大于 3 的素数)。设 $E(p,q)$是定义在 F_p 上的椭圆曲线。选择一个任意的具有 q 阶的点 $P\in E/F_p$。

(2)生成一个随机数 $s\in Z_q^*$，s 即为系统主密钥，s 通过 $p_{pub}=sP$ 方式秘密共享。

(3)选择 4 个哈希函数 $H:F_{p^2}\rightarrow\{0,1\}^n$，$G:\{0,1\}^*\rightarrow F_p$，$H_1:\{0,1\}^n\times\{0,1\}^n\rightarrow F_q$，$G_1:\{0,1\}^n\rightarrow\{0,1\}^n$。明文空间为 $M=\{0,1\}^n$。密文空间为 $C=E/F_p\times\{0,1\}^n$。系统参数为 $params=<p,n,P,P_{pub},G,H,G_1,H_1>$。主密钥为 $s\in Z_q$。

生成算法：PKG 将用户的标识映射到椭圆曲线上一个点 Q_{ID}，计算私钥 $d_{ID}=sQ_{ID}$，将 d_{ID}发送给用户。

随机数生成算法具体流程如下：

(1)取系统当前 8 个寄存器的值，并将其相加，再加上当前系统时间和 CPUID 生成字符串 S。

(2)用 SHA512 计算 S 的 Hash 值，得到字符串 r。

(3)根据 r 选取当前系统中的一个线程，取这个线程结构环境中的 8 个寄存器的值。对这 8 个寄存器的值进行初始化，并随机交换两个位置，即洗牌算法。

(4)将处理后得到的字符串与当前系统时间、CUPID 相加，转步骤(2)。

2.2　统一身份的标识管理机制

该机制的主要目的是实现 IBE 系统用户身份的统一管理。该机制把一个有限域划分为三个相互独立的子域：可信用户子域、可信服务子域、非可信子域，标识管理机制作为这三个子域的边界。标识管理机制具体工作原理如下：

(1)统一身份的标识命名规则：把可信任子域内的各个元素(用户、服务、管理模块)按照身份命名规则域标识＋全部子域标识＋个体身份，进行身份注册。

(2)单点登陆：用户只需从标识管理登陆，就能以这个身份使用域内和域外的所有授权的服务。

(3)标识管理规则：标识管理包括 4 个子模块，分别是用户身份注册机制、用户身份注销机制、用户个人信息维护机制、用户登录验证机制。

(4)对服务和信任服务的访问控制：当用户想要与域内/域外用户或服务交换数据时，用户可以从标识管理/域间互连模块获得相应经过授权的标识或服务列表。

(5)标识访问规则：当标识管理接收到一个用户的登录请求时，首先验证用户身份的合法性，若用户合法则将用户的请求报文用数字签名和数字

信封进行封装,并发送给密钥管理模块。同时标识管理分别向密钥管理模块、域间互连模块、权限管理模块注册该用户的标识、IP地址等特征信息。当标识管理接收到一个用户的安全退出请求时,标识管理向其他3个模块注销该用户。

2.3 集中审计的权限管理机制

权限管理机制是基于信任体系的合法用户提交具体服务请求时,信任体系提供的一种安全策略。它可以保证体系的安全粒度细化。它负责对注册的服务进行管理,是责任追究的支撑系统之一。权限管理机制具体工作原理如下:

(1)集中审计:当用户请求某一个服务的权限时,这个服务首先向权限管理机制提交审计。如果审计通过则返回服务,允许该用户使用这个服务的这个权限。每个服务的门限值和用户的权限值都是由权限管理机构集中管理的。管理可以针对每个用户和每个服务细化处理,有利于降低维护成本,提高管理的灵活性。

(2)服务注册:当有新的服务开通时,权限管理机制会根据需要设定其门限值。

(3)门限规则:每个服务都有自己的门限值,合法用户对应每个服务都有自己的权限值,当且仅当用户的权限值大于服务的门限值时,权限管理机制才将这个服务授权给这个用户使用。

(4)跨域授权:实现可信区域外的用户可以访问域内的服务的过程。

(5)信任继承:一个服务的多个已授权用户可以授予一个合法用户对这个服务的使用权,未注册服务无法被授权。信任继承算法是权限管理的核心算法。信任继承算法的具体过程如下:

1)定义3个函数:信任继承函数 $Request()\in\{N, N>4\}$,用户当前权限值查询函数 $Grant()\in\{N, N>4\}$,服务门限值查询函数 $Threshold()\in\{N, N>4\}$。

设 $Grant(\text{user\_a}, \text{service\_x}, \text{degree\_3})<Threshold(\text{service\_x}, \text{degree\_3})$;

$Grant(\text{user\_b}, \text{service\_x}, \text{degree\_3})>Threshold(\text{service\_x}, \text{degree\_3})$;

$Grant(\text{user\_c}, \text{service\_x}, \text{degree\_3})>Threshold(\text{service\_x}, \text{degree\_3})$。

2)设user_a, user_b, user_c表示三个用户,service_x表示当前服务,每个服务定义若干个权限区,处于不同权限区的用户具有使用该服务不同的权限级别,degree_3表示服务内的第三个权限区的名称。若user_a想以degree_3的权限级别来使用service_x服务,则user_a需要向已具有该权限的用户user_b申请信任继承来增加自己的权限值。user_a计算权限的具体算法为:

$Grant(\text{user\_a}, \text{service\_x}, \text{degree\_3})=Grant(\text{user\_a}, \text{service\_x}, \text{degree\_3})+\text{Request}(\text{user\_a}, \text{service\_x}, \text{degree\_3}, \text{user\_b})$。

3)定义2个函数:取最小值函数min(),取地板值函数 $floor()$。设 $R_{ax3b}=Request(\text{user\_a}, \text{service\_x}, \text{degree\_3}, \text{user\_b})$, $G_{bx3}=Grant(\text{user\_b}, \text{service\_x}, \text{degree\_3})$, $T_{x3}=Threshold(\text{service\_x}, \text{degree\_3})$, $T_{x4}=Threshold(\text{service\_x}, \text{degree\_4})$。

则 $R_{ax3b}=\min(|G_{bx3}-T_{x3}|, |T_{x4}-T_{x3}|)-floor(2(G_{bx3}-T_{x3})^{0.5}(T_{x4}-T_{x3})^{0.5})$。

4)如果user_a获得信任继承后,权限值仍小于门限值,即:$Grant(\text{user\_a}, \text{service\_x}, \text{degree\_3})<Threshold(\text{service\_x}, \text{degree\_3})$,则user_a需要user_b和user_c联席授权,以实现user_a的权限值大于degree_3的门限值。如果服务门限值 $Threshold()$过高,则需多人联席授权。

2.4 域间互连模块的管理机制

该机制的主要功能是解决域间可信身份移动和跨域授权两个问题。域间互连模块为各个信任域内的可信服务和域外用户都生成本域的映射,分别称为虚服务和虚用户,以此来保证域外用户的跨域身份移动的责任链条完整性。由虚服务构成的集合称为静态服务信任列表,由虚用户构成的集合称为动态用户信任列表。用户与标识管理建立可信关系后,由于域间互连模块信任标识管理,所以域间互连模块为用户提供虚服务查询业务,并且为用户在目标域生成虚用户映射,从而实现了身份移动。跨域授权则建立在可信身份移动的基础之上,依靠域间互连模块和权限管理模块实现,虚用户与虚服务机制保证了跨域授权的安全性和责任链条的完整性。

基于信任服务的IBE系统工作流程如图2所示。

成为合法用户:

(1)登录:当标识管理接收到一个用户的登录申请时,首先验证用户的合法性,若用户合法则将用户的请求报文用数字签名和数字信封进行封装,并记录该用户的特征信息。

(2)注册:标识管理模块分别向密钥管理模

块、域间互连模块、权限管理模块注册该用户的标识、IP 地址等特征信息。

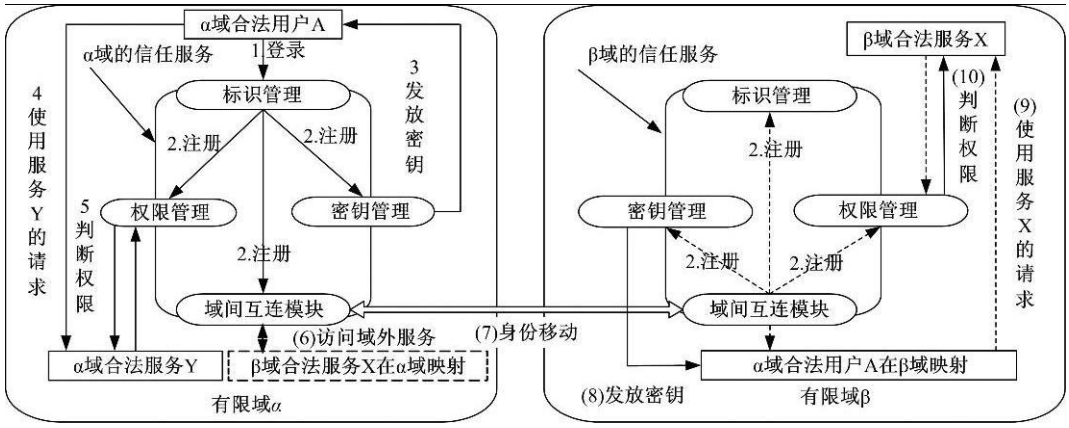

图 2　基于信任服务的 IBE 系统工作原理

Fig. 2　Principle of IBE system based on trust service

访问域内服务：

(3)发放密钥：密钥管理只为标识管理认证为合法的用户发放密钥。给 α 域合法用户 A 发放密钥。

(4)使用服务 Y 的请求：用户 A 请求 α 域合法服务 Y，系统返回给用户可以成功使用信任体系下的相应服务的信息。

(5)判断权限：由权限管理模块判断一个用户是否有权限使用服务。如果用户有权使用，该服务则使用用户的特征信息和封装的报文的为对称密钥，对数据报进行 AES 加密[9]，与用户通信。

访问域外服务：

(6)访问域外服务：如果 α 域内用户 A 要使用β 域的服务 Y，首先该用户要通过域间互连模块查询β 域的服务入口。

(7)身份移动：α 的域间互连模块向β 域的域间互连模块提交该用户的特征信息、封装的请求报文、域签名(由域间互联模块签发)和具体的服务请求。从信任传递的链条看，由于域间互连模块信任标识管理，所以域间互连模块为用户提供虚服务查询业务，并且为用户在目标域生成虚用户映射，从而实现了身份移动。

(8)发放密钥：β 域的密钥管理模块将密钥发放给 α 域合法用户 A 在β 域的映射，由于是 α 域的域间互连模块建立的用户 A 与 α 域合法用户 A 在β 域的映射的关系，所以 α 域的域间互连模块可以把密钥传递给用户 A。

(9)使用服务 X 的请求：α 域合法用户 A 在β 域映射请求β 域合法服务 X，系统返回给用户可以成功使用信任体系下的相应服务的信息。

(10)判断权限：β 域的服务接收到业务请求时，同样地向β 域的权限管理模块提交权限审核，如果权限合理，则用户 A 可以安全地使用β 域的服务 Y。

基于信任服务的 IBE 系统具体流程如图 3 所示。

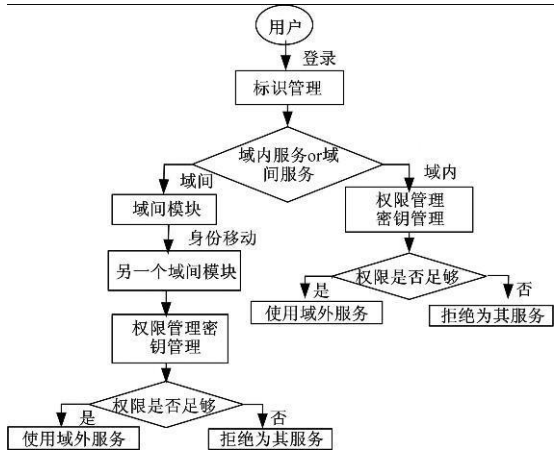

图 3　跨域授权流程图

Fig. 3　Flow chart of cross-domain authorization

3　基于信任服务的 IBE 与 PKI 对比

密钥的分发和管理分静态和动态两种方式。PKI 的公钥保存在证书中，证书采用静态分发，动态管理的模式，LDAP（Lightweight Directory Access Protocol，轻量目录访问协议）目录库在线运行，其维护量很大，运行费用也很高。PKI 用户遗失私钥或用户离职需要更改或撤销证书是一件非常困难的事情。通常的做法是 CA 维护 CRL(Certificate Revocation Lists，证书

废除列表)。假若发送方发出的证书已经被更改或撤销,而接收方在接收消息时没有检测 CRL,只使用保存在本机上的证书,就可能使机密资料被未授权者得到。

基于信任服务的 IBE 系统密钥采用动态分发、动态管理的模式。与 PKI 相比,基于信任服务的 IBE 系统通过定时更换的密钥管理机制切换保存在数据库中的两张密钥表就可以实现系统全部用户密钥的瞬间更新,因此新方案的密钥更换成本与 PKI 相比更低,可以很好地达到电子政务、电子军务要求体系内过期数据定时销毁的要求。与此同时,新方案也极大地提高了系统的安全性和保密性,在 PKI 系统中如果用户私钥丢失,并且没有及时上报到 CA 中心,将导致所有以这个私钥加密的数据泄露,而在新方案中即使私钥丢失,攻击者也只能得到一小段时间内的加密数据,损失要远远小于 PKI。基于信任服务的 IBE 系统与 PKI 系统的具体差异见表 1。

表 1 基于信任服务的 **IBE** 系统与 **PKI** 系统对比

Table 1 Compare IBE system based on trust service with PKI

密钥管理方式	基于信任服务的 IBE 系统	PKI 系统
密钥实体	身份或者标识	数字证书
密钥生成算法	ECC 椭圆曲线	RSA 大素数分解
密钥产生方式	集中式	分散式
密钥分发方式	动态分发	无
密钥管理方式	动态管理	静态管理
密钥更换成本	低	高
体系内过期数据	定时销毁	无法实现定时销毁
用户私钥丢失对系统的影响	小	大
公钥存储方式	公钥即身份	存储在在线 LDAP 目录库
私钥存储方式	PKG 生成	用户自己保存
随时间推移信任体系的安全性变化	稳定	逐渐降低
适用领域	电子政务及电子军务	电子商务

4 结束语

针对现有的 IBE 系统在具体实施过程中存在的问题设计了一个扩充了服务的新的 IBE 系统:基于信任服务的 IBE 系统,使其与原系统相比更具实用性,更加符合电子政务、电子军务高安全性、高效率、高稳定性、数据能够定时销毁、用户权限划分明确的要求。

参考文献:

[1] 胡德斌,王金玲,胡亮,等. 基于身份别名的加入辅助认证方的 IBE 方案[J]. 吉林大学学报:工学版,2008,38(2):419-422.
Hu De-bin, Wang Jin-ling, Hu Liang, et al. ID alias IBE scheme with a trusted third party[J]. Journal of Jilin University (Engineering and Technology Edition), 2008, 38(2): 419-422.

[2] 孟桂娥,董玮文,杨宇航. 公钥基础设施 PKI 的设计[J]. 计算机工程,2001,27(6):111-113.
Meng Gui-e, Dong Wei-wen, Yang Yu-hang. Design of public key infrastructure system[J]. Computer Engineering, 2001, 27(6): 111-113.

[3] 刘远航,鞠九滨. 交叉认证问题研究综述[R]. 北京:全国网络与信息安全技术研讨会,2004.

[4] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C] //Kilian J CRYPTO 2001, Berlin: Springer-Verlag, 2001.

[5] 石艳荣,贺永强. PKI 和基于身份加密的比较[J]. 微计算机信息,2008,24(1-2):83-84.
Shi Yan-rong, He Yong-qiang. A comparison between PKI and IBE[J]. Microcomputer Information, 2008, 24(1/2): 83-84.

[6] 林宇,于孟涛,胡亮,等. 基于 IBE 和数字水印的电子印章解决方案[J]. 吉林大学学报:信息科学版,2007,25(4):406-411.
Lin Yu, Yu Meng-tao, Hu Liang, et al. Scheme of electronic seal based on IBE and digital watermark [J]. Journal of Jilin University (Information and Science Edition), 2007, 25(4): 406-411.

[7] 郑玉丽,申艳光. 对椭圆曲线密码系统性能的几点认识[J]. 网络安全技术与应用,2006(2):72-73.
Zheng Yu-li, Shen Yan-guang. Acknowledge of several characters of elliptic curve cryptosystem[J]. Network Security Technology and Application, 2006 (2): 72-73.

[8] 郑晓林,荆继武. 基于身份加密的密钥管理方案研究[J]. 计算机工程,2006,32(21),145-147.
Zheng Xiao-lin, Jing Ji-wu. Research on key management schemes for IBE[J]. Computer Engineering, 2006, 32(21), 145-147.

[9] 袁巍,胡亮,林宇,等. AES 算法的结构分析与优化实现[J]. 吉林大学学报:工学版,2008,46(5):885—890.
Yuan Wei, Hu Liang, Lin Yu, et al. Structure analysis and optimization implementation of the algorithm of advanced encryption standard[J]. Journal of Jilin University (Engineering and Technology Edition), 2008, 46(5): 885-890.