面向物联网的三因子跨域签密访问控制方案

黄隆坤[1,2],田有亮[1,2,3],谢洪涛[4]
(1. 贵州大学计算机科学与技术学院,贵州贵阳 550025;2. 贵州大学密码学与数据安全研究所,贵州贵阳 550025;
3. 贵州省公共大数据重点实验室,贵州贵阳 550025;4. 中国科学技术大学信息科学与技术学院,安徽合肥 230026)

摘 要: 在5G的海量机器类通信(massive Machine Type Communication,mMTC)物联网环境下,存在跨安全域的公钥加密体制PKI(Public Key Infrastructure)的物联网用户对无证书加密体制CLC(CertificateLess Cryptosystem)的物联网设备跨域安全通信问题. 本文基于用户口令、生物特征和用户智能设备等组成的三因子和国密SM2的加密和签名算法,提出三因子跨域签密的访问控制方案(Three-factor Cross-domain Signcryption Access Control scheme for IoT environment,TCSAC-IoT),用于在跨安全域的情况下实现PKI物联网用户对CLC物联网设备跨域安全通信. 方案通过三因子跨域签密算法对PKI物联网用户进行认证,对合法的PKI物联网用户建立与CLC物联网设备之间的共享秘钥,避免非法用户对CLC物联网设备资源非法访问,并在真实或随机ROR(Real-Or-Random)模型下证明了该方案在DY(Dolev-Yao)模型和CK(Cantti-Krawczyk)模型下满足语义安全性,同时具有抗伪装攻击、抗重放攻击、抗中间人攻击、抗内部特权攻击和抗盗用或丢失PKI用户智能设备攻击,与类似方案对比分析的结果表明本方案有较低的计算开销和通信开销.

关键词: 跨域签密;跨域访问控制;物联网安全;5G
基金项目: 国家重点研发计划项目(No.2021YFB3101100);贵州省高层次创新型人才项目(No.黔科合平台人才[2020]6008);贵州省科技计划项目(No.黔科合平台人才[2020]5017)
中图分类号: TN918.4 **文献标识码:** A **文章编号:** 0372-2112(2023)09-2578-10
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20211348

Three-Factor Cross-Domain Signcryption Access Control Scheme for IoT Environment

HUANG Long-kun[1,2], TIAN You-liang[1,2,3], XIE Hong-tao[4]
(1. *School of Computer Science and Technology, Guizhou University, Guiyang, Guizhou* 550025, *China*;
2. *Institute of Cryptography & Date Security, Guizhou University, Guiyang, Guizhou* 550025, *China*;
3. *Guizhou Provincial Key Laboratory of Public Big Data, Guiyang, Guizhou* 550025, *China*;
4. *School of Information Science and Technology, University of Science and Technology of China, Hefei, Anhui* 230026, *China*)

Abstract: In the massive machine type communication (mMTC) internet of Things environment of 5G, there is the problem of cross-domain secure communication from IoT users with public key infrastructure (PKI) encryption scheme to IoT devices with certificateless cryptosystem (CLC) encryption regime across security domains. In this paper, we propose a three-factor cross-domain signed-encryption access control scheme in the Internet of things (TCSAC-IoT) for PKI users to CLC devices with cross-domain secure communication based on the signcryption algorithm of three-factor and national secret SM2 composed of user passwords, biometrics and user smart device. The scheme authenticates PKI IoT users through a three-factor cross-domain signcryption algorithm, and grants legitimate PKI IoT users a shared secret key with CLC IoT devices to avoid illegal access to CLC IoT device resources by illegal users. It is also demonstrated under the real-or-random (ROR) model that the scheme satisfies semantic security under the Dolev-Yao (DY) model and Cantti-Krawczyk (CK) model, and is also resistant to spoofing attacks, replay attacks, man-in-the-middle attacks, internal privilege attacks and theft or loss of PKI user smart device attacks. The results of the analysis in comparison with similar schemes show that this scheme has low computational overhead and communication overhead.

Key words: cross-domain signcryption; cross-domain access control; IoT security; 5G

收稿日期:2021-10-08;修回日期:2022-03-21;责任编辑:梅志强

Foundation Item(s): National Key Research and Development Program of China (No.2021YFB3101100); Project of High-level Innovative Talents of Guizhou Province (No.[2020]6008); Science and Technology Program of Guizhou Province (No.[2020]5017, No.[2022]065); Science and Technology Program of Guiyang (No.[2022]2-4)

1 引言

随着5G技术的快速发展和在物联网领域的广泛应用,形成了海量机器类通信(massive Machine Type of Communication,mMTC)为特点的物联网环境,mMTC也是5G技术的三大类应用场景之一[1]. 在mMTC的物联网中,存在海量的物联网设备,如传感器、摄像头和用户智能设备等. 然而海量的物联网设备也形成了错综复杂的环境,为了使物联网设备之间相互安全通信,可采用加密的方式来为物联网设备提供保护,由于海量物联网设备采用了不同的加密体制,从而形成了多安全域的物联网环境,可将常用的加密体制分为三类,基于公钥基础设施的加密体制PKI(Public Key Infrastructure)、基于身份的加密体制IBC(Identity-Based Cryptosystem)和基于无证书的加密体制CLC(CertificateLess Cryptosystem)等. 在mMTC中,这些物联网设备通常面临着外部环境恶劣、计算能力弱、内存小、有限的电力和低带宽等物理资源受限的环境. 1997年,Zheng等[2]提出了一种新的密码学原语—签密,在一个逻辑步内实现签名和加密,同步实现保密性、完整性和不可否认性,可用于物理资源受限的物联网中,实现对用户身份的验证和消息的保密性,整体上节省了系统的计算开销和通信开销,从而为物理资源受限的物联网设备之间的相互访问提供了一种了安全的通信访问. 然而,由于mMTC中大规模物联网使用不同的加密体制,形成了多安全域的物联网环境,实现不同加密体制之间的物联网设备安全通信称为跨域安全通信,这也是5G移动通信系统需要考虑关键问题之一[3]. 实现跨域通信可减少在同一个物联网设备使用多种加密体制,适合于物理资源受限的物联网设备. 异构签密是一种可以使不同加密体制的双方实现安全通信的加密算法,因此采用异构签密方案可以在跨安全域的情况下实现不同加密体制的物联网设备间的安全通信. 可将目前实现异构加密的跨域通信分为三种,即PKI-IBC异构跨域通信[4~10]、IBC-CLC[11~13]异构跨域通信和PKI-CLC[14,15]异构跨域通信,每类又可分为单向和双向、单接收者和多接收者. 2010年,Sun等[4]首次提出基于PKI-IBC异构签密方案,实现了从PKI加密体制到IBC加密体制的双向跨域安全通信,然而该方案不满足内部安全[5]. 2013年,Li[6]等提出基于IBC-PKI在线/离线结构的单向异构签密方案,在离线阶段处理复杂的计算,从而提高了传感器节点在签密阶段的计算效率,然而却不能保护传感器节点的隐私. 2016年,Li等[7]提出基于IBC-PKI的单向异构环签密方案,提供发送方隐私保护,但却增加计算开销. 为了提供一种轻型的加密方案用于传感器节点,2016年,Raveendranath等[8]基于椭圆曲线密码学提出PKI-IBC的双向异构签密方案,具有单接收者和多接收者两种方案,然而不满足内部安全. 为了实现不同加密体制之间的用户通信,Niu等[9]提出了基于签密的PKI-IBC密钥交换协议. 2018年,Ting等[10]基于椭圆曲线提出了IBC-PKI单向在线/离线签密方案,实现了IBC传感器节点发送消息给互联中的PKI用户. 在CLC-IBC的跨域安全通信方面,2016年,Li等[11]提出了一种新的异构签密方案HSC,实现了CLC-IBC的跨域安全通信,且提供了消息查询保护,使用户的隐私得到了保护. Li等[12]在分析Niu[13]方案基础上提出IBC-CLC单向异构混合签密方案,不仅能够加密短消息,而且能够实现安全通信. 2018年,Saeed等[14]提出了CLC-PKI在线/离线单向签密方案,实现了CLC传感器节点向PKI中服务器发送消息,使用在线/离线机制减少传感器节点的计算. 2019年,Luo等[15]提出CLC-PKI的单向签密方案,使不同参数的CLC传感器节点发送消息到PKI服务器. 虽然采用异构签密可以实现跨安全域的加密体制的物联网设备之间安全通信,但是在用于mMTC的物联网环境中时,仍然存在如下的问题:(1)物联网设备面复杂的外部环境,可能遭受更强的敌手攻击,如物联网设备丢失和被盗的情况,单独异构签密方案不足以抵抗这些攻击;(2)采用基于双线性对的异构签密对处于物理资源受限物联网设备所需要计算量仍然巨大,会受限于真实的物联网环境;(3)由于IBC存在密钥托管问题,不适合于mMTC中的物联网. 2020年,Mandal等[16]提出了一种基于三因子的无证书签密访问控制方案,采用用户口令、生物特征和用户智能设备等组成的三因子对物联网用户的身份进行认证,通过多因子组合的方式,可提高访问控制方案整体的面临复杂的外部环境时的安全性,之后对通过认证的合法CLC物联网用户和CLC物联网设备之间建立共享密钥,实现CLC物联网用户对CLC物联网设备的安全通信,该方案采用了无双线性对运算的访问控制方法,缓解了物联网设备的计算压力,采用了无证书签密,可有效解决物联网环境中密钥托管的问题,并减少了系统的计算开销和通信开销,适合于mMTC的物联网. 然而,该方法不能实现跨安全域下不同加密体制之间的物联网用户和物联

网设备的安全通信，因此，针对PKI加密体制的物联网用户对CLC加密体制的物联网设备的安全通信需求，基于GB/T 32918.4-2016 SM2加密算法和GB/T 32918.2-2016 SM2签名算法，在DY模型和CK模型下，提出了面向物联网的三因子跨域签密访问控制方案(Three-factor Cross-domain Signcryption Access Control scheme for IoT environment，TCSAC-IoT)，方案面对物联网的三方应用场景，即PKI加密体制的物联网用户、CLC加密体制的网关和物联网设备，PKI物联网用户可通过网关实现对CLC物联网设备的访问数据或获取服务，从而实现安全通信. 本文主要研究内容如下：

(1)基于用户口令、生物特征和用户智能设备的三因子，设计基于国密的PKI-CLC跨域签密访问控制方案，该方案允许合法注册的PKI用户在和CLC物联网设备相互认证成功之后可实时地从物联网设备访问数据或获取服务，具有物联网设备动态添加、合法用户注销、用户口令和生物特征更新等功能.

(2)在实现跨安全域的情况下，可以抵抗由于用户智能设备被盗或丢失、用户口令被字典猜测攻击成功和猜中用户口令而带来的安全隐患，提高了访问控制方案授权部分的可信度，并证明了在ROR模型下，可抵御DY敌手模型和CK敌手模型下的攻击.

(3)与其他类似方案相比，一方面，系统不存在密钥托管问题，从而避免了在大规模物联网中，密钥托管带来的安全问题；另一方面，由于采用了无双线性运算，减少了mMTC物联网环境中物联网设备计算开销和通信开销，更加符合真实的物联网环境中物联网设备资源受限的情况.

2 基础知识

2.1 系统模型

本文使用的TCSAC-IoT物联网模型如图1所示，由Mandal等[16]提出的无证书签密访问控制方案(Certificateless-Signcryption-based User Access Control for the IoT，CSUAC-IoT)和Malani等[17]提出的PKI访问控制方案组成. 其中密钥生成中心(Key Generation Center，KGC)、无证书用户(Certificateless User，CU)、网关-1、无证书物联网(CertificateLess Cryptosystem for IoT，CLC IoT)设备和黄色线路部分组成了基于CLS环境下的用户访问控制方案；证书授权机构(Certificate Authority，CA)、PKI用户(PKI User，PU)、网关-2、PKI IoT设备组成基于PKI环境下的用户访问控制方案.

2.2 威胁模型

本文使用DY敌手模型[18]用来分析物联中被动攻击的情况，在DY敌手模型下，敌手$\mathcal{A}$可以拦截任意通信双方在网络中传输的消息，如网关(Gatew Node，GN)、物联网设备D和PU.

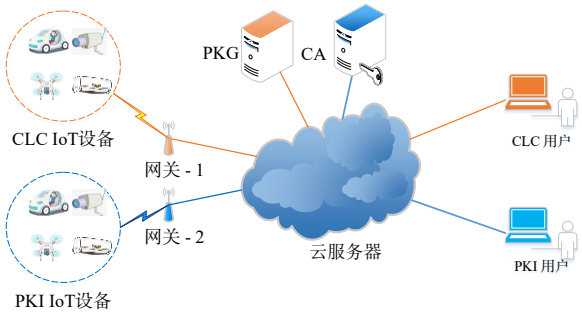


图1 异构IoT下的网络模型

此外，还考虑了CK敌手模型[19]以分析物联网中主动攻击的情况. CK敌手模型是建立在DY模型之上的敌手模型，在CK敌手模型下，如果秘密凭证、密钥和会话状态不是安全的存储在物联网设备，则CK敌手可以在访问控制阶段破坏这些设备. 除此之外，敌手$\mathcal{A}$还可以从用户的移动设备中提取秘密凭证来发起其他潜在的攻击，如仿冒攻击和离线猜测攻击等. 最后还考虑了IoT设备被物理捕获的情况.

2.3 安全模型

定义1 抗碰撞加密单向哈希函数$H(\cdot)$: $\{0,1\}^{*}\rightarrow\{0,1\}^{l_h}$为输入任意长度比特串、输出固定长度比特串的确定性函数. 设$\mathrm{Adv}_{\mathcal{A}1}^{H(\cdot)}(rt)$是敌手$\mathcal{A}$找到$H(\cdot)$哈希碰撞的优势，则$\mathcal{A}$的优势表示为$\mathrm{Adv}_{\mathcal{A}}^{H(\cdot)}(rt)=\Pr[(ls_1,ls_2)\in_r\mathcal{A}: ls_1\neq ls_2, H(ls_1)=\mathrm{H}(ls_2)]$，其中$(ls_1,ls_2)\in_r\mathcal{A}$，表示$\mathcal{A}$随机选择两个比特串，$\Pr(E)$表示随机事件$E$发生的概率，$rt$为$\mathcal{A}$运行的最大时间，$ls_1,ls_2$表示输入的字符串对. 若没有多项式时间(PPT)的敌手$\mathcal{A}$以至少η的优势找到$H(\cdot)$的抗碰撞性，即$\mathrm{Adv}_{\mathcal{A}1}^{H(\cdot)}(rt)\leqslant\eta$，则称$(\eta,rt)$-$\mathcal{A}$满足抗碰撞性.

定义2 计算性Diffie-Hellman问题(ECCDHP). 设$G\in E_q(a,b)$，给定四元组$(G,u\cdot G,v\cdot G,w\cdot G)$且$u,v,w\in\mathbb{Z}_n^{*}$，求$w=u\cdot v$是一个困难性问题.

定义3 椭圆曲线离散对数问题(ECDLP). 设$G\in E_q(a,b)$，给定$u\in\mathbb{Z}_n^{*}$，$uG\in E_q(a,b)$，求解u是一个困难性问题.

定义4 语义安全. 设$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{HSUAC\text{-}IoT}}(t)$是敌手$\mathcal{A}$在多项式时间$t$内破坏HSUAC-IoT语义安全性从而提取用户PU和物联网设备D之间的会话密钥SK的优势，则敌手$\mathcal{A}$优势为

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{HSUAC\text{-}IoT}}(t)=|2\Pr[\beta'=\beta]-1| \tag{1}$$

其中β和β'分别为正确猜测的bit和错误猜测的bit.

3 方案设计

本文设计的TCSAC-IoT方案由KGC、CA、CU(CLS

Uesrs,CU)、PU、GN和D_i组成.D_i、GN、KGC和CU属于CLS访问控制方案,CA和PU属于PKI用户访问控制方案.方案的主要参数如表1所示.

表1　系统主要参数

参数	含义	参数	含义
G	椭圆曲线上的点	CA	认证中心
q	大素数	Z	系统的公开参数
n	G的阶	D_i	第i个物联网设备
λ	安全参数	Bio_i	第i个生物特征
T_{MAX}	最大延迟时间	γ_i	生物识别特征
$E_q(a,b)$	椭圆曲线方程	τ_i	生物识别参数
PU	PKI加密环境的用户	PW_{PU}	用户PU密码
KGC	密钥生成中心	H_i	第i个哈希函数

3.1　系统初始化阶段

输入安全参数λ,系统随机选择一个素数$p(q\geqslant p^k,k$是一个大整数),随机选择$a,b\in\mathbb{Z}_q^*$,且满足$4a^3+27b^2\neq 0\pmod q$,得到一个在有限域GF(q)上的椭圆曲线$E_q(a,b)$:$y^2=x^3+ax+b\pmod q$.然后,在$E_q(a,b)$上随机选择一个点G,满足$nG=O$,且n为q比特长.由于是在异构加密的互联网环境中,因此分别使用了CA和KGC来为PKI加密系统和CLC加密系统中的用户生成数字证书和用户的部分密钥.

(1)CA初始化

CA将自己的ID_{CA}通过安全通道发送给KGC,收到KGC发来的d_{CA}后,随机选择一个整数$x_{CA}\in\mathbb{Z}_n^*$,计算$sk_{CA}=d_{CA}+x_{CA}\pmod n$,将$sk_{CA}$作为CA的私钥,计算$pk_{CA}=sk_{CA}\cdot G$,将$pk_{CA}$作为CA的公钥.

(2)KGC初始化

KGC随机选择一个整数$sk_{KGC}\in\mathbb{Z}_n^*$作为自己的私钥,相应的公钥为$pk_{KGC}=sk_{KGC}\cdot G$.KGC收到CA发来的$ID_{CA}$后,计算出CA的部分私钥$d_{CA}=H(ID_{CA},sk_{KGC})$,则$P_{CA}=d_{CA}G$.KGC通过安全通道发送$(d_{CA},P_{CA})$给CA,并删除$d_{CA}$.最后公开系统公共参数$Z=<E_q(a,b)G,p,pk_{CA},pk_{KGC},P_{CA}>$.

3.2　CLC物联网设备注册阶段

GN和D_i通过安全信道发送各自的ID_{GN}和ID_{D_i}给KGC,KGC收到(ID_{GN},ID_{D_i})后,计算$d_{GN}=H(ID_{GN},sk_{KGC})$和$d_{D_i}=H(ID_{D_i},sk_{KGC})$相应的$P_{GN}=d_{GN}\cdot G$,$P_{D_i}=d_{D_i}\cdot G$,随机选择一个整数$k_i\in\mathbb{Z}_n^*$,再将$(d_{GN},P_{GN},k_i)$和$(d_{D_i},P_{D_i},k_i)$分别通过安全信道发送给GN和$D_i$,KGC公布$(P_{GN},P_{D_i})$,并删除$(d_{GN},d_{D_i},k_i)$.GN和$D_i$收到$(d_{GN},P_{GN},k_i)$和$(d_{D_i},P_{D_i},k_i)$后分别随机选择一个整数$x_{GN},x_{D_i}\in\mathbb{Z}_p^*$,分别计算$sk_{GN}=H(x_{GN},d_{GN})$和$sk_{D_i}=H(x_{D_i},d_{D_i})$.以$sk_{GN},sk_{D_i}$分别作为GN和$D_i$的私钥,则GN和$D_i$各自的公钥为$pk_{GN}=sk_{GN}\cdot G,pk_{D_i}=sk_{D_i}\cdot G$.

3.3　PKI用户注册阶段

用户随机选择一个整数$sk_{PU}\in\mathbb{Z}_p^*$作为私钥,则相应的公钥为$pk_{PU}=sk_{PU}\cdot G$.然后通过安全通道发送(ID_{PU},pk_{CA})给CA,CA收到(ID_{PU},pk_{CA})后,取TS_{ED}为截止日期,计算$cert_{PU}=H(ID_{PU},pk_{PU})\cdot(sk_{CA}+d_{CA})$.将$cert_{PU}$通过公共信道发送给用户PU.用户PU收到$cert_{PU}$后,随机选择一个整数$Q\in\mathbb{Z}_n^*$,计算

$$f(x)=\prod_{i=1}^{2}(x-\gamma_i)+Q\pmod n$$
$$=x^2+a_1x+a_0 \tag{2}$$

其中$a_1,a_0\in\mathbb{Z}_n^*$.计算$C^*=(cert_{PU}\|sk_{PU})\oplus H(ID_{PU},Q,PW_{PU})$,$HPW_{PU}^*=H(ID_{PU},Q,PW_{PU},pk_{PU})$,将$C^*$、$HPW_{PU}^*$、$a_0$和$a_1$存储在移动设备$D_{PU}$内存上,并删除$cert_{PU},sk_{PU}$.

3.4　登录和访问控制阶段

在该阶段,PKI加密体制中的用户PU输入口令和生物特征σ_{PU}登录自己的移动设备,并与需要通信的GN下的物联设备D_i建立共享会话密钥SK(SK′),具体过程如图2所示,要实现这个功能可以通过四个算法实现,分别为PKI用户签密算法、GN解签密算法、D_i解签密和确立会话密钥算法和验证会话密钥算法,如图2所示.

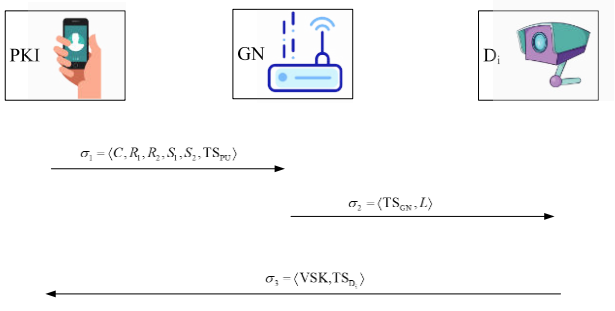


图2　登录和访问控制阶段

3.4.1　PKI用户签密

在该过程中,合法的PKI加密体制中的注册用户PU要访问GN下的物联网设备D_i,先PU需要在移动设备上输入口令PW_{PU}和生物特征信息Bio_i(i=1或2),恢复移动设备上的可用参数以使GN和D_i可以认证自己身份,PU选择自己需要进行访问的物联网设备ID_{D_i},和在移动设备上恢复出来的参数$cert_{PU}$、sk_{PU}和Q等,使用算法1得到$\sigma_1=<C,R_1,R_2,S_1,S_2,TS_{PU}>$,并通过公共信道发送给GN,其中$S_1$是发送GN的签名,$S_2$是发送给物联网设备$D_i$的签名.

3.4.2　GN解签密

在收到PU在TS_{NOW}时刻发送过来的信息σ_1之后,

算法1 PKI用户签密

输入:PW_{PU}, Bio_1或$Bio_2, Z, (ID_{GN}, pk_{GN}, P_{GN}), (ID_{D_i}, pk_{D_i}), TS_{PU}$

输出:$\sigma_1 = <C, R_1, R_2, S_1, S_2, TS_{PU}>$

1:计算$Hdist(Bio_i, Bio_i')$, $i=1$或2

2:IF $Hdist(Bio_i, Bio_i') \leqslant et$ THEN

3: 计算$\gamma_i = Rep(Bio_i, \tau_i)$, $i=1$或2

4: 计算$Q = f(\gamma_i)$, $i=1$或2

5: 计算$H(ID_{PU}, PW_{PU}, Q, pk_{PU})$

6:IF $HPW_{PU}^* = H(ID_{PU}, PW_{PU}, Q, pk_{PU})$ THEN

7: 计算$(cert_{PU} \| sk_{PU}) = C^* \oplus H(ID_{PU}, Q, PW_{PU})$

8: 随机选择$v_1, v_2, v_3 \in \mathbb{Z}_n^*$

9: 计算$V_1 = v_1 G = (x_1, y_1)$和$V_2 = v_2 G = (x_2, y_2)$.将(x_1, y_1)和(x_2, y_2)表示为比特串.

10: 计算$T_1 = h \cdot pk_{GN}$,$T_2 = h \cdot pk_{D_i}$,若T_1或T_2是无穷远点,则报错退出.

11: 计算$(x_{GN}, y_{GN}) = v_1 \cdot pk_{GN} + v_1 \cdot p_{pub_{GN}}$和$(x_{D_i}, y_{D_i}) = v_2 \cdot pk_{D_i} + v_2 \cdot P_{D_i}$.将$x_{GN}, y_{GN}, x_{D_i}, y_{D_i}$表示为比特串;

12: 计算$C = (cert_{PU} \| ID_{D_i} \| v_3) \oplus H(x_{GN}, (pk_{GN} + P_{GN}))$;

13: 计算$e_1 = H(x_{GN}, TS_{PU}, Z, cert_{PU}, ID_{D_i}, v_3, y_{GN})$和$e_2 = H(x_{D_i}, Z, H(e_1, TS_{PU}), y_{D_i})$;

14: 计算$R_1 = e_1 \cdot V_1$和$R_2 = e_2 \cdot V_2$;若$R_1 = O$或$R_2 = O$,则返回8步;

15: 计算$S_1 = ((1 + sk_{PU})^{-1} \cdot (v_1 - R_1 \cdot sk_{PU}))(\mathrm{mod}\, n)$和$S_2 = ((1 + sk_{PU})^{-1} \cdot (v_2 - R_2 \cdot sk_{PU}))(\mathrm{mod}\, n)$;若$S_1 = 0$或$S_2 = 0$,则返回8步;

16:RETURN $\sigma_1 = <C, R_1, R_2, S_1, S_2, TS_{PU}>$

GN首先验证该信息是否是PU产生的,如果验证通过,则GN按照算法2生成一条信息σ_2,并通过公共信道发送给PU需要访问的物联网设备D_i,若验证不通过,则终止这个阶段.

3.4.3 D_i解签密和确立会话密钥

在收到GN发送的σ_2消息之后,物联网设备D_i如算法3执行解签密和确立会话密钥,得到消息$\sigma_3 = <VSK, TS_{D_i}>$,并通过公共信道发送给PKI加密体制中的用户PU.

3.4.4 验证会话密钥

在收到物联网设备D_i发送过来的$\sigma_3 = <VSK, TS_{D_i}>$之后,PU运行算法4进行会话密钥验证,若$VSK' = VSK$,则验证通过,PU存储会话密钥SK在移动设备上用于与物联网设备D_i进行通信. 同样,物联网设备也存储会话密钥SK′,用于与PKI加密体制中的用户PU通信.

3.5 物联网设备添加阶段

当物联网设备D_j需要添加到GN网关下时,D_j通过安全信道发送(ID_{D_j}, ID_{GN})给KGC,KGC收到(ID_{GN}, ID_{D_j})后,计算$d_{D_j} = H(ID_{D_j}, sk_{KGC})$作为部分私钥,相应的部分公钥为$P_{D_j} = d_{D_j} \cdot G$,随机选择一个整数$k_j \in \mathbb{Z}_n^*$,则将$(ID_{D_j}, k_j)$和$(d_{D_j}, P_{D_j}, k_j)$分别通过安全信道发送给GN和$D_i$,KGC公布$P_{D_j}$,并删除$(d_{D_i}, k_j)$.

算法2 GN解签密

输入:$\sigma_1' = (C', R_1', R_2', S_1'), sk_{GN}$

输出:$\sigma_2 = <TS_{GN}, L>$

1:IF $|TS_{PU} - TS_{NOW}| \leqslant T_{MAX}$ THEN

2: 检验$R_1' \in [1, n-1]$是否成立,若不成立,报错退出;

3: 计算$t = (R_1' + S_1')(\mathrm{mod}\, n)$,若$t = 0$,则报错并退出;

4: 计算$t = (R_1' + S_1')(\mathrm{mod}\, n)$,若$t = 0$,则报错并退出;

5: 计算$V_1' = (x_1', y_1') = S_1' \cdot G + t \cdot pk_{PU}$;

6: 计算$T_1' = hV_1'$,若$T_1' = O$,则报错退出;

7: 计算$(x_{GN}', y_{GN}') = (sk_{GN} + d_{GN}) \cdot V_1'$,将$x_{GN}', y_{GN}'$表示为比特串;

8: 计算$(cert_{PU} \| ID_{D_i} \| v_3) = C \oplus H(x_{GN}', pk_{PU} \cdot (sk_{GN} + d_{GN}))$;

9: 计算$e_1' = H(x_{GN}', TS_{PU}', Z_{PU}, cert_{PU}', ID_{D_i}, v_3, y_{GN}')$;

10: 计算$R_1' = e_1 \cdot V_1'$,检验$R_1' = R_1$是否成立,若成立则验证通过,否则报错退出;

11: 计算$cert_{PU} \cdot G = H(ID_{PU}, pk_{PU}) \cdot pk_{CA} + H(ID_{PU}, pk_{PU}) \cdot p_{pub_{CA}}$若不成立,则报错退出;

12: 计算$L = (H(e_1, TS_{PU}), pk_{PU}) \oplus H(k_i, TS_{GN})$;

13:RETURN $\sigma_2 = <TS_{GN}, L>$

算法3 D_i解签密和确立会话密钥

输入:$\sigma_2 = <TS_{GN}, ID_{D_i}, L>, Z, TS_{D_i}, <k_i, ID_{D_i}, sk_{D_i}>$

输出:$\sigma_3 = <VSK, TS_{D_i}>$

1:IF $|TS_{PU} - TS_{NOW}| \leqslant T_{max}$ THEN

2: 计算$(H(e_1, TS_{PU}), pk_{PU}) = L \oplus H(k_i, TS_{GN})$;

3: 计算$V_2' = (x_2', y_2') = S_2' \cdot G + t \cdot pk_{PU}$;

4: 计算$(x_{D_i}', y_{D_i}') = (sk_{D_i} + d_{D_i}) \cdot V_2'$,将$x_{D_i}', y_{D_i}'$表示为比特串;

5: 计算$e_2' = H(x_{D_i}', Z, H(e_1, TS_{PU}), y_{D_i}')$;

6: 验证$R_2' = e_2 \cdot V_2'$,若不成立,报错退出;

7: $VSK = H(x_{D_i}', H(e_1, TS_{PU}), TS_{D_i}, y_{D_i}')$;

8:RETURN $\sigma_3 = <VSK, TS_{D_i}>$

算法4 验证会话密钥

输入:$\sigma_3 = <VSK, TS_{D_i}>, H(e_1 \| TS_{PU})$

输出:State

1:IF $|TS_{PU} - TS_{NOW}| \leqslant T_{MAX}$ THEN

2: 计算$VSK = H(x_{D_i}, H(e_1, TS_{PU}), y_{D_i})$;

3: 计算$VSK' = H(x_{D_i}, H(e_1, TS_{PU}), TS_{D_i}, y_{D_i})$;

4: IF $VSK' = VSK$ THEN

5: State = 1,建立会话密

6: ELSE

7: State = 0,报错退出

8:RETURN State

$H(x_{D_j}, d_{D_j})$. 以 sk_{D_j} 分别作为 D_j 的私钥,则 D_j 相应的公钥为 $pk_{D_j} = sk_{D_j} \cdot G$. 将 (ID_j, sk_{D_j}, k_j) 加载到 D_j 的内存中.

3.6 PKI用户口令和生物识别信息更新

在该阶段,用户可以通过算法5在移动设备 D_{PU} 更新自己的口令或生物识别信息,而不需要第三方CA.

算法5　口令和生物识别信息更新

输入: $D_{PU}, PW_{PU}^{id}, Bio_1^{old}$ 或 $Bio_2^{old}, PW_{PU}^{new}, Bio^{new}$

输出: C^{new}, HPW_{PU}^{new}

1:IF　$Hdist(Bio_{PU}, Bio_{PU}^{old}) \leqslant et$　THEN

2:　计算 $\gamma_i = Rep(Bio_i^{old}, \tau_1)$, $i=1$或$i=2$;

3:　计算 $Q = f(\gamma_i)$, $i=1$或$i=2$;

4:IF　$HPW_{PU}^{old} = H(ID_{PU}, Q, PW_{PU}^{old}, pk_{PU})$ THEN

5:　CASE1: 更新口令

6:　　计算 $C^{new} = (cert_{PU} \| sk_{PU}) \oplus H(ID_{PU}, Q, PW_{PU}^{new})$;

7:　　计算 $HPW_{PU}^{new} = H(ID_{PU}, Q, PW_{PU}^{new}, pk_{PU})$;

8:　CASE2: 更新生物识别信息

9:　　使用公式(1)重新计算 a_0^{new}, a_1^{new} 替换原来的 a_0, a_1;

10:　　计算 $C^{new} = (cert_{PU} \| sk_{PU}) \oplus H(ID_{PU}, Q, PW_{PU}^{old})$;

11:　　计算 $HPW_{PU}^{new} = H(ID_{PU}, Q, PW_{PU}^{old}, pk_{PU})$;

12:ELSE

13:　报错退出;

14:RETURN C^{new}, HPW_{PU}^{new}

4 方案分析

4.1 正确性分析

本节对所提方案进行正确性分析.

(1)解签密的正确性

$$\begin{aligned} V_1' &= (x_1', y_1') \\ &= S_1' \cdot G + t \cdot pk_{PU} \\ &= S_1' \cdot G + R_1 \cdot pk_{PU} + S_1 \cdot pk_{PU} \\ &= S_1' G(1 + sk_{PU}) + R_1' \cdot pk_{PU} \\ &= (v_1' - R_1') \cdot G + R_1' \cdot pk_{PU} \\ &= v_1' G \end{aligned} \tag{3}$$

$(x'_{GN}, y'_{GN}) = V_1' \cdot G$,同理可得 $(x'_{D_i}, y'_{D_i}) = V_1' \cdot G$.

(2)验证的正确性

易算得:$e_1' = H(x'_{GN}, TS'_{PU}, Z_{PU}, cert'_{PU}, ID_{D_i}, v_3, y'_{GN})$,则有 $R_1 = e_1' + x_1'$,同理可得 $R_2 = e_2' + x_2'$.

4.2 形式化安全性分析

本文在Abdalla M等[20]提出的ROR模型下,证明本文提出的TCSAC-IOT方案满足语义安全,且具有CK安全.

ROR模型由以下几个部分组成.

(1)协议参与者:PU、GN和 D_i,实例表示为 $\Pi_{PU}^{j_1}, \Pi_{PU}^{j_2}, \Pi_{PU}^{j_3}$.

(2)接收状态:如果一个实例 Π^j 在接收到最后一个授权协议消息后切换到接收状态,则该实例处于接收状态. 如果按顺序排列所有已发送和已接收的消息,则创建 Π^j 当前的会话的会话标识sid.

(3)匹配会话:若存在任意的两个实例 Π^{j_1} 和 Π^{j_2},满足以下三个条件,则称这两个实例为对彼此也叫做匹配会话:Π^{j_1} 和 Π^{j_2} 处于接收状态;Π^{j_1} 和 Π^{j_2} 有相同的会话标识sid并且他们将会相互认证;Π^{j_1} 和 Π^{j_2} 是彼此共同的伙伴.

(4)时效性:如果在表2中 Π^j 查询的帮助下,攻击者 $\mathcal{A}$ 不知道生成的 U 和 S_i 的会话密钥 SK_{US_i},则称 Π^{j_1} 或 Π^{j_2} 满足时效性.

在ROR模型中,敌手 $\mathcal{A}$ 可以对表2中定义的内容进行大量的查询,模拟真实攻击. 除此之外,定义了抗碰撞加密单向哈希函数 $H(\cdot)$ 表示随机谕言机,所有通信参与者包括敌手 $\mathcal{A}$ 都可访问随机谕言机.

表2　系统参数

查询操作	描述
$Send(\Pi^j, Msg)$	允许敌手 $\mathcal{A}$ 发送一个消息Msg给 Π^j,且 Π^j 收到消息Msg的回应
$Excute(\Pi_{PU}^{j_1}, \Pi_{GN}^{j_2}, \Pi_{D_i}^{j_3})$	允许敌手 $\mathcal{A}$ 拦截PU、GN和 D_i 之间通信的消息
$CorruptDevices(\Pi_U^{j_1})$	允许敌手 $\mathcal{A}$ 从丢失或偷到的智能设备提取 W_{PU}
$Reveal(\Pi^j)$	敌手 $\mathcal{A}$ 可通该查询获得 Π^j 和相应的会话密钥会话密钥
$Test(\Pi^j)$	该查询允许敌手 $\mathcal{A}$ 和揭示 Π^j 的会话密钥

定理1　若存在一个PPT敌手 $\mathcal{A}$ 可以攻破TCSAC-IoT方案,获得PU和 D_i 之间的会话密钥SK,则敌手 $\mathcal{A}$ 为解决ECDDHP问题的优势为:$Adv_{\mathcal{A}}^{HSUAC-IoT}(pt)$,具体等式如下所示:

$$\begin{aligned} Adv_{\mathcal{A}}^{HSUAC\text{-}IoT}(pt) \leqslant & \frac{q_h^2}{|Hash|} + 2(\max\{C' \cdot q_s^{s'}, \frac{q_s}{2^{l_b - 1}}\} \\ & + Adv_{\mathcal{A}}^{ECDDHP}(pt)) \end{aligned} \tag{4}$$

其中 q_h 表示进行哈希查询的次数,q_s 表示send查询的次数,$|Hash|$ 表示 $H(\cdot)$ 的输出空间,l_b 表示生物识别特征 γ_i 的长度,C' 和 s' 是Zipf's的参数,是通过线性回归计算的密码集常数[21].

证明　定理1的证明过程与文献[22]AKE协议中的证明过程相似,不同的是,本文设计的TCSAC-IoT方案口令是由用户进行设置,不服从均匀分布. 用户在设置口令时,会从口令字典中随机选取词组进行组合,此时的口令受限于口令字典,无法充分利用字符的有效空间,口令密钥字典只占用了字符空间的一小部分. 因此本文在证明的过程中还用到了Zipf's定律[21],在文献[16]的证明过程也曾用到.

定义敌手 $\mathcal{A}$ 的四个游戏,表示为

$G_j^{\mathcal{A}}$, $j=0,\ 1,\ 2,\ 3$,如下所示. 令 $\mathrm{Succ}_{G_j}^{\mathcal{A}}$ 表示为 $\mathcal{A}$ 在游戏 $G_j^{\mathcal{A}}$ 成功猜中随机比特 c 的事件,则 $\mathcal{A}$ 在 TCSAC-IoT 方案中,赢得游戏 $G_j^{\mathcal{A}}$ 优势为:

$$\mathrm{Adv}_{\mathcal{A},G_j}^{\mathrm{HSUAC\text{-}IoT}}=\Pr[\mathrm{Succ}_{G_j}^{\mathcal{A}}] \tag{5}$$

游戏 $G_0^{\mathcal{A}}$:该游戏表示敌手 $\mathcal{A}$ 在 ROR 模型下,对 TCSAC-IoT 方案的真实攻击,由于 c 是游戏 $G_0^{\mathcal{A}}$ 开始之前随机选取的,因此 TCSAC-IoT 满足语义安全:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{HSUAC\text{-}IoT}}(\mathrm{pt})=|2\mathrm{Adv}_{\mathcal{A},G_0}^{\mathrm{HSUAC\text{-}IoT}}-1| \tag{6}$$

游戏 $G_1^{\mathcal{A}}$:该游戏表示敌手 $\mathcal{A}$ 可以在使用表 2 中 Excute 查询的帮助下进行窃听攻击,敌手 $\mathcal{A}$ 执行 $\mathrm{Excute}(\Pi_{\mathrm{PU}}^{j_1},\Pi_{\mathrm{GN}}^{j_2},\Pi_{\mathrm{D}_i}^{j_3})$ 查询,可以在访问控制和密钥协商阶段劫持所有参与者的通信信息 $\sigma_1=<C,R_1,R_2,S_1,S_2,\mathrm{TS}_{\mathrm{PU}}>$、$\sigma_2=<\mathrm{TS}_{\mathrm{GN}},L>$、$\sigma_3=<\mathrm{VSK},\mathrm{TS}_{\mathrm{D}_i}>$. 在游戏结束后,敌手 $\mathcal{A}$ 执行 Reveal 和 Test 查询验证得到会话密钥 SK′是真实的还是随机的,验证 $\mathrm{SK}'=H(x_{\mathrm{D}_i},H(e_1,\mathrm{TS}_{\mathrm{PU}}),y_{\mathrm{D}_i})=H(x'_{\mathrm{D}_i},H(e_1,\mathrm{TS}_{\mathrm{PU}}),y'_{\mathrm{D}_i})=\mathrm{SK}$ 是否成立. 很明显通过 σ_1、σ_2 和 σ_3 不能够提高成功计算会话密钥 $\mathrm{SK}'(=\mathrm{SK})$ 的概率. 由于 $G_0^{\mathcal{A}}$ 和 $G_1^{\mathcal{A}}$ 是不可区分的,因此有:

$$\mathrm{Adv}_{\mathcal{A},G_1}^{\mathrm{HSUAC\text{-}IoT}}=\mathrm{Adv}_{\mathcal{A},G_0}^{\mathrm{HSUAC\text{-}IoT}} \tag{7}$$

游戏 $G_2^{\mathcal{A}}$:该游戏模拟 Send 和 |Hash| 查询进行主动攻击. 在 TCSAC-IoT 的设计过程使用的是单向的抗碰撞哈希函数、椭圆曲线的基点和大量的随机数,因此敌手 $\mathcal{A}$ 窃听到的在 PU、GN 和 D_i 中的 σ_1、σ_2 和 σ_3 消息不会产生哈希碰撞. 因此敌手 $\mathcal{A}$ 要从 $R_i(i=1,2)$ 计算出 $e_i(i=1,2)$,则需要解决 ECDLP 问题,或从 $S_i(i=1,2)$ 计算出 $e_i(i=1,2)$. 很明显,除了包含 Send 和 |Hash| 查询,以及解决 ECDDHP 问题之外,$G_2^{\mathcal{A}}$ 和 $G_2^{\mathcal{A}}$ 是不可区分的. 生日悖论结果和解决 ECDDHP 优势如下:

$$\left|\mathrm{Adv}_{\mathcal{A},G_1}^{\mathrm{HSUAC\text{-}IoT}}-\mathrm{Adv}_{\mathcal{A},G_2}^{\mathrm{HSUAC\text{-}IoT}}\right|\leqslant\frac{q_{\mathrm{h}}^2}{2|\mathrm{Hash}|}+\mathrm{Adv}_{\mathcal{A}}^{\mathrm{ECDDHP}}(\mathrm{pt}) \tag{8}$$

游戏 $G_3^{\mathcal{A}}$:在该游戏中,敌手 $\mathcal{A}$ 执行表 3 中的 CorruptDevice 查询获得设备中秘密凭证,如 $E_q(a,b)$、$H(\cdot)$、G、x_{PU}^*、$\mathrm{cert}_{\mathrm{PU}}^*$ 等. 为了获得 PKI 用户的密钥,敌手需要同时猜中口令 $\mathrm{PW}_{\mathrm{PU}}$ 和生物密钥 $\sigma_{\mathrm{PU}}^i(i=1$或$2)$. 敌手 $\mathcal{A}$ 可以根据 Zipf's 定律来猜测用户选择的密码[21],在拖网猜测攻击时,并且在 $q_{\mathrm{s}}=10^7$ 或 $q_{\mathrm{s}}=10^8$ 的情况下,敌手 $\mathcal{A}$ 的优势为 1/2[21];在目标猜测攻击时,敌手 $\mathcal{A}$ 可以利用目标的个人信息,当 $q_{\mathrm{s}}\leqslant10^6$,敌手 $\mathcal{A}$ 的优势将超过 1/2[21]. 通常在系统中,会限制输入错误密码的次数,但是允许发送 q_{s} 次的 send 查询. 因此若忽略敌手 $\mathcal{A}$ 对用户 PU 的口令和生物密钥的猜测攻击,则游戏 $G_2^{\mathcal{A}}$ 和 $G_3^{\mathcal{A}}$ 是不可区分的,则有如下关系:

$$|\mathrm{Adv}_{\mathcal{A},G_2}^{\mathrm{TCSAC\text{-}IoT}}-\mathrm{Adv}_{\mathcal{A},G_3}^{\mathrm{TCSAC\text{-}IoT}}|\leqslant\max\{C'\cdot q_{\mathrm{s}}^{s'},\frac{q_{\mathrm{s}}}{2^{l_{\mathrm{b}}-1}}\} \tag{9}$$

敌手 $\mathcal{A}$ 做完所有查询之后,只有猜对比特 c 才能赢得游戏 $G_3^{\mathcal{A}}$,则敌手 $\mathcal{A}$ 的优势如下:

$$\mathrm{Adv}_{\mathcal{A},G_3}^{\mathrm{TCSAC\text{-}IoT}}=\frac{1}{2} \tag{10}$$

由式(6)、(9)、(10)联立得到如下关系:

$$\begin{aligned}\frac{1}{2}\cdot\mathrm{Adv}_{\mathcal{A}}^{\mathrm{TCSAC\text{-}IoT}}(\mathrm{pt}) &=|\mathrm{Adv}_{\mathcal{A},G_0}^{\mathrm{TCSAC\text{-}IoT}}-\frac{1}{2}|\\ &=|\mathrm{Adv}_{\mathcal{A},G_1}^{\mathrm{TCSAC\text{-}IoT}}-\frac{1}{2}|\\ &=|\mathrm{Adv}_{\mathcal{A},G_1}^{\mathrm{TCSAC\text{-}IoT}}-\mathrm{Adv}_{\mathcal{A},G_3}^{\mathrm{TCSAC\text{-}IoT}}|\end{aligned} \tag{11}$$

由式(6)、式(8)和式(9)联立,推导得到如下等式:

$$\begin{aligned}&\frac{1}{2}\cdot\mathrm{Adv}_{\mathcal{A}}^{\mathrm{TCSAC\text{-}IoT}}(pt)\\ &=|\mathrm{Adv}_{\mathcal{A},G_0}^{\mathrm{TCSAC\text{-}IoT}}-\mathrm{Adv}_{\mathcal{A},G_3}^{\mathrm{TCSAC\text{-}IoT}}|\\ &\leqslant\left|\mathrm{Adv}_{\mathcal{A},G_1}^{\mathrm{TCSAC\text{-}IoT}}-\mathrm{Adv}_{\mathcal{A},G_2}^{\mathrm{TCSAC\text{-}IoT}}\right|\\ &\quad+\left|\mathrm{Adv}_{\mathcal{A},G_2}^{\mathrm{TCSAC\text{-}IoT}}-\mathrm{Adv}_{\mathcal{A},G_3}^{\mathrm{TCSAC\text{-}IoT}}\right|\\ &\leqslant\frac{q_{\mathrm{h}}^2}{2|\mathrm{Hash}|}+\mathrm{Adv}_{\mathcal{A}}^{\mathrm{ECDDHP}}(\mathrm{pt})+\max\{\mathrm{C}'\cdot q_{\mathrm{s}}^{s'},\frac{q_{\mathrm{s}}}{2^{l_{\mathrm{b}}-1}}\}\end{aligned} \tag{12}$$

随后化简式(12),两边乘以 2 得到如下等式:

$$\begin{aligned}\mathrm{Adv}_{\mathcal{A}}^{\mathrm{TCSAC\text{-}IoT}}(\mathrm{pt})\leqslant\frac{q_h^2}{|\mathrm{Hash}|}+2\Bigg(&\mathrm{Adv}_{\mathcal{A}}^{\mathrm{ECDDHP}}(\mathrm{pt})\\ &+\max\left\{C'\cdot q_{\mathrm{s}}^{s'},\frac{q_{\mathrm{s}}}{2^{l_{\mathrm{b}}-1}}\right\}\Bigg)\end{aligned} \tag{13}$$

4.3 非形式化安全分析

如表 3 所示,TCSAC-IOT 具有伪装攻击、抗重放攻击、抗中间人攻击、抗内部特权攻击和抗盗 PKI 用户智能设备攻击等安全特性.

(1)伪装攻击:伪装攻击是在物联网环境敌手常用的一种攻击方式,在本文中是一个三方环境下的访问控制方案,敌手 $\mathcal{A}$ 可以伪装的对象为 PKI 用户、网关 GN 和物联网设备.

PKI 用户伪装攻击:敌手 $\mathcal{A}$ 伪装成合法的 PKI 用户向 GN 发送经授权的消息,然而 $\mathcal{A}$ 没有 PKI 用户的私钥 $\mathrm{sk}_{\mathrm{PU}}$,不能够计算出合法 C、S_1 和 S_2,因此该方案可以抵抗 PKI 用户伪装攻击.

GN 伪装攻击:敌手 $\mathcal{A}$ 伪装成 GN,虽然 $\mathcal{A}$ 可以劫持消息 σ_1,但是由于没有 GN 的私钥 $\mathrm{sk}_{\mathrm{GN}}$,$\mathcal{A}$ 不能解密消息 σ_1,同时 $\mathcal{A}$ 没有 k_i,也不能伪造一个新的消息 σ_2,因此可以抵抗 GN 攻击.

物联网设备伪造攻击:敌手 $\mathcal{A}$ 伪装成物联网设备,

虽然$\mathcal{A}$可以劫持σ_2,但是没有物联网设备的私钥sk_{D_i},$\mathcal{A}$要获得x_G和y_G,则要解决ECDLP问题,这在计算上是不可行的. 因此可以抗物联网设备伪造攻击.

(2)重放攻击:在消息σ_1、σ_2和σ_3都应用了时间戳来防止重放攻击,敌手无法实现重放攻击.

(3)中间人攻击:敌手$\mathcal{A}$伪造消息σ_1,由于没有PKI用户的私钥sk_{PU},$\mathcal{A}$不能伪造出合法的S_1和S2,同样$\mathcal{A}$也无法伪造出σ_2和σ_3. 因此该方案是可防止中间人攻击的.

(4)内部特权攻击:特权攻击指在注册阶段CA和KGC可以访问物联网设备注册请求信息,在PKI用户注册阶段,CA不知道用户的私钥,因此无法伪造一个合法的消息σ_1. 在CLC物联网设备和网关GN注册时,KGC只知道部分私钥,而不知道完整的私钥,因此也不能对σ_1进行解密,伪造消息σ_2和σ_3.

(5)盗用或丢失PKI用户智能设备攻击:对于一个合法授权的PKI用户智能设备被敌手$\mathcal{A}$盗用和丢失的情况,$\mathcal{A}$知道存储在系统上的参数. 但是由于$\mathcal{A}$在猜测用户口令和PKI用户的ID上困难的,根据加密哈希函数的性质的,敌手$\mathcal{A}$伪造一个HPW_{PU}^{*}是不可能的. 综上,该方案在PKI用户智能设备被盗用的情况下仍然没有泄露敏感的信息,因此是可以抵抗盗用户智能设备攻击的.

表3　功能和安全性

功能和安全性	TCSAC-IoT	Mandal S et al.[16]	Tao at al.[24]
伪装攻击	√	√	×
重放攻击	√	√	×
中间人攻击	√	√	×
内部特权攻击	√	√	×
盗PKI用户智能设备攻击	√	√	×
无密钥托管	√	√	×
无双线性运算	√	√	×
跨域	√	×	√

4.4　性能分析

根据文献[15~17]中的方法,Dell电脑、Inter(R) Core(TM) i5-4460S@ 2.90 GHz处理器、4 GB主内存和WIN8操作系统作为CA和KGC的运行环境,三星手机S5、四核2.45 GB处理器、2 GB内存、谷歌安卓4.42操作系统作为物联网环境下PKI加密体制的用户智能设备、CLC加密体制的物联网设备和网关GN,通过以上方法模拟在物联网三方环境下跨安全域的PKI加密体制的物联网用户对CLC加密体制的物联网设备跨域访问控制,具体的实验过程如下:

依据文献[16,17]中的实验过程,为了在同等条件下便于比较,本文采用相同的实验方案,可分为两个部分,分别为对通信开销的评估实验过程和计算开销的实验过程. 在评估TCSAC-IOT通信开销时,假设身份ID、随机数、时间戳、哈希函数和椭圆曲线上的点(x,y)分别需要160 bits、160 bits、32 bits、160 bits和(160+160)=320 bits,主要考虑PKI用户和CLC用户在登录访问控制阶段中的通信开销,其中,在登录访问控制阶段中共发送三条消息,分别为$\sigma_1=<C,R_1,R_2,S_1,S_2,TS_{PU}>$,$\sigma_2=<TS_{GN},L>$和$\sigma_3=<VSK,TS_{D_i}>$,分别需要(480+160+160+160+32)=992 bits、(32+320)=352 bits和(160+32)=192 bits,因此在整个登录访问控制阶段中的通信开销合计为1 536 bits,. 在评估TCSAC-IOT的计算开销时,根据Wu等人[23]的方法,通过1 000次实验得到椭圆曲线点乘、点加、模幂、双线性对运算操作的平均时间分别为T_{ecm}=13.405 ms、T_{eca}=0.081 ms、T_{me}=2.249 ms、T_{bp}=32.731 ms,根据Mandal等人[16]的方法,得到执行哈希函数、模糊提取函数和对称加解密的时间分别为$T_h\approx0.056$ ms、$T_{fe}\approx13.405$ ms和$T_{senc}/T_{sdec}\approx0.056$ ms. 得到如表4所示的通信开销和计算开销表.

通过表3中的数据可知,TCSAC-IoT的通信开销为1 536 bits,与Mandal等人[16]的方案相比,通信开销降低了51%,与Tao等人[24]的方案相比,通信开销降低了31.4%,并且与之相比有着较小的通信次数. 在计算开销上,TCSAC-IoT的计算开销为176.64 ms,与Mandal等人[16]的方案相比,计算开销降低了15%,与Tao等人[24]的方案相

表4　通信开销和计算开销

协议	通信次数	通信开销/bits	计算开销	时间/ms
TCSAC-IOT	3	1 536	$20T_h+12T_{ecm}+12T_{eca}+T_{fe}+2T_{enc}+3T_{sdec}$	176.64
Mandal S et al.[16]	3	3 136	$T_{fe}+14T_{ecm}+8T_{eca}+28T_h$	203.29
Tao et al.[24]	4	2 240	$18T_h+13T_{ecm}+4T_{eca}+13T_{bp}+4T_{senc}+4T_{sdec}$	601.31

比,计算开销降低了70%,因此TCSAC-IoT在通信开销和计算开销上与文献[16,23]相比有着较低的通信和计算开销. 根据表2从安全性和功能上对比可知,TCSAC-IoT具有抗伪装攻击、重放攻击、中间人攻击、内部特权攻击和盗用或丢失PKI用户智能设备攻击,同时具有无密钥托管、无双性运算和跨域等性质. 因此TCSAC-IoT在提高系统通信和计算效率的同时,仍然具备有相同及以上的安全性,在安全性和效率上达到了一个很好的权衡.

5 结论

本文针对5G技术在物联网中的应用场景形成的mMTC中的跨安全的物联网PKI用户对CLC物联网设备安全通信问题,在考虑了物联网安全模型的DY模型和CK模型下,设计基于GB/T 32918.4-2016 SM2加密算法和GB/T 32918.2-2016 SM2签名算法的三因子跨域签密访问控制方案. 该方案为面向mMTC物联网环境中跨安全域的物联网PKI用户和CLC物联网设备安全跨域访问提供了安全可用的访问控制方案,可有效解决mMTC中由于密钥托管而带来的安全问题,拓展了在mMTC物联网中的应用场景,并结合了用户口令、生物特征和用户物联设备组成三因子认证方案,从多个方面对用户的身份进行认证,可以抵抗由于用户智能设备被盗或丢失和用户口令被字典猜测攻击成功猜中用户口令而带来的安全隐患,提高访问控制方案授权部分的可信度;在方案的构造上,基于ECDLP和ECDDH困难问题进行构造,由于没有采用双线性运算,减轻了物联网设备的计算开销,拓宽了在物理资源受限的网联网设备中的应用;最后对本文提出的方案进行了正确性分析、在ROR模型下进行了形式化的安全性分析和非形式化的安全性分析,与类似的方案对比,本文提出的方案具有跨域、抗伪装攻击、抗重放攻击、抗中间人攻击、抗内部特权攻击和抗盗用或丢失PKI用户智能设备攻击的优势,同时与Mandal等人[16]和Tao等人[24]的方案相比,具有着较低的计算开销和通信开销. 本文提出的方案主要面对的是跨安全域,虽然可以跨不同的加密体制来实现安全可靠的访问控制,避免非法的PKI物联网用户对CLC物联网设备资源的非法访问,但是在面临跨安全域且系统加密参数不同的情况下,本文提出的方案仍然具有一定的局限性,为跨安全域且系统加密参数不同的mMTC环境提供一个具有跨域且满足内部安全的访问控制方案,将是未来研究工作的一个重点.

参考文献

[1] CHEN X M, NG D W K, YU W, et al. Massive access for 5G and beyond[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(3): 615-637.

[2] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption)[C]//CRYPTO'97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 1997: 165-179.

[3] CAO J, MA M D, LI H, et al. A survey on security aspects for 3GPP 5G networks[J]. IEEE Communications Surveys & Tutorials, 2020, 22(1): 170-195.

[4] SUN Y X, LI H. Efficient signcryption between TPKC and IDPKC and its multi-receiver construction[J]. Science China Information Sciences, 2010, 53(3): 557-566.

[5] AN J H, DODIS Y, RABIN T. On the security of joint signature and encryption[C]//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Berlin: Springer, 2002: 83-107.

[6] LI F G, XIONG P. Practical secure communication for integrating wireless sensor networks into the Internet of Things[J]. IEEE Sensors Journal, 2013, 13(10): 3677-3684.

[7] LI F G, ZHENG Z H, JIN C H. Secure and efficient data transmission in the Internet of Things[J]. Telecommunication Systems, 2016, 62(1): 111-122.

[8] RAVEENDRANATH S, ANEESH A. Efficient multi-receiver heterogenous signcryption[C]//2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). Piscataway: IEEE, 2016: 1693-1697.

[9] NIU S F, LI Z B, WANG C F. Privacy-preserving multi-party aggregate signcryption for heterogeneous systems [C]//International Conference on Cloud Computing and Security. Cham: Springer, 2017: 216-229.

[10] TING P Y, TSAI J L, WU T S. Signcryption method suitable for low-power IoT devices in a wireless sensor network[J]. IEEE Systems Journal, 2018, 12(3): 2385-2394.

[11] LI F G, HAN Y N, JIN C H. Practical access control for sensor networks in the context of the Internet of Things [J]. Computer Communications, 2016, 89/90: 154-164.

[12] LI S J, TAO F S, SHI T. Security analysis and improvement of hybrid signcryption scheme based on heterogeneous system[C]//2019 14th International Conference on Computer Science & Education (ICCSE). Piscataway: IEEE, 2019: 840-845.

[13] 牛淑芬, 杨喜艳, 王彩芬, 等. 基于异构密码系统的混合群组签密方案[J]. 电子与信息学报, 2019, 41(5): 1180-1186.
NIU S F, YANG X Y, WANG C F, et al. Hybrid group

signcryption scheme based on heterogeneous cryptosystem[J]. Journal of Electronics & Information Technology, 2019, 41(5): 1180-1186. (in Chinese)

[14] SAEED M E S, LIU Q Y, TIAN G Y, et al. HOOSC: Heterogeneous online/offline signcryption for the Internet of Things[J].Wireless Networks, 2018, 24(8): 3141-3160.

[15] LUO M, WEN Y L, HU X T. Practical data transmission scheme for wireless sensor networks in heterogeneous IoT environment[J]. Wireless Personal Communications, 2019, 109(1): 505-519.

[16] MANDAL S, BERA B, SUTRALA A K, et al. Certificateless-signcryption-based three-factor user access control scheme for IoT environment[J]. IEEE Internet of Things Journal, 2020, 7(4): 3184-3197.

[17] MALANI S, SRINIVAS J, DAS A K, et al. Certificate-based anonymous device access control scheme for IoT environment[J]. IEEE Internet of Things Journal, 2019, 6 (6): 9762-9773.

[18] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[19] CANETTI R, KRAWCZYK H. Universally composable notions of key exchange and secure channels[C]//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Berlin: Springer, 2002: 337-351.

[20] ABDALLA M, FOUQUE P A, POINTCHEVAL D. Password-based authenticated key exchange in the three-party setting[C]//International Workshop on Public Key Cryptography. Berlin: Springer, 2005: 65-84.

[21] WANG D, CHENG H B, WANG P, et al. Zipf's law in passwords[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2776-2791.

[22] Srinivas J, Das A K, Kumar N, et al. TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment[J]. IEEE Transactions on Vehicular Technology, 2019, 68(7): 6903-6916.

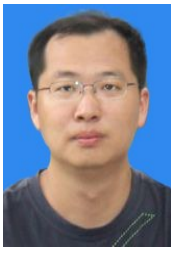
[23] WU L B, WANG J, CHOO K K R, et al. Secure key agreement and key protection for mobile device user authentication[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(2): 319-330.

[24] TAO F S, SHI T, LI S J. Provably secure cross-domain authentication key agreement protocol based on heterogeneous signcryption scheme[C]//2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference. Piscataway: IEEE, 2020: 2261-2266.

作者简介

黄隆坤　男,1995年2月出生于贵州省黔西南布依族苗族自治州望谟县. 现为贵州大学计算机科学与技术学院硕士. 主要研究方向为密码学与数据安全、物联网安全.
E-mail: longkunhuang@163.com

田有亮(通讯作者)　男,1982年11月出生于贵州省盘县. 现为贵州大学教授、博士生导师. 主要研究方向为算法博弈论、密码学与安全协议、大数据安全与隐私保护、区块链与电子货币. 中国电子学会会员编号:E190029411M.
E-mail: youliangtian@163.com



谢洪涛　男,1983年11月出生. 现为中国科学技术大学特任教授、博士生导师. 主要从事多媒体内容安全和医学影像智能分析的研究. 中国电子学会会员编号:E190029114M.
E-mail: htxie@ustc.edu.cn