一种新的信息服务实体跨域认证模型

谢艳容 马文平 罗 维

(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 为解决基于身份的信息服务多信任域认证系统不能实现身份即时撤销的问题,提出了一种可撤销的身份签名方案。在SM9(国产标识密码)签名算法的基础上,引进一个安全仲裁来保管实体的部分私钥,通过终止安全仲裁给实体发送签名信令来撤销实体的签名能力,从而实现身份的即时撤销。在该方案的基础上,利用基于证书的公钥基础设施(PKI)与基于身份的密码体制(IBC)的组合应用优点,提出了一种新的信息服务实体跨域认证模型。该模型不仅具有灵活高效的认证特点,而且适合构建大规模信息服务实体的应用环境。同时,设计了一种跨域认证协议,实现了跨信任域的双向实体认证和密钥协商。分析结果表明,该协议具有较高的安全性及较少的通信量和计算量。

关键词 信息服务,认证,SM9,安全仲裁,身份撤销,密钥协商

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.09.029

New Cross-domain Authentication Model for Information Services Entity

XIE Yan-rong MA Wen-ping LUO Wei

(State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China)

Abstract To solve the problem that the identity of information services entity(ISE) cannot be revoked immediately in the cross-domain authentication system, a revocable identity-based signature scheme was proposed. Based on the SM9 signature algorithm, a security mediator(SEM) was introduced to keep a part of the private key of the ISE. By terminating the SEM to send the token to ISE to revoke its signature capability, the identity of ISE can be revoked immediately. Based on this scheme, a new cross-domain authentication model for ISE was proposed by taking the combining advantages of certificate-based public key infrastructure(PKI) and identity-based cryptography(IBC). The proposed model is not only flexible and efficient, but also suitable for constructing large-scale application environment of ISE. Meanwhile, a cross-domain authentication protocol was designed to realize the mutual authentication with key agreement between cross-domain entities. Analysis shows that the proposed protocol has high security and low communication and computation cost.

Keywords Information services, Authentication, SM9, Security mediator, Identity revocation, Key agreement

1 引言

针对大规模异构网络环境下不同种类信息服务实体(Information Services Entity,ISE)之间存在多业态交互复杂的结构模式,研究信息服务可信标识的签发、更新、撤销和跨域认证机制具有重要意义[1]。

在分布式网络环境中,跨信任域的认证方案主要基于3个框架[2]:1)基于对称密钥的认证框架;2)基于X.509数字证书的公钥基础设施(Public Key Infrastructure,PKI)认证框架,该框架避开了复杂的对称密钥管理难题,适合构建大型的应用环境;3)基于身份的密码体制(Identity-Based Cryptography,IBC)认证框架,该框架简化了证书的管理,具有无目录、使用方便、易于维护等优点。目前,基于身份的多信任域认证模型[2-4]成为主流,较传统PKI认证框架在通信和计算成本上更具优势。文献[2]的模型在实现IBC域间认证的同时保证了实体的匿名性,但是该协议被证明容易受到假冒攻击。文献[5]提出了一种安全的匿名认证方案,其可以抵抗假冒攻击。文献[6]于2013年提出了两种适用于移动设备的基于身份的认证方案,但是这两种方案都存在安全漏洞,容易受到假冒攻击和密钥泄露假冒攻击。文献[7]提出了一种改进的2PAKE方案,该改进方案可以弥补上述缺点,保证了客户端与服务器间的通信安全。为了降低通信成本,文献[8]基于计算Diffie-Hellman问题提出了基于身份的双方认证密钥协商协议,消除了双线性对运算。文献[9]于2017年提出了两种

到稿日期:2017-08-05 返修日期:2017-11-13 本文受国家自然科学基金(61373171),高等学校创新引智计划项目(B08038),国家重点研发计划重点专项(2017YFB0802400)资助。

谢艳容(1992-),女,硕士生,主要研究方向为信息安全和通信理论,E-mail:xyrong1226@163.com;**马文平**(1966-),男,教授,博士生导师,主要研究方向为密码学和信息安全,E-mail:wp_ma@mail.xidian.edu.cn(通信作者);**罗 维**(1987-),男,博士生,主要研究方向为密码学和云计算安全。

异构域之间的密钥协商协议，其可以安全高效地实现 PKI 域与 IBC 域之间的认证。

在基于身份的认证系统中，实体身份的即时撤销是一个难题，而上述方案并未考虑身份的撤销。为了保障用户访问的信息服务资源是合法的，需要设计一种可撤销的签名方案来实现基于身份的信息服务多信任域的跨域认证。现有的基于身份的认证方案通常是由私钥生成中心(Private Key Generator，PKG)停止为实体更新私钥来达到密钥撤销的目的，这就要求 PKG 必须保持在线，并且该方法不能立即撤销实体身份。文献[10]提出将实体的标识和时间有效期附加到实体公钥中，但它需要事先知道何时撤销，不够灵活。文献[11]提出了第一个基于仲裁的身份签名(Mediated Identity-Based Signature，mIBS)方案。该方案引入了一个安全仲裁(Security Mediator，SEM)，PKG 将实体的私钥分割成两部分，分别由 SEM 和实体保管，通过命令 SEM 停止为实体生成签名信令来实现身份的快速撤销。但是，该方案将明文消息发送给 SEM 验证也是不安全的。文献[12-13]利用此思想解决了多媒体互联网中用户的立即撤销和密钥更新问题。

由于政府部门高度重视国产密码算法的推广，SM9 密码算法作为一种基于双线性对的标识密码体制(IBC)得到了迅速的发展[14]。本文基于仲裁的身份撤销机制对 SM9 数字签名算法[14]进行改进，设计了一种可撤销的身份签名方案(SM9_mIBS)。通过分析现有的认证框架可知，IBC 不适合在大型的网络环境中使用，因此结合 PKI 和 IBC 的互补性优点，提出了针对信息服务实体的跨域认证模型来实现大规模异构网络环境下信息服务实体与用户的交互；并且基于 SM9_mIBS 方案设计了跨域双向实体认证协议，通过与现有协议对比得出该协议是安全的，其通信量和计算量的增幅较小，因此该协议不仅具有可撤销性，而且符合国家对国产密码的推广需求。

2 基于仲裁的 SM9 签名方案

2.1 SM9_mIBS 方案

为了实现基于身份的信息服务实体的跨域认证，本文给出了一种可撤销的身份签名方案(SM9_mIBS)。该方案包括 4 个算法：参数生成算法(Setup)、密钥生成算法(KeyGen)、签名算法(Sign)和验证算法(Verify)。

(1)Setup

设$(G_1,+)$，$(G_2,+)$，$(G_T,\cdot)$是 3 个阶为素数 $N(N>2^{\lambda})$的循环群，P_1 是 G_1 的生成元，P_2 是 G_2 的生成元，存在 G_2 到 G_1 的同态映射 ψ，使 $\psi(P_2)=P_1$；双线性对 e 是 $G_1\times G_2\rightarrow G_T$ 的映射，满足双线性性、非退化性、可计算性[10]。

与 SM9 数字签名算法(SM9_IBS)相同，使用两类辅助函数：密码杂凑函数和随机数发生器[14]。选取密码函数 $H_1(Z,n)$和 $H_2(Z,n)$，输入为比特串 Z 和整数 n，输出分别为整数 $h_1\in[1,n-1]$和整数 $h_2\in[1,n-1]$。其中，$H_1(Z,n)$和 $H_2(Z,n)$都调用 SM3 密码杂凑函数 $H_v()$。

PKG 产生随机数 $s\in[1,N-1]$作为系统主密钥，计算 G_2 中的元素 $P_{pub}=[s]P_2$ 作为系统公钥，则主密钥对为(s,P_{pub})。PKG 秘密地保存主密钥 s，系统公开参数为$(N,P_1,P_2,G_1,G_2,P_{pub},H_1,H_2)$。

(2)KeyGen

1)ISE 密钥生成

PKG 选择并公开用一个字节表示的私钥生成函数识别符 hid。

设 ISE 的标识为 ID，公私钥分别为 Q_{ID} 和 d_{ID}。PKG 首先计算 $t_1=H_1(ID\|hid,N)+s$，若 $t_1=0$ 则重新产生主密钥和系统公钥，并更新已有的 ISE 私钥；否则计算 $t_2=s\cdot t_1^{-1}$，$d_{ID}=[t_2]P_1$。

$$d_{ID}=[t_2]P_1=[s/(H_1(ID\|hid,N)+s)]P_1 \tag{1}$$

$$Q_{ID}=[H_1(ID\|hid,N)]P_2+P_{pub} \tag{2}$$

2)密钥分割

PKG 随机选择 $s_1\in[1,N-1]$，计算 $d_{ID}^{ISE}=[s_1/(H_1(ID\|hid,N)+s)]P_1=[\frac{s_1}{t_1}]P_1$，则 $d_{ID}^{sem}=d_{ID}-d_{ID}^{ISE}=[(s-s_1)\bmod N/t_1]P_1$，并将 d_{ID}^{ISE}发送给 ISE，d_{ID}^{sem}交给 SEM 秘密保存。

(3)Sign

设待签名消息为比特串 M，为了获取 M 的数字签名(h,S)，ISE 和 SEM 应执行以下步骤。

1)ISE 对消息 M 签名前

①随机选择点 $P_1\in G_1$，整数 $r\in[1,N-1]$；

②计算群 G_T 中的元素 $w=e(P_1,P_{pub})^r$，将 w 的数据类型转换为比特串；

③计算整数 $h=H_2(M\|w,N)$，$L=(r-h)\bmod N$；若 $L=0$ 则返回①；

④将请求 $R=(ID,L)$发送到 SEM 以申请签名信令。

2)SEM 收到签名请求后

①检查 ISE 的 ID 是否被撤销，如果 ID 已被撤销，则返回“ID 已撤销”，否则进入②；

②SEM 计算签名信令 $S_{sem}=[L]\cdot d_{ID}^{sem}=[L][(s-s_1)\bmod N/t_1]P_1$，并将 S_{sem}发送给 ISE。

3)ISE 签名

①计算签名 $S_{ISE}=[L]\cdot d_{ID}^{ISE}=[L][s_1/t_1]P_1$；

②收到 SEM 的信令 S_{sem}后，计算签名 $S=S_{sem}+S_{ISE}$；

③计算 $P=[H_1(ID\|hid,N)]P_2+P_{pub}$，$w'=e(S,P)\cdot e(P_1,P_{pub})^h$；

④验证：$w'=w$，检验信令 S_{sem}是否为本次签名请求的有效信令。当且仅当 $w'=w$，将 h 和 S 的数据类型转换为字节串，输出消息 M 的数字签名(h,S)。

(4)Verify

验证者收到消息 M'及其数字签名(h',S')后对其进行如下验证。

1)将 h'的数据类型转换为整数，检验 $h'\in[1,N-1]$是否成立，若不成立则验证不通过；

2)将 S'的数据类型转换为椭圆曲线上的点，检验 $S'\in G_1$是否成立，若不成立则验证不通过；

3)计算整数 $h_1=H_1(ID\|hid,N)$，群 G_2 中的元素 $P=[h_1]P_2+P_{pub}$；

4)计算群 G_T 的元素 $g=e(P_1,P_{pub})^{h'}$，$u=e(S',P)$，$w'=$

$u \cdot g$，将 w' 的数据类型转换为比特串；

5）计算整数 $h_2 = H_2(M' \| w', N)$，当且仅当 $h_2 = h'$，接受 ISE 对消息 M 的签名 (h', S')。

2.2 方案正确性

ISE 通过计算验证因子 $w' = w$ 来检验签名信令 S_{sem} 是否为本次请求的有效信令，只有正确的签名响应才能通过 ISE 验证。此外，当 $w' = w$ 时，显然有 $h_2 = h'$，验证签名通过。

$$\begin{aligned} w' &= u \cdot g = e(S, P) \cdot e(P_1, P_{pub})^h \\ &= e([L] \cdot (d_{ID}^{sem} + d_{ID}^{ISE}), P) \cdot e(P_1, P_{pub})^h \\ &= e([L][t_2]P_1, [h_1]P_2 + P_{pub}) \cdot e(P_1, P_{pub})^h \\ &= e([L][t_2]P_1, [h_1]P_{pub}/s) \cdot e([L][t_2]P_1, P_{pub}) \cdot \\ &\quad e(P_1, P_{pub})^h \\ &= e(P_1, P_{pub})^{[L][t_2]\cdot[h_1]/s} \cdot e(P_1, P_{pub})^{[L][t_2]} \cdot e(P_1, \\ &\quad P_{pub})^h \\ &= e(P_1, P_{pub})^{(r-h) \bmod N + h \bmod N} \\ &= e(P_1, P_{pub})^r = w \end{aligned}$$

2.3 不可伪造性

q-SDHP(q-Strong Diffie-Hellman Problem)问题描述为：在阶为素数 p 的群 (G_1, G_2) 中，给定一个 $q+2$ 元组 $(P, Q, \alpha Q, \alpha^2 Q, \cdots, \alpha^q Q)$，寻找一个对 $(c, \frac{\alpha}{c+\alpha}P)$ 是困难的，这里 $c \in Z_p^*$。

定义 1　如果没有概率多项式时间的敌手 A 以不可忽略的优势赢得下面的游戏，则称 SM9_mIBS 是 EUF-mIBS-CMA(Existential Unforgery against Adaptive Chosen Message and Identity Attacks in the mediated Identity Based Signature)安全的。敌手 A 和挑战者 C 分别是一个多项式时间算法，它们之间的游戏如下：

1）挑战者 C 运行 setup 算法生成系统参数并将其发送给敌手 A，C 保存主密钥 s。

2）敌手 A 对以下预言进行一系列的询问。

①私钥询问。给定标识 ID_i，挑战者 C 生成 ID_i 的部分私钥 $d_{ID_i}^{ISE}$ 和由 SEM 保管的部分私钥 $d_{ID_i}^{sem}$，并将 $d_{ID_i}^{ISE}$ 和 $d_{ID_i}^{sem}$ 发送给敌手 A。

②签名询问。给定标识 ID_i 和明文信息 m_i，挑战者 C 生成 SEM 的签名信令 $token$，并对 m_i 签名，将 $token$ 和签名 s_i 发送给敌手 A。

3）挑战。敌手 A 输出 (ID^*, m^*, s^*)，其中标识 ID^* 和待签名消息 m^* 未进行 2）中的一系列询问。若 s^* 是 ID^* 对 m^* 的有效签名，则 A 赢得该游戏。

定理 1　在随机预言模型中，若存在敌手 A 能够在时间 t 内以 $\varepsilon \geqslant 10(q_s+1)(q_s+q_{H_2})/2^\lambda$ 的优势赢得 EUF-mIBS-CMA 游戏，那么存在算法 B 能够在

$$t' \leqslant 120686 q_{H_1} q_{H_2} \frac{t + O(q_s t_e)}{\varepsilon(1 - q/2^\lambda)} + O(q^2 t_M)$$

时间内解决 q-SDHP 问题（$q = q_{H_1}$）。其中，q_{H_i} 表示随机预言 $H_i (i = 1, 2)$ 的询问次数，q_s 分别表示签名询问次数，t_e 表示一个双线性对的运算时间，t_M 表示一个点乘运算 $Z_{N-1}^* \times G_1^*$ 的时间。

证明：本文利用分叉引理[15]来证明 SM9_mIBS 方案。下面证明 B 可以给 A 提供一个完美的模拟并通过与 A 的交互来解决 q-SDHP 问题。算法 B 输入 $(P_1, P_2, \alpha P_2, \alpha^2 P_2, \cdots, \alpha^q P_2)$，尝试求得 $(\omega, \frac{\alpha}{\omega+\alpha}P_1)$。算法 B 在定义 1 中扮演 A 的挑战者并控制着 SEM，敌手 A 可以进行一系列的询问。

在准备阶段，B 建立一个生成元 $G \in G_1$，得到 $q-1$ 对 $(\omega_i, V_i = \frac{\alpha}{\omega_i+\alpha}G)$，$i \in \{1, \cdots, q-1\}$。为了得到这样的二元组，$B$ 进行以下操作。

1）随机选择 $\omega_1, \cdots, \omega_{q-1} \in Z_{N-1}^*$，并展开：

$$f(z) = \prod_{i=1}^{q-1}(z+\omega_i) = \sum_{j=0}^{q-1} c_j z^j$$

其中，$c_i \in Z_{N-1}^*$。

2）设生成元 $H = \sum_{j=0}^{q-1} c_j(\alpha^j P_2) = f(\alpha)P_2 \in G_2$，则生成元 $G = \psi(H) = f(\alpha)P_1 \in G_1$，公钥为 $H_{pub} = \sum_{j=1}^{q} c_{j-1}(\alpha^j P_2) = \alpha f(\alpha)P_2 = \alpha H \in G_2$。

3）二元组 (w_i, V_i) 可以通过扩展 $f_i(z) = f(z)/(z+\omega_i) = \sum_{j=0}^{q-2} d_j z^j$，并计算 $V_i = \sum_{j=0}^{q-2} d_j(\alpha^{j+1}P_2) = \alpha f_i(\alpha)P_1 = \frac{\alpha f(\alpha)}{\alpha+\omega_i}P_1 = \frac{\alpha G}{\alpha+\omega_i}$ 而得到。

系统公钥为 H_{pub}，对应的私钥为 α。B 将系统参数 (H, G, H_{pub}) 发送给敌手 A。算法 B 随机选择一个挑战身份 ID^* 并发送给 A。

攻击阶段：算法 B 模拟定义 1 中 A 的挑战者，同时维护 L_1 和 L_2 两张列表，分别用于追踪 A 对预言机 H_1 和 H_2 的询问。这里假设 H_1 的询问是不同的，并且身份 ID 在被使用到其他询问之前先进行 H_1 询问。

H_1 询问：这里用一个计数器 μ 来标记询问，其初始值为 1。对于一个 $H_1(ID_\mu \| hid, N)$ 询问，如果 $ID_\mu = ID^*$，则 B 返回一个随机值 $\omega^* \in Z_{N-1}^*$ 作为回答；否则 B 返回 ω_μ 作为回答并增加计数器 μ。两种情况下，B 都将询问和回答存入列表 L_1。

H_2 询问：当 A 询问 $H_2(M_i \| w_i, N)$ 时，B 首先检查列表 L_2 中是否已经存在这个询问的条目，如果存在，则 B 返回系统的回答；否则 B 返回一个随机值 $h_{2,i} \in Z_{N-1}^*$ 作为回答，将元组 $(M_i, h_{2,i})$ 存入列表 L_2。

密钥询问：当 A 询问标识 ID_i 的私钥时，如果 $ID_i = ID^*$，那么 B 失败并停止；否则 B 知道 $H_1(ID_i \| hid, N) = \omega_i$ 和 $V_i = \frac{\alpha G}{\alpha+\omega_i}$，计算并返回 $d_{ID_i}^{ISE}$ 和 $d_{ID_i}^{sem} = V_i - d_{ID_i}^{ISE}$。

签名询问：A 提交一个身份 ID_i 和一个消息 M 给 B。B 首先随机选择 $h \in Z_{N-1}^*$ 和 $S \in G_1$，然后计算：

$$w = e(S, Q_i)e(G, H_{pub})^{-h}$$

其中，$Q_i = H_1(ID_i \| hid, N)H + H_{pub}$。最后，将 $H_2(M \| w, N)$ 的值设为 h。如果 $H_2(M \| w, N)$ 的值已经存在，那么 B 将失败；否则，B 返回签名结果 $\sigma = (h, S)$。

挑战阶段：将身份标识 ID^* 和消息 M 结合在一起，变成一个推广的伪造消息 (ID^*, M)，这样就可以用无身份的分叉引理来证明。

由交叉引理可知，如果敌手 A 在上述交互中是一个有效

的伪造者，那么可以构造一个算法 A'。A'可以输出两个有效的签名$((ID^*,M),h_1,S_1)$和$((ID^*,M),h_2,S_2)$，这里 $h_1\neq h_2$。在这个阶段，B 从列表 L_1 中找到(ID^*,ω^*)。可知，$\omega^*\neq\omega_1,\cdots,\omega_{q-1}$的概率至少为 $1-q/2^{\lambda}$。如果伪造是合法的，那么等式 $e(S_1,Q^*)e(G,H_{\text{pub}})^{-h_1}=e(S_2,Q^*)e(G,H_{\text{pub}})^{-h_2}$成立，其中 $Q^*=H_1(ID^*\parallel hid,N)H+H_{\text{pub}}=(\omega^*+\alpha)H$。由于$e((h_1-h_2)^{-1}(S_1-S_2),Q^*)=e(G,H_{\text{pub}})$，因此 $D^*=(h_1-h_2)^{-1}(S_1-S_2)=\frac{\alpha}{\alpha+\omega^*}G=\frac{\alpha f(\alpha)}{\alpha+\omega^*}P_1$。$B$ 使用长除法将多项式 f 写为 $f(z)=\Psi(z)(z+\omega_i)+\Psi_{-1}$，其中 $\Psi(z)=\sum_{j=0}^{q-2}\Psi_j z^j,\Psi_{-1}\in Z_{N-1}^*$。因此：

$$\frac{f(z)}{z+\omega^*}=\Psi(z)+\frac{\Psi_{-1}}{z+\omega^*}=\sum_{j=0}^{q-2}\Psi_j z^j+\frac{\Psi_{-1}}{z+\omega^*}$$

B 可以计算$\frac{\alpha}{\alpha+\omega^*}P_1=\frac{1}{\Psi_{-1}}(D^*-\sum_{j=0}^{q-2}\Psi_j(\alpha^jP_1))$，并输出$(\omega^*,\frac{\alpha}{\omega^*+\alpha}P_1)$作为 q-SDHP 问题的解。

因此，如果敌手 A 能够在 t 时间内以 $\varepsilon\geqslant 10(q_s+1)(q_s+q_{H_2})/2^{\lambda}$ 的优势赢得 EUF-mIBS-CMA 游戏，那么存在算法 B 能够在

$$t'\leqslant 120686q_{H_1}q_{H_2}\frac{t+O(q_st_e)}{\varepsilon(1-q/2^{\lambda})}+O(q^2t_M)$$

时间内解决 q-SDHP 问题。

3 信息服务实体的跨域认证模型

为了实现大规模异构网络环境下不同种类的 ISE 与用户之间的频繁交互，本文利用 PKI 与 IBC 的组合应用优点设计了一种新的信息服务实体跨域认证模型。由于域代理的数量有限，采用 PKI 实现域间身份的相互认证；而信任域内用户和 ISE 数目的数量级可能很大，因此采用 IBC 来实现高效灵活的身份认证。同时，利用 SM9_mIBS 方案设计了一种跨域认证协议，其提高了认证效率，并且可以实现身份的即时撤销。

3.1 系统结构

该认证模型的系统结构如图 1 所示。

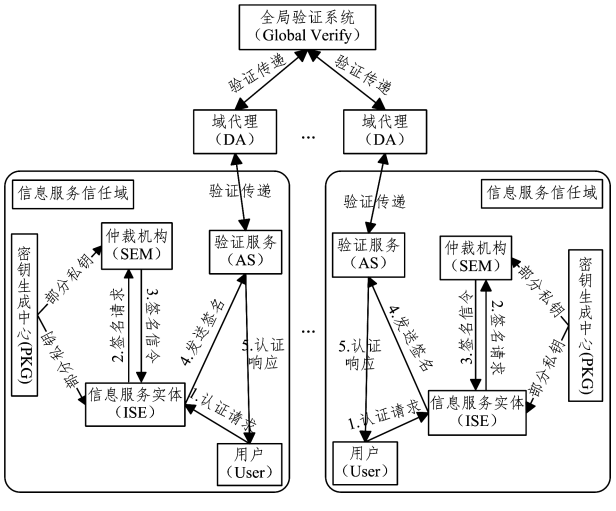

图 1 信息服务实体的跨域认证模型

Fig. 1 Cross-domain authentication model for information services entity

该模型中，用户和信息服务实体 ISE(提供资源的信息服务商)分布在多个 IBC 信任域(即信息服务信任域)中。域内实体采用基于身份的认证方式，实体 ISE 标识本身就是其公钥，PKG 将 ISE 的私钥 d_{ID} 分割成两部分 d_{ID}^{sem} 和 d_{ID}^{ISE}，将 d_{ID}^{sem} 发送给 SEM，d_{ID}^{ISE}发送给 ISE。本域验证服务器(Authentication Server，AS)管理着域内实体信息，验证访问者的身份。同时，每一个 IBC 信任域由域代理(Domain Agent，DA)采用交换数字证书的方式进行域间认证，并辅助域内实体进行跨域认证。

用户 U 想要申请本域的某个信息服务时，需要先向 ISE 申请认证。ISE 收到认证请求后，由于它的私钥不完整，因此先从 SEM 处获得一个签名信令 *token* 后才能完成签名操作，并将签名结果发送给 AS 进行验证。U 根据 AS 返回的认证响应接受或拒绝 ISE 的服务。当 ISE 的服务无效或过期时，管理员通过命令 SEM 停止给 ISE 发送 *token* 来撤销其签名权力，从而实现身份的即时撤销。

3.2 不同信任域间的双向实体认证

跨域协议模型如图 2 所示。

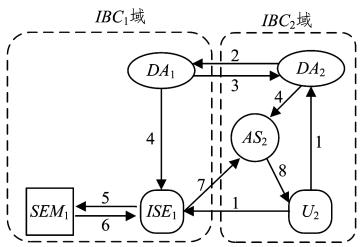

图 2 跨域协议模型

Fig. 2 Cross-domain authentication protocol model

本模型能够支持不同信任域间的双向认证和密钥协商，所有域的 PKG 使用相同的公开参数$(N,P_1,P_2,G_1,G_2,e,H_1,H_2)$，仅有主密钥 s 和公钥 P_{pub}不同。设 PKG_1 和 PKG_2 分别为信息服务实体 ISE_1 和用户 U_2 所信任的 PKG，其选定的主密钥分别为 $s_1,s_2\in[1,N-1]$，对应公钥为 $P_{pub_1}=[s_1]P_2$ 和 $P_{pub_2}=[s_2]P_2$。

当信任域 IBC_2 的用户 U_2 试图访问另一个信任域 IBC_1 的信息服务实体 ISE_1 时，需经过以下流程。

1)用户 U_2 分别向 DA_2 和 ISE_1 发送认证请求，其中 U_2 选取时间戳 T_1，用私钥 d_{U_2} 对消息 $ID_{ISE_1}\parallel ID_{U_2}\parallel T_1$ 进行基于身份的签名(本文侧重于信息服务实体认证的研究，用户采用 SM9 数字签名算法[14]进行签名)，用 d_{U_2} 签名是向 DA_2 证明自己是合法的用户。

$U_2\rightarrow DA_2$：

$\{ID_{ISE_1},ID_{U_2},T_1,IBS\{ID_{ISE_1}\parallel ID_{U_2}\parallel T_1\}d_{U_2}\}$

$U_2\rightarrow ISE_1$：$\{ID_{U_2},request\}$

2)DA_2 验证 U_2 的签名，验证通过后，DA_2 通过数字证书对 DA_1 进行认证，并获得 DA_1 的公钥 PK_{DA_1}；使用 PK_{DA_1} 对认证请求和系统公钥进行非对称加密，将密文发送给 DA_1：

$DA_2\rightarrow DA_1$：$\{ID_{ISE_1},ID_{U_2},P_{pub_2},T_2\}PK_{DA_1}$

3)DA_1 解密后，通过数字证书对 DA_2 进行认证获得 DA_2 的公钥 PK_{DA_2}，再将 P_{pub_1} 返回给 DA_2。

$DA_1\rightarrow DA_2$：$\{P_{pub_1},T_3\}PK_{DA_2}$

4）完成域间认证后，DA_2 计算 $V=H_1(ID_{U_2}\parallel ID_{ISE_1})$，$K=V\cdot[s_2]\cdot P_{pub_1}$，采用基于身份的加密方式（这里采用 SM9 中的加密算法[14]）将会话密钥 K 通过公钥 Q_{AS_2} 发送给 AS_2，只有 AS_2 才能解密；同样，DA_1 计算 $K'=V\cdot[s_1]\cdot P_{pub_2}$（显然 $K'=K$），将 K'发送给 ISE_1。

$DA_2\rightarrow AS_2: IBE\{ID_{ISE_1}, ID_{U_2}, P_{pub_1}, K, T_4\}Q_{AS_2}$

$DA_1\rightarrow ISE_1: \mathrm{IBE}\{K', T_5\}Q_{ISE_1}$

5）ISE_1 根据 SM9_mIBS 签名算法，将消息 M 的签名请求 $R=(ID_{ISE_1}, L)$发送给 SEM_1 以申请签名信令。

6）SEM_1 计算签名信令 $S_{sem_1}=[L]\cdot d_{ISE_1}^{sem_1}$，并将 S_{sem_1} 发送给实体 ISE_1。

7）ISE_1 生成消息 M 的完整数字签名(h,S)，并计算 $C=M\oplus K'$，将$\{C,(h,S)\}$发送给 AS_2。

8）AS_2 利用会话密钥 K 解密 C 得到消息 M，利用 SM9_mIBS 的验证算法对签名(h,S)进行验证，验证通过后 AS_2 相信 AS_2 和 ISE_1 之间共享了会话密钥 $K=K'$，发送 $IBE\{\mathrm{true}, K, T_6\}Q_{U_2}$ 给用户 U_2；否则，返回{false}。跨域认证完成，信息服务实体 ISE_1 与用户 U_2 协商了会话密钥 K，后续 U_2 可通过 K 来接受或拒绝 ISE_1 的服务。

4　安全与性能

4.1　安全分析

该信息服务实体跨域认证协议的安全性是基于已有的可撤销的 SM9_mIBS 签名方案的安全性，已在第 2.3 节进行了讨论。进行认证的双方只有签名验证通过后才能认证对方的身份，攻击者不能伪造有效的签名消息，因此不能进行假冒攻击。基于 SM9_mIBS 方案的可撤销性，该认证协议可以有效地防止已撤销的信息服务实体进行欺骗攻击。在认证过程中加入了随机数和时间戳，能够有效地抵抗重放攻击。此外，攻击者不知道s_1和s_2的值，虽然可以得到 $P_{pub_1}=[s_1]P_2$ 和$P_{pub_2}=[s_2]P_2$，但仍无法计算$[s_1][s_2]P_2$（该问题属于计算 Diffie-Hellman 难题），不能获得会话密钥，因此该协议还具有前向安全性。表 1 列出了本文方案与文献[2,5-9]在安全性方面的比较，由表 1 可知本文方案具有更高的安全性。

表 1　跨域认证协议的安全性比较

Table 1　Security comparison of cross-domain authentication protocols

	文献[2]方法	文献[5]方法	文献[6]方法	文献[7]方法	文献[8]方法	文献[9]方法	本文方案
会话密钥	√	√	√	√	√	√	√
相互认证	√	√	√	√	√	√	√
抗重放攻击	√	√	√	√	√	√	√
抗假冒攻击	×	√	×	√	√	√	√
身份可撤销性	×	×	×	×	×	×	√

4.2　性能分析

假设消息大小为 80-bit，时间戳长度为 16-bit，SM9_mIBS 方案中使用的群的大小为 160-bit，对称（AES）和非对称（ECC）加密/解密的密文大小分别为 128-bit 和 160-bit，基于 ECC 构造的数字证书密文大小为 160-bit，散列函数（SHA-1）或消息认证码（MAC）的摘要消息大小为 160-bit，身份大小为 80-bit[6]。

表 2 列出了本文方案与文献[2,6,9]在跨域认证协议性能方面的比较。由于文献[2,6,9]中未指明协议中的具体算法，本文假设其与本文方案采用同类型的算法。其中，T_{PM} 表示计算群上点乘运算的时间；T_H 表示计算散列函数的时间；T_e 表示计算对运算的时间；T_E 表示计算指数操作的时间；T_{SE}表示计算对称加密/解密的时间；T_{IE}和 T_{IS}分别表示计算基于身份的加/解密和签名的时间；T_{AE}和 T_{AS}分别表示计算非对称加/解密和签名的时间。

表 2　跨域认证协议的性能比较

Table 2　Performance comparison of cross-domain authentication protocols

	通信量/bits	计算量		
		用户（请求方）	ISE（响应方）	第三方（其他参与方）
文献[2]中的方案	4368	$3T_{PM}+3T_H+4T_e+8T_{SE}$	$1T_{PM}+3T_H+4T_e+8T_{SE}+T_E$	$2T_{PM}+2T_H+4T_e+6T_{SE}$
3PAKE[6]	1664	$3T_{PM}+2T_H$	$3T_{PM}+2T_H$	$2T_{PM}+8T_H$
EIMAKP-II[9]	1056	$2T_H+2T_{AS}+2T_{AE}+T_{SE}+T_{IE}$	$2T_{IE}+T_E+2T_{SE}$	$4T_{AE}+3T_{AS}+T_{IE}+2T_{IS}$
本文方案	1936	T_{IS}	$2T_{PM}+2T_H+2T_e+2T_E$	$3T_{PM}+3T_H+T_e+T_E+T_{IS}+4T_{IE}+4T_{AE}+(T_{PM}+T_H+T_e)$

基于身份的签名和加解密算法采用双线性对群构造，基于 ECC 的数字签名和加解密算法采用椭圆曲线上的点乘操作和哈希函数构造。因此，T_{IS}/T_{IE}和 T_{AS}/T_{AE}的计算时间较长。由表 2 可知，文献[9]中的协议的通信量最低，但用户和服务器的计算复杂度较高；文献[6]的计算复杂度最低，但所有消息都是以明文发送，容易受到假冒攻击和密钥泄露假冒攻击，这是以牺牲保密性为代价的。本文方案采用域代理、验证服务器和 SEM 构成第三方，辅助完成实体的双向认证。通过将验证过程转移到第三方，缓解了用户和 ISE 的计算压力，使其可以被应用于资源受限的移动设备。此外，表 2 中括号内的计算式采用了预计算，减少了方案整体的计算量。

结束语　本文提出的 SM9_mIBS 签名方案可以解决基于身份的认证系统中固有的身份即时撤销难题，且被证明是 EUF-mIBS-CMA 安全的；提出的基于身份的信息服务实体跨域认证模型具有安全、高效、灵活、应用范围广等特点。与传统 PKI 或 IBC 认证框架相比，本文模型简化了系统结构，节约了成本；并且本文设计了一种具有前向安全性和可撤销性的跨域认证协议，其可以实现跨信任域的双向实体认证和密钥协商，提高了认证效率。分析结果表明，用户和 ISE 的计算复杂度较低，且在保证较高安全性的条件下通信量的增幅较小。因此，本文方案对指导大规模异构网络环境下的信息服务实体跨域认证提供了参考价值。

参 考 文 献

[1] CASTIGLIONE A, PALMIERI F, CHEN C L, et al. A blind signature-based approach for cross-domain authentication in the cloud environment[J]. International Journal of Data Warehousing and Mining, 2016, 12(1): 34-48.

[2] PENG H X. An identity-based authentication model for multi-domain[J]. Chinese Journal of Computers, 2006, 29(8): 1271-1281. (in Chinese)
彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271-1281.

[3] LU X M, FENG D G. An identity-based multi-trust domain grid authentication model [J]. Journal of Electronics, 2006, 34(4): 577-582. (in Chinese)
路晓明, 冯登国. 一种基于身份的多信任域网格认证模型[J]. 电子学报, 2006, 34(4): 577-582.

[4] ZHANG W B, ZHANG H Q, ZHANG B, et al. An identity-based authentication model for multi-domain in grid environment[C]// 2008 International Conference on Computer Science and Software Engineering. Piscataway, NJ: IEEE Press, 2008: 165-169.

[5] HE D, ZEADALLY S, KUMAR N, et al. Anonymous authentication for wireless body area networks with provable security [J]. IEEE Systems Journal, 2016(99): 1-12.

[6] CHOU C H, TSAI K Y, LU C F. Two ID-based authenticated schemes with key agreement for mobile environments[J]. The Journal of Supercomputing, 2013, 66(2): 973-988.

[7] FARASH M S, ATTARI M A. A secure and efficient identity-based authenticated key exchange protocol for mobile client-server networks [J]. The Journal of Supercomputing, 2014, 69(1): 395-411.

[8] NI L, CHEN G L, LI J H, et al. Strongly secure identity-based authenticated key agreement protocols without bilinear pairings [J]. Information Sciences, 2016, 367: 176-193.

[9] YUAN C, ZHANG W F, WANG X M. EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system [J/OL]. Arabian Journal for Science and Enginee-ring (2017-02-23) [2017-08-02]. https://link.springer.com/article/10.1007/s13369-017-2447-9.

[10] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C]// Annual International Cryptology Conference. Berlin: Springer-Verlag, 2001: 213-229.

[11] CHENG X G, GUO L F, WANG X M. An identity-based mediated signature scheme from bilinear pairing [J]. International Journal of Network Security, 2006, 2(1): 29-33.

[12] MARTINS P, SOUSA L, CHAWAN P. Featuring immediate revocation in Mikey-Sakke (FIRM) [C]// 2015 IEEE International Symposium on Multimedia (ISM). Piscataway, NJ: IEEE, 2015: 501-506.

[13] CHEN Y, JIANG Z L, YIU S M, et al. Fully secure ciphertext-policy attribute based encryption with security mediator[C]// International Conference on Information and Communications Security. Cham: Springer-Verlag, 2014: 274-289.

[14] YUAN F, CHENG Z H. Overview on SM9 identity-based cryptographic algorithm[J]. Information Security Research, 2016, 2(11): 1008-1027. (in Chinese)
袁峰, 程朝辉. SM9 标识密码算法综述[J]. 信息安全研究, 2016, 2(11): 1008-1027.

[15] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of cryptology, 2000, 13(3): 361-396.

(上接第 170 页)

[5] ZHANG X J, LU Y, TIAN F, et al. Double-threshold cooperative spectrum sensing for cognitive radio based on trust[J]. Acta Physica Sinica, 2014, 63(7): 362-372. (in Chinese)
张学军, 鲁友, 田峰, 等. 基于信任度的双门限协作频谱感知算法[J]. 物理学报, 2014, 63(7): 362-372.

[6] JIANG X L. Double threshold collaborative spectrum sensing algorithm based on energy sensing [J]. D'd Journal of Heilongjiang University of Science and Technology, 2016, 26(1): 75-79. (in Chinese)
江晓林. 基于能量检测的双门限协作频谱感知算法[J]. 黑龙江科技大学学报, 2016, 26(1): 75-79.

[7] LI M Y, LI O, SUN W J. Double-threshold Cooperative Spectrum Sensing Algorithm Based on Noise Uncertainty[J]. Computer Engineering, 2014, 40(4): 81-86. (in Chinese)
李明源, 李鸥, 孙武剑. 基于噪声不确定性的双门限协作频谱感知算法[J]. 计算机工程, 2014, 40(4): 81-86.

[8] ZENG Y H, LIANG Y C. Maximum Minimum eigenvalue detection for cognitive radio[C]// The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. Athens, Greece, 2007: 1-5.

[9] WANG Y X, LU G Y. DMM Based Spectrum Sensing Method for Cognitive Radio Systems[J]. D'd Journal of Electronics & Information Technology, 2010, 32(11): 2572-2574. (in Chinese)
王颖喜, 卢光跃. 基于最大最小特征值之差的频谱感知技术研究[J]. 电子与信息学报, 2010, 32(11): 2572-2574.

[10] TSINOS C G, BERBERIDIS K. Decentralized Adaptive Eigenvalue-Based Spectrum Sensing for Multiantenna Cognitive Radio Systems[J]. IEEE Transactions on Wireless Communications, 2013, 14(3): 1703-1715.

[11] LI Z, WANG D, QI P, et al. Maximum-Eigenvalue-Based Sensing and Power Recognition for Multiantenna Cognitive Radio System[J]. IEEE Transactions on Vehicular Technology, 2016, 65(10): 8218-8229.

[12] ZOU W X, DING Q, ZHOU Z, et al. Double threshold spectrum sensing algorithm based on limiting eigenvalue distribution[J]. Systems Engineering and Electronics, 2012, 34(3): 588-591. (in Chinese)
邹卫霞, 丁奇, 周正, 等. 基于特征值极限分布的双门限频谱感知算法[J]. 系统工程与电子技术, 2012, 34(3): 588-591.

[13] HAREESH K, SINGH P. An energy efficient hybrid co-operative spectrum sensing technique for CRSN[C]// International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing. IEEE, 2013: 438-442.

[14] PENG Y, CUI Z R. CHEN C K. Selectively Triggered Cooperative Specturm Sensing in Wireless Cognitive Network[J]. Computer Engineering, 2017, 43(3): 89-93. (in Chinese)
彭艺, 崔自如, 陈昌凯. 无线认知网络中的选择触发协作频谱感知[J]. 计算机工程, 2017, 43(3): 89-93.