计算机科学
COMPUTER SCIENCE

基于密码学累加器的电力物联网设备接入管理

陈彬，徐欢，奚建飞，雷美炼，张锐，秦诗涵

引用本文

陈彬，徐欢，奚建飞，雷美炼，张锐，秦诗涵基于密码学累加器的电力物联网设备接入管理[J]．计算机科学, 2022, 49(11A): 210900218-6.

CHEN Bin, XU Huan, XI Jian-fei, LEI Mei-lian, ZHANG Rui, QIN Shi-han. Power Internet of Things Device Access Management Based on Cryptographic Accumulator [J]. Computer Science, 2022, 49(11A): 210900218-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210900218

基于密码学累加器的电力物联网设备接入管理

陈 彬[1] 徐 欢[1] 奚建飞[2] 雷美炼[2] 张 锐[3] 秦诗涵[3]
1 中国南方电网有限责任公司 广州 510663
2 南方电网数字电网研究院 广州 510663
3 中国科学院信息工程研究所 北京 100093
(chenbin@csg.cn)

摘 要 设备安全接入是电力物联网安全防护的第一道防线,是实现访问控制、入侵检测等安全机制的前提。完备的设备接入管理涵盖设备的可信认证和安全撤销两个关键环节,现行系统大多依赖PKI来建立可信基础设施,通过公钥证书的颁发、验证及撤销实现接入管理。然而,在电力物联网场景下,该方案为数量众多、资源受限的设备带来了额外的开销负担和效率问题,随之提出的轻量级认证方案实现了开销及效率的优化,但在功能上存在不足,无法实现安全撤销这一关键环节。针对以上不足,基于密码学累加器及布隆过滤器提出了一种电力物联网设备接入管理方案,同时实现了设备的可信认证及安全撤销,并有效地兼顾功能和效率。通过安全性分析,本方案实现了设备对网关的匿名认证、身份凭证的不可伪造性以及强制撤销安全性。实验结果表明,与主流的基于PKI的设备接入管理方案相比,本方案在设备身份验证及凭证撤销环节大大降低了通信开销和存储开销,在电力物联网场景下具备更高的实用性。

关键词:密码学累加器;电力物联网;接入认证;安全撤销;匿名
中图法分类号 TP309

Power Internet of Things Device Access Management Based on Cryptographic Accumulator

CHEN Bin[1],XU Huan[1],XI Jian-fei[2],LEI Mei-lian[2],ZHANG Rui[3] and QIN Shi-han[3]
1 China Southern Power Grid,Guangzhou 510663,China
2 China Southern Power Grid Digital Power Grid Research Institute,Guangzhou 510663,China
3 Institute of Information Engineering,Chinese Academy of Sciences,Beijing 100093,China

Abstract Device access is the first line of defense for the security protection of the power Internet of Things,and it is the premise for realizing security mechanisms such as access control and intrusion detection. Complete device access management covers two key links:trusted authentication and secure revocation. Most existing systems rely on PKI to establish trusted infrastructure,and realize access management through the issuance,verification and revocation of public key certificates. However,in the scenario of power Internet of Things,this scheme brings extra overhead burden and efficiency problems to a large number of devices with limited resources. The lightweight authentication scheme has realized the optimization of overhead and efficiency,but it is not functional enough to realize the key link of safe revocation. In view of the above shortcomings,this paper proposes an access management scheme for power Internet of Things devices based on cryptography accumulator and Bloom filter,which simultaneously realizes trusted authentication and security revocation of devices,and effectively considers both functions and efficiency. Through security analysis,this scheme realizes anonymous authentication of gateway,unforgeability of identity certificate and security of forced revocation. Experimental results show that,compared with the mainstream PKI-based device access management scheme,this scheme greatly reduces the communication overhead and storage overhead in the process of device authentication and revocation,and has higher practicability in the power Internet of Things scene.

Keywords Cryptographic accumulator,Power Internet of things,Access authentication,Secure revocation,Anonymous

1 概述

随着我国能源和电力需求的不断增长,电力系统的安全稳定运行及数据应用服务面临着新的挑战[1]。物联网凭借先进的现代信息技术和通信技术,与电力系统的上述需求高度契合。电力物联网将电力系统的用户、电网及发电企业连接在一起[2],并通过泛在感知技术大幅提高了电力系统的灵活感知、实时通信、智能控制等能力[2],推进了智能电网的升级。

电力物联网典型架构主要包括物联网设备(如智能电表)、通信模块(如4G、LTE)、控制中心。物联网设备定期监测电量消耗和电能稳定性,通过网关认证后,将采集到的数据依赖通信模块传输至相应的控制中心,控制中心向用户或

基金项目:国家自然科学基金(61772520,61802392,61972094)
This work was supported by the National Natural Science Foundation of China(61772520,61802392,61972094).
通信作者:秦诗涵(qinshihan@iie.ac.cn)

公共设施提供电力资源和服务，并根据从智能设备传输的记录信息进行收费[3]。

电力物联网赋能电力系统智能化升级的同时，也面临着一定的安全风险和技术挑战。国内外电力物联网面临的恶意攻击及安全隐患日益严重，特别是在终端设备层面，由于其数量多、分布广，且计算、存储、通信资源受限，通常面临安全防护能力不足、安全管控薄弱等问题，通过攻击智能设备来降低电费、恶意切断用户用电的行为层出不穷。电力物联网设备层面潜在的威胁远不止于此，随着电力大数据分析技术的发展，设备身份信息的泄露也严重威胁着用户的隐私安全，使攻击者能够窃取用户的习惯和行为[4]。因此，如何实现电力物联网设备的接入安全管理具有十分重要的研究价值。

1.1 问题描述及现有工作

电力物联网设备的接入管理应涵盖可信设备的认证管理以及不可信设备的撤销管理。一方面，身份认证作为安全防护的第一道防线，是设备接入物联网管理平台进行数据安全传输的前提条件；另一方面，已经注册过的物联网设备有可能遭遇黑客入侵变成恶意设备，即使采取强制隔离措施，攻击者仍可以将获取到的设备密钥加载至其他载体上进行攻击，因此必须采取安全的撤销管理措施。

1.1.1 可信设备安全认证

目前电力物联网设备的认证可分为：1）基于公钥基础设施（Public Key Infrastructure，PKI）[5]的认证方案，设备的公钥存储在证书中，通过证书进行身份认证，由证书授权中心（Certificate Authority，CA）统一进行证书的生成、分发、更新以及撤销；2）基于标识密码体制（Identity-based Cryptography，IBC）[6]的认证方案，将设备的身份标识作为其公钥，由密钥生成中心（Key Generation Center，KGC）为其生成部分私钥[7]；3）基于默克尔树[8]、哈希消息认证码[9]、Diffie-Hellman 密码体制[10]、椭圆曲线加密[11]等实现的轻量级认证方案。

其中，基于 PKI 的身份认证方式需要依赖 CA，且需要为每一个终端生成一个证书[12]。一方面，由于设备的资源受限且证书的解析太过复杂，基于证书的认证机制并不适用[13]；另一方面，电力物联网设备数量庞大，证书的分发、更新、撤销使得其认证管理成为负担[13]。基于标识的认证方案虽然具有密钥分配独立、算术运算量小等优点，但身份标识作为公钥会泄露设备隐私信息，也存在易受身份欺骗被攻击的缺点[14]。轻量级认证相比于前两种认证方式要求更低的存储成本、更高效的算法及尽量精简的通信过程，更符合存储、计算、通信资源有限的电力物联网设备的认证需求。此外，在轻量级认证的同时如何隐藏设备的身份实现隐私保护也是研究的热点[14]。因此，利用轻量级算法实现兼顾隐私保护的电力物联网设备轻量级认证成为亟需解决的问题之一。

1.1.2 不可信设备撤销管理

与可信设备的安全认证密不可分的是不可信设备的安全撤销。在基于 PKI 的认证方案中，不可信设备的认证撤销是由 CA 撤销其证书并通过证书撤销列表（Certificate Revocation List，CRL）[15]来实现。一方面，由于电力物联网设备数量巨大，其证书有效期可以是终生的，造成 CRL 文件较大，而且需要经常更新、分发；另一方面，电力物联网设备的存储、通信、计算资源有限，给 PKI 体系下的认证撤销管理带来了很大的负担[16]。然而，其他不基于 PKI 的认证方案往往忽视了安全撤销这一重要要求，并未从密钥管理层面实现不可信设备的强制性安全撤销。因此，在减小电力物联网设备各项开销的同时实现其安全撤销是亟需解决的另一个问题。

综上所述，现有工作中同时实现安全认证和安全撤销的方案未实现轻量级，而现有轻量级认证方案需要依赖强制隔离等措施实现设备的撤销，无法基于方案本身实现安全撤销。同时，设备的身份隐私保护也应是方案设计的重点。

1.2 本文的贡献

面对上述挑战，本文综合考虑安全认证和撤销两个方面，设计了轻量级的电力物联网设备接入管理方案。采用布隆过滤器技术及密码学累加器技术对设备进行可信身份凭证的颁发、认证及撤销。依赖布隆过滤器的时空高效性，实现设备的快速检索；依赖密码学累加器凭证不可伪造的安全性，实现可信设备的安全接入和不可信设备的安全撤销；依赖累加器的数据结构实现认证和撤销的方式，管理平台仅需维护和分发一个短的累加器值和凭证，既可以有效防范单点失效，又大大降低了存储和通信开销。为进一步降低计算开销，本文采用了设备分区域管理的方式。同时，本方案兼顾隐私保护的需求，实现了设备对认证网关的匿名性。

2 预备知识

2.1 布隆过滤器（Bloom Filter）

布隆过滤器[17]是由 Bloom 于 1970 年提出，它能够快速检索元素是否在一个数据集，并且节约了存储空间。对特定字符串建立布隆过滤器通常包含以下 3 种算法。

（1）初始化算法。该算法首先将长度为 m 的比特数组全置为 0，然后定义 l 个独立的哈希函数 $h_i:\{0,1\}^* \rightarrow \{0,1,\cdots,m-1\}$，$i=1,2,\cdots,l$，每一个哈希函数都随机地将每一个输入元素映射到比特数组中的一个位上。

（2）插入算法 $Insert(x)$。输入待插入的元素 x，计算 $h_i(x)$，$i=1,2,\cdots,l$，得到的 l 个哈希值在集合 $\{0,1,\cdots,m-1\}$ 中，对应比特数组的 l 个位置。对每一个哈希值，将比特数组相应位置置为 1。如果相应位置已经是 1，就不再处理。

（3）查询算法 $Find(x)$。输入待查询的元素 x，对 x 做同样的 l 次哈希运算。检查比特数组相应的 l 个位置的值是否全为 1，若有一位为 0，则表示该字符串一定不在这个数据集中；若全为 1，则以一定的误判率判定该字符串属于该数据集。

2.2 累加器（Accumulator）

密码学累加器最早是由 Benaloh 等[18]于 1993 年在欧密会议上提出，它能够将一个集合里的元素累加成一个短值，并且为每个元素生成一个成员证明，使得该元素通过成员证明来证明自己在这个集合中。累加器通常包含以下 4 种算法。

（1）密钥生成算法 $Gen(1^\lambda)$。输入安全参数 1^λ，该算法输出累加器的私钥 k。

（2）累加值计算算法 $Eval(k,x_1,\cdots,x_n)$。输入累加器私钥 k 及集合 L 中的 n 个元素 $x_1,\cdots,x_n$，该算法输出累加值 a 和辅助信息 aux。

（3）成员证明生成算法 $Wit(k,x_i,aux,a)$。输入累加器私钥 k、成员 x_i、辅助信息 aux 及当前累加值 a，该算法输出 x_i 的成员证明 w_i。

（4）成员验证算法 $Ver(x_i,w_i,a)$。输入成员 x_i、成员证明 w_i 及当前累加值 a，验证通过时，输出 1；否则，输出 0。

动态累加器（Dynamic Accumulator）[19]是由 Camenisch 等于 2002 年首先提出，动态累加器是在累加器的基础上，动态地增加或者删除元素，使得增加或者删除元素的代价独立于被累加的成员数。除基础累加器所包含的 4 个算法外，动态累加器还包含以下 3 种算法。

（1）成员增加算法 $Add(k,a,L,x')$。输入累加器私钥 k、当前累加值 a、当前集合 L 及新成员 x'，该算法输出新的累加值 a'、对应新的集合 $L\cup\{x'\}$、x' 的成员证明 w' 及辅助信息 aux_{Add}。

（2）成员删除算法 $Del(k,a,L,y)$。输入累加器私钥 k、当前累加值 a、当前集合 L 及待删除的成员 y，该算法输出新的累加值 a'、对应新的集合 $L/\{y\}$ 及辅助信息 aux_{Del}。

（3）成员证明更新算法 $Upd(k,x,w,a',aux_{op})$。输入累加器私钥 k、成员 x 及其待更新的成员证明 w、当前累加值 a' 及辅助信息 aux_{op}（其中 op 为 Add 或 Del），该算法输出 x 更新后的成员证明 w'。

2.3 RSA 累加器

RSA 累加器[19]基于强 RSA 假设[20]，支持成员的增加和删除，且能够实现抗碰撞的安全成员证明。RSA 累加器的具体算法过程如下：

（1）初始化及密钥生成 Gen：随机选取一个 RSA 模 $N=pq$，其中 p 和 q 为强素数，$p=2p'+1$，$q=2q'+1$，p' 和 q' 均为素数，从模 N 的二次剩余循环群中随机选取 g。私钥 k 为 (p,q)。

（2）累加值计算 $Eval$：对于素数集合 $L=\{x_1,\cdots,x_n\}$，计算其累加值 $a=g^{x_1x_2\cdots x_n} \bmod N$。

（3）成员证明生成 Wit：对于集合 L 中的成员 x_i，其成员证明 $w_i=g^{x_1\cdots x_{i-1}x_{i+1}\cdots x_n} \bmod N$。

（4）成员验证 Ver：验证成员 x_i 是否属于集合 L，计算 $w_i^{x_i}$ 是否等于当前累加值。

（5）成员增加 Add：当新增成员 x' 时，累加值更新为 $a'=a^{x'}$，x' 的成员证明即为 a，输出辅助信息 $aux_{\text{Add}}=x'$。

（6）成员删除 Del：当删除成员 y 时，累加值更新为 $a'=a^{y^{-1}\bmod(p-1)(q-1)} \bmod N$，输出辅助信息 $aux_{\text{Del}}=(y,a')$。

（7）成员证明更新 Upd：当新增成员 x' 时，成员 x_i 的证明更新为 $w_i'=w_i^{x'}$；当删除成员 y 时，成员 x_i 的证明更新过程如下：

由于 x_i 和 y 为互素的整数，由 Bezout 定理可知必存在整数 α 和 β 使得 $\alpha x_i+\beta y=1$。通过扩展的欧几里得算法计算得到 α 和 β，则成员 x_i 的证明更新为 $w_i'=w_i^{\beta}(a')^{\alpha}$。

3 系统及安全模型

3.1 系统模型

系统模型如图 1 所示，包含物联网管理平台、网关和设备。

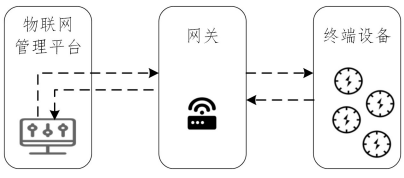

图 1　系统模型图

Fig. 1　System model diagram

物联网管理平台：物联网管理平台对设备及其采集的数据进行统一管理，负责生成设备的可信身份凭证；在发现恶意设备时，撤销其可信身份凭证。本方案中假设物联网管理平台是安全可信的，并可以在设备撤销时恢复其真实身份。

网关：网关作为设备和物联网管理平台之间通信的桥梁，需对接入的设备进行身份认证。本方案中假设网关是半诚实的，想从设备的认证信息中获取其隐私。

设备：设备在出厂前完成注册，并预置匿名身份标识 ID^* 及可信身份凭证 w。设备对网关匿名，通过网关认证后，可与物联网管理平台进行双向通信。本方案中设备可被攻击者入侵变为恶意设备。

假设设备和物联网管理平台之间的通信信道是安全的（在实际应用中可考虑 SSH 等协议进行安全传输），同时，假设电力物联网系统中已经配备了入侵检测系统，能够及时发现恶意设备入侵，并及时通知物联网管理平台。

3.2 敌手能力

本文假设敌手拥有以下能力：

（1）敌手可以知道通信系统中所有用户的匿名身份标识 ID^*；

（2）敌手可以是入侵者也可以是系统中的不诚实设备或半诚实网关。

3.3 安全目标

本文提出的安全目标包括认证安全和撤销安全。

（1）匿名性：为了用户在获得电力物联网服务的同时保护其隐私，需要确保设备的匿名性，保证敌手不能确认设备的身份。

（2）认证安全：为保证只有可信的设备才能接入电力物联网管理平台，需要实现认证安全。

（3）撤销安全：为防止恶意设备再次接入，需要实现撤销安全。

4 电力物联网设备接入管理方案

4.1 核心思想

本文提出的电力物联网设备接入管理方案主要包括注册、认证、撤销和凭证更新 4 个阶段。在设备注册阶段，由物联网管理平台使用布隆过滤器将设备添加至所在群组，再使用 RSA 累加器为设备生成可信身份凭证；在设备认证阶段，设备凭借其可信身份凭证向物联网管理平台申请认证，首先由布隆过滤器做初步筛查，再由 RSA 累加器计算验证，只有通过认证的设备可接入物联网管理平台进行数据的传输；对于遭受攻击或篡改的设备，物联网管理平台可撤销其可信身份凭证，凭证失效后，该设备将不能通过认证，实现安全撤销。

4.2 具体方案

本方案选取结构简单、性能高效的 RSA 累加器，但由于其原语的限制，累加器的输入只能为素数，同时在计算开销方面尚需优化。

（1）生成满足 RSA 累加器要求的素数输入。为满足此输入要求，本方案需为每个设备的唯一身份标识 ID 计算一个素数标识（素数标识不可重复）。因此，本方案使用文献[21]中的素数生成器，通过随机预言机 $\Omega(\ )$，为输入 ID 生成一个随机数 r，并找到一个 256 比特的数 d，则 ID 的素数标识为：$ID^*=2^{256}\times\Omega(ID)+d$。此要求为每个设备生成一个素数身份标识，恰满足设备匿名的要求。

（2）降低累加值的计算开销。使用 RSA 累加器计算累加值时，需要先计算指数 $\prod_{i=1}^{n}x_i$，再进行模指数运算。然而，由于

电力物联网设备众多，指数会非常大，同样也增加了模指数运算的开销。为解决这个问题，本方案采用分组的方式，先将设备划分为不同的群组，对于同一组内的设备，先进行模指数运算，再为其颁发可信身份凭证。例如，可对设备进行分区域管理。

具体方案如图 2 所示，包括设备注册、认证、撤销及更新 4 个阶段。

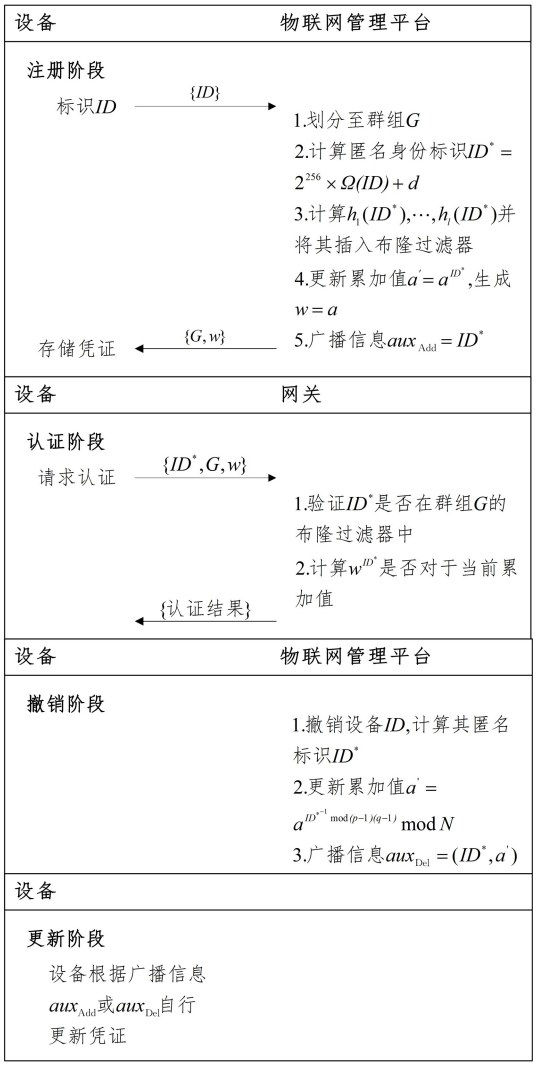

图 2 具体方案

Fig. 2 Concrete scheme

4.2.1 系统建立阶段

物联网管理平台根据实际需求，采用合适的方式对设备进行群组划分，不同群组之间的设备注册、认证及删除过程独立运行。对在同一个群组的设备操作，首先要进行初始化，生成所需参数。

算法 1 初始化算法

1. 对于每一个群组 G，都有与之对应的一个布隆过滤器比特数组 BF. G。调用布隆过滤器的初始化算法 BF. Setup(m,l)，将长度为 m 的比特数组全置为 0，然后定义 l 个独立的哈希函数。
2. 确定安全参数 λ，调用 RSA 累加器的密钥生成算法 Acc. Gen(1^λ)，随机选取一个 RSA 模 N=pq(模 N 可选取为 2048 或 4096 等)，从模 N 的二次剩余循环群中随机选取 g，输出群组累加器私钥 k=(p,q)。

4.2.2 设备注册阶段

设备在接入物联网管理平台之前，要进行设备注册。对于可信的设备，首先由物联网管理平台对其进行分组，然后计算其匿名标识，将其插入到所属群组的布隆过滤器比特数组中；再将其添加至所属的群组累加器中，并生成该设备的可信身份凭证。

算法 2 可信身份凭证颁发算法

输入：当前群组累加值 a，设备唯一身份标识 ID

输出：该设备所属群组 G，匿名身份标识 ID^*，可信身份凭证 w，辅助信息 aux_{Add}

1. 物联网管理平台划分该设备至群组 G，对应初始化的布隆过滤器比特数组 BF. G 和 l 个独立的哈希函数；
2. 调用随机预言机 Ω()，计算设备匿名身份标识 $ID^* = 2^{256} \times \Omega(ID) + d$；
3. 调用 BL. Insert(ID^*)算法，计算 ID^* 在比特数组 BF. G 的 l 个位置：$h_1(ID^*), h_2(ID^*), \cdots, h_l(ID^*)$，将上述位置的值置为 1；
4. 调用 Acc. Add(a,ID^*)算法，计算 $a' = a^{ID^*}$，生成设备的可信身份凭证即为 w=a，输出辅助信息 $aux_{Add} = ID^*$；
5. 将(G,ID^*,w)返回至该设备，并将辅助信息 $aux_{Add} = ID^*$ 广播至所有设备。

4.2.3 设备认证阶段

设备通过网关接入物联网管理平台，需要进行可信身份认证。设备凭借匿名身份标识 ID^*、所属群组 G 及可信身份凭证 w 向网关提出接入申请；网关首先查询该设备是否属于群组 G，然后通过可信身份凭证 w 验证其是否安全可信。

算法 3 可信身份凭证验证算法

输入：设备匿名身份标识 ID^*，所属群组 G，可信身份凭证 w，当前群组累加值 a'

输出：该设备的身份认证结果

1. 调用 BL. Find(ID^*)算法，对 ID^* 做同样的哈希计算：$h_1(ID^*)$，$h_2(ID^*)$，…，$h_l(ID^*)$，查询设备所属群组 G 对应的布隆过滤器比特数组 BF. G 的上述 l 个位置是否为 1；
2. 若上一步验证通过，则调用 Acc. Ver(ID^*,w,a')算法，计算 w^{ID^*} 是否等于当前累加值 a'，输出认证结果；
3. 将认证结果返回给设备。

4.2.4 设备撤销阶段

在上述过程中验证通过的设备，说明其是安全可信的，可成功接入物联网管理平台；对于验证失败的设备，说明其可信身份凭证可能发生了篡改，物联网管理平台可对其行为进行重点监控，并进一步撤销其可信身份凭证，将该设备从群组累加器删除。

算法 4 可信身份凭证撤销算法

输入：群组累加器私钥 k，当前群组累加值 a，待撤销的设备唯一身份标识 ID

输出：该设备的可信身份凭证撤销结果，辅助信息 aux_{Del}

1. 计算匿名身份标识 $ID^* = 2^{256} \times \Omega(ID) + d$；
2. 调用 Acc. Del(k,a,ID^*)算法，撤销设备的可信身份凭证，计算并更新群组累加值为 $a' = a^{ID^{*-1} \bmod (p-1)(q-1)} \bmod N$；
3. 将辅助信息 $aux_{Del} = (ID^*, a')$ 广播至所有设备。

4.2.5 凭证更新阶段

当群组中新增或删除设备时，累加值会相应更新；同样地，群组中所有设备的可信身份凭证也需要更新。物联网管理平台将辅助信息广播至各个设备，由设备本地自行更新。

算法 5 可信身份凭证更新算法

输入：设备 ID_i 及其待更新的可信身份凭证 w_i，辅助信息 aux_{op}

输出：更新后的可信身份凭证 w_i'

1. 设备收到辅助信息aux_{Add}时，调用 Acc. Upd(w，aux_{Add})算法，其可信身份凭证更新为$w_i' = w_i^{aux_{Add}}$；
2. 设备收到辅助信息aux_{Del}时，调用 Acc. Upd(w，aux_{Del})算法，计算 α 和 β 满足 $\alpha ID_i^* + \beta ID^* = 1$，其可信身份凭证更新为$w_i' = w_i^{\beta}(a')^{\alpha}$。

5　方案分析

下面从安全、存储开销、计算开销、通信开销 4 个方面对本方案进行分析。

5.1　安全性分析

(1)匿名性：在认证阶段，设备使用匿名身份标识ID_i^*，若网关想要从中获取设备的真实 ID，需要猜测 ID 对应的随机数 r 及 256 比特长的 d。然而，即使网关能够获得匿名身份标识的计算算法，也无法正确猜测随机数 r，因此，该方案提供了设备对网关的匿名性。

(2)认证安全：设备凭借可信身份凭证进行认证，若敌手想要假冒为可信的设备接入物联网管理平台，需要伪造可信身份凭证。敌手在没有 RSA 累加器私钥的情况下，基于 RSA 累加器成员证明不可伪造的性质，无法成功伪造可信身份凭证。因此，只有可信的设备可以安全接入，该方案实现了认证安全。

(3)撤销安全：即使可信身份凭证难以伪造，敌手仍有其他方式对设备开展攻击，在此情况下，入侵检测系统可检测出恶意行为并及时通知物联网管理平台，由物联网管理平台撤销设备的可信身份凭证。一旦撤销，敌手就无法使用设备已被撤销的可信身份凭证通过认证，该方案实现了撤销安全。

5.2　性能评估

为评估本文方案的性能，我们对底层算法进行了测试，使用 Crypto＋＋进行 RSA 模数的生成和匿名标识的计算。为对比基于 PKI 的方案，我们按照 RFC5280 标准生成了 PKI 证书及证书撤销列表 CRL 文件。软件实现语言为 C＋＋，实验环境为 Intel(R) Core(TM) i5-1135G7@2.40 GHz，网络带宽为 100 Mbps。

5.2.1　存储开销

由于现有方案中仅基于 PKI 的方案同时考虑了设备的安全认证及撤销，相比之下，本文提出的方案极大地降低了存储开销，且能够有效避免单点失效。

本方案中，设备方仅需存储一个可信身份凭证值，网关和物联网管理平台仅需存储最新累加值和布隆过滤器，无需维护一个庞大的列表，存储开销与设备数量线性无关。基于 PKI 的认证方案中，设备方需要存储各自的证书，网关和物联网管理平台需存储 CRL 文件，随着撤销设备的增多，CRL 膨胀速度快。表 1 给出了当撤销设备数量为 1 000 时的存储开销对比。

表 1　存储开销对比

Table 1　Comparison of storage overhead

(单位：MB)

	Scheme based on PKI	Our scheme
Device	0.087	0.001
Gateway	1.772	0.005
IoT management platform	1.772	0.018

5.2.2　计算开销

本方案的计算开销主要包括设备匿名标识的计算、累加值的计算、可信身份凭证的生成及验证。其中，匿名标识及累加值的计算、可信身份凭证的生成由物联网管理平台执行，可信设备凭证的验证由网关执行，布隆过滤器和累加器验证时间复杂度均为 O(1)。通过设备分组的方式对本方案进行优化，降低了计算开销。实验结果如图 3 所示。

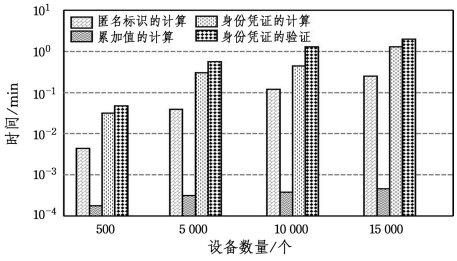

图 3　计算开销

Fig. 3　Computation overhead

5.2.3　通信开销

本方案的通信开销主要来源于不可信设备的撤销，物联网管理平台每撤销一个设备，需要广播一次辅助信息至各个设备，相比于基于 PKI 的方案在每次设备撤销时需要分发一次 CLR 文件，本方案大大降低了通信开销。每次撤销设备的通信开销如表 2 所列。

表 2　通信开销对比

Table 2　Comparison of communication overhead

(单位：min)

	Scheme based on PKI	Our scheme
Communication overhead	0.970	0.016

结束语　本文提出了一种基于密码学累加器的电力物联网设备接入管理方案，该方案同时实现了可信设备的认证和不可信设备的撤销，为保护设备身份隐私，实现了设备向网关的匿名认证。实验表明，该方案降低了存储及通信开销，且具备良好的计算开销，具有较高的实用性。该方案可进一步拓展以实现设备、网关及管理平台之间的双向认证，结合安全通信信道发挥更安全高效的作用。

参 考 文 献

[1]　FU Z X，LI X Y，YUAN Y. Research on Key Technologies of Ubiquitous Power Internet of Things [J]. Electric Power Construction，2019，40(5)：1-12.

[2]　REN T Y，WANG X H，GUO G X，et al. Design of power Internet of Things data security system based on multiple authentication and lightweight password[J]. Journal of Nanjing University of Posts and Telecommunications，2020，40(6)：12-19.

[3]　ZHANG L，ZHAO L，YIN S，et al. A lightweight authentication scheme with privacy protection for smart grid communications [J]. Future Generation Computer Systems，2019，100(Nov.)：770-778.

[4]　ZUO J Y. A privacy-preserving data aggregation algorithm in Smart Grid networks[J]. Journal of Terahertz Science and Electronic Information Technology，2021，19(3)：485-489.

[5]　HOUSLEY R，POLK W，FORD W，et al. RFC，3280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile[J]. Rfc，2002.

[6] SHAMIR A. Identity Based Cryptosystems and Signature Scheme[M]. Blakley G R, Chaum D, eds. , 1984.

[7] TAN C, CHEN M J, AMUAH E A. Research on distributed identity authentication mechanism of IoT device based on blockchain[J]. Chinese Journal on Internet of Things, 2020, 4(2): 70-77.

[8] LI H, LU R, LIANG Z, et al. An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid[J]. IEEE Systems Journal, 2014, 8(2): 655-663.

[9] CHIM T, YIU S, HUI L, et al. PASS: Privacy-preserving authentication scheme for smart grid network[C]// Proceedings of the 2011 IEEE International Conference on Smart Grid Communications. IEEE, 2011.

[10] FOUDA M M, FADLULLAH Z M, et al. A Lightweight Message Authentication Scheme for Smart Grid Communications [J]. IEEE Transactions on Smart Grid, 2011, 2(4): 675-685.

[11] KHALI D, MAHMOO D, SHEHZA D, et al. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication[J]. Future Generations Computer Systems: FGCS, 2018, 81: 557-565.

[12] LIAO H M, YU G, BAN G M, et al. Research on Identity Authentication Technology in Power Internet of Things Based on SM9 Algorithm [J]. Shandong Electric Power, 2020, 47(10): 1-5.

[13] SHEN H P, CHEN Y C. Study of Authentication Mechanism in Federated Internet of Things[J]. Computer Engineering, 2016, 42(9): 110-115.

[14] YAN H Q, WANG L J. Research of authentication techniques for the Internet of things[J]. Journal on Communications, 2020, 41(7): 213-222.

[15] MAHMOUD M M E A, MIŠIĆ J, AKKAYA K, et al. Investigating public—key certificate revocation in smart grid[J]. IEEE Internet of Things Journal, 2015, 2(6): 490-503.

[16] MC A, KA B. Communication-efficient certificate revocation management for Advanced Metering Infrastructure and IoT Integration[J]. Future Generation Computer Systems, 2021, 115: 267-278.

[17] BLOOLM B H. Space/time trade-offs in hash coding with allowable errors[J]. Communications of the ACM, 1970, 13(7): 422-426.

[18] BENALOH J, MARE M D. One-Way Accumulators: A Decentralized Alternative to Digital Signatures[C]// Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology. 1995.

[19] CAMENISCH J, LYSYANSKAYA A. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials[C]// 22nd Annual International Cryptology Conference (CRYPTO 2002). Santa Barbara, California, USA, 2002: 18-22.

[20] BARIC N, PFITZMANN B. Collision-free accumulators and fail-stop signature schemes without trees[C]// The 16th Annual International Conference on Theory and Application of Cryptographic Techniques. Konstanz, Germany, 1997: 480-494.

[21] TRIANDOPOULOS N, PAPAMANTHOU C, TAMASSIA R. Authenticated hash tables[C]// Proceedings of the 15th ACM Conference on Computer and communications security. ACM Conference on Computer & Communications Security. DBLP, 2008.

CHEN Bin, born in 1983, Ph. D. His main research interests include power grid big data security and so on.

QIN Shi-han, born in 1997, master. Her main research interests include cryptography technology and application, security certification agreement.