基于零知识的多实体联合身份认证算法

麻付强[1,2,3],徐 峥[1],宋桂香[1]
(1. 浪潮(北京)电子信息产业有限公司,北京 100085;
2. 高效能服务器和存储技术国家重点实验室,北京 100085;
3. 浪潮集团有限公司,山东 济南 250101)

摘 要:针对需要多人操作的强安全云计算系统的身份认证问题,该文提出了一种基于零知识的多实体联合身份认证算法,有效解决了多实体同时联合身份认证问题。采用秘密共享技术将私钥拆分成多个私钥份额,并分发给多个实体。基于零知识证明协议,实体无需传输私钥份额到身份认证中心,降低了传输过程中的泄露风险。采用门限签名算法构造零知识证明协议,每次身份认证需要多个实体参与。同时,身份认证中心无需存储实体的私钥份额,降低了私钥份额的存储泄露风险。进一步,身份认证中心运行在机密计算环境中,每个实体可以对身份认证中心的真实性进行认证。该方案降低单一实体对系统的访问权限,能够容忍少量不可用或恶意实体。最后,该方案从完备性、正确性、零知识性方面分析了算法的安全性。

关键词:身份认证;零知识证明;门限签名;机密计算;多实体
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2023)11-0113-06
doi:10.3969/j.issn.1673-629X.2023.11.017

Multi-entity Joint Identity Authentication Algorithm Based on Zero-knowledge Proof

MA Fu-qiang[1,2,3], XU Zheng[1], SONG Gui-xiang[1]
(1. Inspur (Beijing) Electronic Information Industry Co., Ltd., Beijing 100085, China;
2. State Key Laboratory of High-end Server & Storage Technology, Beijing 100085, China;
3. Inspur Group Co., Ltd., Jinan 250101, China)

Abstract: In view of the joint identity authentication problem of strong security cloud computing system, we propose a multi-entity joint identity authentication algorithm based on zero knowledge, which can effectively solve the problem of multi-entity joint identity authentication. The private key is split into multiple private key shares by using secret sharing technology and distributed to multiple entities. Based on the zero-knowledge proof protocol, the entity does not need to transmit the share of the private key to the identity authentication center, which reduces the risk of disclosure in the transmission process. The zero-knowledge proof protocol is constructed by using threshold signature algorithm. Each identity authentication requires multiple entities to participate. At the same time, the identity authentication center does not need to store the private key share of entity, reducing the risk of storage leakage. Further, the identity authentication center is placed in a confidential computing environment. Each entity can verify the authenticity of the identity authentication center. The proposed scheme reduces the access permission of a single entity to the system and can tolerate a small number of unavailable or malicious entities. Finally, the proposed scheme analyzes the security from the aspects of completeness, correctness and zero knowledge.

Key words: identity authentication; zero-knowledge proof; threshold signature; confidential computing; multi-entity

0 引 言

当前,云计算技术快速发展[1],但云计算平台仍然面临着很多关键性的安全问题,并且已经成为制约其发展的重要因素,其中身份认证安全尤其突出。身份认证是云计算安全的基础[2-3],为用户和云服务提供商的访问控制提供保证,防止非法用户进入云系统,并

收稿日期:2023-01-17 **修回日期**:2023-05-18
基金项目:山东省自然科学基金创新发展联合基金项目(ZR2022LZH013)
作者简介:麻付强(1991-),男,中级工程师,博士,通信作者,研究方向为网络安全、密码协议、云计算安全;通信作者:宋桂香(1978-),女,高级工程师,CCF 标委会委员(F3103M),研究方向为网络安全、密码算法、操作系统安全等。

限制非法用户访问云资源。

身份认证[4-5]在整个信息安全中占据着很重要的位置,是其他安全机制的基础,进而保证安全审计、访问控制、入侵防范等安全机制的有效实施。目前身份认证技术已经广泛应用于信息安全中的数据保护、网络管理等领域。但是随着应用场景的不断扩展,特定的身份认证协议[6]不可能对所有的应用场景都适用,需要针对不同的应用环境设计相应的身份认证协议。

目前,主流的身份认证方案分为以下 3 种:(1)基于静态口令[7]的身份认证,利用用户所知道的信息来证明身份;(2)基于动态口令的身份认证[8],依据用户所拥有的知识来证明身份;(3)基于生物特征的身份认证[9],利用人脸、虹膜等独一无二的生物特征来证明身份。

针对身份认证系统中信任中心权利过大的问题,研究者提出了门限签名的身份认证方案。门限签名算法[10-11]是一种基于秘密共享的技术。(t,n) 秘密共享是指将一个秘密信息利用密码学原理分割成 n 个子秘密信息,只有至少 t 个合法成员合作才可以恢复原始秘密。刘洋宇等人[12]将证书中心分成多个,利用门限签名技术实现对用户证书的颁发。林香等人[13]利用门限盲签名实现了联合身份认证,可以由多个在线的证书生产者进行签名,有效地降低了证书生产者的信任程度。上述门限签名方案均降低了信任中心的权利,尚未研究基于门限签名降低认证实体登录权利集中的问题。

针对身份认证系统中传输信道不安全、信任中心易受攻击等问题,研究者提出利用机密计算技术来增强其安全性[14]。机密计算[15-16]将代码和数据置入到可信执行环境,实现“数据的可用不可见”。Yoon 等人[17]利用 Intel SGX 构建了高效的可搜索加密技术,提高了数据安全性和搜索效率。Bao 等人[18]分析了机密计算在区块链中的应用方案,全面提升了区块链共识算法、智能合约的安全性。Kim 等人[19]利用 Intel SGX 增强了 Tor 网络的安全性和隐私性。零知识证明也可以实现安全的身份认证而不泄露用户隐私信息[20-21]。零知识证明是指证明者能够在不向验证者提供任何有用信息的情况下,使验证者相信某个知识是正确的。基于零知识证明的身份认证机制的研究主体为服务器和用户。服务器不知道用户的登录密钥或者私钥信息,而能够验证用户身份的过程,从而降低身份信息在服务器上的泄露风险,同时还能够减少用户直接发送密码或者私钥的风险。Fiat 等人[22]第一次提出了交互式零知识证明协议,服务器在不获取用户隐私身份信息情况下就能验证用户身份,但是 Fiat-Shamir 只针对单一实体的身份验证。Jelle 等人[23]基于 Fiat-Shamir 变换理论研究了抗量子攻击的零知识证明协议。汪存燕等人[24]提出了基于椭圆曲线的零知识证明,运算过程简单,但是认证实体也是单用户,无法降低实体的登录权限。

上述身份认证都是针对单一实体的访问场景,缺少关注多实体同时联合身份认证问题。针对安全级别较高的系统,例如云计算中的安全管理系统、云密码服务器的后台配置系统,需要多人同时在线进行认证,相互监督,才能够进行操作。如果由单一实体持有重要信息系统的登录权限,则系统会面临两个危险:一是该实体权利过大,一旦成为恶意节点,整个系统将受到攻击;二是一旦该实体失效,整个系统中的服务将无法正常运行。联合身份认证可以保证系统的访问权限不是单独集中在某一个实体上,从而保证安全。但是目前的多人在线认证只是静态口令认证的一种,需要后台单独判断每个实体的身份信息,没有有效实现联合认证。

针对需要多实体操作的强安全云计算系统的身份认证问题,该文提出了一种基于零知识的多实体联合身份认证算法。采用秘密共享技术将私钥拆分成多个私钥份额,并分发给多个实体。基于零知识证明协议,实体无需传输私钥份额到身份认证中心,降低了传输过程中的泄露风险。采用门限签名算法构造零知识证明协议,每次身份认证需要多个实体参与。同时,身份认证中心无需存储实体的私钥份额,降低了私钥份额的存储泄露风险。进一步,身份认证中心运行在机密计算环境中,每个实体可以对身份认证中心的真实性进行认证。

1 零知识证明协议

零知识证明协议包括验证者和证明者[24]。验证者设定算法参数。以椭圆曲线算法为例,包括 p 、q 、E 和 G ,其中 p 是大素数, E 是定义在有限域 F_p 上的椭圆曲线, $G=(x,y)$ 是椭圆曲线 E 上 q 阶的基点。

(1)验证者产生零知识证明私钥 d ,对应公钥为 $P=dG$ 。将私钥 d 发送给证明者。同时生成一个随机数 k ,并发送给证明者。

(2)证明者产生临时私钥 r ,并计算对应临时公钥 rG ,将 rG 发送给验证者。证明者计算 $h=r-kd$,发送 h 到验证者。

(3)验证者验证 rG 是否等于 $kP+hG$,确认证明者具有登录系统的私钥信息,从而实现零知识身份认证。

2 基于零知识的多实体联合身份认证算法

该文方案主要针对强安全云计算系统中实体访问

控制场景,基于椭圆曲线算法设计了零知识的身份认证。如图 1 所示,该方案由客户端和身份认证中心组成,包括身份认证中心机密部署阶段、实体私钥份额生成阶段、零知识认证阶段。身份认证中心的部分重要代码运行在由 Intel SGX 构成的可信执行环境中,执行机密计算。身份认证中心包括基于 SGX 的自签名证书模块、安全信道生成模块、系统参数生成模块、私钥份额生成模块、联合认证模块。客户端包括实体子集合选取模块、安全信道建立模块、零秘密分享模块、临时秘密分享模块、零知识份额计算模块。

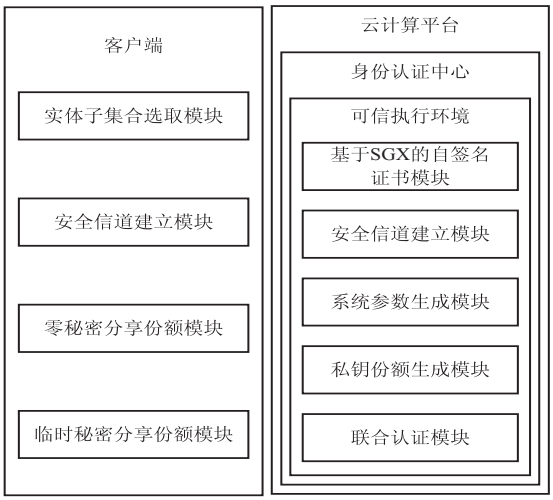

图 1　系统模块

2.1　身份认证中心机密部署

为了降低对身份认证中心权威性的依赖,该方案将身份认证中心的相关负载运行在 Intel SGX 构建的机密计算环境中,可以有效保护身份认证过程中私钥份额生成的机密性,以及联合身份认证过程的真实性。

客户端的实体在与身份认证中心构建安全通信信道时,首先必须验证身份认证中心的工作负载是否在真实的可行执行环境中运行,并且运行的代码是符合预期的。因此,身份认证中心引入了自签名的 X. 509 证书机制[25],并将 Intel SGX 的远程证明数据 Quote 作为证书对象扩展标识的一部分。

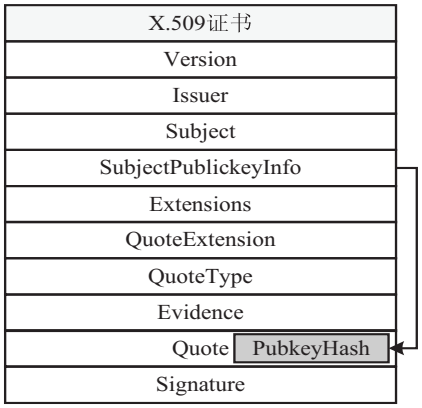

图 2　基于 SGX 的自签名证书

如图 2 所示,远程证明数据 Quote 含有公钥 Hash 值,实现证书与远程证明数据相互绑定。客户端的实体通过验证远程证明数据 Quote 来确认身份认证中心的工作负载确实运行在可信执行环境中,并通过 Quote 中的相关证据验证运行的代码符合预期,没有恶意代码。进而,通过自签名的 X. 509 证书与身份认证中心可以随时建立 TLS 安全信道。

2.2　实体私钥份额生成

身份认证中心在可信执行环境中基于系统参数生成模块设定椭圆曲线上的公开参数,实现系统的初始化,包括 p 、q 、E 和 G ,其中 p 是大素数, E 是定义在有限域 F_p 上的椭圆曲线, $G=(x,y)$ 是椭圆曲线 E 上 q 阶的基点。身份认证中心将多实体联合身份认证的访问控制私钥设置为 d ,公钥为 $P=dG$ 。

身份认证中心执行 Shamir 门限秘密共享,设定 (t,n) 门限签名算法的实体集合。根据私钥为实体的集合中的每个实体各自生成相应的私钥份额,并安全删除私钥。将公钥保存在身份认证中心。身份认证中心将访问控制私钥 d 拆分成 n 份,分发给 n 个有访问权限的实体 $U_1,U_2,\cdots,U_n$ 。任意 t 个或者以上的实体可以执行零知识身份认证方案,从而登录强安全云计算系统,实现重要任务或者数据操作行为。任意 $t-1$ 个或者少于 $t-1$ 个实体均不能实现强安全云计算系统的有效登录。具体生成过程如下:

(1)身份认证中心构造 $t-1$ 阶多项式 $f(x)=\sum_{h=0}^{t-1}a_h x^h$,其中私钥 $d=f(0)=a_0$。

(2)身份认证中心计算 $d_i=f(i)$,$1\leqslant i\leqslant n$,每个实体 U_i 的私钥份额为 d_i 。

基于 TLS 安全信道,身份认证中心将每个客户端实体对应的私钥份额分别发送给每个实体。实体各自安全存储私钥份额,可以将私钥份额存储在安全的硬件介质中,例如 U 盾等。

2.3　零知识身份认证

实体首先协商零知识身份认证的子集合,子集合中的实体都是实体集合中的成员。根据 Shamir 门限秘密共享设定的门限参数,至少有 t 个实体参与多实体联合身份认证,才能有效登录强安全云计算系统。

子集合中的实体开始联合构造基于零知识的多实体联合身份认证方案。假设某次登录由 t 个实体 U_1, $U_2,\cdots,U_t$ 组成的集合 C 登录多实体联合认证系统。此时,每个实体 $U_i\in C$ 。

子集合的实体在临时秘密分享模块执行 Shamir 随机门限秘密共享。每个实体获得临时秘密分享份额 r_i 和临时秘密分享份额公钥 r_iG 。具体生成过程如下:

(1)每个实体 $U_i\in C(1\leqslant i\leqslant t)$ 将自己作为信任

中心,选择随机的秘密值 $a_0^{(i)}$,构造多项式为 $f_i(x)=\sum_{h=0}^{t-1}a_h^{(i)}x^h$。并计算 $f_i(j)$,$1\leqslant j\leqslant t$,并通过发送给其他实体 $U_j\in C(1\leqslant j\leqslant t,j\neq i)$。

(2)实体 $U_j\in C(1\leqslant j\leqslant t)$ 收到其余 $t-1$ 个实体 $U_i\in C(1\leqslant i\leqslant t,i\neq j)$ 发送给自己的 $f_i(j)$,计算 $r_j=\sum_{i=1}^{t}f_i(j)(1\leqslant j\leqslant t)$。

(3)实体 $U_i\in C(1\leqslant i\leqslant t)$ 计算临时秘密分享份额 r_i 对应的临时秘密分享份额公钥 r_iG。实体临时秘密分享份额公钥 r_iG 发送到身份认证中心。

身份认证中心接收 t 个实体的临时秘密分享份额公钥 r_iG,执行 Shamir 门限秘密共享恢复方案,采用拉格朗日插值公式计算整体临时秘密分享公钥 $rG=(\sum_{i\in C}r_i\prod_{j\in C,j\neq i}\frac{j}{j-i})G=(\sum_{i\in C}r_iG\prod_{j\in C,j\neq i}\frac{j}{j-i})$。

身份认证中心的联合认证模块产生一个随机数 k,并将随机数通过 TLS 信道发送给子集合中的实体。

子集合中的实体分别在零秘密分享份额模块执行 Shamir 零秘密门限秘密共享方案,子集合中的实体各自获得零秘密分享份额 u_i。

(1)每个实体 $U_i\in C(1\leqslant i\leqslant t)$ 将自己作为信任中心,选择固定秘密值 $a_0^{(i)}=0$,构造多项式为 $f_i(x)=\sum_{h=0}^{t-1}a_h^{(i)}x^h$。并计算 $f_i(j)$,$1\leqslant j\leqslant t$,并通过发送给其他实体 $U_j\in C(1\leqslant j\leqslant t,j\neq i)$。

(2)实体 $U_j\in C(1\leqslant j\leqslant t)$ 收到其余 $t-1$ 个实体 $U_i\in C(1\leqslant i\leqslant t,i\neq j)$ 发送给自己的 $f_i(j)$,计算 $u_j=\sum_{i=1}^{t}f_i(j)(1\leqslant j\leqslant t)$。其中联合共享秘密 $u=\sum_{i=0}^{t}a_0^{(i)}=0$。

子集合中的实体根据零秘密分享份额 u_i、临时秘密分享份额 r_i、私钥份额 d_i 在零知识份额计算模块中计算零知识身份认证份额 $h_i=r_i-kd_i+u_i(1\leqslant i\leqslant t)$。并分别将零知识身份认证份额 h_i 发送给身份认证中心。

身份认证中心接收子集合中的实体的所有身份认证份额 $h_i(1\leqslant i\leqslant t)$。身份认证中心的联合身份认证模块执行 Shamir 门限秘密共享恢复方案计算联合认证份额 $h=\sum_{i\in C}h_i\prod_{j\in C,j\neq i}\frac{j}{j-i}$。然后,验证 $rG==hG+kP$ 是否相等。如果相等,t 个实体 $U_i\in C(1\leqslant i\leqslant t)$ 的多人联合认证成功,t 个实体可以同时对云计算系统进行重要操作。否则登录失败,则拒绝访问系统。

3 性能分析

(1)完备性:若方案是完备的,则公式 $rG=hG+kP$ 成立。

证明:其中:$h_i=r_i-kd_i+u_i$。t 个实体执行门限秘密共享恢复 h:$h=\sum_{i\in C}h_i\prod_{j\in C,j\neq i}\frac{j}{j-i}=r-kd+u$。其中 $u=0$,则:$h=r-kd$。

完备性可以转换为证明:$hG+kP=hG+kdG=(h+kd)G=(r-kd+kd)G=rG$

因此,公式 $rG==hG+kP$ 成立。

(2)正确性:若公式 $rG=hG+kP$ 成立,则身份认证中心相信 t 个实体的身份,即身份认证中心相信 t 个实体各自知道 $(r_i,u_i)(1\leqslant i\leqslant t)$ 并具有对应私钥份额 $d_i(1\leqslant i\leqslant t)$。若 t 个实体不具有对应私钥份额 $d_i(1\leqslant i\leqslant t)$,那么假定 t 个实体和身份认证中心按照协议完成全部步骤,接受 t 个实体证明的概率是 2^{-p}。

证明:假设 t 个实体能够在较高概率情况下欺骗身份认证中心。由于 t 个实体不知道各自的 d_i,且不能在多项式时间内通过 $P=dG$ 计算 d 或者 d_i,进而无法利用 d_i 来计算 $h_i=r_i-kd_i+u_i$;为了能欺骗成功,对于一个 k,必须从 $hG=rG-kP$ 中求解出 h,进而推导 h_i。但是,从 hG 中推导 h 是一个离散对数问题,是无法求解 h 的,进而无法构造 h_i。

若实体对于随机数 k 可预测,可以通过先选择一个随机数 h_i,并将 h_iG+kd_iG 作为 r_iG 发送给身份认证中心,则身份认证中心接受 t 个实体的身份证明过程。但是预测随机数 k 的概率为 2^{-p}。

(3)零知识性:基于离散对数困难问题,r_iG,rG 的公开不会泄露任何关于 r_i,r 的信息;实体 i 仅知道自己的 r_i,无法获得其他的 $r_j(1\leqslant j\leqslant t,j\neq i)$。同时任何实体也无法获得 r。由于身份证明过程中使用了 t 个实体的秘密值 (r_i,u_i),只有实体可以构造此身份证明,而其他人如果想要构造此身份证明,则必须在不知道用户私钥的情况下,构造公式 $h_i=r_i-kd_i+u_i$,这是困难的;由于离散对数难解,身份认证中心无法得到用户选择的 r_i,r,即使验证者获取 h_i,也无法获取 $h=r-kd+u$。同时如果实体少于 t,那么也无法构造 $h=r-kd+u$,故该方案是零知识的。综上所述,在离散对数难解的假设下,该方案是安全的。

4 安全性分析

4.1 私钥安全性

私钥是在身份认证中心的可信执行环境中生成的,在生成过程中不存在泄露风险。同时,身份认证中心不存储私钥和私钥份额,不存在存储泄露风险。每个实体保存自己的私钥份额,只要泄露不超过 t 个,私钥就是安全的,进而无法进行零知识认证。

4.2　零知识身份认证份额安全性

在构造零知识身份认证份额 $h_i = r_i - kd_i + u_i$ 过程中,增加零秘密分享份额 u_i ,增加零知识身份认证份额的安全性。

4.3　不可伪造性

攻击者即使获取随机数 k ,也无法获得有效的零知识身份认证份额 $h_i = r_i - kd_i + u_i$,因为无法破解 r_i , d_i , u_i 。

4.4　抗重放攻击

基于零知识的身份认证每次认证过程都会随机产生一个新的随机数 k ,并仅使用一次,因此可以抗重放攻击。

5　效　率

5.1　通信量

在实体私钥份额生成阶段,需要将私钥份额和公钥发送给 n 个实体,私钥份额长度为 $|q|$ 及公钥 $2|q|$,其中 $|q|$ 为对应数据的比特位数。

在零知识身份认证阶段,实体间交换 $t(t-1)$ 个临时秘密分享份额的 $f_i(j)$,$1 \leqslant j \leqslant t$,其长度均为 $|q|$ 。实体间交换 $t(t-1)$ 个零秘密分享份额的 $f_i(j)$,$1 \leqslant j \leqslant t$,其长度均为 $|q|$ 。身份认证中心接收 t 个临时秘密分享份额公钥 r_iG ,其长度均为 $2|q|$ 。身份认证中心发送给 t 个实体随机数 k ,其长度均为 $|q|$ 。身份认证中心接收 t 个零知识身份认证份额 h_i ,其长度均为 $|q|$ 。

整体通信发送的数据长度为 $(2t^2 + 2t + 3n)|q|$ 。不同阶段的通信量如表 1 所示。

表 1　不同阶段的通信量

阶段	实体私份额生成	零知识身份认证
通信量	$3n\|q\|$	$(2t^2 + 2t)\|q\|$

5.2　计算量

该文以椭圆曲线上点加、点乘运算的计算量来估计零知识身份认证的计算复杂度。相比上述运算,零知识身份认证其他运算的计算量都很小。并与汪存燕的基于椭圆曲线的零知识身份认证方案进行了比较[24]。

在实体私钥份额生成阶段,计算实体公钥执行了 1 次点乘运算。

在零知识身份认证阶段,计算临时秘密分享份额公钥时执行了 t 次点乘运算。计算整体临时秘密分享公钥执行了 t 次点加运算。计算联合认证时执行了 1 次点加运算、2 次点乘运算。

总体计算复杂度为 $t + 3$ 次点乘运算, $t + 1$ 次点加运算。不同阶段的点加计算量和点乘计算量分别如表 2 和表 3 所示。

表 2　不同阶段的点加计算量

点加计算量	实体私钥份额生成	零知识身份认证
文中算法	0	$t + 1$
传统零知识证明[24]	0	1

表 3　不同阶段的点乘计算量

点乘计算量	实体私钥份额生成	零知识身份认证
文中算法	1	$t + 2$
传统零知识证明[24]	1	3

在实体私钥份额生成阶段,文中算法和传统的基于椭圆曲线的零知识证明在点加和点乘运算上具有相同的运算量。在零知识证明阶段,文中算法和传统的基于椭圆曲线的零知识证明相比,点加运算多了 t 次,点乘运算多了 $t - 1$ 次。主要是文中算法采用秘密共享技术,增加了相关运算量,但是降低了每个实体的登录权限。

6　结束语

该文提出了一种基于零知识的多实体联合身份认证算法,可以有效解决多实体同时联合身份认证问题。将门限签名技术应用到零知识身份认证过程中。基于零知识证明协议,实体无需传输私钥份额到身份认证中心,降低了传输过程中的泄露风险。采用门限签名算法构造零知识证明协议,每次身份认证需要多个实体参与。同时,身份认证中心无需存储实体的私钥份额,降低了私钥份额的存储泄露风险。进一步,身份认证中心运行在机密计算环境中,每个实体可以对身份认证中心的真实性进行认证。该方案降低了单一实体对系统的访问权限,能够容忍少量不可用或恶意实体。未来将可验证技术应用到零知识身份认证中,提高系统的安全性。

参考文献:

[1] 王于丁,杨家海,徐　聪,等. 云计算访问控制技术研究综述[J]. 软件学报,2015,26(5):1129-1150.

[2] 李　建,何永忠,沈昌祥,等. 可信移动平台身份管理框架[J]. 计算机应用研究,2008,25(12):3710-3712.

[3] 张佳乐,赵彦超,陈　兵,等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报,2018,39(3):1-21.

[4] JAIN A K,HONG L,PANKANTI S,et al. An identity-authentication system using fingerprints[J]. Proceedings of the IEEE,1997,85(9):1365-1388.

[5] 邹菁琳. 基于区块链的云辅助物联网身份认证方案研究[D]. 武汉:武汉大学,2022.

[6] ZAWADZKI P. Quantum identity authentication without entanglement[J]. Quantum Information Processing,2019,18

(1):1-12.
[7] 蒋才平,亢 洋,李景华,等. 网络身份认证中隐私计算技术应用初探[J]. 信息安全研究,2022,8(9):863-870.
[8] SETA H,WQATI T,KUSUMA I C. Implement time based one time password and secure hash algorithm 1 for security of website login authentication[C]//2019 international conference on informatics, multimedia, cyber and information system (ICIMCIS). Jakarta:IEEE,2019:115-120.
[9] 张富友,王琼霄,宋 利. 基于生物特征识别的统一身份认证系统研究[J]. 信息网络安全,2019,19(9):86-90.
[10] ABDALLA M,MINER S,NAMPREMPRE C. Forward-secure threshold signature schemes[C]//Cryptographers' track at the RSA conference. San Francisco:Springer,2001:441-456.
[11] PILARAM H,EGHLIDOS T,TOLUEE R. An efficient lattice-based threshold signature scheme using multi-stage secret sharing[J]. IET Information Security,2021,15(1):98-106.
[12] 刘洋宇,侯整风. 基于椭圆曲线的门限身份认证方案[J]. 计算机工程与设计,2005,26(10):2858-2859.
[13] 林 香. 基于盲签名的联合身份认证研究[D]. 武汉:武汉理工大学,2018.
[14] 王 鹃,樊成阳,程越强,等. SGX 技术的分析和研究[J]. 软件学报,2018,29(9):2778-2798.
[15] SOBCHUK J,O´MELIA S,UTIN D,et al. Leveraging Intel SGX technology to protect security-sensitive applications[C]//2018 IEEE 17th international symposium on network computing and applications (NCA). Cambridge: IEEE,2018:1-5.
[16] ZHANG D,WANG G,XU W,et al. Sgxpy:protecting integrity of python applications with intel sgx[C]//2019 26th Asia-Pacific software engineering conference (APSEC). Putrajaya:IEEE,2019:418-425.
[17] YOON H,HUR J. A comparative analysis of searchable encryption schemes using SGX[C]//2020 international conference on information and communication technology convergence (ICTC). Jeju:IEEE,2020:526-528.
[18] BAO Z,WANG Q,SHI W,et al. When blockchain meets sgx:an overview,challenges,and open issues[J]. IEEE Access,2020,8:170404-170420.
[19] KIM S,HAN J,HA J,et al. Sgx-tor:a secure and practical tor anonymity network with sgx enclaves[J]. IEEE/ACM Transactions on Networking,2018,26(5):2174-2187.
[20] WENG C,YANG K,XIE X,et al. Mystique:efficient conversions for zero-knowledge proofs with applications to machine learning[C]//30th USENIX security symposium. Berkeley:USENIX,2021:501-518.
[21] 张小红,樊中奎,钟小勇. Schnorr 协议的一次一密双重身份认证研究[J]. 计算机工程与应用,2010,46(19):81-84.
[22] FIAT A,SHAMIR A. How to prove yourself:practical solutions to identification and signature problems[C]//Advances in cryptology—CRYPTO´86. Berlin: Springer,1986:186-194.
[23] DON J,FEHR S,MAJENZ C,et al. Security of the Fiat-Shamir transformation in the quantum random-oracle model[C]//Advances in cryptology - CRYPTO 2019:39th annual international cryptology conference. Santa Barbara:Springer,2019:356-383.
[24] 汪存燕. 基于椭圆曲线零知识证明的身份认证系统的研究和实现[D]. 上海:上海师范大学,2010.
[25] WALTHER R,WEINHOLD C,ROITZSCH M. RATLS:integrating transport layer security with remote attestation[C]//International conference on applied cryptography and network security. Berlin:Springer,2022:361-379.