混合 P2P 网络中可证安全的信任数据安全传输协议

林怀清 王 斌 周 岩
(海军工程大学电子工程学院 武汉 430033)

摘 要 P2P 网络的开放、匿名特性使得系统极易遭受恶意用户的攻击,信任模型是减少此类威胁的有效方法。信任模型的有效性依赖于信任数据的可靠性,因此信任数据对于信任模型来说至关重要。无证书加密方案可以消除传统 PKI 系统的证书管理开销,同时可以消除基于身份加密系统中的密钥泄露问题。提出了一种基于无证书加密方案的安全协议,用于混合式 P2P 网络中信任数据的管理。加密系统的安全性基于双线性 Diffie-Hellman 问题,利用串空间证明了协议可以实现交互双发认证以及信任数据安全性。

关键词 信任,安全,串空间,点对点,无证书密码系统
中图法分类号 TP393 **文献标识码** A

Provable Secure Trust Data Sharing Protocol for Hybrid P2P Networks

LIN Huai-qing WANG Bin ZHOU Yan
(College of Electronic Engineering, Naval University of Engineering, Wuhan 430033, China)

Abstract The open and anonymity nature of P2P networks makes it extremely susceptible to malicious users attacking. On way to minimize threats is to build the trust model for P2P network. The trust data is critical to the trust model of P2P system which validity is relied on the reliability of trust data. We presented a CL-PKC-Based protocol which provides the ability for sharing trust data securely in the hybrid P2P networks. The protocol avoids the authentication of the public key and the key escrow problem of identity-based cryptosystem. The security of cryptosystem is based on Bilinear Diffie-Hellman Problem. And the strand space model was used to prove that the secure protocol can achieve agreement properties and keep secrecy of trust data.

Keywords Trust, Security, Strand space, P2P, CL-PKC

1 引言

信任模型可以有效地改进 P2P 网络的性能。已有相当多的学者致力于信任计算的研究,而信任模型的准确性和有效性依赖于信任数据的准确性和有效性。但是,关注信任值安全传输的研究工作并不多。信任模型需要某种机制保证用户提交的信任数据能在 P2P 网络中安全传播。现有的 P2P 网络的消息在到达目的地前需要经过若干节点,而这些中转节点是完全不可控的,因此此类传播机制无法满足信任数据传播的安全性要求。

TrustMe 协议[1]是目前为止较全面讨论信任数据安全传输的信任传输协议。这种选择方案面临以下 2 个安全问题:

1)系统的所有密钥全部由 bootstrap server 生成,系统的安全性完全依赖 bootstrap server;

2)没有讨论多个信任存储点之间的信任数据同步问题。

基于 PKI 的加密方案可以解决信任数据的安全存储问题,但是 PKI 需要很大的存储空间和计算开销来存储和验证为数众多的用户的公钥证书。为减轻传统公钥密码系统的维护开销,Shamir 等人[2]提出一种创新的解决思路,但是基于身份的密码系统的密钥产生方法导致 PKG 拥有所有用户的私钥,称之为密钥泄露问题。在 P2P 此类由陌生用户组成的网络中,密钥泄露问题显得更加突出。在 2003 年,Al-Riyami 和 Paterson[3]提出一种称之为无证书密码系统(CL-PKC, certificateless public key cryptography)的解决方法,在保留基于身份密码系统无需数字证书和能减少维护开销的优点的同时,CL-PKC 克服了基于身份密码系统的密钥泄露问题。自从 Al-Riyami 提出此概念之后,相继推出了许多无证书加密方案[4-7]。

部署 CL-PKC 需要解决的一个问题是如何选择 KGC。纯 P2P 网络由于可扩展性差,应用越来越少。而混合 P2P 网络结合了纯 P2P 网络和中心化 P2P 网络的优点,显示出强大的生命力。因此我们主要讨论在混合式 P2P 网络中信任数据的安全传输。在混合 P2P 网络中可以选择服务器或超级节点完成 KGC 的任务。

本文提出了一种高效简洁的信任数据安全存取协议,协议由无证书密码系统提供安全保证。协议避免了 TrustMe 协议中的密钥泄露问题,不仅能保证数据的秘密性,同时可以防止恶意用户随意杜撰交互信息。用串空间理论证明协议具

到稿日期:2009-11-09 返修日期:2010-01-20 本文受国家自然科学基金(50909096)资助。
林怀清(1973-),男,博士,讲师,主要研究方向为网络安全等,E-mail:whoamisir@163.com;王 斌(1978-),硕士,讲师,主要研究方向为信息网络等;周 岩(1978-),硕士,讲师,主要研究方向为信息网络等。

备一致性和安全性。

2 信任数据安全传输协议(STDSP:Secure Trust Data Sharing Protocol)

我们希望得到信任数据时可以获得以下几点保证:

1)保证信任数据确实是由数据中声明的提供者产生;

2)保证信任数据在传输过程中没有被篡改;

3)保证评估者提交的信任数据是在与评估对象发生过交互的基础上,防止用户随意提高或降低信任度;

4)在发现虚假评估时可以追溯评估起源,这与保持评估者匿名相矛盾。对于 P2P 这种不可靠网络,我们认为保持可追溯性要比匿名性更重要,因此协议中牺牲匿名性。

本节将详细描述信任数据安全传输协议。协议中需要使用的符号定义如下:S_A 表示节点 A 的私有密钥,而 O_A 表示节点 A 的公开密钥,符号'|'用于消息的联接,$ENC_K(M)$ 表示用加密密码 K 对消息 M 加密,$DEC_K(C)$ 表示用解密密码 K 对密文消息 C 执行解密操作,$SIG_K(M)$ 表示用签名密码 K 对消息 M 执行签名操作。$SupReplay_B$ 表示节点 B 发起对节点 A 的信任数据查询,$SupReplay_B$ 表示向节点返回信任数据,$Proof_{AB}$ 表示节点 A 向节点 B 发放的交互证明,$Report_{BA}^{sup}$ 表示节点 B 向超级节点 sup 提交节点 A 的信任数据。

2.1 协议概述

安全协议工作方式描述如下:每个加入网络的节点按照无证书加密方案获得公/私密钥,用于完成加密/解密以及签名/检验工作。节点将信任数据提交给超级节点,并由超级节点响应信任查询。在此过程中通过无证书密码系统完成各消息的加密/解密和签名/检验工作。

2.2 协议详细描述

以下协议描述中,G_1 和 G_2 为两个具有相同素数阶 $q(>2^k)$的双线性群,$e:G_1\times G_1\rightarrow G_2$ 为 admissible 双线性对,H_1,H_2,H_3 和 H_4 为安全 hash 函数。

2.2.1 系统参数建立

根据 CL-PKC 方案,KGC 输出系统的主密钥 $S\in Z_q^*$ 以及系统的参数 $params=\{G_1,G_2,e,q,l,P,P_0,H_1,H_2,H_3,H_4\}$。参数 $params$ 向网络中的所有用户公开。在节点加入网络时,由 KGC 向其发送 $params$,将是一个传播 $params$ 的好机会。

2.2.2 用户密钥生成

当节点 A 加入网络时,它首先产生一个秘密值 $x_A\in Z_q^*$ 并计算自己的公开密钥 $O_A=\langle X_A,Y_A\rangle=\langle x_AP,x_AP_0\rangle$。为获得私有密钥,节点 A 将 O_A 发送给 KGC,KGC 以系统主密码 s、节点 A 的身份 ID_A 以及它的公开密钥 O_A 为参数,计算节点 A 的部分密钥 $D_A=sH_1(ID_A,O_A)=sQ_A$。节点 A 在获得部分密钥 D_A 后可以计算 $S_A=x_AD_A$。S_A 即为节点 A 的私有密钥。

2.2.3 信任数据查询

任意节点 B,若想查询节点 A 的信任值,它可以向超级节点发起查询消息。超级节点 sn 收到节点 B 的信任查询后一种可行方法是将缓冲在超级节点的信任数据按如下方法返回给查询节点:

$$SupReplay_B=ID_{sn}\mid ENC_{O_B}(M_1\mid M_2\mid\cdots\mid M_n)\mid SIG_{S_1}(M_1)\mid SIG_{S_2}(M_2)\mid\cdots\mid SIG_{S_n}(M_n)$$

式中,$M_i=ID_B\mid ID_A\mid ID_{sn}\mid TV_A\mid Proof_{AB}(i=1,\cdots,n)$。

但是,当超级节点管辖的叶子节点较多时,缓冲的信任数据数量会很大,因此直接用节点 B 的公钥对数据加密会导致计算开销较大。用对称加密方式将是一个理想的选择。此时节点 B 的查询消息如下:

$$QuerySup_B=ENC_{O_{sn}}(ID_{sn}\mid ID_B\mid ID_A\mid xP)\mid SIG_{S_B}(ID_{sn}\mid ID_B\mid ID_A\mid xP)$$

式中,ID_B 表示查询消息的源节点,ID_A 表示需要查询的目标节点,ID_{sn} 是超级节点,x 是由节点 B 产生的随机数。用节点 B 的私钥对 M 签名可以向对方证明自己的身份。

2.2.4 信任查询应答

超级节点 sn 收到节点 B 的查询消息后,将向其返回如下应答消息:

$$SupReplay_B=ENC_{O_B}(ID_{sn}\mid ID_B\mid ID_A\mid yP\mid xyP)\mid SENC_{K_s}(M)\mid SIG_{S_{sn}}(M)$$

式中,ID_s 用于指明此应答消息的来源地,ID_B 指明消息的目的地,M 是此消息的实际负载,$M=M_1\mid SIG_{S_1}(M_1)\mid M_2\mid SIG_{S_2}(M_2)\mid\cdots\mid M_n\mid SIG_{S_n}(M_n)$,$M_i(i=1,\cdots,n)$与 2.2.3 节的 M 定义相同,其中 y 是超级节点 s 产生的随机数,双方协商的对称密钥 $K_s=Hash(xyP)$,$SENC_{K_s}(M)$表示用密钥 K_s 对 M 完成对称加密。

节点 B 收到 $SupReplay_B$ 后,可以用自己的私钥 S_B 解密消息的第一部分,获得 yP,从而可以计算 $K_s=Hash(xyP)$,获得对称加密密钥,解密消息的第二部分获得信任值。

2.2.5 收集交互证据

两个节点 A 和 B 若发生交互,在交互结束后交换交互证据,作为服务端的 A 向 B 发放交互证明 $Proof_{AB}=SIG_{S_A}(ID_A\mid ID_B\mid Num)$,节点 B 以此向其他节点证明交互的真实性。

交互证据可以实现以下功能:

- 交互证据中的 ID_A 和 ID_B 指明此证书是由节点 A 发给节点 B 的;
- Num 是节点 A 向 B 提供服务的次数,在每次交互前 B 将交互证据提交给 A,在交互结束后,Num 将被加 1;
- 签名可以向其他节点证明此交互证据确实是由节点 A 发放的。

2.2.6 提交信任数据

为加快检索速度,我们在超级节点上实现缓冲机制,节点的信任数据发送给超级节点,当有信任数据检索要求时,由超级节点完成应答。在信任数据发生更新时,节点需要将更新后的信任数据提交给超级节点。提交的更新报告格式如下:

$$Report_{BA}^{sn}=ID_B\mid ENC_{O_{sn}}(M\mid TS)\mid SIG_{S_B}(M\mid TS)$$

式中,O_{sn} 是超级节点 sn 的公开密钥,M 与 2.2.3 节中的定义相同。

更新报告可以实现以下功能:

- 交互证据中的 ID_A、ID_B 和 ID_{sn} 指明此报告是由节点 B 提交给超级节点 sn 的节点 A 信任数据;
- 用 O_{sn} 对消息加密,可以确保只有超级节点 sn 能解开;
- 用 S_B 对消息签名,可以确保消息的完整性;
- TS 用于防止重发攻击。

3 协议的安全性证明

3.1 串空间扩展

Fábrega 等人提出的串空间理论[8-10]是以 Dolev-Yao 模

型[11]为基础的安全协议分析模型。它的3个核心理论包括丛(bundle)概念、理想(ideal)概念和认证测试(authentication test)方法,共同形成了一套验证协议安全性的方法族。但是,现有的串空间模型不能表达丰富的密码原语,因此不能分析较复杂的安全协议。通过对串空间理论的扩展,使其充分地表达较多的密码学原语[12,13],以满足分析复杂安全协议的需要。本节将利用扩展的串空间理论证明STDSP协议的安全性。

3.2 代数运算的扩展

增加一个新的数据类型集 D 来表示DH值,其中的元素为 $d_1,d_2,\cdots$,每个元素表示为一个元组 (P,n),其中 P 是生成元,n 是任意数。并定义 D 操作如下:

$D\times D\rightarrow D$

例如,$d_1=xP,d_2=yP$,则 $DH(d_1,d_2)=xyP$。

3.3 运算符的扩展

为更广泛地抽象密码学原语,增加签名运算符、Hash运算、对称加密、非对称加密和DH运算,我们通过定义1指定串空间中的项集合以及运算符。

定义1 A 为项集合,包含相互独立的两个子集,其中:

$T\subseteq A$ 为原子消息集;

$K\subseteq A$ 为密钥集合。$K\cap T=\Phi$,并且 K 中具有一元运算符 $inv:K\rightarrow K$。假设INV是单射的,则在非对称密钥中 inv 是每一个密钥对中两个密钥的相互影射,而在对称密钥中 inv 影射到该密钥本身;

$R\subseteq A$ 为不可预见的随机值;

$D\subseteq A$ 用于计算的DH值;

7个二元运算符:

$join:A\times A\rightarrow A$

$Sign:K\times A\rightarrow A$

$Hash:A\rightarrow K$,Hash运算用来将消息项映射为一个对称密钥

$SymEncr:K_{sym}\times A\rightarrow A$

$AsyEncr:K_{asy}\times A\rightarrow A$

$DH:D\times D\rightarrow D$

通常,K^{-1} 表示 $inv(K)$,gh 表示串联消息 $join(g,h)$,用 $[m]_K$ 表示用 K 对 m 签名,用 $H(m)$ 表示对消息项 m 执行Hash运算,$(m)_{K_{sym}}$ 表示用对称密钥 K_{sym} 加密消息项 m,$\{m\}_{K_{asy}}$ 表示用公钥 K_{asy} 加密消息项 m。

其中 T,K,R,D 两两不相交。$T=T_{name}\cup T_{sig}\cup T_{enc}\cup T_{tv}$ 是原子消息空间集合,T_{name} 是名字集,T_{sig} 是签名消息集,T_{enc} 是加密消息集,T_{tv} 是信任数据集,T_{name},T_{sig},T_{enc} 和 T_{tv} 两两不相交;$K=K_{sym}\cup K_{asy}\cup K_{sig}$,$K_{sym}$ 是对称密钥集,K_{asy} 是非对称密钥集,K_{sig} 是签名集,K_{sym},K_{asy},K_{sig} 两两不相交。

扩展后的子项关系如定义2。

定义2 子项关系$\sqsubset$定义如下:

1)如果 $a=b$,则 $a\sqsubset b$;

2)如果 $a\sqsubset g$,则 $a\sqsubset\{g\}_K$;

3)如果 $a\sqsubset g$,则 $a\sqsubset[g]_K$;

4)如果 $a\sqsubset g$,则 $a\sqsubset(g)_K$;

5)如果 $a\sqsubset g$,则 $a\sqsubset H(g)$;

6)如果 $a\sqsubset g$ 或者 $a\sqsubset h$,则 $a\sqsubset gh$;

7)如果 $a\sqsubset g$ 或者 $a\sqsubset h$,则 $a\sqsubset DH(g,h)$。

3.4 入侵串类型扩展

定义3 扩展的入侵串如下:

M. 产生原子消息:$\langle+t\rangle,t\in T$

F. 接收消息:$\langle-g\rangle$

T. 接收并多次发送消息:$\langle-g,+g,+g\rangle$

C. 串联收到的消息:$\langle-g,-h,+gh\rangle$

S. 分解收到的消息:$\langle-gh,+g,+h\rangle$

K. 发送密钥:$\langle+K\rangle,K\in K_P$

R. 产生随机值:$\langle+r\rangle$

EA. 公钥加密消息:$\langle-K,-m,+\{m\}_K\rangle,K\in K_{asy}$

DA. 私钥解密消息:$\langle-K^{-1},-\{m\}_K,+m\rangle,K\in K_{asy}$

ES. 对称加密消息:$\langle-K,-m,+\{m\}_K\rangle,K\in K_{sym}$

DS. 对称解密消息:$\langle-K,-\{m\}_K,+m\rangle,K\in K_{sym}$

Si. 签名:$\langle-K,-m,+[m]_K\rangle,K\in K_{asy}$

Ve. 验证:$\langle-K^{-1},[m]_K,+m\rangle,K\in K_{asy}$

H. Hash计算:$\langle-m,+H(m)\rangle$

DH. 计算DH值:$\langle-x,-yP,+xyP\rangle$

3.5 查询协议的安全性证明

定义4 令$\sum$为一串空间,则有:

1)$Init[ID_A,ID_B,ID_D,xp,xyP,TV_D,Proof_{DB}]$ 是发起者串,其轨迹为

$\langle+\{ID_B|ID_A|ID_D|xP\}_{O_B}[ID_B|ID_A|ID_D|xP]_{S_A},$

$-\{ID_B|ID_A|ID_D|yP|xyP\}_{O_B}(M)_{K_s}[M]_{S_B}\rangle$

$\sum_{init}$ 是发起者串集合;

2)$Resp[ID_A,ID_B,ID_D,xp,xyP,TV_D,Proof_{DB}]$ 是响应者串,其轨迹为

$\langle-\{ID_B|ID_A|ID_D|xP\}_{O_B}[ID_B|ID_A|ID_D|xP]_{S_A},$

$+\{ID_B|ID_A|ID_D|yP|xyP\}_{O_B}(M)_{K_s}[M]_{S_B}\rangle$

$\sum_{Resp}$ 是发起者串集合;

其中的 $ID_A,ID_B,ID_D\in T_{name}$,$TV_D\in T_{tv}$,$Proof_{DB}\in T_{sig}$,且 T_{name},T_{tv} 和 T_{sig} 两两不相交,则串空间记为 $(\sum,P)=\sum_{Init}\cup\sum_{Resp}\cup P$,其中 P 为攻击者串集合。图1为查询协议的丛示意图。

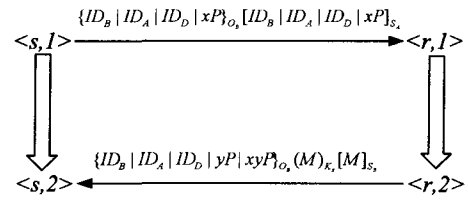

图1 查询协议的丛

命题1 协议双方共享一致的 O_A,S_A,O_B,S_B,K_s,等价于它们共享一致的 x,y。

证明:由离散对数的计算困难性可以得到结论:若 xP 起源于攻击者节点,则 x 也起源于攻击者节点。集中查询协议的秘密性等价于Diffie-Hellman交换的秘密性。在发起者与响应者成功执行协议的前提下,证明 x,y 是安全的,即可证明协商的密钥是安全的。

命题2 x,y,xyP,K_s 的秘密性,假设 C 是 $(\sum,P)$ 上的丛,xP,yP 唯一起源于 C 上的正常串,$xP\neq yP$,$S_A\notin K_P$,$S_B\notin K_P$,Hash是哈希函数,DH问题是难解的,则 x,y 的秘密性可保持。

证明:根据假设求解DH问题是困难的,因此攻击者为了

计算 xyP，必须知道 x 和 y，或者知道 x 和 yP，或者知道 xP 和 y。

根据项产生的因果关系，显然存在 $s\in\sum_{Init}$，使得

$unterm(\langle s,1\rangle)=\{ID_B|ID_A|ID_D|xP\}_{O_B}[ID_B|ID_A|ID_D|xP]_{s_A}$

$unterm(\langle s,2\rangle)=\{ID_B|ID_A|ID_D|yP|xyP\}_{O_B}(M)_{K_s}[M]_{s_B}$

因为 xP 唯一起源于 C 上的正常串，存在 $r\in\sum_{Resp}$，xP 唯一起源于节点 $\langle r,1\rangle$，项的形式为 $\{ID_B|ID_A|ID_D|xP\}_{O_B}[ID_B|ID_A|ID_D|xP]_{s_A}$。由于 yP 唯一起源于 C 上的正常串，项形式为 $+\{ID_B|ID_A|ID_D|yP|xyP\}_{O_B}(M)_{K_s}[M]_{s_B}$，由于 $S_A\notin K_P$，因此攻击串节点不可能从节点 $DA\langle -K^{-1},-\{m\}_K,+h\rangle$ 获得任何有用信息，即攻击者无法获得 y，所以攻击者无法计算 xyP，也就无法计算共享密钥 K_s。

命题 3 在集中查询协议中，设 C 是 $(\sum,P)$ 上的丛，$K'\notin K_P$，则形如 $\{M\}_{K'}$ 和 $[M]_{K'}$ 的项不起源于 C 中的攻击节点。

证明：设 $\{M\}_{K'}$ 产生于一个攻击者节点，则可能源于 C 的攻击者串 p 类型为 EA 的节点 $\langle K,-m,+\{m\}_K\rangle$，$K\in K_{asy}$ 和 ES 节点 $\langle -K,-m,+\{m\}_K\rangle$，$K\in K_{sym}$。假设 $\{M\}_K$ 产生于节点 $\langle p,1\rangle$，则如果 $\{M\}_{K'}=\{m\}_K$，根据自由加密假设有 $M=m,K'=K$，则有 $K'\sqsubset\langle p,1\rangle$，即 $K'\in K_P$，与假设矛盾，所以 $\{M\}_{K'}$ 一定产生于正常节点。

同理可证 $[M]_{K'}$ 一定产生于正常节点。

命题 4 在集中查询协议中，设 $\{h\}_{K'}$ 和 $[h]_{K'}$ 起源于正规串，如果 $s\in\sum_{Init}$，则 $h=ID_B|ID_A|ID_D|xP$，或者 $h=ID_B|ID_A|ID_D|yP|xyP$，或者 $h=ID_B|ID_A|ID_D|TV_D|Proof_{DB}$；如果 $s\in\sum_{Resp}$，则 $h=ID_B|ID_A|ID_D|xP$，或者 $h=ID_B|ID_A|ID_D|yP|xyP$，或者 $h=ID_B|ID_A|ID_D|TV_D|Proof_{DB}$。

证明：由定义 4 和命题 3 可直接得到。

命题 5 在集中查询协议中，设 C 是上丛，$A\neq B$，S_A，S_B，$K_s\notin K_P$，如果发起者串 $s\in Init[ID_A,ID_B,ID_D,xp,xyP,TV_D,Proof_{DB}]$ 在 C 上丛高是 2，则存在常规响应者串 $r=Resp[ID_A,ID_B,ID_D,xp,xyP,TV_D,Proof_{DB}]$，它在 C 上丛高为 2。

证明：$s\in Init[ID_A,ID_B,ID_D,xp,xyP,TV_D,Proof_{DB}]$ 在 C 上的串轨迹是

$\langle +\{ID_B|ID_A|ID_D|xP\}_{O_B}[ID_B|ID_A|ID_D|xP]_{s_A},$

$-\{ID_B|ID_A|ID_D|yP|xyP\}_{O_B}(M)_{K_s}[M]_{s_B}\rangle$

由于 S_A，S_B，$K_s\notin K_P$，由命题 3，$[ID_B|ID_A|ID_D|xP]_{s_A}$，$(M)_{K_s}$ 起源于 C 中的常规串。$r\in Resp[ID_A,ID_B,ID_D,xp,xyP,TV_D,Proof_{DB}]$，由于

$unterm\langle r,2\rangle=\{ID_B|ID_A|ID_D|yP|xyP\}_{O_B}(M)_{K_s}[M]_{s_B}$

所以 r 在 C 上丛高是 2。

如果发起者能正确解析第二条消息，那么发起者一定能确定响应者身份，而且意味着它们进行了唯一的 Diffie-Hellman 密钥生成。

从以上命题可以发现，签名项可以保证认证的正确性，加密和散列能保证数据 xyP 的完整性和秘密性。

结束语 信任数据的准确性和责任性是信任推理的基础，其重要性不言而喻。由于 P2P 网络的特点，很难部署 PKI 用于支持网络的安全传输，而无证书加密方案可以消除传统 PKI 系统的证书管理开销，同时可以消除基于身份加密系统中存在的密钥泄露问题，这些特点使得该方案特别适用于 P2P 网络环境。本文基于 CL-PKC 设计了一种安全可靠的信任数据传输协议，协议可提供信任数据安全、可靠和可追责的分发和访问。原始的串空间理论不能表达丰富的密码原语，无法分析较复杂的安全协议。我们扩展了串空间的代数运算、运算符和入侵者串，利用扩展的串空间理论分析 STDSP 协议，给出的定理证明了 STDSP 的安全性和可鉴别性。

参 考 文 献

[1] Singh A, Liu L. TrustMe: Anonymous management of trust relationships in decentralized p2p systems [C]// IEEE International Conference on P2P Computing. Linköping, Sweden, vol. 1, 2003: 142-149

[2] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology-Crypto'84. Santa Barbara, California, Springer, 1984: 47-53

[3] Al-Riyami S S, Paterson K. Certificateless public key cryptography [C]// The Ninth International Conference on the Theory and Application of Cryptology and Information Security. Taipei, Taiwan, China, Springer, 2003: 452-473

[4] Yum D H, Lee P J. Generic construction of certificateless signature [C]// Australasian Conference on Information Security and Privacy (ACISP). Australasian, Springer, 2004: 200-211

[5] Libert B, Quisquater J J. On construction certificateless cryptosystems from identity based encryption [C]// The Ninth International Conference on Theory and Practice in Public-Key Cryptography. New York, USA, Springer, 2006: 474-490

[6] Zhang Z, Wong D, Xu J, et al. Certificateless public-key signature: security model and efficient construction [C]// ACNS 2006, LNCS 3989. Springer-Verlag, 2006: 293-308

[7] Au M, Chen J, Liu J, et al. Malicious KGC Attacks in Certificateless Cryptography [C]// ACM ASIACCS'07. Singapore, 2007: 302-311

[8] Fábrega F J T, Herzog J C, Guttman J D. Strand spaces: Why is a security protocol correct [C]// The 1998 IEEE Symp on Security and Privacy. Los Alamitos, IEEE Computer Society Press, 1998: 160-171

[9] Fábrega F J T, Herzog J C, Guttman J D. Strand spaces: Proving security protocols correct [J]. Journal of Computer Security, 1999, 7(10): 191-230

[10] Fábrega F J T, Herzog J C, Guttman J D. Authentication tests [C]// 2000 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, May 2000: 96-109

[11] Dolev D, Yao A. On the security of public-key protocols [J]. IEEE Trans. on Information Theory, 1983, 29(2): 198-208

[12] Long Shi-gong, Luo Wen-jun, Pen Chang-gen, et al. Modeling and Analysis of Guessing Attacks in Strand Spaces [C]// The IET International Conference on Wireless, Mobile&Multimedia Networks (IET ICWMMN2006). Hangzhou, China, IEEE, 2006: 565-568

[13] 沈海峰，薛锐，黄河燕，等. 串空间理论扩展[J]. 软件学报，2005, 16(10): 1784-1789

[14] Shen H F, Xue R, Huang H Y, et al. Extending the theory of strand spaces [J]. Journal of Software, 2005, 16(10): 1784-1789