基于椭圆曲线密码体制的高效虚拟企业跨域认证方案

张文芳[1,2],王小敏[1],郭伟[1,2],何大可[1,2]
(1.西南交通大学信息科学与技术学院,四川成都 610031;
2.西南交通大学信息安全与国家计算网格四川省重点实验室,四川成都 610031)

摘 要: 针对虚拟企业的敏捷、动态、低成本、组织模式多样等特点利用无可信中心椭圆曲线门限签名和可变多方协议提出一个基于虚拟桥CA的高效的广义虚拟企业跨域认证方案.方案借助虚拟桥CA的分布式创建和运行提供了灵活的跨域认证策略并避免实体桥CA的维护成本,可适应虚拟企业不同的组织模式及其动态变化,具备比特安全性高、计算量和通信量小、信任链短、抗合谋攻击等优点,能更好的满足虚拟企业盟员间(特别是终端计算资源或通信带宽受限情况下)的跨域认证需求.

关键词: 虚拟企业;跨域认证;虚拟桥认证中心;椭圆曲线密码体制;门限签名
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2014) 06-1095-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.06.010

An Efficient Inter-Enterprise Authentication Scheme for VE Based on the Elliptic Curve Cryptosystem

ZHANG Wen-fang[1,2], WANG Xiao-min[1], GUO Wei[1,2], HE Da-ke[1,2]
(1. *School of Information Science and Technology, Southwest Jiaotong University, Chengdu, Sichuan* 610031, *China*;
2. *Key Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu, Sichuan* 610031, *China*)

Abstract: In order to meet the special requirements of virtual enterprises (VE), this paper proposed an efficient generalized inter-enterprise authentication scheme. The scheme employed the elliptic curve threshold signature algorithm and the variable multi-party protocols to realize efficient cross certifications between VE partners through a virtual bridge CA. Analysis shows that the proposed scheme can provide a flexible distributed trust policy for VE, and has the advantages of low computation and communication cost, high bit-security, short certificate-chains, and adaptability to various structures of VE, so it can better satisfy the special requirements of inter-enterprise authentication in VE, especially when the computation and communication resource is constrained.

Key words: virtual enterprise (VE); inter-enterprise authentication; virtual bridge certificate authority (VBCA); elliptic curve cryptosystem (ECC); threshold signature

1 引言

经济全球化带来的动态瞬变的市场机遇和激烈竞争的外部环境,对企业快速响应市场需求和持续创新能力提出了更高的要求.在此背景下,借助于大型分布式网络实现伙伴企业核心业务集成和优势资源共享的虚拟企业(Virtual Enterprise, VE),在管理、技术、资源等方面拥有明显的竞争优势,成为21世纪先进的企业组织与运作模式[1].虚拟企业构建于开放网络之上,通过合作伙伴甚至是竞争对手的临时性动态联盟赢取某一机遇性市场竞争,这种协同制造模式决定了虚拟企业通常具有敏捷性、时限性、异构性、组织结构多样性、动态性、自动化和低成本等特点[1],因此其安全问题比单一企业或传统企业模式更加复杂.

建立安全高效的盟员间跨信任域认证机制,是实现盟员业务资源安全共享和虚拟企业有效运作的前提.针对分布式环境下的信任模型,大量研究成果被先后提出[2~12].由于PKI(Public Key Infrastructure)技术的成熟、

收稿日期:2013-01-23;修回日期:2013-07-16;责任编辑:梅志强
基金项目:国家自然科学基金(No.61003245, No.60903202, No.61371098);四川省杰出青年学术带头人培育计划(No.2011JQ0027);铁道部重大项目(No.2012X004-A);中央高校基本科研业务费专项资金(No.SWJTU12CX099, No.SWJTU11CX041)

安全和广泛部署,目前一般采用基于公钥证书的认证机制进行构建.文献[5,6]直接依据各企业域已有的PKI结构及其拓扑关系构建认证路径,当信任域间为等级(hierarchy)、对等(peer to peer)或网状(Web)认证结构,且两个域并非相邻节点时,需要经过多个中间节点才能相互认证,信任链的查找和建立较复杂,认证路径长,认证效率低[9].文献[7]采用桥式CA(Bridge Certificate Authority,BCA)认证方案,通过专门建立一个所有域都信任的第三方桥CA,只须N次交叉认证即可建立起N个域间的完全信任路径.2012年,Xu等[8]引入一个权威机构SA(Session Authority)实现信任域间的交互认证及会话密钥协商,SA的核心作用与桥CA相同.

相较于网状、等级等其他PKI信任模型,上述基于BCA的跨域认证模型具有信任链短且易于查找的特点,但在实际中找到一个所有域都信任的可信第三方并不容易,而且临时建立并维护一个第三方桥CA的成本较高,制约了桥CA认证模型在虚拟企业中的实际应用.针对上述问题,文献[9~12]给出了基于虚拟认证中心(Virtual Certificate Authority,VCA)和动态PKI的信任模型,通过构建一个所有盟员都信任的虚拟CA,搭建起企业域间的交互认证关系,系统运行成本得到有效降低.但文献[9]方案由于签名构造和验证中的理论缺陷,并不成功.而利用门限RSA签名实现的VCA方案[10]虽能突出盟主的主导地位,但因引入密钥分发中心(Key Distribution Center,KDC)存在VCA私钥泄漏的安全隐患.该问题在基于分布式DSA门限签名构造的VCA方案[11,12]中得到解决.

然而,已有的VCA认证方案仍存在密钥长、效率低、不易硬件实现等问题,在虚拟企业终端用户(如移动终端)计算资源或通信带宽受限情况下并不适用.为此,本文首先给出虚拟桥认证中心(Virtual Bridge Certificate Authority,VBCA)信任模型,并在此基础上提出一个基于椭圆曲线公钥密码体制(Elliptic Curve Cryptosystems,ECC)的广义虚拟企业跨域认证方案.该方案借助无可信中心椭圆曲线门限签名分布式实现了VBCA的创建和运行,从而避免实体桥CA的维护成本并提供了灵活的分布式信任策略.安全性分析和效率评测表明:所提方案具有敏捷动态、成本低、认证路径短、抗合谋攻击以及对各种组织模式普适等优点;与现有VCA方案相比,还具有更高的比特安全性及计算/通信效率,能够更好的解决虚拟企业特别是终端资源和通信带宽受限环境下的盟员间跨信任域认证问题.

2 虚拟桥CA(VBCA)信任模型

由前述分析可知,直接利用现有的BCA模型实现虚拟企业的跨域认证不满足其动态性、临时性、自动化和低成本要求.为此,本文提出虚拟桥CA(VBCA)信任模型来解决虚拟企业盟员间的跨域交互认证问题.

虚拟桥CA(VBCA)信任模型:VBCA信任模型的基本认证结构类似于BCA模型,但该桥CA不是真实存在的,而是由各盟员域的信任锚CA利用秘密分享和门限签名等密码学技术临时构建出的虚拟的逻辑桥CA,当虚拟企业因任务完成而解散时,它会随着各盟员分别吊销对其的证书而自动消失,如图1所示.在该模型中,构建N个盟员企业域间的完全信任路径只需N次交叉认证,且任意两个盟员间的跨域认证路径长度均为2.因此,VBCA模型继承了BCA模型的优点,但无需投入额外的建设和维护成本,能够在满足虚拟企业对敏捷动态性、临时性、自动化和低成本要求的基础上,实现虚拟企业盟员间的高效、安全的跨域认证.

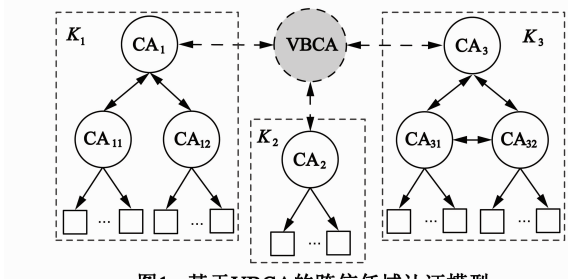

图1 基于VBCA的跨信任域认证模型

图1中,K_i表示虚拟企业中第i个盟员企业,CA_i表示K_i中用来进行域间认证的信任锚CA;"□"表示终端用户.从图1中可以看出,各CA_i之间通过VBCA即可搭建起信任链长度均为2的跨域认证路径.

3 基于椭圆曲线密码体制的高效虚拟企业跨域认证方案

在VBCA信任模型的基础上,本节利用无可信中心椭圆曲线门限签名技术提出一种高效的抗合谋攻击广义虚拟企业跨域认证方案,其示意图如图2所示.

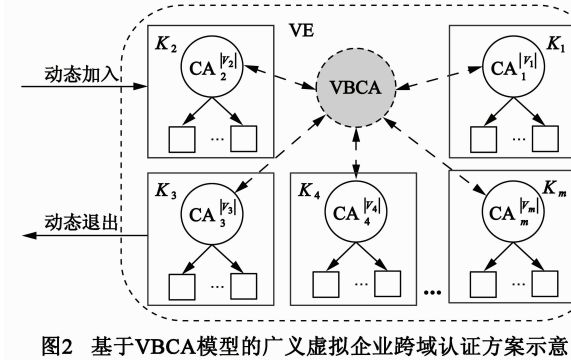

图2 基于VBCA模型的广义虚拟企业跨域认证方案示意图

图2中,$CA_i^{|V_i|}$中的上标$|V_i|$表示根据虚拟企业不同的组织模式为CA_i分配的权限值.不失一般性,设

K_1 代表盟主,K_2 为动态加入的盟员,K_3 为动态退出的盟员,随着盟员的动态加入/退出以及 VE 组织模式的改变,各 CA_i 的权限值也会相应改变.

3.1 相关定义

E:定义在有限域 F 上的一条椭圆曲线,该椭圆曲线上的离散对数是难解的;

$\#E$:E 中元素的个数;

P:E 上的一个阶为 q 的基点;

q:P 的阶,为 $\#E$ 的大素因子;

t:门限群的门限值;

m:虚拟企业盟员数;

n:密钥分享数,$n \geqslant m$;

K_i:虚拟企业中第 i 个盟员企业,$1 \leqslant i \leqslant m$,且令 K_1 为盟主;

CA_i:K_i 中负责跨域认证的信任锚认证中心,$1 \leqslant i \leqslant m$;

$Cer_{i,j}$:X.509 证书,i 为证书主体,j 为证书颁发者;

d:VBCA 私钥;

Q:VBCA 公钥;

$\{v, d_v\}$:v 为 Lagrange 秘密分享算法的输入值(公开),d_v 为 d 的影子值(保密);

Q_v:d_v 的承诺值(公开);

V_i:CA_i 的权限集(公开),为分配给 CA_i 的所有 $\{v, d_v\}$ 中 v 组成的集合,且 $\bigcup_{i=1}^{m} V_i = \{1,2,\cdots,n\}$;

$|V_i|$:CA_i 的权限,易知 $\sum_{i=1}^{m} |V_i| = n$;

B:有效签名组,为虚拟企业中满足权限之和等于 t 的 CA_i 集合,即 $\sum_{CA_u \in B} |V_i| = t$;

(x_i, Y_i):$CA_i(1 \leqslant i \leqslant m)$ 的固有公私钥对,其中 $x_i \in Z_q^*$ 为固有私钥,$Y_i = x_i P$ 为固有公钥,且须满足任意有效签名组成员的 Y_i 之和 $Y = \sum_{K_i \in B} Y_i$ 均不相等(各有效签名组的 Y 及其相应的组成员身份需要预先计算并列表存储,以备签名成员身份追查所用;同时还须维护一个与退出成员相关的 Y 值吊销列表,用于检验参与 VBCA 证书签名的成员组的有效性);

T:VBCA 签名接受公开验证的时限.

3.2 VBCA 的创建

(1)虚拟企业所有成员共同选择系统公共参数:椭圆曲线 E 及其 q 阶基点 P.

(2)虚拟企业所有成员根据其特定的组织模式,通过协商共同决定盟主和盟员的权限集 $V_i(1 \leqslant i \leqslant m)$ 并公布.

(3)利用分布式密钥分发协议(DKG)生成和分发 VBCA 密钥,步骤如下:

步骤 1　各盟员域的信任锚 $CA_i(1 \leqslant i \leqslant m)$ 分别选择一个 Z_q 上的 $t-1$ 次随机多项式 $f_i(x) \in {}_R Z_q[x]$:

$$f_i(x) = f_{i0} + f_{i1}x + f_{i2}x^2 + \cdots + f_{i(t-1)}x^{t-1} \bmod q,$$

计算并广播 $f_i(x)$ 的系数承诺值:$F_{ij} = f_{ij}P$ $(j = 0, 1, \cdots, t-1)$.

步骤 2　$CA_i(1 \leqslant i \leqslant m)$ 计算并秘密发送 $f_i(v)(v \in V_j)$ 给 $CA_j(1 \leqslant j \leqslant m$ 且 $j \neq i)$,自己保留 $f_i(v)(v \in V_i)$.收到 $f_i(v)(v \in V_j)$ 后,CA_j 验证等式:$f_i(v)P = \sum_{j=0}^{t-1} v^j F_{ij}$ 是否成立.如果不成立,协议重新开始.

步骤 3　如果验证通过,$CA_i(1 \leqslant i \leqslant m)$ 计算得到 VBCA 公钥 Q、密钥影子 d_v 及其承诺 Q_v(这里定义 $f(x) = \sum_{i=1}^{m} f_i(x)$):$Q = \sum_{i=1}^{m} F_{i0} = \sum_{i=1}^{m} f_{i0}P = f_0 P = f(0)P$,$\{(v, d_v) \mid d_v = \sum_{i=1}^{m} f_i(v) \bmod q = f(v), v \in V_i\}$,$Q_v = d_v P$,$v \in V_i$.其中,$Q$ 和 Q_v 公开,d_v 保密.VBCA 私钥 $d = f(0) = \sum_{i=1}^{m} f_i(0) \bmod q$ 则始终不被任何 CA_i(包括盟主 CA_1)所知.

(4)虚拟企业中各 $CA_i(1 \leqslant i \leqslant m)$ 分别签发对 VBCA 公钥的证书 Cer_{VBCA, CA_i},并保存在各自证书库中.

3.3 VBCA 的运行

3.3.1 VBCA 证书的颁发

VBCA 对各 $CA_i(1 \leqslant i \leqslant m)$ 公钥的证书签发过程如下:

步骤 1　CA_i 根据各盟员的权限选择另外 l 个伙伴(在盟成员)共同组成有效签名组 B,使得 B 中 $l+1$ 个成员的权限之和满足 $\sum_{CA_u \in B} |V_u| = t$.为叙述方便,设:$V = \bigcup_{CA_u \in B} V_u$.

步骤 2　B 中各成员 CA_u 分别选择一个随机整数 $k_u \in [1, q-1]$,计算:$R_u = k_u P$,并将 R_u 和 CA_u 的固有公钥 Y_u 广播给 B 中其他成员,将 k_u 保密.

步骤 3　B 中各成员 CA_u 首先通过原始 PKI 信任路径验证其他 l 个成员固有公钥的有效性,然后计算:$Y = \sum_{CA_u \in B} Y_u$,$(x, y) = R = \sum_{CA_u \in B} R_u$.

步骤 4　CA_i 向 B 中其他成员 $CA_j(CA_j \in B$ 且 $j \neq i)$ 发送消息:$\{M_i \| h(M_i)\}$,其中 M_i 包括 CA_i 的固有公钥 Y_i 及其主体信息,$h(\cdot)$ 为安全 hash 函数.

步骤 5　收到消息后,CA_j 首先验证 M_i 是否完整.如果完整,CA_j 计算:$r = x - h(M_i) \bmod q$.

$$s_j(M_i) = \sum_{v \in V_j} (C_v \cdot d_v) \cdot r + k_j + x_j \bmod q \qquad (1)$$

其中 $C_v=\prod_{w\in V,w\neq v}\frac{-w}{v-w}\bmod q$.

然后,CA_j 向 CA_i 发送其对 M_i 的部分签名:$\{M_i\|(r,Y_j,s_j(M_i))\}$.否则,如果 M_i 不完整,协议重新开始.

步骤 6 CA_i 收到 CA_j 的部分签名后,根据下式是否成立验证其有效性:

$$R_j=s_j(M_i)P-r\sum_{v\in V_j}C_vQ_v-Y_j \tag{2}$$

如果无效,则广播对 CA_j 的抱怨并要求 CA_j 重新计算.

步骤 7 若其他 l 份部分签名都有效,则 CA_i 计算:

$$r=x-h(M_i)\bmod q,$$

$$s_i(M_i)=\sum_{v\in V_i}(C_v\cdot d_v)\cdot r+k_i+x_i\bmod q.$$

其中 $C_v=\prod_{w\in V,w\neq v}\frac{-w}{v-w}\bmod q$.

然后,CA_i 将 B 中的 $l+1$ 份部分签名 $s_u(M_i)$ 合成 VBCA 签名:

$$s(M_i)=\sum_{CA_u\in B}s_u(M_i)\bmod q \tag{3}$$

最后,CA_i 将 VBCA 对 M_i 的签名 $\{M_i\|(r,Y,s(M_i))\}$ 公布,并接受公开验证.

步骤 8 在验证时限 T 内,虚拟企业中的任何成员均可按照以下步骤检验该 VBCA 签名的有效性.

首先,检查 Y 是否处于 Y 值吊销列表.如果不是,则计算:$(x',y')=s(M_i)P-rQ-Y$,并验证等式:

$$x'\equiv r+h(M_i)(\bmod q) \tag{4}$$

是否成立.如果成立,则认为该 VBCA 签名有效.否则,认为签名无效,并发布一个签名质疑.

如果在时限 T 内,没有任何人发布质疑,则认为签名合法,并为 CA_i 颁发 VBCA 证书:

$$\mathrm{Cer}_{CA_i,VBCA}:\{M_i\|(r,Y,s(M_i))\}$$

否则,一旦收到一个质疑,即认为签名不合法,要求协议重启.

3.3.2 跨域认证路径

证书分布情况:

不失一般性,设虚拟企业各盟员域 $K_i(1\leqslant i\leqslant m$,包括盟主)中均只拥有一个认证中心,即 CA_i,它直接与 K_i 中所有的终端用户相连.

从 3.3.1 节可知,当 VBCA 创建完成并与各 $CA_i(1\leqslant i\leqslant m)$相互颁发证书后,在 CA_i 的证书库中至少包含三类证书:Cer_{VBCA,CA_i},$\mathrm{Cer}_{CA_i,VBCA}$以及 CA_i 对其终端用户签发的证书.此时,不同盟员企业域的终端用户可直接借助该 VBCA 实现高效的跨域交互认证,避免了复杂的认证路径查找和构建过程.具体可分如下三种情况讨论:

(1)盟主企业 K_1 中用户 Alice 验证 K_i 中用户 Bob:

Alice 信任 CA_1 公钥,验证路径为:$\mathrm{Cer}_{Bob,CA_i}\rightarrow\mathrm{Cer}_{CA_i,VBCA}\rightarrow\mathrm{Cer}_{VBCA,CA_1}$.Alice 只需搜索本地($CA_1$)证书库和 CA_i 证书库,认证路径长度为 3.

(2)K_i 中用户 Bob 验证盟主企业 K_1 中用户 Alice:

Bob 信任 CA_i 公钥,验证路径为:$\mathrm{Cer}_{Alice,CA_1}\rightarrow\mathrm{Cer}_{CA_1,VBCA}\rightarrow\mathrm{Cer}_{VBCA,CA_i}$.Bob 需要搜索本地($CA_i$)证书库和 CA_1 证书库,认证路径长度为 3.

(3)K_i 中用户 Bob 验证 K_j 中用户 Carol:

Bob 信任 CA_i 公钥,验证路径为:$\mathrm{Cer}_{Carol,CA_j}\rightarrow\mathrm{Cer}_{CA_j,VBCA}\rightarrow\mathrm{Cer}_{VBCA,CA_i}$.Bob 需要搜索本地($CA_i$)证书库和 CA_j 证书库,认证路径长度为 3.

从以上分析可以看出,借助于 VBCA,不同企业的"终端用户"(非信任锚)进行跨域认证时只需要搜索两个证书库,认证路径长度均为 3.因此该 VBCA 模型保持了 BCA 认证模型的优点.

3.3.3 盟员增减

虚拟企业盟员的加入和退出,是由盟主根据择优等原则决定的(而盟主不会变动),也存在由于各种原因(如破产等)盟员主动退出的情况.设虚拟企业结构变化后的盟员数为 m',协议步骤如下:

步骤 1 盟主 K_1 根据各盟员原有的权限选择另外 l 个可信伙伴共同组成有效签名组 B(B 中均为状态稳定的盟员,既非新加入盟员也非将要退出的盟员),使其权限之和满足 $\sum_{CA_i\in B}|V_i|=t$,且设:$V=\bigcup_{CA_i\in B}V_i$.

步骤 2 B 中各 CA_i 分别计算:$e_i=\sum_{v\in V_i}d_v\cdot\prod_{w\in V,w\neq v}\frac{-w}{v-w}\bmod q$,并新选一个 Z_q 上的 $t-1$ 次随机多项式 $a_i(x)=e_i+a_{i1}x+a_{i2}x^2+\cdots+a_{i(t-1)}x^{t-1}\in_R Z_q[x]$,其中 $a_i(0)=e_i$.然后,CA_i 计算并广播 $a_i(x)$ 的系数承诺值:$A_{i0}=e_iP$,$A_{ij}=a_{ij}P(j=1,2,\cdots,t-1)$.

步骤 3 虚拟企业结构变化后,各盟员通过协商重新分配盟主和盟员的权限集 $V_i'(i=1,2,\cdots,m')$并公布.

步骤 4 B 中各 CA_i 根据新公布的权限集,计算并秘密分发$\{v',a_i(v')\}(v'\in V_j')$ 给 $CA_j(1\leqslant j\leqslant m'$且$j\neq i)$,$CA_i$ 自己保留 $a_i(v')(v'\in V_i')$.

CA_j 验证等式:$a_i(v')P=\sum_{j=0}^{t-1}(v')^jA_{ij}$是否成立.如果成立,则接受 $a_i(v')$;否则,协议重新开始.

步骤 5 各 $CA_j(1\leqslant j\leqslant m')$将其权限集更新为 V_j',并重新计算密钥影子和承诺:

$$\{(v',d_{v'})\mid d_{v'}=\sum_{CA_i\in B}a_i(v')\bmod q,v'\in V_j'\},$$

$$Q_{v'}=d_{v'}P,v'\in V_j'$$

最后将 Q_v 公布.

上述密钥影子的更新协议可以适应虚拟企业盟员的动态加入和退出,而 VBCA 密钥则保持不变.如果有新盟员 K_a 需要加入,可以根据新协商的权限集,按照上述步骤 3~5 为其分配相应的密钥影子和承诺,并按照 3.3.1 节协议为其 CA_a 公钥签发 VBCA 证书;如果有盟员 $K_i(2\leqslant i\leqslant m)$ 退出,则需要吊销证书 Cer_{VBCA,CA_i} 和 $Cer_{CA_i,VBCA}$.随着密钥影子的更新,退出盟员所持有的旧密钥影子会自动失去作用.

此外,还需要更新身份追查数据库和 Y 值吊销列表:若有盟员加入,计算与该新成员相关的所有"有效签名组 Y 值-组成员身份"数据项,并将其添加到身份追查数据库;若有盟员退出,将所有与该盟员相关的"有效签名组 Y 值"数据项添加到身份吊销列表,并将该盟员添加到退出成员名单.

3.3.4 参与 VBCA 签名盟员的身份追查

当事后发生纠纷,需要追查出参与签发 VBCA 证书 $\{M_i\|(r,Y,s(M_i))\}$ 的盟员身份时,执行以下协议:搜索身份追查数据库,找到其中与待查 VBCA 证书 $\{M_i\|(r,Y,s(M_i))\}$ 中 Y 值($Y=\sum_{CA_u\in B}Y_u$)相匹配的"有效签名组 Y 值-组成员身份"数据项,通过组成员身份即可追查出参与签名的盟员身份,而 VBCA 证书颁发阶段的签名公开验证协议(3.3.1 节步骤 8)可保证其一定是当时的有效盟员.

3.4 VBCA 的吊销

当虚拟企业因任务完成而解散时,各盟员 $CA_i(1\leqslant i\leqslant m)$ 分别吊销证书 Cer_{VBCA,CA_i} 和 $Cer_{CA_i,VBCA}$.此时,VBCA 也会随着相关证书的吊销而自动消失.

4 方案性能分析

4.1 安全性分析

定理 1(不可伪造性) 在 VBCA 证书颁发阶段,攻击者不能假冒 $CA_i(1\leqslant i\leqslant m)$ 提交有效的部分签名,也不能假冒有效签名组 B 直接生成合法的 VBCA 签名证书.

证明:假设攻击者试图伪造 $CA_i(1\leqslant i\leqslant m)$ 对 m 的部分签名.由部分签名生成式(1):$s_j(M_i)=\sum_{v\in V_j}(C_v\cdot d_v)\cdot r+k_j+x_j \bmod q$ 可知,攻击者若想构造出满足验证方程(2)的有效部分签名,必须获得 CA_i 的固有私钥 x_i 和密钥影子集 $\{d_v\mid v\in V_i\}$,即需要从 CA_i 的固有公钥 $Y_i=x_iP$ 和承诺 $Q_v=d_vP$ 中求出 x_i 和 d_v,而这等价于求解椭圆曲线上的离散对数难题.因此,攻击者无法假冒 CA_j 提交有效的部分签名.

又假设攻击者试图假冒有效签名组 B 直接伪造出对消息 m 的 VBCA 签名.由 VBCA 签名公式(3):$s(M_i)=\sum_{CA_u\in B}s_u(M_i)\bmod q=\sum_{CA_u\in B}\left(\sum_{v\in V_u}(C_v\cdot d_v)\cdot r+k_u+x_u\right)\bmod q=d\cdot r+\sum_{CA_u\in B}k_u+\sum_{CA_u\in B}x_u \bmod q$ 可知,攻击者若想构造出满足验证方程(4)的有效 VBCA 签名,必须获得 VBCA 私钥 d 和 B 中各成员的固有私钥 $x_u(CA_u\in B)$,即需要从 VBCA 公钥 $Q=dP$ 和成员固有公钥 $Y_u=x_uP$ 中求出 d 和 x_u,但这等价于求解椭圆曲线上的离散对数难题.因此,攻击者不能假冒 B 直接生成合法的 VBCA 签名证书.

定理 2(抗合谋攻击性 1) 即使拥有 t 个秘密份额的恶意 CA_i 合谋(可能包含盟主 CA_1),也不能伪造出其他 CA_j 的有效部分签名.

证明 假设拥有 t 个秘密份额的恶意 CA_i(可能包含 CA_1)合谋,组成攻击者集合 A(即满足 $\sum_{CA_j\in A}|V_j|=t$,并令 $V=\bigcup_{CA_j\in A}V_j$),则他们可利用其掌握的 t 个秘密份额 $\{(v,d_v=f(v)\bmod q)\mid v\in V\}$,通过构造并求解 t 维方程组恢复出秘密多项式 $f(x)$(的 t 个系数),进而求出其他 $CA_i(1\leqslant i\leqslant m$ 且 $CA_i\notin A)$ 的密钥影子集 $\{d_v=f(v)\bmod q\mid v\in V_i\}$.但是,由部分签名生成公式(1)可知,只知道 $\{d_v\mid v\in V_i\}$,不知道 CA_i 的固有私钥 x_i,A 仍然无法伪造出满足验证等式(2)的有效部分签名.而 A 若想从 CA_i 的固有公钥 $Y_i=x_iP$ 中求出 x_i,等价于求解椭圆曲线上的离散对数难题.因此,即使拥有 t 个秘密份额的恶意 CA_i 合谋,也不能伪造出其他 CA_j 的有效部分签名.

定理 3(抗合谋攻击 2) 即使拥有 t 个秘密份额的恶意 CA_i 合谋(可能包含盟主 CA_1),也不能假冒其它有效签名组 B 生成合法的 VBCA 签名证书.

证明 假设同定理 2,攻击者集合 A 可利用其掌握的 t 个秘密份额 $\{(v,d_v=f(v)\bmod q)\mid v\in V\}$,通过求解 Lagrange 插值方程恢复出 VBCA 私钥 $d=f(0)=\sum_{v\in V}d_v\cdot\prod_{w\in V,w\neq v}\frac{-w}{v-w}$.但是,由 VBCA 签名公式(3):$s(M_i)=\sum_{CA_u\in B}s_u(M_i)\bmod q=d\cdot r+\sum_{CA_u\in B}k_u+\sum_{CA_u\in B}x_u \bmod q$ 可知:只知道 d,不知道签名组 B 中各成员的固有私钥 $x_u(CA_u\in B)$,A 仍然无法假冒 B 伪造出满足验证等式(4)的有效 VBCA 签名.而 A 若想从 B 中成员的固有公钥 $Y_u=x_uP(CA_u\in B)$ 中求出 x_u,等价于求解椭圆曲线上的离散对数难题.因此,即使拥有 t 个秘密份额的恶意 CA_i 合谋,也不能假冒其它签名组 B 生成合法的 VBCA 签名证书.

4.2 分布式特性

新方案采用无可信中心椭圆曲线门限签名机制分布式的实现了 VBCA 的创建、证书颁发和盟员增减情况

下的证书更新.

首先,在 VBCA 创建阶段,VBCA 密钥是所有盟员 $CA_i(1\leqslant i\leqslant m)$利用分布式秘密共享协议共同生成的,私钥 $d=f(0)=\sum_{i=1}^{m}f_i(0)\bmod q$ 是各 CA_i 所选秘密多项式$f_i(x)$的首项系数之和.由于每个 $CA_i(1\leqslant i\leqslant m)$(包括盟主)都仅知道 d 的一个分量$f_i(0)$,因此可有效避免因引入密钥分发中心(一般由盟主充当)所带来的 VBCA 私钥泄漏隐患.其次,在 VBCA 证书颁发和更新阶段,各盟员可根据实际情况合理选择有效签名组 B(满足 $\sum_{CA_u\in B}|V_u|=t$)以实现 VBCA 证书的高效分布式签发,进而避免了因盟主必须参与 VBCA 签名所导致的效率瓶颈问题.

4.3 对不同组织模式的动态普适性(广义特性)

虚拟企业虽然由盟主发起、组织并管理,但是盟主和盟员之间除了一主多从模式之外,还存在供应链、策略联盟、合资经营、转包加工、虚拟合作等多种组织模式.

在 VBCA 创建阶段,新方案能够根据 VE 的不同组织模式灵活设置盟员权限$|V_i|(1\leqslant i\leqslant m)$.例如,在合资经营模式中,$|V_i|$可与盟员投入资金的多少成正比;在一主多从模式中,可为盟主分配较大权限(如:$|V_1|=t-1$),为其他盟员分配较小权限(如:$|V_i|=1,2\leqslant i\leqslant m$);在供应链模式中,可为每个盟员分配相同权限;在策略联盟模式中,可根据各联盟企业所提供的核心技术及资源的重要程度为其分配相应权限(详见 3.2 节).在合理配置盟员权限的基础上,选择满足 $\sum_{CA_u\in B}|V_u|=t$ 的有效签名组 B,通过执行 3.3.1 节的可变多方协议,即可实现 VBCA 证书的门限签发.此外,在盟员增减阶段,新方案能够根据虚拟企业结构和组织模式的动态变化重新设置盟员权限值,并在不改变 VBCA 原始密钥的前提下,利用 3.3.3 节的可变参与方协议完成密钥影子更新.

因此,新方案不仅能够满足虚拟企业各种组织模式的不同需求,还可以灵活适应盟员加入/退出时组织结构的动态变化.

4.4 效率分析

由前述分析可知,基于 VCA 的认证方案[9~12]和本文基于 VBCA 的认证方案能够满足虚拟企业跨域认证的敏捷性、动态性、自动化和低成本要求,本文方案还进一步了具备分布式、广义性和抗合谋攻击等特点.因此,我们将在对上述方案效率比较的基础上给出本文方案的效率评估.

4.4.1 密钥长度比较

本文方案和文献[9~12]方案的密钥长度对比数据如表 1 所示.

表 1 等效安全级别下的密钥长度对比

	本文方案		文献[9~12]方案(DSA,RSA)	本文方案与文献[9~12]方案的密钥长度比	
	ECC-GF(p)	ECC-GF(2^m)		ECC-GF(p)	ECC-GF(2^m)
安全级别(等效密钥长度)(bit)	192	163	1024	1:5,	1:6
	224	233	2048	1:9,	1:9
	256	283	3072	1:12,	1:11
	384	409	7680	1:20,	1:19
	521	571	15360	1:30,	1:27

从表 1 可以看出:本文方案建立在椭圆曲线公钥密码体制(ECC)基础上,在同等安全级别下,其密钥长度远低于采用 DSA 类或 RSA 公钥密码机制的虚拟企业跨域认证方案[9~12];且随着安全级别的升高,其密钥长度的增长幅度也远低于文献[9~12]方案.此外,在这些方案中,由于签名长度与密钥长度相同,因此本方案的签名长度也远低于文献[9~12]方案.由以上分析可以看出,本文基于 ECC 的 VBCA 认证方案与文献[9~12]方案相比,不仅大大减少了密钥/签名存储空间,而且降低了信任链建立所需的通信代价,这些特点在虚拟企业终端用户计算/存储资源受限(如移动终端)或通信带宽受限(如无线链路)情况下显得尤为重要.

4.4.2 运算效率比较

我们在 Intel Core2 Duo E7500 CPU 的 32 位 Windows XP 环境下,采用 Visual C++ 6.0 开发工具通过调用 WinNTL5.5.2 和 OpenSSL1.0.1 函数库实现了本文及文献[9~12]方案的仿真软件,分别对 VCA/VBCA 创建、VCA/VBCA 证书颁发、盟员增减三个阶段进行了功能验证和效率测试比较.其中,文献[9,10]属于 RSA 类 VCA 方案,文献[11,12]属于 DSA 类 VCA 方案,本文算法属于 ECC 类 VBCA 方案.由于采用同类公钥密码体制的 VCA 方案效率接近(属于同一数量级),因此我们取各类方案的平均仿真时间进行比较.不失一般性,程序参数设置如下:虚拟企业组织模式为策略联盟式,初始盟员数 $m=4$,初始秘密分享数 $n=8$,门限值 $t=5$;在盟员增减阶段,有 1 个老盟员退出、1 个新盟员加入.同时,由于本文及文献[11,12]属于广义认证方案,因此在这几个方案的盟员增减阶段令盟员权限值随组织模式的动态改变发生了变化,变化后的秘密分享数 $n'=10$.不同的等效安全级别下,上述方案的 VCA/VBCA 创建、证书颁发及盟员增减阶段仿真时间比较详见表 2.

从表 2 可以看出,本文方案在不同的等效安全级别下均比文献[9~12]方案高效,且随着密钥长度的增加

和安全级别的升高,其耗时增长速度也远低于文献[9~12]方案.在 1024-192-163bit 安全级别下,RSA 类 VCA 方案[9,10]和 DSA 类 VCA 方案[11,12]的三阶段时耗分别是本文方案(采用 F_p 上椭圆曲线实现)的 5 倍/1.5 倍/1.8 倍以及 2.8 倍/1.7 倍/1.2 倍;而在 2048-224-233bit 安全级别下,RSA 类方案和 DSA 类方案的三阶段时耗则是本文方案的 17.6 倍/5.1 倍/5.8 倍以及 10.2 倍/6.1 倍/4.4 倍.

表 2　等效安全级别下的各阶段仿真时间比较

安全级别		RSA/DSA-1024bit, ECC-GF(p)-192bit/GF(2^m)-163bit				RSA/DSA-2048bit, ECC-GF(p)-224bit/GF(2^m)-233bit			
算法		RSA 类 VCA 方案[9,10]	DSA 类 VCA 方案[11,12]	本文 ECC 类 VBCA 方案		RSA 类 VCA 方案[9,10]	DSA 类 VCA 方案[11,12]	本文 ECC 类 VBCA 方案	
				GF(p)-192	GF(2^m)-163			GF(p)-224	GF(2^m)-233
仿真时间(ms)	VCA/VBCA 创建	63.259	35.422	12.804	22.317	383.476	222.281	21.793	35.261
	VCA/VBCA 证书颁发	1.579	1.703	1.023	1.328	9.834	11.875	1.943	3.012
	盟员增减	1.153	0.643	0.542	0.607	5.307	3.985	0.912	1.336

综上,本文方案在保证与文献[9~12]方案具备同等甚至更高安全强度的前提下,极大的缩短了密钥/签名长度,降低了存储和通信代价,而且计算效率也得到了显著提高.因此,本文方案更适用于虚拟企业盟员间安全、高效、敏捷、动态、自动化和低成本的跨域认证,特别对终端用户资源及通信带宽受限情况下的跨域认证具有突出的优势和重要的应用价值.

5　结束语

本文提出一个基于椭圆曲线密码体制的高效广义虚拟企业跨信任域认证方案.该方案不仅具备对各种组织模式普适、敏捷动态、成本低、认证路径短及安全可靠等优点,而且还在保证与同类方案具有同等甚至更高安全强度的前提下,极大地缩短了密钥/签名长度,提高了签名/验证效率,降低了通信/存储代价,对虚拟企业终端用户计算资源或通信带宽受限情况下的盟员间跨域认证具有重要的实用意义,此外在虚拟组织及云计算网络认证中也具有良好的应用前景.

参考文献

[1] Camarinha-Matos L M, Afsarmanesh H. The Virtual Enterprise Concept[M]. Boston: Kluwer Academic Publishers, 1999. 3 – 14.

[2] 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.
Lu Xiao-ming, Feng Deng-guo. An identity-based authentication model for multi-domain grids[J]. Acta Electronica Sinica, 2006,34(4):577 – 582. (in Chinese)

[3] Liu H, Luo P, Wang D. A distributed expansible authentication model based on Kerberos[J]. Journal of Network and Computer Applications, 2008,31(4):472 – 486.

[4] 代战锋,温巧燕,李小标.基于分布式 PKI 的 P2P 网络认证技术[J].电子学报,2009,37(11):2561 – 2564.
Dai Zhan-feng, Wen Qiao-yan, Li Xiao-biao. The authentication technology of P2P network based on distributed PKI[J]. Acta Electronica Sinica, 2009,37(11):2561 – 2564. (in Chinese)

[5] Djordjevic I, Dimitrakos T, Romano N, Mac Randal D, Ritrovato P. Dynamic security perimeters for inter-enterprise service integration[J]. Future Generation Computer Systems, 2007, 23(4):633 – 657.

[6] Rouibah K, Ould-Ali S. Dynamic data sharing and security in a collaborative product definition management system [J]. Robotics and Computer-Integrated Manufacturing, 2007, 23(2): 217 – 233.

[7] Lopez Millan G, Gil Perez M, Martinez Perez G, Gomez Skarmeta A F. PKI-based trust management in inter-domain scenarios[J]. Computers & Security, 2010, 29: 278 – 290.

[8] Xu J, Zhang D, Li X. Dynamic authentication for cross-realm SOA-based business processes[J]. IEEE Transactions on Service Computing, 2012, 5(1): 20 – 32.

[9] 刘端阳,潘雪增.虚拟企业的安全交互模型[J].计算机研究与发展,2003,40(9):1307 – 1311.
Liu Duan-yang, Pan Xue-zeng. A new VCA scheme in virtual enterprises[J]. Journal of Computer Research and Development, 2003, 40(9): 1307 – 1311. (in Chinese)

[10] 张文芳,王小敏,何大可.一个改进的基于门限 RSA 签名的虚拟企业安全交互模型[J].计算机研究与发展,2012,49(8):1662 – 1667.
Zhang Wen-fang, Wang Xiao-min, He Da-ke. An improved VCA interaction model for virtual enterprises based on threshold RSA signature[J]. Journal of Computer Research and Development, 2012, 49(8): 1662 – 1667. (in Chinese)

[11] 张文芳,何大可,王小敏.基于可变权限集的广义虚拟企业信任交互方案[J].计算机集成制造系统-CIMS,2007,13(5):1001 – 1007.
Zhang Wen-fang, He Da-ke, Wang Xiao-min. Generalized trust-interaction scheme for virtual enterprises based on variable privilege sets [J]. Computer Integrated Manufacturing Systems, 2007, 13(5): 1001 – 1007. (in Chinese)

[12] 张文芳,王小敏,何大可.身份可追查的抗合谋攻击广义

虚拟企业信任交互方案[J].计算机集成制造系统-CIMS,2010,16(7):1558 – 1567.
Zhang Wen-fang, Wang Xiao-min, He Da-ke. Novel conspiracy attack immune generalized interactive authentication scheme for virtual enterprises with traceability[J]. Computer Integrated Manufacturing Systems, 2010, 16(7): 1558 – 1567. (in Chinese)

作者简介

张文芳 女,1978 年生于山西太原,西南交通大学副教授,博士,硕士生导师.研究方向为密码学与信息安全、分布式网络安全.
E-mail: wfzhang@swjtu.edu.cn

郭 伟 男,1980 年生于四川峨眉,西南交通大学讲师,博士.研究方向为信息安全,混沌密码设计与分析.

王小敏 男,1974 年生于江西萍乡,西南交通大学教授,博士,博士生导师.研究方向为信息安全、轨道交通安全工程.
E-mail: xmwang@swjtu.edu.cn

何大可 男,1944 年生于重庆,西南交通大学教授,博士生导师.研究方向为密码学与信息安全.