

异构云匿名身份认证方案设计

王崇霞¹, 高美真², 刘 倩³, 周贤伟³

(1 长治学院 计算机系, 山西 长治 046010; 2 焦作师范高等专科学校 计算机与信息工程学院, 河南 焦作 454000;
3 北京科技大学 计算机与通信工程学院, 北京 100083)

摘 要: 针对异构云间资源互访、信息交互的需求, 提出了一种基于双线性映射和身份密码体制的异构云匿名身份认证协议. 该协议避免了传统认证协议建立和维护证书的繁琐弊端, 实现了异构云间双向实体认证和资源访问主体匿名性. 通过认证过程的鉴别验证和设置身份期限, 既保障了认证安全性、密钥新鲜性, 又减少了频繁异构云服务申请的过渡认证开销. 通过分析对比, 协议具有安全高效的特点, 能满足异构云间用户数量众多、服务访问频繁的认证需求.

关键词: 异构云; 身份认证; 匿名性; 双线性映射; 信息交互; 安全性

中图分类号: TP393.0

文献标识码: A

文章编号: 1000-7180(2014)07-0037-05

Anonymous Authentication Scheme Design for Heterogeneous Clouds

WANG Chong-xia¹, GAO Mei-zhen², LIU Qian³, ZHOU Xian-wei³

(1 Department of Computer Science, Changzhi University, Changzhi 046010, China;

2 Department of Computer and Information Engineering, Jiaozuo Teachers College, Jiaozuo 454000, China;

3 School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: In view of the resources visits and information interaction among heterogeneous clouds, the paper proposes a heterogeneous cloud anonymous identity authentication protocol based on bilinear map and identity - based cryptography for heterogeneous clouds. The protocol avoids the drawback of the traditional authentication protocols to establish and maintain certificates, achieves mutual authentication and identity anonymity in heterogeneous clouds. In the other hand, the protocol realizes authentication security and key freshness through the process of Identification and Authentication and set a deadline of identity, and reduces a lot of authentication cost of applying for frequent heterogeneous cloud services. By analyzing the contrast, the protocol is secure and efficient, and satisfies authentication requirement for many users and service access frequently for heterogeneous clouds.

Key words: Heterogeneous cloud; Identity Authentication; Anonymity; Bilinear map; Information interaction; Security

1 引言

为保护云中资源免受非授权用户的访问, 云服务提供商通过认证授权机制限制用户对云中资源的访问, 由于不同的云可能使用不同的认证授权体系, 这就导致了用户在访问不同云中资源时需要多次注册认证, 一方面增加运行开销, 降低系统执行效率;

另一方面, 用户在不同的应用中使用不同的身份和口令(或相同的身份和口令)多次登录, 极易造成密码被攻击. 由于云中认证信息应在保证用户隐私的前提下进行, 当其他云用户请求服务时, 云服务提供商必须在确保用户身份有效时, 才能为用户提供服务^[1].

签名算法集合签名和加密的功能, 可以极大的提高通信的安全性和认证性. 文献[2-4]中提出了签名

收稿日期: 2013-09-28; 修回日期: 2013-11-22

基金项目: 国家自然科学基金(61003250, 61170014); 教育部科学技术研究重大项目(311007)

算法,实现一个 PKG (Private Key Generator, PKG) 中的用户可通过签密实现安全信息传输,而文献[2]中的签密算法存在不具有语义安全性的缺陷。

本文以私有云为例,设计了一种基于身份的通用的异构云间认证模型.该模型的主要目的是通过异构云 PKG 间的安全签密算法,实现异构云间的匿名身份认证,达到异构云间共享资源和服务的目的。

2 相关知识

云分为三种类型:公共云(Public Cloud)、私有云(Private Cloud)和混合云(Hybrid Cloud)^[5]。

基于身份的密码体制 IDPKC^[6]中使用主密钥、用户公钥、用户私钥三种密钥,公钥通常是从标识用户身份的信息中提取,用户私钥由私钥生成器根据主密钥和公钥生成.IDPKC 不使用证书,但它能够实现在不交换密钥的情况下使实体间安全通信,避免了建立维护证书、保护证书链的繁琐弊端。

目前大多数基于身份的密码方案都是基于离散对数和双线性对来构造的,离散对数和双线性对描述如下:

定义 1 离散对数问题(discrete logarithm problem, DLP)^[7]: 对于一个有限循环群 $G = \langle p \rangle$ 和元素 $x \in G$, 寻找整数 $r \in \mathbb{Z} q^* (0 \leq r \leq |G|)$, 使得 $x = p^r$ 成立. 离散对数问题是公认数

学难题,目前还没有有效的解决离散对数的算法。

定义 2 双线性映射^[7]: G_1, G_2 分别是阶为 q 的循环加法和循环乘法群,假设 G_1, G_2 中的离散对数问题是困难问题,则称 $e: G_1 \times G_1 \rightarrow G_2$ 为双线性映射,且 e 满足下面属性:

① 双线性: 对任意 $Q, R, S \in G_1, a, b \in \mathbb{Z} q^*$, 有

$$e(aQ, bR) = e(Q, bR)^a = e(aQ, R)^b = e(Q, R)^{ab}$$

$$e(Q, R + S) = e(Q, R) e(Q, S)$$

$$e(Q + R, S) = e(Q, S) e(R, S)$$

② 非退化性: 存在 $P, Q \in G_1$, 使 $e(P, Q) \neq 1_{G_2}$.

③ 可计算性: 存在一个有效的算法对于任何 $Q, R \in G_1$, 计算 $e(Q, R)$ 。

3 异构云身份认证模型设计

3.1 异构云身份认证模型

如图 1 所示,假设私有云 A 和 B 均有自己的认证授权机制,当用户 U_A 希望成为云 A 的用户时,必须首先在云 A 中注册成为云 A 的成员,云 A 的认证服务器 $AS_A(PKG_A)$ 为其发放私钥,当用户 U_A 申请访问本云的资源或服务时,直接认证申请服务;当用户 U_A 申请云 B 的资源或服务时,云 A、B 的认证服务器就需要联合起来,实现对 U_A 的异构云认证。

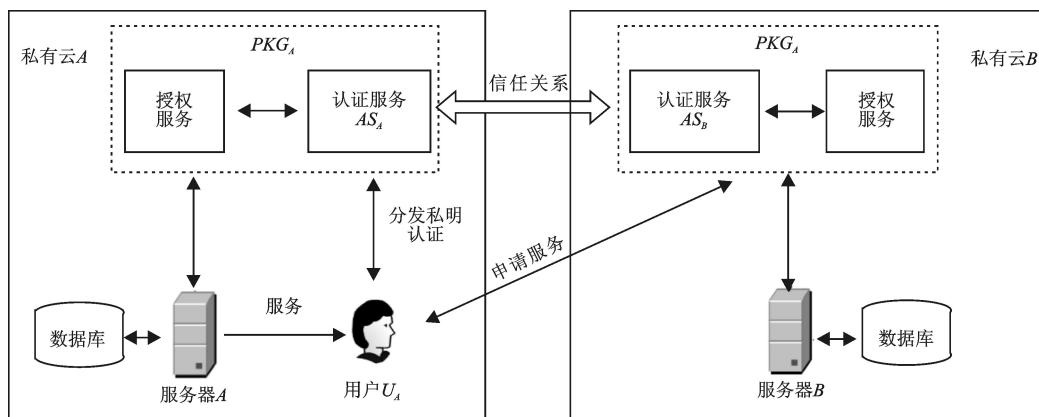


图 1 异构云认证模型

3.2 异构云认证服务器间信任关系的建立

本文提议的异构云的 PKG 间的信任关系是通过签密算法建立的,首先假设通信双方使用的系统参数完全相同,这个假设在现实 IDPKC 签密方案中是完全可行的. 签密算法从四个方面描述,系统初始化(Setup)、用户密钥产生(Extract)、签密(Signcrypt)、解签密(Unsigncrypt)。

Setup: 设 q 是一个大素数, G_1, G_2 分别为 q 阶加法循环群和乘法循环群,且 $e: G_1 \times G_1 \rightarrow G_2$ 是双线性映射, p 是 G_1 的生成元,定义对称加解密算法 (E, D) 和 hash 函数 $H_1, H_2, H_3: H_1: \{0, 1\}^* \times G_1 \rightarrow G_1, H_2: \{0, 1\}^* \rightarrow \mathbb{Z} q^*, H_3: G_2 \rightarrow \{0, 1\}^n (n \in \mathbb{Z})$ 。

Extract: 在云 A 中, PKG_A 产生随机数 $S_A \in \mathbb{Z} q^*$, 计算 $P_{pubA} = S_A p \in G_1$, 并选择随机数 S_A 为

主私密钥, P_{pubA} 为公钥, PKG_A 保存主密钥 S_A , 并公布系统参数 $parameterA = \{q, G_1, G_2, p, P_{pubA}, H_1, H_2, H_3\}$

同理云 B 中产生的类似的系统参数:

$S_B \in \mathbb{Z} q^*, P_{pubB} = S_B p \in G_1, S_B$ 为主密钥, P_{pubB} 为公钥, 公布系统参数 $parameterB = \{q, G_1, G_2, p, P_{pubB}, H_1, H_2, H_3\}$.

Signcrypt(m): 云 A 的认证服务器使用自己的公私钥 S_A, P_{pubA} 、云 B 的公钥 P_{pubB} 、云 A 和 B 的身份信息对数据 m 签密, 建立 PKG_A 与 PKG_B 间的信任关系, 过程如下:

选择随机数 $x \in \mathbb{Z} q^*$, 计算: $U = xp, y = e(p, xP_{pubB})^{S_A} \in G_2, k = H_3(y), r = H_2(U \parallel ID_{ASA} \parallel m), C_{B0} = H_1(ID_{ASB}), C = E_k(m), V = S_A C_{B0} + r x P_{pubB}$, 发送密文 $\sigma = (C, U, V)$

Unsigncrypt(σ): PKG_B 用私钥 S_B 及云 A、B 的身份信息解密密文 σ 并验证信息.

计算: $y = e(P_{pubA}, U)^{S_B}, k = H_3(y), m = D_k(C), r = H_2(U \parallel ID_{ASA} \parallel m)$. 验证: $e(V, p) = e(C_{B0}, P_{pubA}) e(U, P_{pubB})^r$ 是否成立, 若成立, 则云 B 接受数据, 否则验证失败.

本文提出的签密算法借鉴文献[3]中对称加密算法的思想对文献[2]中的签密算法进行改进, 与文献[2]中的签密算法相比, 本文提出的签密算法实现在两个 PKG 间建立通信信任关系, 与原方案具有同样的机密性和不可伪造性(具体证明同文献[2-3]), 且具有语义安全性, 说明如下:

不具有语义安全性是因为在 IND-IDSC-CCA 游戏中, 攻击者不能简单验证区分签名的明文(如 m_0, m_1) 与之对应的密文^[3]. 在本签密方案中, $y = e(p, xP_{pubB})^{S_A} = e(P_{pubA}, U)^{S_B}, k = H_3(y), C = E_k(m)$, 密钥 k 依据随机数 x 的不同而具有随机性, 所以对明文 m_0 和 m_1 加密的密钥不同, 致使密文也不同, 即使同一明文由于随机密钥而计算出不同的随机密文, 所以消息 m 的密文具有随机性和保密性. 因此, 本签密算法具有语义安全性.

4 异构云身份认证协议

异构云间的身份认证主要包括: 系统建立, 用户注册, 用户认证(云间), 密钥更新四个阶段. 系统建立由云 A、B 的 PKG 设置需要的系统参数.

4.1 用户注册

如 3.2 节所示, 云 A 的系统公私钥分别为 S_A 和 P_{pubA} , 云 B 的系统公私钥分别为 S_B 和 P_{pubB} , 云中用

户注册过程描述如下(以云 A 为例):

(1) 用户 U_A 提出注册申请, 将身份信息 $ID_{UA} \in \{0, 1\}^*$ 发送给认证服务器 AS_A .

(2) PKG_A 生成随机数 $r_A, r_A \in \mathbb{Z}_p^*$, PKG_A 计算 $R_A = r_A p, S_{UA} = S_A C_{UA}, C_{UA} = H_1(ID_{UA}, R_A)$, PKG_A 将私钥 (S_{UA}, R_A) 通过安全信道发送给用户 U_A .

(3) U_A 收到密钥后, 计算等式 $S_{UA} p = H_1(ID_{UA}, R_A) P_{pubA}$ 是否成立来验证用户私钥的正确性, 若正确, 用户保存私钥; 否则反馈信息.

(4) 认证服务器 AS_A 在认证数据库中建立以 Ind_{UA} 为索引关键字的 U_A 账户信息, 包括 Ind_{UA}, ID_{UA}, R_A , 有效期等, 其中 $Ind_{UA} = H_3(e(S_{UA}, P_{pubA}))$, 并为用户建立授权属性信息, 以便服务器在用户申请资源时授权.

4.2 异构云间用户认证

当用户 U_A 申请访问本云中的资源和服务时, 按照云内用户管理和认证方式申请资源, 若用户 U_A 申请访问云 B 中的资源而云 B 没有关于 U_A 的账户信息时, 需要实现异构云认证, 以 U_A 申请云 B 资源为例描述如下:

(1) 用户 U_A 选择随机数 n_1 .

(2) 计算 $N_{UA} = n_1 p, C_{UA} = H_1(ID_{UA}, R_A), \omega = e(n_1 C_{UA}, P_{pubA})$, 并为用户建立临时身份 $L_{UAid}, L_{UAid} = \{\omega, C_{UA}\}$.

(3) U_A 向认证服务器 AS_B 发送消息 $\{ID_{ASA}, N_{UA}, L_{UAid}\}$.

(4) AS_B 收到 U_A 发来的认证申请信息, 产生签密信息 $M_1 = \text{Signcrypt}(m_1)$ 并发送到 AS_A , 其中 $m_1 = \{ID_{ASA}, L_{UAid}, N_{UA}, ID_{ASB}\}$.

(5) AS_A 收到密文 M_1 , 计算 $\text{Unsigncrypt}(M_1)$, 若正确解密, AS_A 通过对 AS_B 的验证, 计算 $Ind_{UA} = H_3(e(C_{UA}, P_{pubA})^{S_A})$, 在认证数据库中检索 Ind_{UA} 的用户, 取出此账户的其他信息如 ID_{UA}, R_A 等, 计算 $\omega = e(N_{UA}, S_{UA})$, 验证 $\omega = \omega$ 是否成立, 成立则确定请求资源的用户 U_A 为云 A 的合法用户. 然后计算 $\delta = e(N_{UA}, S_A R_A), K = H_2(R_A \parallel N_{UA})$, K 即为此后 AS_B 和 U_A 的会话密钥, 产生签密信息 $M_2 = \text{Signcrypt}(m_2)$ 并发送到 AS_B , 其中 $m_2 = \{\delta, ID_{ASA}, ID_{ASB}, K\}$.

(6) AS_B 收到密文 M_2 , 计算 $\text{Unsigncrypt}(M_2)$, 若解密正确, AS_B 通过对 AS_A 和 U_A 的验证, 确认 U_A 为 AS_A 的一名合法用户. AS_B 为用户 U_A 建立账户 L_{UAid} , 并赋予其访问云 B 需要的信息, 包含私钥

(R_A', S_{UA}')、访问许可、权限、身份保留期及身份有效期(身份保留期将根据 L_{UAid} 申请云 B 服务而动态调整,如每访问一次云 B 服务器身份保留时间期将增加 x 秒;身份有效期 = 身份保留时间 + y 秒,在实际应用中,为了实现密钥的及时更换,可以设置身份保留期的最大时间,当身份保留期到达最大时间时,必须更换 U_A 与云 B 的会话密钥), L_{UAid} 成为云 B 的一名临时成员. AS_B 通过安全信道将 L_{UAid} 的私钥 (R_A', S_{UA}') 发送到 U_A , 产生密文 $m_3 = E_k(L_{UAid}', \delta)$, 并将 m_3 发送到 U_A .

(7) U_A 收到消息后, 计算密钥 $K = H_2(R_A \parallel xp)$, 解密密文 m_3 , 计算 $\delta = e(P_{pubA}, R_A)^{n_1}$, 验证 $\delta = \delta$ 是否成立, 若成立, U_A 验证 AS_B , 确认本次异构云认证申请通过, U_A 暂时保存身份信息 L_{UAid} 、私钥(R_A', S_{UA}')、密钥 K 等信息, 并以身份 L_{UAid} 申请云 B 的资源.

4.3 密钥更新

在 L_{UAid} 的身份保留期限内, 如果用户 U_A 再次申请云 B 中资源或服务时, 可以以身份 L_{UAid} 及云 B 赋予的其他身份信息按照云 B 的认证方式申请认证. 当 L_{UAid} 身份保留期限到而没有到达身份有效时间, 用户 U_A 再次申请服务时, 需要更新会话密钥 K 和 L_{UAid} 的私钥.

(1) 用户 L_{UAid} 选择随机数 n_2 .

(2) 计算 $N_{UA}' = n_2 p$, $C_{UA}' = H_1(L_{UAid}, R_A')$.

(3) L_{UAid} 向认证服务器 AS_B 发送密文 $E_k(L_{UAid}, N_{UA}')$, AS_B 解密密文, 为用户 L_{UAid} 产生新的私钥(R_A', S_{UA}'), 并通过安全信道将其发送给用户 U_A , 计算新的会话密钥 $K' = H_2(R_A' \parallel N_{UA}')$, 密钥 K' 即为此后 AS_B 和 U_A 的会话密钥.

当 L_{UAid} 的身份有效期已到, L_{UAid} 的身份将从云 B 的认证服务器中删除, 当用户 U_A 申请访问云 B 中资源时, 需重新申请异构云认证.

5 方案分析

5.1 安全性分析

(1) 认证安全性

本文提议的认证协议是基于实体双向认证和接收方验证的基础上实现的. 当用户 U_A 申请异构云服务时, 首先向 AS_B 提出申请, 同时发去验证信息 ω , AS_B 向 AS_A 发出密文 M_1 , AS_A 解密 M_1 时也验证了 AS_B 的身份; AS_A 计算 Ind_{UA}' 和 ω' , 确认 U_A 为云 A 合法用户, 依据认证数据库中 U_A 的身份信息, 计算 δ , 发出密文 M_2 , AS_B 解签密, 实现了 AS_B 对 AS_A

验证, AS_A 、 AS_B 对 U_A 的认证. AS_B 为 U_A 建立访问云 B 的临时身份信息, 并用密钥 K 加密信息 m_3 发送给 U_A , U_A 通过计算密钥和验证 δ 实现对 AS_A 、 AS_B 的认证, 因此整个认证过程实现 AS_A 、 U_A 、 AS_B 间的相互双向认证. 由于提议的异构云间认证方案采用可证明安全的签密算法和随机数, 可以有效地预防伪造和重放攻击, 即使攻击者截获了密文, 也不能实现信息的进一步验证, 所以提议的异构云间认证协议是认证安全的.

(2) 密钥的安全性

本文提议的异构云认证方案中, 用户 U_A 和云 B 之间的会话密钥 K 是安全的. AS_A 在确定 U_A 为其合法用户后, 利用 U_A 私钥 R_A , 计算会话密钥 K , 并将会话密钥 K 通过签密发送给 AS_B , 由于签密算法是可证明安全的, 具有机密性和不可伪造性, 且仅只有 AS_A 和 U_A 知道用户 U_A 的私钥 R_A , R_A 并不在网络中传输, 所以攻击者是不可能获得 R_A 的信息, 而 $\delta = e(N_{UA}, S_{AR_A})$, $\delta' = e(P_{pubA}, R_A)^{n_1}$, 在 δ 、 δ' 中的参数只有 AS_A 和 U_A 能获得, 攻击者是无法验证 $\delta = \delta'$, 所以用户 U_A 和云 B 之间的会话密钥 K 是安全的.

其次, 本文提议的认证方案中为临时身份 L_{UAid} 设置了两个身份期限: 身份保留期和身份有效期. 通过临时身份期限的设定, 实现会话密钥的及时更换和临时身份有效期的限制, 保障了密钥的新鲜性和安全性.

(3) 主体匿名性

匿名性是指通信实体的一种状态, 使该实体无法从一个实体集合中识别出来^[8]. 本文所述的匿名性主要是指网络通信过程中用户身份标识的不确定.

在本文提议的认证方案中, 用户 U_A 以临时身份 L_{UAid} 发起异构云身份认证申请, 在整个认证过程中, 用户 U_A 一直以临时身份 L_{UAid} 完成与 AS_A 、 AS_B 的交互认证, 整个认证过程中仅只有 AS_A 在计算出 Ind_{UA}' 并核实 $\omega' = \omega$ 后, AS_A 才了解并确定 L_{UAid} 的身份, AS_B 在整个认证过程中仅只知道临时身份 L_{UAid} 为云 A 中的合法用户, 无法确定用户的真实身份. 所以本文提议的认证方案具有主体匿名性.

5.2 性能分析

当用户申请异构云资源时, 本文提议的认证方案类同于一次一密, 但当异构云间用户数量众多, 服务访问频繁时, 如果采用一次一密, 生产密钥的开销太大, 提议的认证方案为申请异构云服务的用户设置临时身份 L_{UAid} , 并设置了两个身份期限: 身份保

留期和身份有效期. 由于身份保留期根据用户申请服务的频率动态调整, 在身份有效期内, 当用户频繁申请异构云服务时, 只需在第一次申请异构云资源时执行云间认证协议; 在身份保留期内, 用户 U_A 和云 B 之间的会话密钥 K 的保留时间可以达到身份保留期的最大时间, 避免了频繁更换密钥所带来的额外开销; 在身份保留期到而身份有效期未到时, 更换 U_A 与 AS_B 之间的密钥, 不需执行跨云认证, 既保障了密钥的新鲜性, 又减少了认证开销; 一旦身份有效期到, 必须重新申请异构云认证. 这样即保障了异构云认证中更换密钥的安全需求, 又减少了异构云间的大量用户频繁服务申请所带来的过渡认证负担, 实现了在服务动态和环境异构的前提下安全高效的云间认证.

另外, 提议的认证方案采用了基于身份的密码体制, 不需要证书, 减少了证书的管理开销. 用户和异构云间的信息传输采用对称加解密算法, 计算量小, 有利于提高认证访问效率.

综合安全与性能分析的各个方面, 与文献[9-10]比较, 结果如表1所示.

表1 方案比较

方案	双向 认证	密钥 安全性	主体 匿名性	预防重 放攻击	预防伪 造攻击	握手 次数
文献[9]	是	*	是	是	是	6
文献[10]	是	*	否	是	是	8
提议方案	是	是	是	是	是	5

注: 表中“*”表示没有涉及此项内容.

6 结束语

为实现异构云间的服务互访, 本文提出了一种基于双线性映射的异构云间匿名身份认证协议, 该协议避免了基于证书的认证协议建立、维护证书的各种资源消耗, 实现了异构云间双向实体认证和资源访问主体匿名性, 通过设置异构云间认证过程中各阶段对认证实体的鉴别验证, 提高了认证安全性. 当异构云间用户数量众多、服务访问频繁时, 提议的认证方案通过设置两个身份期限既保障了密钥新鲜性, 又减少了频繁异构云服务申请的过渡认证开销. 通过性能分析, 该协议具有安全高效的特点, 能够满足异构云间的认证需求. 下一步将对云计算环境的

多服务器协作进行研究.

参考文献:

- [1] Yan L, Rong C, Zhao G. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography[C]//First International Conference, CloudCom 2009. Beijing, China, 2009:167-177.
- [2] Malone Lee J. Identity-based signcryption[R]. Cryptology ePrint Archive, 2002/098, 2002.
- [3] Libert B, Quisquater J J. A new identity-based signcryption schemes from pairings[C]//2003 IEEE Information Theory Workshop. Paris, France, 2003:155-158.
- [4] 曾诚, 李兵, 何克清. 云计算的栈模型研究[J]. 微电子学与计算机, 2009, 26(8): 23-27.
- [5] 马蕾, 杨洪雪, 朱青松. 基于改进身份认证协议的单点登录系统研究[J]. 微电子学与计算机, 2012, 29(7): 180-184.
- [6] Shamir A. Identity-based cryptosystems and signature schemes[C]//Pro 4th Annual International Cryptology Conference on Advances in Cryptology. New York, USA: Springer-Verlag, 1984: 47-53.
- [7] 张华, 温巧燕, 金正平. 可证明安全算法与协议[M]. 北京: 科学出版社, 2012: 45-50.
- [8] Ian Goldberg, Douglas Stebila, Berkant Ustaoglu. Anonymity and one-way authentication in key exchange protocols [J]. Designs, Codes and Cryptography, 2012, 67(2): 245-269.
- [9] Zhang Qikun, Li Yuanzhang, Song Danjie, et al. Alliance-authentication protocol in clouds computing environment[J]. 中国通信, 2012, 9(7): 43-54.
- [10] Kim J, Hong S. A consolidated authentication model in cloud computing environments [J]. International Journal of Multimedia and Ubiquitous Engineering, 2012, 7(3): 151-160.

作者简介:

王崇霞 女, (1970-), 硕士, 副教授. 研究方向为密码学与网络安全、云计算.

高美真 女, (1970-), 硕士, 副教授. 研究方向为图形图像处理、云计算.

刘倩 女, (1987-), 博士研究生. 研究方向为智能网络及网络安全.

周贤伟 男, (1963-), 博士, 教授、博士生导师. 研究方向为云计算、智慧网络、空间网络等.