基于区块链技术的跨域认证方案

马晓婷,马文平,刘小雪
(西安电子科技大学综合业务网国家重点实验室,陕西西安 710071)

摘 要: 针对现有交互频繁的信息服务信任域(PKI 域和 IBC 域)之间不能实现信息服务实体(ISE)安全高效的跨域认证的问题,提出一种基于区块链的跨异构域认证方案.在 IBC 域设置区块链域代理服务器参与 SM9(国产标识密码)算法中密钥生成,并与 PKI 域区块链证书服务器等构成联盟链模型,利用区块链技术去中心化信任、数据不易篡改等优点保证模型内第三方服务器的可信性.基于此设计了跨域认证协议与重认证协议,并进行 SOV 逻辑证明.分析表明,与目前相关方案相比,协议在满足安全需求的前提下,降低了用户终端的计算量、通信量和存储负担,简化了重认证过程,实现域间安全通信,在信息服务跨异构域身份认证过程中具有良好的实用性.

关键词: 跨域认证; 区块链; SM9 算法; 信息服务
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018) 11-2571-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.11.002

A Cross Domain Authentication Scheme Based on Blockchain Technology

MA Xiao-ting, MA Wen-ping, LIU Xiao-xue
(*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: Existing information service entities (ISE) in various domains (PKI domain and IBC domain) interact more frequent. To solve the obstacle to the development of services caused by unsafe and inefficient cross-domain authentication, a novel blockchain-based cross-domain authentication scheme is proposed. A blockchain domain agent server is set in IBC to participate in SM9 key generation and build up the consortium blockchain model along with the blockchain certificate server (PKI). Based on the high credible model with the advantages of blockchain technology, a cross-domain authentication protocol and re-authentication protocol are proposed, and are proved by SOV logic. Compared with the related schemes, our scheme reduces the computation and communication on user side and simplifies the heavy authentication process. Therefore, the scheme has good practicability in domain authentication.

Key words: across domains authenticated; blockchain; SM9; information services

1 引言

信息服务实体(Information Services Entity, ISE)指互联网中公开性、共享性信息的服务活动提供者,对 ISE 的管理将直接制约信息服务的安全性发展.随着移动终端的轻量级化,其与多信任域结构模式中的 ISE 交互越来越频繁,能保证资源受限的移动终端用户接受安全高效的信息服务成为主要需求.目前对 ISE 仅是信任域内部简单的身份管理与认证,用户需要访问外域 ISE 时,就存在跨信任域身份认证问题.

目前信息服务信任域较多应用的基于公开密钥的认证框架有:基于证书的公钥基础设施(Public Key Infrastructure, PKI)[1]和基于身份的密码体制(Identity-Based Cryptography, IBC).PKI 技术成熟且应用广泛,适用于构建大型网络;IBC 直接以实体有效标识作为公钥[2],适用于小型网络.实现 PKI 和 IBC 域间安全高效的跨域认证是保证安全信息服务的前提.文献[3,4]基于第三方信任 CA 建立信任链路,实现 PKI 域间认证.文献[5]提出基于网格的 PKI 多信任域认证模型,但模型无法抵抗伪造攻击.文献[6,7]都将 IBC 域认证服务器作为 PKI 域内实体,采用交换证书的方式认证,效率不高且信任域间不等级.文献[8]提出两种异构域间的密钥协商,实现等级信任域间跨域认证,但用户承载较大计算量和通信量.

收稿日期:2018-01-29;修回日期:2018-07-04;责任编辑:蓝红杰
基金项目:国家自然科学基金(No. 61373171);高等学校创新引智计划项目(No. B08038);国家重点研发计划重点专项(No. 2017YFB0802400)

区块链(Blockchain,BC)技术在身份认证领域的应用逐步受到重视,其核心优势是去中心化[9],颠覆了传统的中心化系统架构.以比特币系统框架构建 PKI 体系,存在隐私泄露等问题,文献[10]提出隐私保护的 PKI 方案,文献[11]基于以太坊实现 PKI 认证体系,通过优化区块链证书使用减少通信量,降低维护成本.文献[12]在此基础上设计基于区块链的 PKI 跨域认证方案.以上均未研究基于区块链的 IBC 与 PKI 跨域认证.

SM9 国密算法是一种基于双线性对的标识密码算法,主要用于数字签名、数据加密、密钥交换以及身份认证等[13].本文改进 SM9 密钥生成算法,基于区块链构建 PKI 与 IBC 联盟链模型,实现对外域 ISE 安全高效的跨域认证和重认证,并通过安全性和效率分析证明方案的实用性.

2 技术基础

2.1 区块链技术

区块链是由多独立节点参与的分布式数据库系统[14],记录节点上发生的所有交易信息,过程高度透明,数据高度安全,凡是需要公平、公正、诚实的领域,都可应用区块链技术[9].区块链的数据结构可以从三个层次来描述:链、区块和交易,同一个时间周期中所有交易组成区块,区块按时间顺序链接起来就形成了区块链.区块体内交易采用 Merkle 树结构组织,内部任何一个数据改动都会引起交易总哈希值的变化,导致区块链从该区块断开,因此可保证数据不易篡改、很难伪造、可追溯.

根据中心化的不同,区块链可分为公有链、私有链和联盟链.联盟链介于公有链和私有链之间,节点少,交易速度较快,交易成本低,且保留了区块链其他特性,逐步成为商业应用领域的主流.

2.2 改进 SM9 算法

国产密码 SM9 算法中,IBC 域中由私钥生成中心(Private Key Generation,PKG)独自进行密钥的生成,存在密钥托管问题,若出现恶意的 PKG,则系统安全存在很大的隐患.为此,本节改进 SM9 密钥生成算法,在 IBC 域中增加区块链域代理服务器(Blockchain Domain Agent,BCDA)参与系统密钥的生成,改进后的算法和正确性验证如算法 1 所示.

算法 1 改进密钥生成算法

(1) BCDA 生成系统参数$(N,P_1,P_2,G_1,G_2,e,\mathrm{H}_1,\mathrm{H}_2)$.

(2) BCDA 参与实体(Entity,E)的密钥生成,生成过程如下:

第一阶段:

1. 实体 E 向 BCDA 和 PKG 发送密钥申请.

2. BCDA 验证其身份信息通过之后,

①选择随机数 $s_1 \in [1,N-1]$ 作为实体的部分主密钥,对应公钥为 $P_{pub}^1 = [s_1]P_2$,其秘密地保存 s_1;

②计算 $t_1 = \mathrm{H}_1(ID_E \| hid,N) + s_1$,$hid$ 为私钥生成符,若 $t_1 = 0$,则重新选择 s_1,并更新主密钥和公钥,否则计算 $t_2 = s_1 t_1^{-1}$,则部分私钥为 $d_{ID_E}^1 = [t_2]P_1$;

③计算 $Q_{ID_E}^1 = [\mathrm{H}_1(ID_E \| hid,N)]P_2 + P_{pub}^1$ 为实体的部分公钥,将 BCDA 产生的消息$\{hid,d_{ID_E}^1,Q_{ID_E}^1,t_1\}$加密发送给 PKG.

第二阶段:

(3) PKG 收到来自 BCDA 的消息之后,

①解密得到 $hid,d_{ID_E}^1,Q_{ID_E}^1,t_1$,选择随机数 $s_2 \in [1,N-1]$ 为实体另一部分主密钥,对应公钥 $P_{pub}^2 = [s_2]P_2$,秘密地保存 s_2;

②结合前一部分公钥计算 $Q_{ID_E} = Q_{ID_E}^1 + P_{pub}^2$ 为实体公钥.计算 $t_3 = t_1 + s_2$,实体的私钥为 $d_{ID_E} = ((t_1)d_{ID_E}^1 + [s_2]P_1)t_3^{-1}$.

正确性验证:$s_1 + s_2 = s$, $P_{pub} = sP_2$

$$Q_{ID_E} = Q_{ID_E}^1 + P_{pub}^2 = (\mathrm{H}_1(ID_E \| hid,N))P_2 + P_{pub}^1 + P_{pub}^2$$
$$= (\mathrm{H}_1(ID_E \| hid,N))P_2 + s_1P_2 + s_2P_2 = (\mathrm{H}_1(ID_E \| hid,N))P_2 + (s_1+s_2)P_2 = (\mathrm{H}_1(ID_E \| hid,N))P_2 + P_{pub}$$
$$d_{ID_E} = (t_1 d_{ID_E}^1 + s_2P_1)t_3^{-1} = (t_1t_2P_1 + s_2P_1)(t_1+s_2)^{-1}$$
$$= s(\mathrm{H}_1(ID_E \| hid,N) + s_1 + s_2)^{-1}P_1$$
$$= (s/(\mathrm{H}_1(ID_E \| hid,N) + s))P_1$$

由 BCDA 和 PKG 共同完成密钥生成,彼此不共享主密钥,可改善密钥托管问题.同时 BCDA 在第一阶段生成的(P_{pub}^1,d_{ID}^1)具有完整密钥功能,可作为外域实体的临时公私钥.

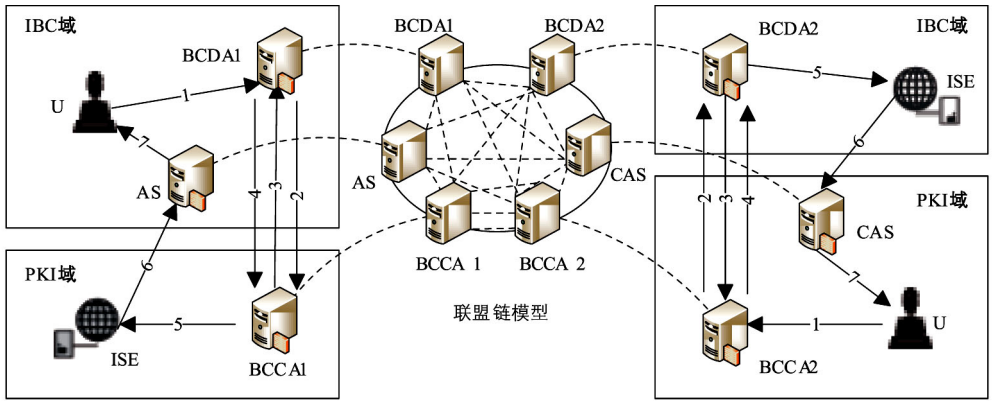
3 跨异构域认证方案

3.1 联盟链模型

模型采用联盟链为原型,BCDA 和 PKI 域区块链证书服务器[12](Blockchain Certificate Authority,BCCA)作为指定节点,可参与验证后续节点的加入.为实现身份验证,同时设置 PKI 域证书验证服务器(Certificate Authentication Server,CAS)和 IBC 域身份验证服务器(Authentication Server,AS)为辅助节点,辅助节点不参与验证新节点,不进行数据同步,模型如图 1.联盟系统内设置加密、签名算法,节点相互怀疑、互相监督、周期性相互验证,保证了去中心化联盟具有较高的可信度.联盟链模型基础架构如图 2,应用层、合约层和数据层根据跨异构域的需求设计各部分功能[15].

3.2 区块链证书

本节依据 X.509 数字证书 3.0 分别设计 BCDA 域代理证书和外域实体的临时证书.如图 3,加入联盟链时,BCCA 生成自身证书[12],BCDA 由 BCCA 颁发域代理证书;跨域过程中临时证书由 BCCA 颁发给外域实体.根据文献[9],证书写入区块链接口定义为 put(*action*,hash(Cert)),查询接口定义为 get(hash(Cert)),查询返回 *action* 标明证书当前状态,分别为声明 *issue* 和撤销 *revoke*.可利用证书生成哈希值在区块链上快速高效



I:IBC域内用户请求验证PKI域内信息服务实体身份　　II: PKI域内用户请求验证IBC域内信息服务实体身份

图1　联盟链模型和跨域模型

图2　联盟链模型基础架构

图3　BCDA区块链域代理证书和实体临时证书

的查询证书的状态 *action*. 不设置 CRL，证书有效期约束证书存活时间.

3.3　跨域模型及跨域协议

基于图 1 所示两个跨域模型 Ⅰ 和 Ⅱ 设计跨域协议，协议中用到的符号如表 1. 协议初始化: 各域内实体完成认证，PKI 域中实体证书、联盟链上节点证书可查询证书状态.

表 1　协议中符号含义

符号	含义
Q_E^X, d_E^X	X 域内实体 E 利用 SM9 生成的公私钥
C_E^*	区块链代理或临时证书
$Sig_K^{SM9、PKI、BC}(M)$	IBC 域内、PKI 域内、节点间签名算法
$En_K^{SM9、PKI、BC}(M)$	IBC 域内、PKI 域内、节点间加密算法
Inf_{IBC}	IBC 域中系统标识信息

3.3.1　跨域协议 Ⅰ

U_{IBC}请求ISE_{PKI}的服务，需要对该ISE_{PKI}进行认证，认证流程如图 1 中 Ⅰ，跨域协议如下:

(1) $M_{1(U_{IBC}\rightarrow BCDA1)}: En_{PK^{BCDA1}}^{SM9}(ID_U^{IBC}, ID_{ISE}^{PKI}, Request_1)$

U_{IBC}向 BCDA1 发送验证请求 $Request_1$，请求验证ISE_{PKI}的身份.

(2) $M_{2(BCDA1\rightarrow BCCA1)}: En_{SK^{BCCA1}}^{BC}(C_{BCDA1}^*, text_1, Request_2)$

$text_1 = T_1 \| ID_{ISE}^{PKI} \| N$

BCDA1 解密来自 U_{IBC}的消息，确认身份合法则响应 $Request_1$，查询ISE_{PKI}对应证书服务器 BCCA1 在联盟链内位置; 对ID_{ISE}^{PKI}和域参数 N 加盖时间戳 T_1，与代理证书 C_{BCDA1}^*、认证请求 $Request_2$ 一起加密发至 BCCA1.

(3) $M_{3(BCCA1\rightarrow BCDA1)}: En_{PK^{BCDA1}}^{BC}(Sig_{SK^{BCCA1}}^{BC}(text_2), text_2)$

$text_2 = S \| T_2$

BCCA1 解密来自 BCDA1 的消息，时间戳 T_1 鲜活则与 CAS 合作查询域代理证书 C_{BCDA1}^*合法性和证书状态，状态返回为 *issue* 则响应验证请求 $Request_2$; 选择随机数 $S \in [1, N-1]$ 为ISE_{PKI}临时主密钥，秘密保存 S，对 S 和时间戳 T_2 签名、加密发至 BCDA1.

(4) $M_{4(BCDA1\rightarrow BCCA1)}: En_{PK^{BCCA1}}^{BC}(T_3, Sig_{SK^{BCDA1}}^{BC}(text_3), text_3)$

$text_3 = Q_{ISE}^{PKI} \| d_{ISE}^{PKI} \| P_{pub}^{ISE}$

BCDA1 解密来自 BCCA1 的消息，时间戳 T_2 鲜活则结合 $text_2$ 验证签名消息，验证通过则利用改进 SM9 密钥生成算法第一阶段，以 S 为主密钥生成ISE_{PKI}的临时公私钥$(Q_{ISE}^{PKI}, d_{ISE}^{PKI})$; 对$(Q_{ISE}^{PKI}, d_{ISE}^{PKI})$和主公钥 P_{pub}^{ISE}签名，与时间戳 T_3 一起加密后发至 BCCA1.

(5) $M_{5(BCCA1\rightarrow ISE_{PKI})}: En_{PK^{ISE}}^{PKI}(T_4, Sig_{SK^{BCCA1}}^{PKI}(text_3), text_3)$

BCCA1 解密来自 BCDA1 的消息，时间戳 T_3 鲜活、签名验证通过且ISE_{PKI}证书查询合法则进行签名并加密转发 $text_3$.

(6) $M_{6(ISE_{PKI}\rightarrow AS)}: En_{PK^{AS}}^{SM9}(Sig_{d_{ISE}^{PKI}}^{SM9}(T_5), T_5, P_{pub}^{ISE}, Q_{ISE}^{PKI})$

ISE_{PKI}解密来自 BCCA1 的消息，时间戳 T_4 鲜活则结合 $text_3$ 验证签名，验证通过后选择时间戳 T_5 作为验证因子，利用临时公私钥$(Q_{ISE}^{PKI}, d_{ISE}^{PKI})$和 SM9 算法对 T_5

进行签名与公钥 Q_{ISE}^{PKI}、主公钥 P_{pub}^{ISE} 和 T_5 一起加密发至验证服务器 AS.

(7) $M_{7(AS\rightarrow U_{IBC})}$: $success \oplus ID_{ISE}^{PKI}$

AS 解密来自 ISE_{PKI} 的消息,时间戳 T_5 鲜活则结合 Q_{ISE}^{PKI} 和 P_{pub}^{ISE} 验证签名结果(参见 SM9 算法),验证通过发送认证成功的消息给 U_{LBC};

U_{IBC} 收到后,验证 $M_7 \oplus ID_{ISE}^{PKI}$,若得到 *success* 则接受 ISE_{PKI} 的信息服务,ISE_{PKI} 利用临时身份与 U_{IBC} 进行通信.

3.3.2 跨域协议Ⅱ

U_{PKI} 请求 ISE_{IBC} 的服务,需要对 ISE_{IBC} 身份进行验证.认证流程如图 1 中Ⅱ,跨域协议如下:

(1) $M_{1(U_{PKI}\rightarrow BCCA2)}^{*}$: $En_{PK^{BCCA2}}^{PKI}(C_U, ID_{ISE}^{IBC}, Request_1^*)$

U_{PKI} 向 BCCA2 发送验证请求 $Request_1^*$,请求验证外域 ISE_{IBC}.

(2) $M_{2(BCCA2\rightarrow BCDA2)}^{*}$: $En_{PK^{BCDA2}}^{BC}(C_{BCCA}, text_1^*, Request_2^*)$

$text_1^* = T_1^* \| ID_{IBC}^{ISE}$

BCCA2 解密来自 U_{PKI} 的消息,与 CAS 合作查询证书 C_U 合法性和证书状态,状态为 *issue* 且签名验证通过则响应 $Request_1^*$,对 ID_{IBC}^{ISE} 加盖时间戳 T_1^*,与证书 C_{BCCA} 和验证请求 $Request_2^*$ 一起加密发至 BCDA2.

(3) $M_{3(BCDA2\rightarrow BCCA2)}^{*}$: $En_{PK^{BCCA2}}^{BC}(T_2^*, Sig_{SK^{BCDA2}}^{BC}(text_2^*), text_2^*)$

$text_2^* = lifetime \| PK_{pub}^{ISE} \| Inf_{IBC}$

BCDA2 解密来自 BCCA2 的消息,时间戳 T_1^* 鲜活则用 $text_1^*$ 验证签名消息,验证通过则查询证书状态,状态为 *issue* 则响应 $Request_2^*$;生成 ISE_{IBC} 临时证书有效期 *lifetime*,与 Inf_{IBC}、PK^{ISE} 一起加盖时间戳 T_2^* 后签名、加密发送给 BCCA2.

(4) $M_{4(BCCA2\rightarrow BCDA2)}^{*}$: $En_{PK^{BCDA2}}^{BC}(Sig_{SK^{BCCA2}}^{BC}(C_{ISE}^*), T_3^*, C_{ISE}^*)$

BCCA2 解密来自 BCDA2 的消息,时间戳 T_2^* 鲜活则结合 $text_2^*$ 验证签名消息,验证通过则利用 *lifetime*、PK^{ISE}、Inf_{IBC} 及本域信息生成 ISE_{IBC} 的临时证书 C_{ISE}^*,对临时证书签名,加盖时间戳 T_3^* 后加密发送至 BCDA2.

(5) $M_{5(BCDA2\rightarrow ISE_{IBC})}^{*}$: $En_{PK^{ISE}}^{SM9}(Sig_{SK^{BCDA2}}^{SM9}(C_{ISE}^*), C_{ISE}^*, T_4^*)$

BCDA2 解密来自 BCCA2 的消息,时间戳 T_3^* 鲜活、签名验证通过且 ISE_{IBC} 身份验证通过,则对证书 C_{ISE}^* 签名并加密转发.

(6) $M_{6(ISE_{IBC}\rightarrow CAS)}^{*}$: $En_{PK^{CAS}}^{PKI}(T_5^*, C_{ISE}^*, Sig_{SK^{ISE}}^{PKI}(C_{ISE}^*))$

ISE_{IBC} 解密来自 BCDA2 的消息,保存临时证书 C_{ISE}^*;T_4^* 鲜活且验证签名消息通过则解析临时证书,结合其中 PKI 域加密算法对临时证书 C_{ISE}^* 加密,与时间戳 T_5^* 一起加密发送至 CAS.

(7) $M_{7(CAS\rightarrow U_{PKI})}^{*}$: $success \oplus ID_{ISE}^{IBC}$

CAS 用本域解密算法解密来自 ISE_{IBC} 的消息,时间戳 T_5^* 鲜活则对签名和临时证书进行验证,验证合法发送认证成功的消息给 U_{PKI};

U_{PKI} 收到后,验证 $M_7^* \oplus ID_{ISE}^{ISE}$,若得到 *success* 则接受 ISE_{IBC} 的信息服务,U_{PKI} 利用 PKI 域加密与 ISE_{IBC} 算法通信.

3.4 认证凭证与重认证

成功认证 ISE 后,节点服务器收到认证凭证 $Deal^{BCDA} = ID_{BCDA}^{IBC} \oplus ID_{ISE}^{PKI}$、$Deal^{BCCA} = ID_{BCCA}^{PKI} \oplus ID_{ISE}^{IBC}$,定义 put(*Time*, hash(Deal)) 为认证凭证写入区块链的接口,get(hash(Deal)) 为查询接口,查询返回时间戳 *Time*. 认证凭证的有效时间可根据交易信息安全级别设定(如 24 小时),通过查询返回 *Time* 确定该实体是否经过认证,计算认证凭证是否失效. 成功认证后,若有域内其他用户需要访问该 ISE 时,重认证过程如下:

(1) 用户向节点发送验证申请(同协议Ⅰ、Ⅱ);

(2) 节点利用 ISE 的 ID 合成认证凭证,在区块链上进行查询,若返回时间戳,且时间戳在有效时间则将认证通过消息返回给用户;

(3) 收到认证成功消息,用户和 ISE 安全通信.

使用认证凭证简化对 ISE 的重认证过程,在有效时间内,实现对相同 ISE 的快速高效重认证.

4 安全性分析

4.1 协议的 SOV 证明

SOV 逻辑是 BAN 逻辑中较为成熟的一种,基于 SOV 逻辑术语及公理[16] $A_0 - A_{20}$ 对本文的两个协议进行证明. 协议Ⅰ需达到的目标是:

1: AS $\models ISE_{PKI} \ni Q_{ISE}^{PKI}$;

2: AS $\models ISE_{PKI}$ $(Sig_{d_{ISE}^{PKI}}^{SM9}(T_5), T_5, P_{pub}^{ISE}, Q_{ISE}^{PKI})$;

协议Ⅱ需达到的目标是:

1: CAS $\models ISE_{IBC} \ni C_{ISE}^*$;

2: CAS $\models ISE_{IBC}$ $(T_5^*, C_{ISE}^*, Sg_{SK^{ISE}}^{PKI}(C_{ISE}^*))$;

(1) 初始假设:

P_0: 所有已生成证书可查询证书状态;

P_1: 所有时间戳的新鲜性可被验证;

P_2: BCCA1 $\models$ BCDA1 $\xrightarrow{PK^{BCCA1}}$ BCCA1;

P_3: 各域实体已完成身份认证,拥有公私钥;

P_4: BCCA1 $\models$ BCDA1 $\models\Rightarrow \{Q_{ISE}^{PKI}, d_{ISE}^{PKI}, P_{pub}^{ISE}\}$;

P_5: $ISE_{PKI} \models PK_\sigma(BCCA1, PK^{BCCA1})$;

P_6: $ISE_{PKI} \models SV(Sig_{SK^{BCCA1}}^{BC}(text_3), PK^{BCCA1}, BCCA1)$;

P_7: AS $\lhd M_6$;

P_8: AS $\models PK_\sigma(ISE_{PKI}, Q_{ISE}^{PKI})$;

P_9: AS $\models PK_\psi(AS, PK^{AS})$;

P_{10}: AS $\models ISE_{PKI} \Rightarrow ISE_{PKI} \xrightarrow{PK}$ AS;

P_{11}: BCDA2 ⊨ BCCA2 $\xrightarrow{PK^{BCDA2}}$BCDA2;

P_{12}: BCDA2 ⊨ BCCA2 ⊢C^*_{ISE};

P_{13}: ISE_{IBC}⊨ PK_σ(BCDA2,PK^{BCDA2}) ;

P_{14}: ISE_{IBC}⊨ $SV(Sig^{SM9}_{SK^{BCDA2}}(C^*_{ISE}),PK^{BCDA2},BCDA2)$;

P_{15}: CAS◁M^*_6;

P_{16}: CAS ⊨ PK_σ(ISE_{IBC},PK^{ISE}) ;

P_{17}: CAS ⊨ PK_ψ(CAS,PK^{CAS}) ;

P_{18}: CAS ⊨ISE_{IBC}⇒$ISE_{IBC}\xrightarrow{PK^{ISE}}$CAS;

(2) **协议Ⅰ中** AS **和**ISE_{PKI}**之间协议证明:**

Step1: **条件** P_0 **下查询** BCDA1 **域代理证书合法后,根据** P_1 **得** R_1: BCCA1 ⊨ BCDA1 ≈ M_4;

Step2: **条件** P_2 **和** P_3 **下,结合结论** R_1,**利用** A_8 **得** R_2: BCCA1 ⊨ BCDA1 ≈$(Sig^{BC}_{SK^{BCDA1}}(text_3),text_3)$;

Step3: **条件** P_4 **下,结合结论** R_2,**利用规则** A_{16} **得** R_3: BCCA1 ⊨$(Sig^{BC}_{SK^{BCDA1}}(text_3),text_3)$;

Step4: **条件** P_5 **和** P_6 **下,结合结论** R_3,**利用** A_4 **得** R_4: ISE_{PKI}⊨ BCCA1 $(Sig^{PKI}_{SK^{BCCA1}}(text_3),text_3,T_4)$;

Step5: **条件** P_1 **下,结合结论** R_4,**利用规则** A_{17} **和** A_{19} **得** R_5 : ISE_{PKI}⊨$(Sig^{PKI}_{SK^{BCCA1}}(text_3),text_3)$;

Step6: **条件** P_3 **和** P_7 **下,结合结论** R_5,**利用规则** A_8 **得** R_6: AS◁$(Sig^{SM9}_{d^{PKI}_{ISE}}(T_5),T_5,P^{ISE}_{pub},Q^{PKI}_{ISE})$;

Step7: **条件** P_8 **和** P_9 **下,结合结论** R_6,**利用** A_4 **得** R_7: AS ⊨ISE_{PKI} $(Sig^{SM9}_{d^{PKI}_{ISE}}(T_5),T_5,P^{ISE}_{pub},Q^{PKI}_{ISE})$;

达到协议Ⅰ预期目标 2;

Step8: **条件** P_1 **下利用规则** A_{18}**得** R_8: AS ⊨#M_6;

Step9: **结合结论** R_7 **和** R_8,**利用规则** A_{19}**得** R_9: AS ⊨ ISE_{PKI}≈ Q^{PKI}_{ISE}

Step10: **条件** P_{10} **下,结合结论** R_9,**利用规则** A_{16} **可** R_{10}: AS ⊨$ISE_{PKI}\xrightarrow{Q^{PKI}_{ISE}}$AS;

Step11: **结合结论** R_7 **和** R_{10},**利用规则** A_3 **得** R_{11}: AS ⊨ISE_{PKI} ∋ $(Sig^{SM9}_{d^{PKI}_{ISE}}(T_5),T_5,P^{ISE}_{pub},Q^{PKI}_{ISE})$;

Step12: **结合结论** R_{11},**利用规则** A_{11} **得** R_{12}: AS ⊨ ISE_{PKI} ∋ Q^{PKI}_{ISE};

达到协议Ⅰ预期目标 1;

(3) **协议Ⅱ中** CAS **和**ISE_{IBC}**之间协议证明:**

Step1: **条件** P_0 **下查询** BCCA2 **证书合法后,根据条件** P_1,**判断得到** R^*_1 : BCDA2 ⊨ BCCA2 ≈ M^*_4;

Step2: **条件** P_3 **和** P_{11} **下,结合结论** R^*_1,**利用** A_8 **得** R^*_2 : BCDA2 ⊨ BCCA2 ≈$(Sig^{BC}_{SK^{BCCA2}}(C^*_{ISE}),C^*_{ISE})$;

Step3: **条件** P_{12} **下,结合结论** R^*_2 ,**利用规则** A_{16} **得** R^*_3 : BCDA2 ⊨$(Sig^{BC}_{SK^{BCCA2}}(C^*_{ISE}),C^*_{ISE})$;

Step4: **条件** P_{13} **和** P_{14} **下,结合** R^*_3 ,**利用** A_4 **得** R^*_4 : ISE_{IBC}⊨ BCDA2 $(Sig^{SM9}_{SK^{BCDA2}}(C^*_{ISE}),C^*_{ISE},T^*_4)$;

Step5: **条件** P_1 **下,结合结论** R^*_4 ,**利用规则** A_{17} **和** A_{19} **得** R^*_5 : ISE_{IBC}⊨$(Sig^{SM9}_{SK^{BCDA2}}(C^*_{ISE}),C^*_{ISE})$;

Step6: **条件** P_3 **和** P_{15} **下,结合** R^*_5 ,**利用规则** A_8 **得** R^*_6 : CAS◁$(T^*_5,C^*_{ISE},Sig^{PKI}_{SK^{ISE}}(C^*_{ISE}))$;

Step7: **条件** P_{16} **和** P_{17} **下,结合** R^*_6 ,**利用规则** A_4 **得** R^*_7 : AS ⊨ISE_{PKI} $(T^*_5,C^*_{ISE},Sig^{PKI}_{SK^{ISE}}(C^*_{ISE}))$;

达到协议Ⅱ预期目标 2;

Step8: **条件** P_1 **下,利用** A_{19}**得** R^*_8 : CAS ⊨#M^*_6;

Step9: **根据结论** R^*_7 **和** R^*_8 ,**利用规则** A_{19}**得** R^*_9 : CAS ⊨ISE_{IBC}≈ C^*_{ISE};

Step10: **根据结论** R^*_9 **及条件** P_{18},**利用规则** A_{16}**得** R^*_{10}: CAS ⊨$ISE_{IBC}\xrightarrow{PK^{ISE}}$CAS;

Step11: **根据结论** R^*_7 **和** R^*_{10},**利用规则** A_3 **得** R^*_{11}: CAS ⊨ISE_{IBC} ∋ $(T^*_5,C^*_{ISE},Sig^{PKI}_{SK^{ISE}}(C^*_{ISE}))$;

Step12: **根据结论** R^*_{11},**利用规则** A_{11}**得** R^*_{12}: CAS ⊨ ISE_{IBC} ∋ C^*_{ISE};

达到协议Ⅱ预期目标 1.

4.2　安全属性分析

本文模型具备的安全属性如下:

(1) **抵抗内部攻击: 联盟链模型保证节点服务器的可信; 改进** SM9 **密钥生成算法,**PKG **无法获取** BCDA **的部分主私钥** S_1,**有改善密钥托管问题; 协议Ⅰ中** BCDA **验证** U_{IBC}**身份,协议Ⅱ中** BCCA **查询** U_{PKI}**证书,因此本方案有效抵抗内部攻击.**

(2) **抵抗仿冒攻击:** BCDA1 **和** AS **验证** U_{IBC}**身份,** BCCA2 **和** CAS **查询** U_{PKI}**证书进行身份验证,敌手无法仿冒用户获取信息服务;** M_5 **和** M^*_5 **通过非对称加密算法加密,由于破解信息窃取私钥或证书的概率相当于破解困难性难题,敌手不能获取临时身份完成认证,有效抵抗仿冒攻击.**

(3) **抵抗重放攻击:** BCDA **与** BCCA **交互消息** M_2 – M_4 **和** M^*_2 – M^*_4 、ISE_{PKI}**与** AS **交互消息** M_6、ISE_{PKI}**与** CAS **交互消息** M^*_6 **都由时间戳来保证消息的新鲜性,由于时间戳无法篡改,若攻击者重用截获消息,因时间戳失效而验证失败,有效防止重放攻击.**

(4) **双向认证: 协议Ⅰ:** BCCA1 **通过签名和证书对** BCDA1 **进行验证,** BCDA1 **通过签名对** BCCA1 **进行验证;** BCCA1 **通过证书对**ISE_{PKI}**进行验证,**ISE_{PKI}**通过签名验证** BCDA1. **协议Ⅱ:** BCDA2 **通过签名和证书对** BCCA2 **进行验证,** BCCA2 **通过对签名** BCDA2 **进行验证;** BCDA2 **通过身份认证对**ISE_{IBC}**进行验证,**ISE_{IBC}**通过签名对** BCCA2 **进行验证. 以上完成实体双向认证.**

(5) **抵抗中间人攻击:** (2) **中实体间的交互消息、** BCDA **和** U_{IBC}**交互消息** M_5、BCCA **和** U_{PKI}**交互消息** M^*_5 ,

以上消息发送方都利用自身私钥进行签名，若攻击者对消息进行篡改，则该签名消息不能通过接收方的验证，有效抵抗中间人攻击.

(6) 协议理性安全性: 根据博弈论机制[17]，如图4中实例的博弈树，A、B 是通信双方，C 是敌手，CE 是通信环境. 博弈最佳结果 $(\alpha,\beta,\varepsilon)$ 的纳什均衡为 $q_1q_2q_3q_4q_5q_7q_9$，显然在安全通信阶段所使用的密码算法直接影响博弈结果.

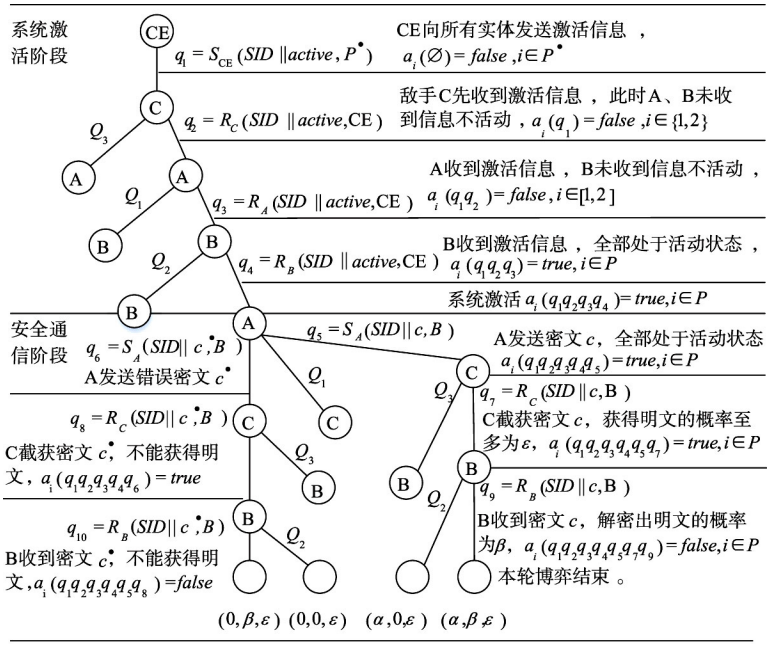


图4 博弈 $\Omega^{A,B,C,CE}_{\alpha,\beta,\varepsilon}(C)$

表2 表明，单一签名算法或加密算法不能保证安全通信，本文通信认证时结合签名和加密，满足博弈论机制下对理性协议的安全性要求.

表2 签名加密算法的安全性意义

算法	保密性	认证性	纳什均衡	安全
签名算法	NO	YES	$q_1q_2q_3q_4Q_1Q_3Q_2$	NO
加密算法	YES	NO	$q_1q_2q_3q_4q_5Q_3Q_2$	NO
签密算法	YES	YES	$q_1q_2q_3q_4q_5q_7q_9$	YES

通过表3 的比较可以看出，本方案在安全性上优于其他方案.

表3 模型协议的安全分析

	抵抗内部攻击	抵抗仿冒攻击	抵抗重放攻击	双向实体认证	抗中间人攻击	理性安全性
EIMAKP-Ⅰ[8]	YES	YES	YES	NO	YES	YES
EIMAKP-Ⅱ[8]	YES	YES	YES	NO	YES	YES
文献[12]	YES	YES	NO	YES	NO	NO
本文协议Ⅰ	YES	YES	YES	YES	YES	YES
本文协议Ⅱ	YES	YES	YES	YES	YES	YES

5 性能分析

5.1 效率分析

Kilinc 等人在配置为双 CPU E2200 2.20GHz、RAM 2GB 的计算机中进行了实验[18]，得出各运算的平均耗时，如表4. 假设本方案、文献[8]和[12]中，所有 IBC 域采用相同的基于身份的加密/签名算法，所有 PKI 域采用相同的非对称加密/签名算法，本方案联盟链上与 PKI 域使用相同算法. 假设消息长度为 80bit; 时间戳 16bit; 文献[8]和 SM9 算法使用的群变量 160bit; 密钥 160bit; 非对称加解密的密文 160bit; 对称加密密文 256bit; 签名消息 160bit; 证书密文 160bit; 身份 80bit. SM9 算法中使用串到整数的哈希函数，因此本文 2.2 节 H_1 与 H_2 对应上表 H_n，G_1 为 q 阶群，G_2 为乘法群，文献[12]和本方案对证书采用输入、输出都为固定长比特串的 H_3，输出为长度 128bit，对以上方案的数据进行分析.

表4 运算耗时

运算	耗时/ms	运算	耗时/ms
基于身份的签名 T_{IBS}	23.866	对称解密 T_{SD}	0.0046
基于身份的签名验证 T_{IBV}	5.872	点乘运算 T_M	2.226
非对称签名 T_{AS}	3.85	双线性对 T_P	5.811
非对称签名验证 T_{AV}	0.1925	$H_n:\{0,1\}^*\rightarrow Z_n$	0.0023
基于公钥的加密 T_{PE}	3.85	$H_P:\{0,1\}^*\rightarrow G_1$	12.418
基于公钥的解密 T_{PD}	3.85	$H_M\{0,1\}^*\rightarrow G_2$	0.947
对称加密 T_{SE}	0.0046	$H_S:\{0,1\}^*\rightarrow\{0,1\}^*$	0.0046

通过统计和比较得到表 5 和图 5 ~ 7. 图 5 表明,本方案的通信量均低于文献 [8] 和 [12],计算量小于文献 [8]. 图 6、7 表明,用户端,本方案的计算量和通信量均都比文献 [8] 和 [12] 小很多; 在 ISE 端,ISE 需进行身份认证并提供高速的信息服务,因此计算量有一定程度的增加,通信量有所降低; 第三方服务器端,本方案计算量低于文献 [8].

表 5　效率分析

		计算量/ms	耗时/ms	通信量/bit	耗时总量/ms	通信总量/bit
EIMAKP-Ⅰ [8]	用户	$T_{IBV}+T_{AV}+2T_{PE}+2T_{PD}+T_{SE}+T_{SD}+3T_M+T_P+H_M$	31.17	1522	116.25	1808
	资源	$T_{AV}+2T_{PD}+T_{SE}+T_{SD}$	7.99	832		
	服务器	$T_{IBS}+3T_{AS}+T_{AV}+3T_{PE}+T_{PD}+T_{SE}+T_{SD}+2T_P+2H_M+H_P$	77.09	1232		
EIMAKP-Ⅱ [8]	用户	$T_{IBV}+T_{AS}+2T_{PE}+T_{PD}+T_{SE}+T_{SD}+H_P$	33.78	992	111.05	1408
	资源	$T_{IBV}+2T_{PD}+T_{SE}+T_{SD}$	13.66	832		
	服务器	$2T_{IBS}+T_{AS}+2T_{AV}+2T_{PE}+T_{PD}+T_{SE}+T_{SD}$	63.61	992		
文献 [12]	用户	$2T_{AS}$	7.70	1440	32.92	2720
	服务器	$2T_{AV}+H_S$	25.22	3360		
本文协议Ⅰ	用户	T_{PE}	3.85	240	96.98	1040
	ISE 资源端	$T_{IBS}+T_{AV}+T_{PE}+T_{PD}$	31.76	320		
	服务器	$T_{IBV}+3T_{AS}+2T_{AV}+4T_{PE}+5T_{PD}+4T_M+2H_n+H_S$	61.37	1520		
本文协议Ⅱ	用户	T_{PE}	3.85	240	80.27	1040
	ISE 资源端端	$T_{IBV}+T_{AS}+T_{PD}$	13.57	320		
	服务器	$T_{IBS}+2T_{AS}+3T_{AV}+4T_{PE}+4T_{PD}+2H_S$	62.85	1520		

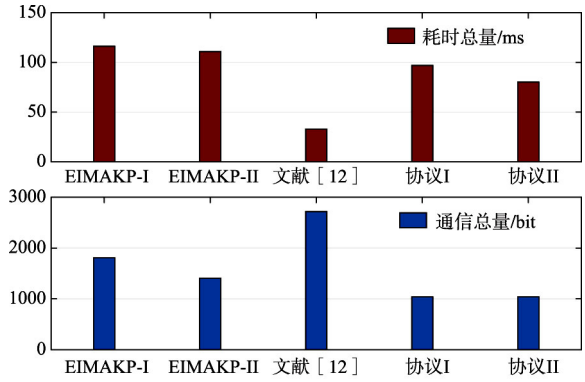


图5　通信总量与耗时总量分析

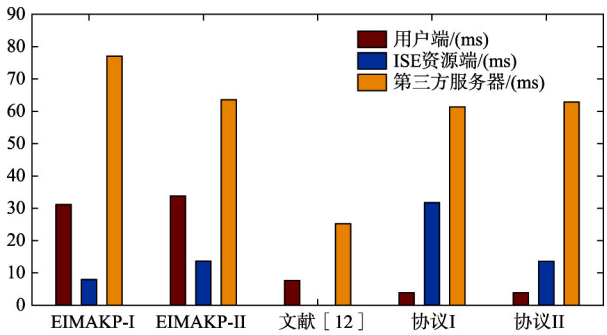


图6　各端运算耗时分析

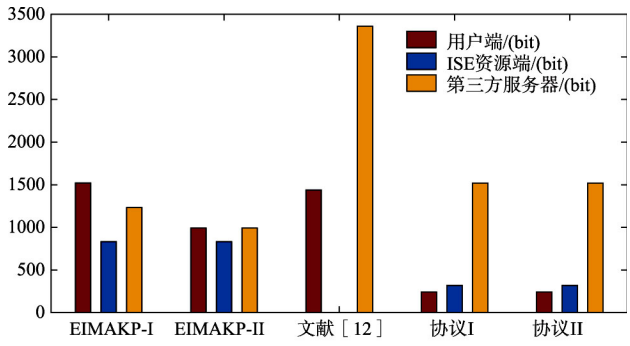


图7　各端通信量分析

分析可知,本方案的计算量和通信量在比文献 [8] 总体都有所降低的前提下,更多的将其承载于服务器端,文献 [8] 要求用户端拥有较强的计算及通信能力,因此比较之下本方案更适用于信息服务信任域的主流用户,即资源受限的便携式移动终端. 当终端用户增加时,以上几种方案的认证效率都会有所降低,但本方案优于文献 [8] 和 [12]. 文献 [12] 交互信息全部以明文形式发送,极易导致信息泄露.

在存储负担方面,用户端资源不承载任何存储负担. ISE 端,重认证时只需更新存储的临时证书(或临时公私钥) ,存储大小是固定的. 服务器端增加的存储负担在 5.2 节详细分析.

5.2 联盟链模型性能分析

联盟链指定的节点可拥有交易权限,节点数远小于公有链.采用文献[9]中对 ABC/TBC 双链架构分析的举例假设分析方法,参考 5.1 节,认证凭证大小为 128bit,假设每 10 分钟生成一个区块,每分钟 50% 用户请求外域访问,其中的 10% 申请访问未认证或认证凭证失效的 ISE,对一台节点服务器生成认证凭证的理论数据值计算如表 6. 可以看出,24 小时内用户之间访问不重复,若区块上限为 1M,联盟链可允许 1312 个(代理 100 个用户)或者 131 个(代理 1000 个用户)服务器节点同时以上述假设访问强度的工作.联盟链与公有链类似,可由通信能力强的完全节点同步所有数据.因访问信息服务具有持续性和重复性,实际访问量密集度会降低,且信息服务实体数量有限,实际生成认证凭证值的大小比表 6 中理论分析值更小.

表 6 一台节点服务器的理论数据

代理用户数量	100 个	1000 个
10min 生成认证凭证大小	0.78kb	7.8kb
一年生成认证凭证大小	0.04G	0.4G
24 小时认证 ISE 总量	7200 个	72000 个
联盟可容纳节点上限	1312 个	131 个

不失一般性假设:联盟内有 500 个节点,10min 内每个节点不重复认证 10 个 ISE,生成大小约 80kb 的区块.全节点需增加约 80kb 的通信量.若在凭证有效期 24 小时内,上述完成认证的 5000 个 ISE 各平均接受 20 次的重复访问,则可节省二次认证通信量约 12.4G.

基于联盟链搭建认证模型,增加的存储负担在可控范围内非常小.节点服务器同步数据需要消耗额外的通信量,但是通过以上分析可知,增加的通信量远小于大量重认证过程的通信量,这部分存储和通信的开销优化了整体方案的资源布局,具有实际意义.因此本方案基于联盟链构建,具有良好的可行性.

6 结语

针对信息服务信任域间对 ISE 的跨域认证要求,本文基于区块链技术实现异构域间对 ISE 的安全认证,改善服务器端负担,降低终端用户通信量和计算量,满足轻量级终端用户的需求,具有良好的实用性.但本文并未解决区块链系统固有的因存储数据造成的开销浪费的问题,另外 ISE 端的计算量有待优化.为了使本方案更具有普适性,下一步的研究方向可以着眼于云服务器等广义分布式网络环境下的身份认证,建立广泛的信任交互关系.

参考文献

[1] R Housley, W Ford, et al. IETF RFC2459. Internet X.509 public key infrastructure: certificate and CRL profile [S]. Jan. 1999.

[2] A Shamir. Identity-based cryptosystems and signature schemes [J]. Advances in cryptology (Santa Barbara, Calif), 1984, 21(2): 47 – 53.

[3] G Lopze Millan, M Gil Perze, et al. PKI-based trust management in inter-domain scenarios [J]. Computers and Security, 2010, 29: 278 – 290.

[4] 张文芳,汪小敏,等.基于椭圆曲线密码体制的高效虚拟企业跨域认证方案[J].电子学报,2014,42(6):1095 – 1120.
Zhang W F, Wang X M, et al. An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem [J]. Acta Electronica Sinica, 2014, 42(6): 1095 – 1102. (in Chinese)

[5] 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):579 – 582.
Lu Xiao-ming, Feng Deng-guo. An identity-based authentication model for multi-domain grids [J]. Acta Electronica Sinica, 2006, 34(4): 579 – 582. (in Chinese)

[6] 杨斌,陈国庆,孙永红.一种新的基于身份的多信任域认证模型研究[J].计算机安全,2010,8: 15 – 18.
Yang B, Chen G Q, Sun Y H. Research on a new identity-based authentication model for multi-domains [J]. Computer Security, 2010, 8: 15 – 18. (in Chinese)

[7] 杨斌. IBC 和 PKI 组合应用研究[D].郑州:解放军信息工程大学,2009.
Yang B. Research on the combination of identity-based cryptographic techniques and public key infrastructure [D]. Zhengzhou: PLA Information Engineering University, 2009. (in Chinese)

[8] Yuan C, Zhang W F, et al. EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system [J]. Arabian Journal for Science and Engineering, 2017, 42(8): 3275 – 3287.

[9] 蔡维德,郁莲,等.基于区块链的应用系统开发方法研究[J].软件学报,2017,28(6):1474 – 1487.
Tsai W T, Yu L, et al. Blockchain application development techniques [J]. Journal of Software, 2017, 28(6): 1474 – 1487. (in Chinese)

[10] L Axon. Privacy-awareness in blockchain-based PKI [J]. Oxford University Research Archive, 2015.

[11] K Lewison, F Corella. Backing rich credentials with a blockchain PKI [R]. Tech Rep, 2016.

[12] 周致成,李立新,李作辉.基于区块链技术的高效跨域认证方案[J].计算机应用,2018,38(2):316 – 320.
Zhou Z C, Li L X, Li Z H. Efficient cross domain authentication scheme based on blockchain technology [J]. Journal of Computer Applications, 2018, 38(2): 316 – 320.

(in Chinese)

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

[14] Kosba A, Miller A, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts [A]. IEEE Symposium on Security and Privacy (SP) [C]. 2016, San Jose, CA, USA: IEEE Press, 2016. 839 - 858.

[15] 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报 [J]. 2016,42(4) : 481 - 494.
Yuan Y, Wang F Y, Blockchain: The state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4) : 481 - 494. (in Chinese)

[16] 王远敏. 基于 SVO 逻辑的多方不可否认协议的形式化分析与研究 [D]. 贵州大学, 2009.
Wang Y M. The application study on formalism of multi-party non-repudiation protocols on SOV logic [D]. Guizhou University, 2009. (in Chinese)

[17] 田有亮, 彭长根, 马建峰等. 安全协议的博弈论机制 [J]. 计算机研究与发展, 2014, 51(2) : 344 - 352
Tian Y L, Peng C G, Ma J F, et al. Game-Theoretic Mechanism for Cryptographic Protocol [J]. Journal of Computer Research and Development 2014, 51(2) : 344 - 352. (in Chinese)

[18] H Kilinc, T Yanik. A survey of SIP authentication and key agreement schemes [J]. Communications Surveys \& Tutorials, IEEE, 2014, 16(2) , 1005 - 1023.

作者简介

马晓婷　女, 1992 年出生与河北张家口, 硕士研究生, 研究方向为信息安全、密码学.
E-mail: Ma_xting@ 163. com

马文平　男, 1966 年出生, 陕西西安人, 韩国全州全北国立大学的博士后研究员, 研究方向为通信理论、纠错码和信息安全等.