IBE 体系的密钥管理机制

胡 亮 初剑峰 林海群 袁 巍 赵 阔
(吉林大学计算机科学与技术学院 长春 130012)

摘 要 现有 IBE 的密钥管理机制存在许多问题和不足,例如用户私钥的安全分发问题(缺少一个安全的、定时的、自动的密钥更换机制)以及如何保证数据报的保密性、完整性、不可伪造性和不可否认性等问题.文中针对以上问题,提出一种改进的密钥管理方案,即密钥管理机制.它能够定时更换域内密钥并且安全分发,同时使用安全服务来保障数据报的保密性、完整性、不可伪造性和不可否认性.数据报的安全服务包括双重数字签名、数字信封以及数字时间戳.最后文章使用随机预言模型 RO(Random Oracle)对文中提出的相关协议给出了安全性证明.

关键词 IBE;密钥管理;双重数字签名;可证明安全性;密钥分发;密钥定时更换
中图法分类号 TP393 **DOI** 号: 10.3724/SP.J.1016.2009.00543

The Key Management Mechanism of IBE System

HU Liang CHU Jian-Feng LIN Hai-Qun YUAN Wei ZHAO Kuo
(*College of Computer Science and Technology, Jilin University, Changchun* 130012)

Abstract There still exist several problems in the prototype of IBE proposed by Boneh and Franklin, such as how to distribute private keys safely, the lack of a secure timing key replaced management mechanism and how to ensure message security of privacy, integrity and non-forgeability. Upon these above, a new scheme of the improved key management mechanism of IBE has been put forward, which is named as the trustworthy key management mechanism of IBE system. And it can change users' private keys regularly in this domain, which are subsequently distributed safely. Meanwhile it can also guarantee message security of privacy, integrity and non-forgeability by security service, which mainly includes Double Digital Signature, Digital Envelope and Digital Time-stamping. Finally, the proposed network protocols are proved to be secure by RO (Random Oracle) model.

Keywords IBE; key management mechanism; double digital signature; provable security; keys distribution; keys timing replacement

1 引 言

随着信息网络的基础性、全局性作用日益增强,传统的网络理论与技术,尤其是网络安全,已经不能满足网络发展的需要,提供系统的安全可信的服务已经成为网络研究的新趋势.可信的网络应该是网络和用户的行为及其结果总是可预期与可管理的[1],它能够保障所支撑的服务的安全性和可生存性[2].

收稿日期: 2008-09-17; 最终修改稿收到日期: 2009-02-16.本课题得到国家自然科学基金(60873235, 60473099)、教育部新世纪优秀人才支持计划(NCET-06-0300)和吉林省重点项目(20080318)资助.胡 亮, 男, 1968 年生, 博士, 教授, 博士生导师, 主要研究领域为网格计算与网络安全. E-mail: hul@jlu.edu.cn. 初剑峰, 男, 1978 年生, 博士研究生, 研究方向为计算机系统结构. 林海群, 女, 1985 年生, 硕士研究生, 研究方向为网络信息安全. 袁 巍, 男, 1984 年生, 硕士研究生, 研究方向为网络信息安全. 赵 阔(通信作者), 男, 1977 年生, 博士, 研究方向为计算机系统结构. E-mail: zhaokuo@jlu.edu.cn

以 PKI(Public Key Infrastructure)为广泛应用的公钥体系已经成为国际标准 X.509. 但是和 PKI 具有相同职能的公钥体系模型 IBE[3] (Identity-based Encryption)却因自身的不完善而没有得到实际应用. IBE 将用户公开的字符串信息(如邮件地址等)用作公钥的加密方式. IBE 原型[4] 系统是由 Boneh 和 Franklin 在 2001 年提出的, 它是一个以密钥生成中心 PKG(Private Key Generate)为主体的系统. 但它不是一套完整的、可信的公钥体系. 虽然后人在签名方案[5]、签密方案[6]、加密方案[7-8]、构架方案[9]、密钥分发方案[10]、授权方案[11] 等诸多方面做出改进和完善, 但是仍然存在许多问题和不足, 例如:

(1) 体系内的责任链条不连贯完整.

(2) 如何保证身份不会被伪造.

(3) 如何安全地分发私钥.

(4) 如何实现电子政务或其它领域的特定需求, 即体系内的所有数据报务必定时销毁.

(5) 如何保证体系定时更换密钥不会出现系统瓶颈.

(6) 大的数据报报文如何加密传输.

针对以上问题, 本文首先引出基于信任服务的 IBE 体系, 然后重点论述该体系核心的密钥管理机制. 其中的双重数字签名可以保证责任链条连贯完整; 数字时间戳服务用来避免重放攻击; 数字信封用来实现大的数据报报文如何加密传输; 密钥分发模块是解决如何安全分发私钥的问题, 密钥定时更换模块是解决体系内的所有数据报是否定时销毁的问题. 本文最后使用随机预言模型对文中提出的相关协议给出了安全性证明.

2 基于信任服务的 IBE 体系

基于信任服务的 IBE 体系作为新一代网络体系[12] 的框架方案, 正是由于它有别于 PKI 的密钥管理方案, 使它更适用于电子政务领域及电子军务领域. 它是由密钥管理、标识管理、权限管理和域间互联机制组成的集中式管理的公钥体系, 如图 1 所示.

(1) 密钥管理机制为合法用户生成对应用户标识的私钥, 同时它还需要完成系统初始化以及密钥定时更换. 它是整个系统的核心与支撑.

(2) 标识管理机制则主要针对信任域内用户的管理问题, 该机制主要完成用户的标识管理, 包括用户的注册、用户身份的验证、维护以及注销等问题. 它是域内用户使用该系统的入口.

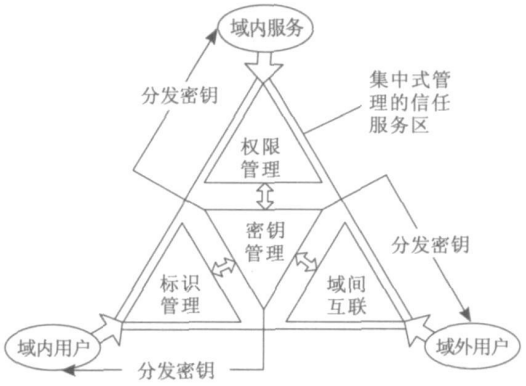

图 1 基于信任服务的 IBE 体系结构

(3) 权限管理机制主要是通过对域内服务和相应权限的管理来保证合法用户能够得到恰当的权限来使用域内的服务和资源, 防止用户越权. 它可以使体系的权限粒度细化.

(4) 域间互联机制主要是解决域间可信身份移动和跨域授权问题, 即实现同构信任域或异构信任域之间的互操作.

由图 1 可以看出, 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以及域间互连机制的管理机制形成一个集中式管理的信任服务区. 密钥管理机制只信任在信任服务区内的权限管理、标识管理和域内互联机制, 他们之间的通信采用的是可信的紧耦合方式. 同时密钥管理机制只为权限管理、标识管理和域内互联机制以及它们所信任的用户和服务发放私钥.

密钥管理机制(Key Management Mechanism, KMM)作为基于信任服务的 IBE 体系的核心机制, 是本文的研究重点. 它由以下 3 个部分组成: 密钥分发模块、密钥定时更换模块和数据报的安全服务, 三者之间的关系如图 2 所示.

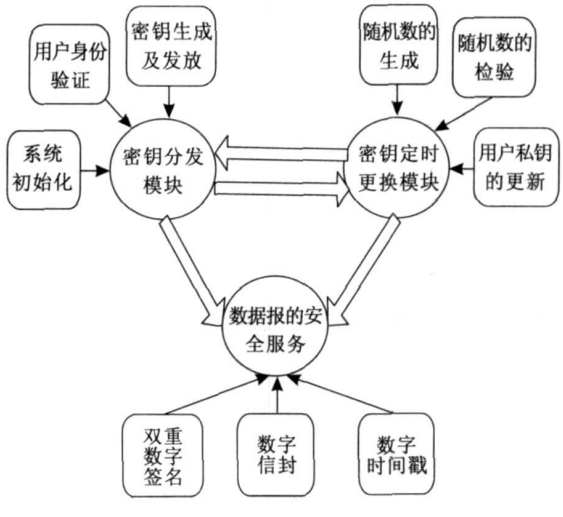

图 2 密钥管理机制

3　密钥分发模块

3.1　系统初始化

系统的初始化过程主要包括密钥管理机制的系统参数初始化、域内用户的系统参数初始化.

(1) 系统参数的初始化过程. 选取一个素数有限域 F_p, 并且生成一条安全的椭圆曲线[13], 产生系统参数 $T=(p, a, b, G, P_{pub}, q, h, H, I, H_1, I_1)$. 具体过程如下:

①选取域元素 $a, b\in F_p$ 满足方程 E: $y^2\equiv x^3+a\cdot x+b \pmod p$. 其中 $4\cdot a^3+27\cdot b^2\neq 0 \pmod p$.

②在曲线 $E(F_p)$ 上选取一个基点 $G=(x_G, y_G)$, 并计算 G 点的阶 q, $h=\sharp E(F_p)/q$. 这些参数满足如下限制: $\sharp E(F_p)\neq p$; $p^B\neq 1 \pmod q$, 其中 $1\leq B<20$; $h\leq 4$. 同时, 根据椭圆曲线算法本身的需要, p, q 还要满足 $p=2 \bmod 3$ 并且 $p=6q-1$.

③生成一个随机数 $s\in Z_q^*$, s 即为系统的主密钥, 并计算 $P_{pub}=s\cdot G$.

④选择 4 个 Hash 函数:

H: $F_{n^2}\rightarrow\{0, 1\}^n$,

I: $F_{n^2}\rightarrow\{0, 1\}^n$,

H_1: $\{0, 1\}^n\times\{0, 1\}^n\rightarrow F_q$,

I_1: $\{0, 1\}^n\rightarrow\{0, 1\}^n$.

⑤将标识管理、权限管理以及域间互联机制对应的标识 ID_{id}、ID_{pr}、ID_{dm} 映射到椭圆曲线 $E(F_p)$ 上的点 P_{id}, P_{pr}, P_{dm}, 并生成对应的私钥 $PID_{id}=s\cdot P_{id}$, $PID_{pr}=s\cdot P_{pr}$, $PID_{dm}=s\cdot P_{dm}$.

(2) 用户的初始化过程. 每个域内用户都必须在标识管理机制注册并提供唯一的用户标识、登陆密码以及用户其它的属性信息. 用户注册成功之后, 由标识管理机制激活并给这些域内用户发放系统参数 $T=(p, a, b, G, P_{pub}, q, h, H, I, H_1, I_1)$. 同时, 为了实现双重数字签名, 域内用户还必须生成私签私钥 K_U. 设一个域内用户为 U, 则该用户标识为 ID_U. 用户 U 选择一个随机数 $m_U\in Z_q^*$ 作为自己的主密钥 s', 然后根据系统给定的参数 T, 计算出 $PU_{pub}=m_U\cdot G$. 并将标识 ID_U 映射到椭圆曲线 $E(F_p)$ 上的一个点 P_I, 计算对应于标识 ID_U 的私签签名私钥 $K_U=m_U P_I$, K_U 对应的椭圆曲线参数为 $T'=(p, a, b, G, PU_{pub}, q, h, H, I, H_1, I_1)$.

3.2　用户身份验证

在初始化过程完成之后, 域内用户可以请求发放私钥. 密钥管理机制与标识管理机制之间是互信的, 因此在基于信任服务的 IBE 体系下, 域内用户的身份确认过程交给标识管理机制完成, 这样既可保证密钥管理机制的安全性, 又可减轻密钥管理机制负担. 在对用户的身份验证完成之后, 标识管理机制才会通知密钥管理机制生成对应于该用户标识的私钥并安全分发到用户手中, 具体的过程如下:

(1) 用户 U 将自己在标识管理机制注册的密码属性 k_{mu} 用散列函数得到该密码属性的消息散列值: $k_m=HASH(k_{mu})$.

(2) 用户 U 发送加密数据报 M, 并发送给标识管理机制:

$$M=\{ID_{id}, DM_{id}, ID_u, PU_{pub}, k_m, t, w_{01}\},$$

其中, ID_{id} 是标识管理机制的标识; DM_{id} 为域标识, 即为了实现域间互联时区分不同的域; t 是当前的日期和时间; w_{01} 为一个业务代码, 表示该报文为请求发放私钥报文.

由于该数据报 M 是短数据报, 因此可以直接用标识管理机制的标识 ID_{id} 和系统参数 T 加密数据报 M, 产生密文 X. 加密过程: 根据系统参数 T 将标识管理机制的标识 ID_{id} 映射到一个 q 阶的点, 同时选择一个随机串 σ, 设置 $r=H_1(\sigma, M)$, 计算密文 $X=EC(M, r, ID_{id}, P_{pub})$, 其中函数 EC 为椭圆曲线加密算法.

(3) 标识管理机制收到密文 X 之后用自己的私钥 PID_{id} 解密报文 X, 获得明文 $M=DC(X, PID_{id}, P_{pub})$, 函数 DC 为椭圆曲线解密函数, 若函数测试不成功, 则退出并拒绝该密文; 否则标识管理确定收到的消息即为报文 M.

在得到的解密消息中, 标识管理机制依次验证域标识 DM_{id}、接收者标识 ID_{id} 是否正确, 发送者用户 U 的标识 ID_{id} 是否为合法用户并且判断用户 U 的标识 ID_{id} 与密码属性对应的散列值 k_m 是否有映射关系. 若通过以上验证过程, 则说明该用户的身份验证过程成功; 否则失败.

(4) 在验证了用户 U 的身份之后, 标识管理机给该用户发送应答报文: $M1=\{ID_U, t, w_{10}, \beta\}$. 其中 w_{10} 同样也是一个业务代码, 表示该报文为请求发放私钥报文的应答报文. 字段 β 为一个结果字段, 当 $\beta=0$ 时说明身份验证成功; 当 $\beta=1$ 时, 则说明因为该身份没有激活而导致身份验证失败.

(5) 在给用户 U 发送应答报文 $M1$ 时, 使用用户 U 的标识 ID_U 和他的椭圆曲线参数 $T'=(p, a, b, G, PU_{pub}, q, h, H, I, H_1, I_1)$ 来加密报文 $M1$, 得到密文 $M2$: $M2=EC(M1, r, ID_U, PU_{pub})$ 并附上标识管

理机制的签名 $SIG_{PID_{id}}(hash(M1), P_{pub})$. 函数 SIG 是椭圆曲线数字签名算法.

上述过程安全地完成了标识管理机制对用户 U 的身份验证过程,即验证了用户 U 是否为系统合法用户.若验证成功,标识管理机把用户 U 的请求给密钥管理机制,然后由密钥管理机制为用户 U 生成对应于该用户标识 ID_U 的私钥并发放.

3.3 用户私钥的生成及发放

在基于信任服务的 IBE 体系下,密钥管理机制只信任标识管理机制所信任的域内用户,只对这些用户发放私钥.在标识管理机制验证了用户 U 的合法身份后,就将由密钥管理机制为该合法用户生成对应用户身份标识的私钥.用户私钥的生成及发放过程是基于 3 1 节的系统初始化过程实现的,具体过程如下:

(1)密钥管理机制将用户 U 的标识 ID_U 映射到椭圆曲线 $E(F_p)$ 上的一个点 P_U 并计算用户 U 的私钥 $PID_U = s \cdot P_U$,同时将该用户的私钥存入密钥表中.当密钥管理机制收到标识管理机制发送用户请求报文时就立刻从密钥表中查找到该请求用户 U 的私钥 PID_U 并附上该私钥的有效期 Lt 后将消息 $M = (PID_U, Lt)$ 传送给标识管理机制.

(2)标识管理机制生成一个随机串 σ,设置 $r = H_1(\sigma, M)$ 后加密消息 M 得密文 X: $X = EC(M, r, ID_U, PU_{pub})$ 并用标识管理机制的私钥签名得 $SIG_{PID_{id}}(hash(M), P_{pub})$,并同时将密文 X 和签名 $\{EC(M, r, ID_U, PU_{pub}), SIG_{PID_{id}}(hash(M), P_{pub})\}$ 发送给用户 U.

(3)用户 U 收到消息后,验证标识管理机制的签名并用自己生成的私签私钥 K_U 解密消息获得自己的私钥 PID_U 以及私钥的有效期: $(PID_U, Lt) = DC(X, K_U, PU_{pub})$.

私钥有效期表示发放给该用户私钥的使用期限,过了该时间期限后密钥管理机制会自动更换主密钥并同时更换所有可信用户的私钥,这就是密钥的定时更换模块.

4 密钥定时更换模块

密钥分发模块解决了域内用户私钥的安全分发问题.但是 IBE 系统的私钥安全性则需要通过密钥定时更换模块来维护,具体原因有以下 3 点:

(1)椭圆曲线的密码长度越长,则系统的安全性也越高[14],但是密钥长度越长,加解密和签名等操作的实现时间也比较长,同时密钥管理机制根据用户身份计算用户私钥所花费的开销也比较大.

(2)随着时间推移,域内的恶意攻击者可能会通过收集用户的公私钥对来尝试破解系统的主密钥.虽然主密钥的长度越长,被猜解出来的可能性也越小,但是利用如 Pollard' s ρ[8] 这样的算法或者其他更高效的方法,仍然存在猜解出系统主密钥的可能性.

(3)某些有特定要求的系统如电子政务系统等要求所有的数据报能够定时销毁,而这只可以通过密钥管理机制定时更换所有用户的私钥来实现.

综合以上原因,在不增加密钥长度的前提下,又要保证体系拥有很高的安全强度,我们可以通过密钥管理机制下的密钥定时更换模块来实现.并且在 IBE 体系下,私钥是集中式管理的,即所有私钥都是根据系统的主密钥生成得来.一旦密钥管理机制更换了自己的主密钥,它就更换了域内所有的私钥.因此 IBE 的密钥机制是密钥的定时更换的前提条件.

所谓密钥定时更换模块是指系统的密钥管理机制将定期更换自己的主密钥,同时根据更换后系统的主密钥重新生成域内的私钥,并发放给对应标识.图 3 给出了密钥定时更换模块的算法流程.

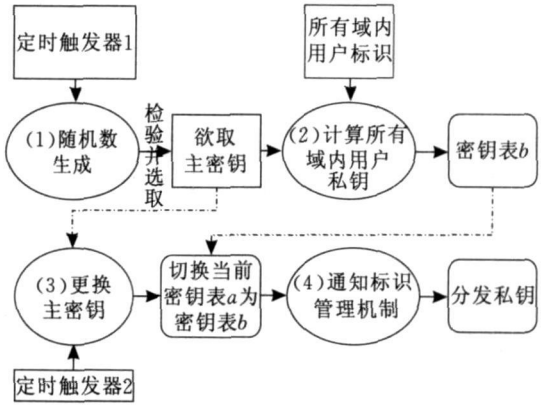

图 3 密钥定时更换模块

(1)随机数的生成,也就是主密钥的生成过程.它由标准的 BBS[15] 随机数算法生成,再用 χ^2 检验[15] 方法检验随机数的随机性,满足要求的则可以被选取作为新的主密钥.

(2)根据欲取的主密钥,首先计算出欲更换的主密钥下的系统参数 $P'_{pub} = s' \cdot G$,再计算域内所有用户的私钥 $PID = s' \cdot P$.并且存入另一密钥表 b 中.

(3)当产生定时触发时,首先向所有机制、所有域内用户发放新的系统参数 $T = (p, a, b, G, P'_{pub}, q, h, H, I, H_1, I_1)$ 并且将事先产生的密钥表 b 作为当前密钥表.之所以需要事先产生欲更换的主密钥下

的所有域内用户的私钥是为了要实现当前域内用户所使用的密钥表 a 与预先产生的密钥表 b 之间的瞬间切换操作.

(4) 通知标识管理机制, 由标识管理机制发送广播消息给域内所有用户申请更换私钥并为用户发放私钥. 由于更新的用户私钥都已实现产生, 这样所有域内用户无需等待系统生成即可瞬间获得用户对应的私钥.

由于电子军务或电子政务的特定要求, 所有数据报务必定时销毁. 密钥定时更换虽可满足该要求, 但也会给密钥分发模块带来一个处理峰值. 下面对这种情况进行评估, 密钥定时更换模块应在公钥体系处于空闲时段(例如每一个月的最后一个星期日凌晨), 更换系统主密钥, 计算出系统内全部身份对应的私钥并存入中央数据库内. 然后激活密钥分发模块推送在线用户更换私钥, 对于离线用户, 私钥会在上线时被获得. 密钥定时更换所带来的处理峰值, 可以通过控制在特定时段完成, 来避免延迟或排队.

5　数据报的安全服务

数据报的安全服务主要是把双重数字签名、数字信封、数字时间戳这 3 个安全机制结合起来, 以保障数据报的保密性、完整性、不可伪造性和不可否认性.

5.1　双重数字签名(Double Digital Signature)

域内用户在成为合法用户之后, 通过安全的密钥分发模块, 用户 U 获得了对应于自己标识 ID_U 的私钥 PID_U, 进而用户 U 就可以与其他用户、服务进行通信.

作为一个主要的信息安全手段, 数字签名技术可以解决否认、伪造、篡改及冒充等问题[17]. 在 IBE 系统下, 用户与其他用户、服务之间的通信过程中, 为了实现 IBE 体系对用户的认证以及保证数据报的不可抵赖性, 我们采用双重数字签名. 双重数字签名包括两个部分, 分别称为公签(public signature)和私签(private signature), 私签是使用用户 U 自己生成的私钥 K_U 对消息摘要进行的签名, 而公签是使用密钥管理机制为其生成的私钥 PID_U 进行的签名.

双重数字签名的基本原理与 ECDSA[18] 相似, 都是使用私钥进行签名, 使用公钥进行验证. 不同的是双重数字签名需要同时使用公签私钥和私签私钥进行签名, 验签时需要使用该签名对应的身份分别进行公签验签和私签验签.

(1) 验签参数生成流程

① 公签验签的验签参数由密钥更换模块生成并存入中央数据库中.

② 私签验签的验签参数由用户自己生成, 并验证后加密上传入库.

③ 在验签时, 用户需先从可信机构密钥分发模块获得该签名的公签验签参数和私签验签参数.

④ 最后利用下面的验签算法, 使用该签名对应的身份作为私签公钥 ID_U 和公签公钥 ID_U 进行验签.

(2) 双重数字签名过程

对于双重数字签名的不可伪造性, 将在第 6 节中给予安全性证明.

设两个域内用户 PID_U 和 V 需要互相通信, 此时双方在通信之前都已经明确了对方的标识, 用户要将欲发送给用户 V 的消息 M 进行签名, 具体实现过程如下(设发送方 U 需要传送的消息为 M, 示意图见图 4):

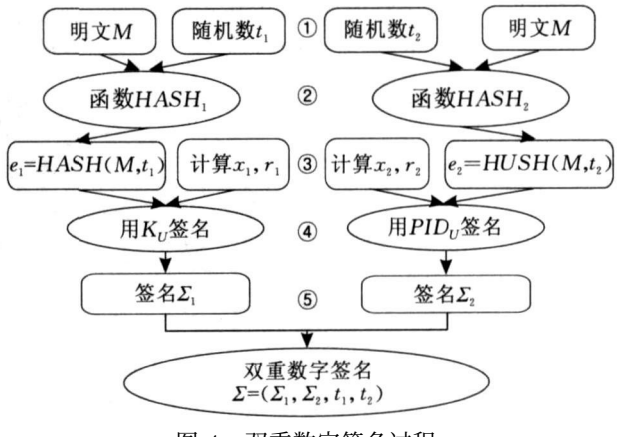

图 4　双重数字签名过程

① 选取 4 个随机数 k_1, k_2, t_1, t_2:

$$k_1 \xrightarrow{R} \{0,1\}^{n_{t_1}}, \quad k_2 \xrightarrow{R} \{0,1\}^{n_{t_2}},$$

$$t_1 \xrightarrow{R} \{0,1\}^{n_{t_1}}, \quad t_2 \xrightarrow{R} \{0,1\}^{n_{t_2}}.$$

② 计算 $e_1=HASH_1(m, t_1)$, $e_2=HASH_2(m, t_2)$.

③ 计算 $k_1G=(x_1, y_1)$, $k_2G=(x_2, y_2)$ 以及 $r_1=x_1 \bmod n$, $r_2=x_2 \bmod n$; 如果 $r_1=0$ 或者 $r_2=0$ 转步①, 计算 $k_1^{-1} \bmod n$, $k_2^{-1} \bmod n$.

④ 计算 $S_1=(K_U \cdot e_1-k_1r_1) \bmod n$, $S_2=(PID_U \cdot e_2-k_2r_2) \bmod n$, 如果 $S_1=0$ 或 $S_2=0$ 转步①.

⑤ 用户 U 对消息 M 的签名是 Σ_1: (r_1, S_1) 和 Σ_2: (r_2, S_2). 其中, (r_1, S_1) 是私签的签名过程; (r_2, S_2) 则是由公签的签名过程.

(3) 验签过程

①验证 r_1, r_2 和 S_1, S_2 是[1, $n-1$] 中的整数.

②计算 $e_1=HASH_1(m, t_1)$, $e_2=HASH_2(m, t_2)$.

③计算 $w_1=r_1^{-1} \bmod n$ 和 $w_2=r_2^{-1} \bmod n$.

④计算 $u_{11}=e_1 w_1$, $u_{12}=S_1 w_1$ 和 $u_{21}=e_2 w_2$, $u_{22}=S_2 w_2$.

⑤计算 $X_1=u_{11} ID_U-u_{12} G$, $X_2=u_{21} ID_U-u_{22} G$. 并记 X_1 坐标为 (x_1, y_1), X_2 的坐标为 (x_2, y_2), 若 $x_1=0$ 或 $x_2=0$, 则拒绝验签; 否则计算 $v_1=x_1 \bmod n$ 和 $v_2=x_2 \bmod n$.

⑥当且仅当 $v_1=r_1$, 并且 $v_2=r_2$ 时接受验签. 当 $v_1=r_1$ 时可以证明该消息的签名者就是该用户 U; 当 $v_2=r_2$ 成立时, 则说明用户 U 是该 IBE 系统下的合法用户.

双重数字签名可以解决存在于 IBE 体系下的数字签名的问题, 域内用户使用由系统发放的私钥进行数字签名, 只能够说明该数据报是被该信任域所认可的合法用户的数据报. 只有私签签名才能证明该数据报与该用户有直接的责任链条关系.

5.2 数字信封(Digital Envelope)

数字信封技术就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, 使加密传输安全可靠又有很高的效率. 封包的算法流程如图 5 所示.

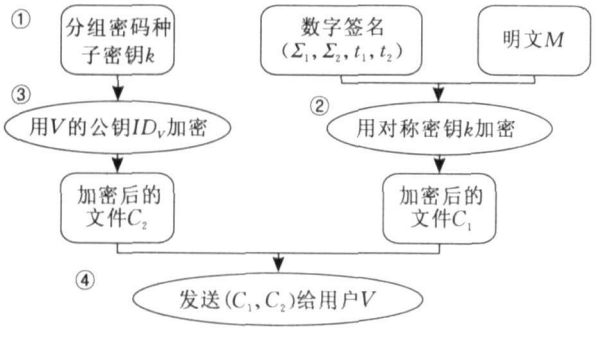

图 5 数字信封的封包过程

(1) 当发送方 U 给接收方 V 发送消息 M 时:

①U 随机生成一个对称会话密钥 k;

②用该对称密钥 k 加密明文 M 以及图 2 所示的数字签名 Σ, $(\Sigma_1, \Sigma_2, t_1, t_2)$, 产生密文 C_1;

③用户 V 将用户 U 的身份 ID_U 映射到一个 q 阶的点. 选择一个随机串 σ, 设置 $r=H_1(\sigma, k)$. 计算密文 $C_2=\langle r \cdot G, \sigma \oplus H(g_{ID}^r), k \oplus G_1(\sigma) \rangle$, 其中 $g_{ID}=e(ID_V, P_{pub}) \in F_{P^2}$.

④将用会话密钥加密的密文 C_1 及会话密钥加密后的文件 C_2 一起传递给接收方 V.

(2) 当接收方 V 收到消息后: 设接收方受到的文件 C_2 的形式为 $C_2=\langle X, Y, Z \rangle$. 计算 $X \oplus H(e(PID_V, X))=\sigma$; 计算 $Z \oplus G_1(\sigma)=k$; 计算 $r=H_1(\sigma, k)$; 测试 $X=r \cdot G$, 若不成功, 则退出; 否则用户 V 将用计算出的会话密钥 k 解密消息密文 C_1. 这样就得到了明文 M, 同时还可以对得到的消息 M 验证数字签名以及时间戳信息.

5.3 数字时间戳服务(Digital Time-stamp Service)

数字签名技术可以保证信息的不可抵赖性, 但是如果有用户否认曾发送多次相同的数据报, 或者抵赖发送两个数据报的顺序, 此时就需要有一个第三方仲裁, 即数字时间戳服务. 该服务可以解决上述的问题, 并可以保证数据报的时限有效性, 即规定了数据报的有效时限, 还可以防止用户恶意的重放攻击[19].

基于信任服务的 IBE 体系中, 统一身份的标识管理规定了每个用户和服务都有相对应的标识. 因此数字时间戳服务 DTS 同样具有它自己的标识 DTS_P 以及对应于标识 DTS_P 的私钥 DTS_S. 算法流程如图 6 所示.

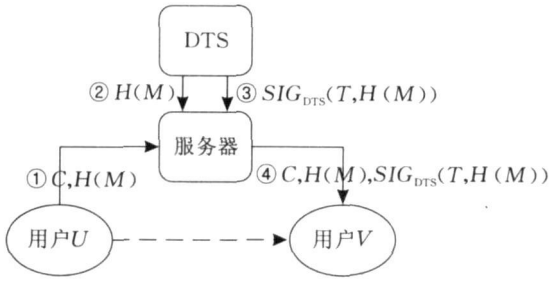

图 6 数字时间戳服务过程

(1)用户 U 将要发送给用户 V 的密文消息 C 和明文 M 的消息摘要 $H(M)$ 发送给服务 S.

(2)服务 S 将从用户 U 收到的明文消息摘要提交 DTS 服务器, 这时, 由 DTS 为该明文消息摘要附上时间戳信息, 也就是 DTS 收到消息的日期及时间, 同时用 DTS 服务器的私钥签名消息摘要以及时间戳信息:

①为消息摘要 $H(M)$ 附上时间戳信息 T. 设 $m=(H(M), T)$.

②DTS 选择一个随机数 k, $1 \leq k \leq n-1$.

③计算 $kG=(x_1, y_1)$, $r=x \bmod n$, 如果 $r=0$, 则转步②.

④计算 $k^{-1} \bmod n$.

⑤计算 $e=HASH(m)$.

⑥计算 $S=(DTS_S \cdot e-k \cdot r) \bmod n$, 如果 $S=0$, 转步骤②.

⑦DTS 对消息 m 的签名是 $SIG_{DTS}=(r, S)$.

(3) DTS 给服务 S 发回加盖时间戳的消息: (r, S).

(4) 服务器 S 将消息 $X=(C, H(M), SIG_{DTS})$ 一起发送给接受方 V.

消息的接受方 V 收到的消息 X 就是经过数字时间戳服务签名的时间戳. 用户 V 可以通过该时间戳来判断该消息是及时的消息还是重放的消息, 从而可以有效地防止重放攻击.

6 安全性证明

由于可证明安全性理论[20-21]中的 RO(Random Oracle)模型[22]可以证明本文所提出的协议是归约安全[13]的, 所以先给出两个基础假设: BDH[4,23]假设和 CDH[23-24]假设.

定义 **1**(BDH 假设). 设 G_1, G_2是阶数为素数 q 的两个循环群, $e: G_1\times G_1\to G_2$ 是一个双线性映射, P 为 G_1的生成元, 则$\langle G_1, G_2, e\rangle$上的 Bilinear Diffie-Hellman 问题是: 对于任意 $a, b, c\in Z_q^*$, 由$\langle P, aP, bP, cP\rangle$计算 $e(P,P)^{abc}$.

定义 **2**(CDH 假设). 一个概率多项式时间算法 A 在子群 $G_{p,g}=\{g^0, \cdots, g^{q-1}\}$ 中 (t,ε)-解决 CDH 问题, 如果满足以$((p,q), (g^a, g^b))$为输入, 在至多运行 t 步后, A 计算出$DH_{p,g}(g^a, g^b)=g^{ab}$的概率至少为 ε. 如果不存在(t,ε)-解决 CDH 问题的概率多项式时间算法 A, 则称该群 $G_{p,g}=\{g^0, \cdots, g^{q-1}\}$是一个$(t,\varepsilon)$-CDH 群.

6.1 双重数字签名的不可伪造性

定理 **1**. 如果 G 是一个(t', ε')-CDH 群, 则在 RO 模型中, 双重签名是$(t, q_H, q_{SIG}, q'_H, q'_{SIG}, \varepsilon)$-安全的, 即不存在如下有效算法: 在 t 步内, 任意做 q_H 次 HASH 询问和 q_{SIG}次 K_U 签名询问, 任意做q'_H 次 HASH′询问和q'_{SIG}次 PID_U 签名询问之后, 至少以概率 ε 伪造一个合法签名. 其中,

$$t'\approx t+(q_H+q'_H+4\ 4q_{SIG}+4\ 4q'_{SIG})C_{\exp}(G_{g,p});$$

$$\varepsilon'=\varepsilon-[q_{SIG}q_H2^{-n_{t_2}}+q'_{SIG}q'_H2^{-n_{t_1}}+q_{SIG}(q_{SIG}+q_H)2^{-2n'_q}+q'_{SIG}(q'_{SIG}+q'_H)2^{-2n'_q}+2^{-n_q}+2^{-n'_q}+q_H2^{-n_q}+q'_H2^{-n'_q}].$$

证明. 假设 F 是双重数字签名的一个$(t, q_H, q_{SIG}, q'_H, q'_{SIG}, \varepsilon)$-伪造者, 即在 t' 步内, 任意做 q_H 次 HASH 询问和 q_{SIG} 次 K_U 签名询问, 任意做q'_H 次 HASH′询问和q'_{SIG}次 PID_U 签名询问之后, F 至少以概率 ε 伪造一个合法签名. 构造这样一个算法 S, 以$((p,q), (g^a, g^b))$为输入, 至多 t'后, 至少以概率 ε'计算出$DH_{p,g}(g^a, g^b)=g^{ab}$, 从而与 CDH 假设矛盾.

首先S 根据目标身份 ID_U和密钥管理公布的参数 $T=(p, a, b, G, P_{pub}, q, h, H, I, H_1, I_1)$, 在不知道主密钥 s 的前提下, 运行 EXTRACT 算法生成 ID_U 对应的私钥 PID_U; 然后根据目标用户身份 ID_U 和该用户 ID_U 所公布的参数 $T'=(p, a, b, G, PU_{pub}, q, h, H, I, H_1, I_1)$, 在不知道主密钥 s'的前提下, 运行 EXTRACT 算法生成 ID_U 对应的私钥 K_U; 然后 S 向F 模仿签名协议, 并回答 F 的 Hash oracle (H_s, H'_s)询问、公签的 oracle 询问、Hash oracle (H_{ID}, H'_{ID})询问、私签的 oracle 询问, 目的是把 F 的一个可能伪造(m, Σ_1, Σ_2)转化为计算 $DH_{p,g}(g^a, g^b)=g^{ab}$的算法. 下面构造回答 oracle H_s, H'_s, 公签, H_{ID}, H'_{ID}, 私签的算法即 H_s, H'_s, PublicSIG, H_{ID}, H'_{ID}, PrivateSIG.

H_s: 如果 F 的询问是新的, S 随机选择d, 回答 $g^{bd}=(g^b)^d$;

H'_s: 对新的询问随机回答.

PublicSIG:

(1) $t_2\xrightarrow{R}\{0,1\}^{n_{t_2}}$, 如果$(m, t_2)$已问过, 放弃;

(2) 否则定义 $e_2=HASH_2(m, t_2)$;

(3) 随机取 $s\xrightarrow{R}\{0,1\}^{n_{t_2}}$, 根据欲伪造目标身份 ID_U和$T=(p, a, b, G, P_{pub}, q, h, H, I, H_1, I_1)$, 生成该用户 ID_U身份对应私钥 $PID_U=s\cdot P_U$;

(4) 随机选取$k_2\in Z_n$, 计算 $k_2G=(x_2, y_2)$, $r_2=x_2 \bmod n$, $k_2^{-1}\bmod n$, $S_2=(PID_U\cdot e_2-k_2r_2)\bmod n$;

(5) 如果 H'_s已经被问过, 则放弃; 否则定义 $c=H'_s(e_2, ID_U, PID_U, x_2, r_2, S_2)$, 返回对 m 的签名 $\Sigma_2=(t_2, s, ID_U, k_2)$.

H_{ID}: 如果 F 的询问是新的, S 随机选择 d', 回答 $g^{b'd'}=(g^{b'})^{d'}$

H'_{ID}: 对新的询问随机回答;

PrivateSIG: $t_1\xrightarrow{R}\{0,1\}^{n_{t_1}}$, 如果$(m, t_1)$已问过, 放弃; 否则定义 $e_1=HASH_1(m, t_1)$; 随机取 $s'\xrightarrow{R}\{0,1\}^{n_{t_1}}$, 根据欲伪造目标身份 ID_U和 $T'=(p, a, b, G, PU_{pub}, q, h, H, I, H_1, I_1)$, 生成该用户 ID_U身份对应私钥 $PID_U=s'\cdot P_U$; 随机选取 $k_1\in Z_n$, 计算 $k_1G=(x_1, y_1)$, $r_1=x_1 \bmod n$, $k_1^{-1}\bmod n$, $S_1=(K_U\cdot e_1-k_1r_1)\bmod n$; 如果 H'_{ID}已经被问过, 则放弃; 否则定义 $c=H'_{ID}(e_2, ID_U, PID_U, x_2, r_2, S_2)$ 返回对 m 的签名 $\Sigma_1=(t_1, s', ID_U, k_1)$.

解决 **CDH** 问题: 调用 F, 以不可忽略概率输出

一个合法签名(m, Σ_1, Σ_2);如果 F 没有向 H_s 询问过(m, t_2),并且没有向 H_{1D} 询问过(m, t_1),则放弃;否则 $h=H_s(m, t_2)=g^{bd}$ 或者 $h=H_{1D}(m, t_1)=g^{bd}$.

概率分析:PublicSIG 可能在第一步就失败,即(m, t_2)已经询问过 H_s oracle,因为至多有 q_H 个这样的 t_2,故碰撞概率至多为 $q_H 2^{-n_{t_2}}$,这样对 q_{SIG} 个签名询问而言,失败概率至多为 $q_{SIG}q_H 2^{-n_{t_2}}$;PublicSIG 也可能因为$(e_2, ID_U, PID_U, x_2, r_2, S_2)$已经询问过 H_s' oracle 而失败,且 H_s' oracle 至多被询问过$(q_{SIG}+q_H)$次,所以碰撞概率不会超过$(q_{SIG}+q_H)2^{-2n_q}$,对 q_{SIG} 个签名询问而言,失败概率至多为 $q_{SIG}(q_{SIG}+q_H)2^{-2n_q}$;当 F 未经过询问 H_s,就伪造出了一个合法签名并且没有找到用户 ID_U 的私钥 PID_U 时,这时是无法解决 CDH 难题的.由于 H_s 和 H_s' 是随机预言,所以失败的概率至多为 $q_H 2^{-n_q}+2^{-n_q}$.因为公签与私签的数学模型相同,所以 PrivateSIG 过程失败的概率为 $q'_{SIG}q'_H 2^{-n_{t_1}}+q'_{SIG}(q'_{SIG}+q'_H)2^{-2n'_q}+q'_H 2^{-n'_q}+2^{-n'_q}$.综上说述,$S$ 至少能以概率 $\varepsilon=[q_{SIG}q_H 2^{-n_{t_2}}+q'_{SIG}q'_H 2^{-n_{t_1}}+q_{SIG}(q_{SIG}+q_H)2^{-2n_q}+q'_{SIG}(q'_{SIG}+q'_H)2^{-2n'_q}+2^{-n_q}+2^{-n'_q}+q_H 2^{-n_q}+q'_H 2^{-n'_q}]$ 成功地解决 CDH 难题,因此原假设和 CDH 假设矛盾.证毕.

6.2 数字信封的保密性

由于数字信封可以等价地分解为两个过程:一是使用公钥体系加密传输分组密码的种子密钥 k;二是使用分组密码的种子密钥 k 对明文 M 进行对称加密传输.所以数字信封的保密性直接依赖于种子密钥 k 的安全性,而种子密钥 k 的安全性传输问题就是定义 1 的困难问题,即数字信封的保密性问题与 BDH 问题等价.所以数字信封在适应性选择密文攻击下具有不可区分性.

6.3 密钥发放的保密性

3.3 节已经详尽描述了密钥发放算法,它的核心思想可以概括为:(1)合法用户 U 生成自己的主密钥 s';(2)然后使用系统发放的参数 $T=(p, a, b, G, P_{pub}, q, h, H, I, H_1, I_1)$ 计算出 $PU_{pub}=m^U \cdot G$;(3)利用自己的身份标识 ID_U 计算出对应私签私钥 $K_U=m^U P_I$;(4)把自己的参数 $T'=(p, a, b, G, PU_{pub}, q, h, H, I, H_1, I_1)$ 和身份标识 ID_U 发送给 IBE 系统;(5)IBE 系统使用该用户的标识 ID_U 和参数 $T'=(p, a, b, G, PU_{pub}, q, h, H, I, H_1, I_1)$ 在椭圆曲线上加密发放给该标识 ID_U 的私钥 PID_U 并发送给该用户 U;(6)用户 U 使用私签私钥 K_U 解密并获得 IBE 系统发放的公签私钥 PID_U.显而易见,密钥发放算法就是 IBE 核心算法的应用,其保密性问题等价于 BDH 问题,所以密钥发放算法在适应性选择密文攻击下具有不可区分性.

7 结 论

针对现有 IBE 的密钥管理中存在的问题和不足,本文提出了一个 IBE 的密钥管理机制,主要解决了 IBE 体系的密钥分发问题、密钥的定时更换问题以及数据报的安全服务问题.密钥分发模块、密钥定时更换模块和数据报的安全服务模块三者的有机结合,使得 IBE 成为不同于 PKI 的有广泛应用前景的可信的公钥体系.在详细的描述可信密钥管理方案之后,本文使用随机预言模型证明了相关通信协议的安全性,即在 BDH 问题和 CDH 问题是困难的假设下,数字信封协议、双重数字签名协议和密钥分发协议被证明是安全的.

参 考 文 献

[1] Lin Chuang, Wang Yuan-Zhuo. Development of trustworthy network and facing scientific challenges. ZTE Communications, 2008, 14(1): 13-41(in Chinese)
(林闯, 王元卓. 可信网络的发展及其面对的技术挑战. 中兴通讯技术, 2008, 14(1): 13-41)

[2] Lin Chuang, Peng Xue-Hai. Research on trustworthy networks. Chinese Journal of Computers, 2005, 28(5): 751-758(in Chinese)
(林闯, 彭学海. 可信网络研究. 计算机学报, 2005, 28(5): 751-758)

[3] Shamir A. Identity-based cryptosystems and signature schemes// Proceedings of the Advances in Cryptology — CRYPTO'84. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1984, 196: 47-53

[4] Boneh D, Franklin M. Identity-based encryption from the Weil pairing// Proceedings of the Advances in Cryptology — CRYPTO 2001. Lecture Notes in Computer Science 2139. Berlin: Springer-Verlag, 2001: 213-229

[5] Benoît Libert, Jean-Jacques Quisquater. Identity based undeniable signatures// Proceedings of the Topics in Cryptology — CT-RSA 2004, 2004, 2964: 1997

[6] Chow Sherman S M, Yiu S M, Hui Lucas C K, Chow K P. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity// Proceedings of the Information Security and Cryptology — ICISC 2003. 2004, 2971: 352-369

[7] Boneh Dan, Boyen Xavier. Efficient selective-ID secure identity based encryption without random oracles// Proceedings of the Advances in Cryptology—EUROCRYPT 2004. Lecture Notes in Computer Science 3027. 2004: 223-238

[8] Waters Brent. Efficient identity-based encryption without random oracles// Proceedings of the Advances in Cryptology — EUROCRYPT 2005. 2005: 114-127

[9] Al-Riyami Sattam S, Paterson Kenneth G. Certificateless public key cryptography//Proceedings of the Advances in Cryptology — ASIACRYPT 2003, 2003: 452-473

[10] Lee Byoungcheon, Boyd Colin, Dawson Ed, Kim Kwangjo, Yang Jeongmo, Yoo Seungjae. Secure key issuing in ID-based cryptography//Proceedings of the 2nd Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation. Dunedin, New Zealand, Australian, 2004, 32: 69-74

[11] Chen, Harrison K, Moss A, Soldera D, Smart N P. Certification of public keys within an identity based system//Proceedings of the Information Security 5th International Conference ISC 2002. Sao Paulo, Brazil, 2002

[12] Lin Chuang, Lei Lei. Research on next generation internet architecture. Chinese Journal of Computers, 2007, 30(5): 693-711(in Chinese)
(林闯, 雷蕾. 下一代互联网体系结构. 计算机学报, 2007, 30(5): 693-711)

[13] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation . USA: JSTOR. 1987

[14] Hankerson Darrel, Menezes Alfred J, Vanstone Scott. Guide to Elliptic Curve Cryptography. Berlin: Springer-verlag Publishers, 2004

[15] Enge Andreas. Elliptic Curves and Their Applications to Cryptography. Holland: Kluwer Academic Publishers, 1999

[16] William Stallings. Cryptography and Network Security Principles and Practices. 4th edition. USA: Prentice Hall, 2005

[17] Paterson K G. ID-based signatures from pairings on elliptic curves. Electronics Letters, 2002, 38(18): 1025-1026

[18] Accredited Standards Committee X9. Public key cryptography for the financial services industry. American National Standard X9 62-2005. The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005

[19] Lowe G. An attack on the needham-schroeder public key authentication protocol. Information Processing Letters, 1995, 56(3): 131-136

[20] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols//Proceedings of the 1st Conference on Computer and Communications Security. Fairfax, Virginia, United States, 1993: 62-73

[21] Feng Deng-Guo. Research on theory and approach of provable security. Journal of Software, 2005, 16(10): 1743-1756 (in Chinese)
(冯登国. 可证明安全性理论与方法研究. 软件学报, 2005, 16(10): 1743-1756)

[22] Canetti Ran, Goldreich Oded, Halevi Shai. The Random oracle methodology. Journal of the ACM, 2004, 51(4): 557-594

[23] Diffie Whitfield, Hellman Martin. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[24] Goh E J, Jarecki S. A signature scheme as secure as the Diffie-Hellman problem//Proceedings of the Advances in Cryptology EUROCRYPT 2003. Berlin: Springer-Verlag Publishers, 2003, 2656: 401-415

HU Liang, born in 1968, Ph. D., professor, Ph. D. supervisor. His current research interests include information security and trustworthy computing.

CHU Jian-Feng, born in 1978, Ph. D. candidate. His research interests focus on computer architecture.

LIN Hai-Qun, born in 1985, M. S. candidate. Her research interests include cryptography and information security.

YUAN Wei, born in 1984, M. S. candidate. His research interests include block cipher, public-key cryptography and information security.

ZHAO Kuo, born in 1977, Ph. D.. His research interests focus on computer architecture.

Background

This research is supported by the National Natural Science Foundation of China under grant Nos. 60873235, 60473099 and Program for New Century Excellent Talents in University of China under grant No. NCET-06-0300 and the Key project No. 20080318 of Jilin province.

An important objective of the projects is to probe the trend of network security, which can satisfy the need of constructing high-speed, large-scale and multi-services networks. Various complex attacks can not be dealt with by simple defense. And to add mechanisms to network architecture results in decreasing performance. In a word, fundamental re-examination of how to build trustworthy distributed network should be made.

To satisfy the need of the next generation internet architecture above, this paper puts forward the trustworthy key management mechanism of IBE system, which can solve several problems of the current IBE, such as keys' distribution, keys' timing replacement and message's secure service. And these improvements make IBE more practical especially for e-government and e-military affairs. Furthermore, the proposed network protocols in this paper are proved to be secure by RO (Random Oracle) model. Therefore this trustworthy key management mechanism of IBE system is based on secure network protocols.

In addition the authors have published several papers in international journals and conferences on block cipher and identity-based cryptography.