支持第三方仲裁的智能电网数据安全聚合方案

丁 勇[1,2],王冰尧[3],袁 方[4],王玉珏[1],张 昆[5],田 磊[1]
(1. 广西密码学与信息安全重点实验室,桂林电子科技大学,广西桂林 541004;
2. 鹏程实验室网络空间安全研究中心,广东深圳 518055;
3. 桂林电子科技大学数学与计算科学学院,广西桂林 541004;
4. 外交部通信总台,北京 100045;5. 国家信息中心,北京 100045)

摘 要: 智能电网作为新一代的电力系统,显著提高了电力服务的效率、可靠性和可持续性,但用户侧信息安全问题也日渐突出. 本文针对智能电网系统中用户数据信息泄露的问题,提出了一个具有隐私保护的数据安全采集方案. 收集器能够对采集到的电表数据进行验证,聚合为一个新的数据包,发送给电力服务中心解密和存储,且第三方仲裁机构能够解决用户端智能电表与电力服务中心发生的纠纷. 同时,本方案支持收集器,电力服务中心和第三方仲裁机构执行批量验证操作,以提升验证效率. 本文的理论分析与实验比较表明,该方案比同类型方案具有更高的运算效率和通信效率.

关键词: 智能电网; 公钥加密; 数字签名; 数据聚合; 标准模型
中图分类号: O29 **文献标识码:** A **文章编号:** 0372-2112 (2020)02-0350-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.02.018

Secure Data Aggregation Scheme in Smart Grid with Third-Party Arbitration

DING Yong[1,2], WANG Bing-yao[3], YUAN Fang[4], WANG Yu-jue[1], ZHANG Kun[5], TIAN Lei[1]
(1. *Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*;
2. *Pengcheng Laboratory Cyberspace Security Research Center, Shenzhen, Guangdong* 518055, *China*;
3. *School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*;
4. *Foreign Affairs and Communications Administration, Beijing* 10045, *China*; 5. *National Information Center, Beijing* 100045, *China*)

Abstract: Smart gird is a new generation of power system, which significantly improves the efficiency, reliability and sustainability of power service. However, the issue of privacy information leakage of users in smart grid is becoming increasingly prominent. To address this problem, we propose a privacy-preserving data security collection scheme, where the collector is able to verify all the collected data and aggregate them into a new data packet, then send it to the electricity service provider (ESP) for decryption and storage. This paper also introduces a third-party to arbitrate disputes between the smart meter users and ESP. In our solution, collectors, ESP, and the third-party can perform batch verification on multiple (aggregated) ciphertexts, respectively, so as to efficiently verify their authenticity and integrity. The theoretical analysis and experimental comparison show that the proposed scheme enjoys more computational efficiency and communication efficiency compared with existing scheme.

Key words: smart grid; public-key encryption; digital signature; data aggregation; standard model

1 引言

电力系统已经成为当今社会必不可少的基础设施,随着经济社会的高速发展,传统电网已不能满足现代经济发展的需要,而智能电网的出现给电力系统带来了很大的变革. 与传统电网相比,智能电网是建立在

收稿日期:2019-02-28;修改日期:2019-10-17;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61772150, No. 61862012, No. 61962012);国家密码发展基金(No. MMJJ20170217);广西重点研发计划(No. AB17195025);广东网络技术仿真验证平台(No. PCL2018KP004);广西自然科学基金(No. 2018GXNSFDA281054, No. 2018GXNSFAA281232, No. AD19245048, No. 2019GXNSFFA245015)

集成的、高速双向通信网络的基础上,通过先进技术和方法的支持与应用,实现了电网的可靠、安全、经济、高效、环境友好和使用安全的目标[1].

然而,在享受智能电网带来的社会效益和技术优势的同时,一些安全和隐私问题也随之产生[2]. 随着智能电网终端设备智能电表的部署,用户侧信息安全问题也日渐突出[3]. 例如,通过分析收集到的电表用户详细的用电信息,可以很容易地推断出用户在家中的活动情况以及家里成员数目[4]. 这类敏感数据如果不能得到有效的保护,则会被敌手利用,从目标用户或商业竞争对手中获得非法利益. 此外,攻击者可能利用这些数据对电网进行大规模的恶意攻击[5]. 因此需要加强智能电网中对于隐私保护方法的研究,其中通讯开销和计算成本的问题[6,7],也应该成为隐私保护方法关注的重点. 针对上述问题,本文提出了一种新的数据聚合方案,能够防止用户数据信息泄露,保证了用户数据信息的完整性和机密性,并且提高了计算效率,减少了通讯成本. 本文方案支持第三方可信实体参与密文的加密过程,并对聚合数据包进行再验证和再解密处理,解决纠纷,提出仲裁.

1.1　相关工作

利用匿名化方法使用户身份和用户数据分离而达到隐私保护的目的是一种常用的手段. Efthymiou 和 Kalogridis 采用第三方托管服务,以匿名高频计量数据的方式解决用户的细粒度隐私问题[8]. Fan、Huang 和 Lai 提出了盲因子创建盲数据库的方法,使内部攻击者只能获得电网系统中的总用电量,而无法分析出每个用户的用电量[9]. Yu 等人研究了环签名技术,用于实现对智能电网中用户身份的隐私保护[10]. 张木玲提出了利用群签名技术从消息来源的角度保证隐私,并可实现对消息来源的认证[11]. 夏卓群等人提出了一种基于虚拟环架构的智能电网用户隐私保护方法,使高频数据在环内实现匿名性,保障了电网操作与账单计算功能的有效性,实现了用户电表数据隐私性和完整性保护[12]. 从智能电表硬件安全的角度来保障用户电表数据的隐私,能够抵抗外部攻击,但目前公开文献对于这类技术的研究较少. 一般情况下,可以利用消息验证码的方式实现身份认证[13],但对于用户敏感数据的储存效果达不到预期的安全目标. 引入第三方存储数据能够减轻系统用户的负担,在智能电网,消息传递[14]以及车联网[15]等众多系统中被普遍采用,显然,数据的安全保护关系到用户的隐私. 曹波等人在其构建的安全数据聚合方案中,可信第三方实体专门负责保管所有通信过程涉及的密钥,保证了智能电网中通讯过程的安全性[16]. 龚凡提出的电量统计和收费方案中,用户管理、认证和群密钥的生成都需要借助可信第三方实现[17]. 陈明提出了一个基于身份的密钥托管服务,可确保用户密钥不被泄露,具有较高的安全性[18].

通过对密文形式的智能电表数据进行聚合,不但能够保障智能电表数据的隐私,而且可以有效减少实体间的通信开销. Wang,Mu 和 Chen 基于 Paillier 的同态加密方案和可验证的秘密共享模型,提出了具有隐私保护和数据聚合功能的计费系统[19]. 需强调的是,由于用户的用电数据位数较短,上述基于 Paillier 加密方案的系统效率较低. 余勇等人的方案中采用了 DGK 密码体制[20],因此比文献[19]的 Paillier 加密效率高,减少了计算开销. 除此之外,通过构造聚合树灵活地处理用户的接入与撤离,极大地降低了系统通讯成本. Wang 构建的基于身份的聚合协议[21],将基于身份的加密方案和基于身份的签名方案相结合,使它们享有相同的私钥和公共参数,降低了协议的复杂性. Ding 等人提出了基于身份的智能电表数据聚合协议,可同时确保电表侧用户数据的隐私性和完整性等需求[22],与 Wang[21]相比降低了智能电表侧的计算成本.

张思佳,顾春华和温蜜从功能和计算成本等方面对比分析了智能电网系统中的数据聚合方案[23],其结论能够为研究或改进现有的数据聚合方法提供良好的借鉴依据. He,Kumar 和 Lee 改进了 Fan,Huang 和 Lai 的数据聚合方案[9],但由于智能电表的计算能力有限,使得改进方案的性能不太适用于智能电网环境[24]. He 等人提出的具有隐私保护的数据聚合方案[25],比文献[24]具有更高的安全性和较好的计算性能. Shi 等人提出了基于分组的错误检测聚合协议[26],巧妙的将差分隐私技术应用到了数据聚合的过程. Guan 等人提出了一种基于秘密共享模型的智能电表数据聚合方案[27],采用替换技术实现智能电表数据聚合时的容错,与文献[26]中的方案相比,该方案具有更低的错误率和计算成本.

1.2　本文主要工作

针对智能电网中用户数据信息面临的安全威胁,本文构建了一种支持第三方参与仲裁的具有隐私保护和完整性验证的数据聚合安全方案(Secure Data Aggregation Scheme,SDA). 该方案能够确保用户端智能电表数据的隐私,并支持聚合器、电力中心等实体对接收到的数据进行合法性验证. 本方案引入的第三方仲裁机构,能在用户和电力中心之间出现电表数据的纠纷时进行有效仲裁. 通过标准模型下的安全分析,表明该方案能够抵抗选择明文攻击和自适应选择消息攻击,保证用户的用电行为隐私和完整性,满足实际应用需求. 理论分析与实验比较表明,该方案相比已有的智能电网数据聚合方案具有较高的计算效率.

2 预备知识

本章简要介绍双线性群,Decisional Bilinear Diffie-Hellman(DBDH)问题以及 q-Strong Diffile-Hellman(q-SDH)问题. 设 G 和 G_T 为两个具有相同素数阶 p 的乘法循环群,其中 g 为 G 的生成元. 定义双线性关系 $\hat{e}:G\times G\rightarrow G_T$,则双线性对具有以下性质.

双线性: $\forall g_1,g_2\in G,a,b\in Z_p^*$,有 $\hat{e}(g_1^a,g_2^b)=\hat{e}(g_1,g_2)^{ab}$.

非退化性:存在 $g\in G$,使得 $\hat{e}(g,g)\neq 1$.

高效性:对任意的 $g_1,g_2\in G$,存在有效算法可以计算 $\hat{e}(g_1,g_2)$.

DBDH 问题:设 G 和 G_T 是两个 p 阶素数循环群,G 的生成元为 g. 已知任意一个五元组 (g,g^a,g^b,g^c,Z),其中 $Z\in G_T,a,b,c\in Z_p^*$ 未知,判断 $Z=\hat{e}(g,g)^{abc}$ 是否成立. 如果存在多项式算法 ξ,使 $|\Pr[\xi(g,g^a,g^b,g^c,\hat{e}(g,g)^{abc})=1]-\Pr[\xi(g,g^a,g^b,g^c,Z)=1]|\geq 2\varepsilon$ 成立,则称算法 ξ 解决 DBDH 问题的优势是 ε.

q-SDH 问题:设 G 和 G_T 是两个 p 阶素数循环群,G 的生成元为 g. 已知任意一个 $(q+1)$ 元组 $(g,g^x,g^{(x^2)},\cdots,g^{(x^q)})\in G^{q+1}$ 和 $c\in Z_p\setminus\{-x\}$,计算二元组 $(c,g^{1/(x+c)})\in Z_p\times G$. 如果存在多项式算法 ξ,使 $|\Pr[\xi(g,g^x,g^{(x^2)},\cdots,g^{(x^q)},g_T,g_T^x)=(c,g^{\frac{1}{x+c}})]|\geq\varepsilon$ 成立,则称算法 ξ 解决 q-SDH 问题的优势是 ε.

3 系统模型及安全需求

3.1 系统模型

如图 1 所示,一个 SDA 系统中由四类实体构成,分别为用户端的智能电表,面向区域的收集器,电力服务中心和可信的第三方仲裁机构.

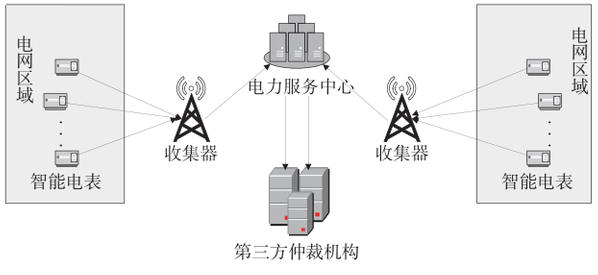

图1 系统模型图

智能电表是智能电网的终端设备,负责计量用户侧的用电信息. 整个电网区域共有 n 个智能电表,当收到电力服务中心发出的响应消息后,智能电表及时对某个固定时间段内用户侧的用电数据信息进行隐私保护处理,发送给收集器.

收集器是连接智能电表和电力服务中心的桥梁,负责收集来自本区域的智能电表用电信息. 当确认这些电表数据的来源真实可靠后,收集器将接收到的所有数据信息聚合为一个新的数据包,并发送给电力服务中心. 电力服务中心负责发布收集电表用电信息的响应消息,并及时处理、分析接收到的聚合数据包,为整个智能电网的正常工作提供可靠的服务. 当与用户发生纠纷时,电力服务中心将接收到的聚合数据包发送给第三方机构,请求仲裁.

第三方仲裁机构可以对电网区域内部的信息交流活动进行合法性的验证. 当电网区域内部发生纠纷需要仲裁时,第三方仲裁机构对电力服务中心发送的聚合数据包进行解密处理,为电表数据信息提供真实性和完整性的验证服务,从而解决纠纷,提出仲裁.

3.2 安全需求及设计目标

在智能电网中,恶意的实体可能通过窃听、恶意攻击等手段尽可能多的获取用户数据信息. 一个安全的数据聚合方案不仅要能够很好的适用于智能电网环境,同时也要在传输过程中保证数据的安全隐私性. 针对上述问题,一个 SDA 系统应满足如下的安全需求及功能需求:

数据机密性:数据的机密性是指智能电表数据在传输的过程中,仅允许收发双方能够得到信息的真实内容,其余任何实体机构和任何人都无权获知. 即使敌手可以窃听、截获传输数据或者入侵到收集器、电力服务中心和第三方的后台数据库,也无法获取用户的用电信息.

数据完整性:数据完整性是确保智能电表数据安全的基本要求,在数据传输过程中,敌手不能伪造和篡改传输数据. 当电表数据被篡改时,可以被收集器及时发现.

高效性:因为智能电表的计算能力较低,而智能电网的通讯过程需要进行频繁的数据计算与数据传输,因此 SDA 方案应该具有较高的计算效率和通讯效率,能够满足智能电网的实际应用需求.

3.3 系统框架

一个 SDA 方案中由 9 个多项式时间算法组成,分别为初始算法(Setup)、智能电表密钥生成算法(UKeyGen)、收集器密钥生成算法(OKeyGen)、电力服务中心密钥生成算法(EKeyGen)、第三方仲裁机构密钥生成算法(MKeyGen)、密文生成算法(CTGen)、聚合密文生成算法(Aggregation)、解密算法(Decryption)以及仲裁算法(Arbitration).

Setup:输入安全参数 l,输出系统参数 $param$.

UKeyGen:智能电表根据系统参数 $param$ 分别生成自己的公钥 pk 和私钥 sk.

OKeyGen:收集器根据系统参数 $param$ 分别生成

自己的公钥 pk 和私钥 sk.

EKeyGen:电力服务中心根据系统参数 $param$ 分别生成自己的公钥 pk 和私钥 sk.

MKeyGen:第三方仲裁机构根据系统参数 $param$ 分别生成自己的公钥 pk 和私钥 sk.

CTGen:输入系统参数 $param$,电表数据 $m_{i,j}$,输出密文和签名 $(CT_{i,j},(S_{i,j},r_{i,j,2}))$.

Aggregation:收集器收到 $(CT_{i,j},S_{i,j})$,批量验证真实性后,生成聚合密文 $CT_{k,j}$ 和签名 $(S_{k,j},r_{k,j,2})$.

Decryption:电力服务中心收到聚合密文和签名 $(CT_{k,j},(S_{k,j},r_{k,j,2}))$,验证真实性后,输出电表总数据信息 $M_{k,j}$ 或者符号"⊥"表示解密失败.

Arbitration:第三方仲裁机构收到聚合密文和签名 $(CT_{k,j},(S_{k,j},r_{k,j,2}))$,验证真实性后,输出电表总数据信息 $M_{k,j}$ 或者符号"⊥"表示解密失败,提出仲裁.

一个正确的 SDA 方案需要满足如下条件:

(1)签名的可验证性:智能电表利用 CTGen 算法生成的一对密文和签名 $(CT_{i,j},(S_{i,j},r_{i,j,2}))$,需能够通过收集器的签名验证.

(2)签名的批量验证:智能电表利用 CTGen 算法生成的一组密文和签名 $(CT_{i,j},(S_{i,j},r_{i,j,2}))$,需能够通过 Aggregation 算法的批量验证.

(3)签名的可验证性:收集器利用 Aggregation 算法生成的一对密文和签名 $(CT_{k,j},(S_{k,j},r_{k,j,2}))$,需能够通过电力服务中心的签名验证.

(4)签名的批量验证:收集器利用 Aggregation 算法生成的一组密文和签名 $(CT_{k,j},(S_{k,j},r_{k,j,2}))$,需能够通过电力服务中心和第三方仲裁机构的批量验证.

(5)聚合密文的可恢复性:电力服务中心对收到的合法聚合密文和签名 $(CT_{k,j},(S_{k,j},r_{k,j,2}))$,能够执行 Decryption 算法进行解密得到电表总数据 $M_{k,j}$.

(6)仲裁:当用户和电力服务中心出现纠纷时,仲裁机构能够对合法聚合密文和签名 $(CT_{k,j},(S_{k,j},r_{k,j,2}))$ 执行 Arbitration 算法,解密得到电表总数据 $M_{k,j}$.

3.4　安全模型

针对 SDA 系统中智能电表数据隐私保护需求,我们定义如下的游戏.

准备阶段:输入安全参数 l,输出系统参数 $param$.

密钥产生阶段:挑战者 C 由系统参数 $param$ 和密钥产生算法得到用户公钥 pk 和私钥 sk,并将 pk 发送给敌手 A.

挑战阶段:敌手 A 选择提交两个长度相同的电表数据 m_0 和 m_1,并发送给挑战者 C,挑战者 C 随机选择 $\gamma\in\{0,1\}$,计算 $CT^*=CTGen(param,pk,m_\gamma)$,并发送给 A.

输出:敌手 A 输出一个猜测 γ'. 如果 $\gamma'=\gamma$,则 A 赢得游戏.

敌手 A 的优势定义为 $Adv(A)=\left|\Pr[\gamma'=\gamma]-\frac{1}{2}\right|$.

定义 1(IND-CPA 安全性)　如果敌手 A 在多项式时间内攻破一个 SDA 方案的优势至多是 ε,则称该 SDA 方案是 ε-IND-CPA 安全的(Indistinguishable against Chosen-Plaintext Attack). 针对 SDA 系统中智能电表数据完整性保护需求,我们定义如下的安全游戏.

准备阶段:输入安全参数 l,输出系统参数 $param$.

密钥产生阶段:挑战者 C 由系统参数 $param$ 和密钥产生算法得到用户的公钥 pk 和私钥 sk,并将 pk 发送给敌手 A.

签名询问:敌手 A 自适应的选择密文形式的智能电表数据 CT,并发送给挑战者 C,挑战者 C 返回一个签名 S.

输出:最后,敌手 A 输出一个密文 CT^* 和一个签名 S^*,其中,CT^* 没有被执行过签名询问. 如果 $Verify(CT^*,S^*)=1$,则 A 赢得游戏.

敌手 A 的优势定义为 $Adv(A)=|\Pr[Sigforge_A^{cma}(l)=1]|$.

定义 2(EU-CMA 不可伪造性)　如果敌手 A 在多项式时间内做至多 q_s 次签名询问后,攻破 SDA 方案的优势至多是 ε,称 SDA 方案是 (ε,q_s)-EU-CMA 不可伪造的(Existentially Unforgeable under Adaptively Chosen-Message Attack).

4　基于双线性群的 SDA 方案

Setup:输入安全参数 l 后,选取两个素数阶 p 的循环群 $(G,\cdot)$ 和 $(G_T,\cdot)$,定义双线性映射 $\hat{e}:G\times G\to G_T$,其中 g 为 G 的生成元,选取抗碰撞 Hash 函数 $H:\{0,1\}^*\to Z_p^*$. 因此系统参数为 $param=(G,G_T,\hat{e},H,g,g_t,p)$.

UKeyGen:输入安全参数 l 后,用户 U 根据系统参数 $param$ 产生公钥 pk 和私钥 sk. 每个用户 U_i 随机选择 $x_i,y_i\in Z_p^*$,令 $u_i=g^{x_i},v_i=g^{y_i}$. 因此公钥为 $pk_i=(u_i,v_i)$,私钥为 $sk_i=(x_i,y_i)$.

OKeyGen:输入安全参数 l 后,收集器 O 根据系统参数 $param$ 产生公钥 pk 和私钥 sk. 每个收集器 O_k 随机选择 $x_k,y_k\in Z_p^*$,令 $u_k=g^{x_k},v_k=g^{y_k}$. 因此公钥为 $pk_k=(u_k,v_k)$,私钥为 $sk_k=(x_k,y_k)$.

EKeyGen:电力服务中心随机选择一个 $x_{esp}\in Z_p^*$,令 $u_{esp}=g^{x_{esp}}$. 则公钥为 $pk_{esp}=u_{esp}$,私钥为 $sk_{esp}=x_{esp}$.

MKeyGen:第三方仲裁机构随机选择一个 $x_{mon}\in Z_p^*$,令 $u_{mon}=g^{x_{mon}}$,则公钥为 $pk_{mon}=u_{mon}$,私钥为 $sk_{mon}=x_{mon}$.

CTGen:智能电网中第 k 个用电区域的第 i 个智能电表 U_i 针对电表数据 $m_{i,j}$,随机选取 $r_{i,j,1},r_{i,j,2}\in Z_p^*$,

计算：

$$CT_{i,j}=(c_{i,j,1},c_{i,j,2})=(g^{r_{i,j,1}},g_t^{m_{i,j}}\cdot\hat{e}(g^{x_{esp}},g^{x_{mon}})^{r_{i,j,1}})$$

即将第 i 个用户端的第 j 个消息 $m_{i,j}$ 加密. 计算：

$$S_{i,j}=g^{1/(x_i+y_ir_{i,j,2}+H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j}))}$$

则密文 $CT_{i,j}$ 的签名为 $(S_{i,j},r_{i,j,2})$. 随后，第 i 个智能电表将密文 $CT_{i,j}$ 和签名 $(S_{i,j},r_{i,j,2})$ 发送给该区域中的收集器 O_k.

Aggregation：当收集器 O_k 收到 n 个智能电表的密文 $(CT_{i,j},(S_{i,j},r_{i,j,2}))$ 时，需要逐一验证真实性和完整性. 为了减少验证时间，提高效率，收集器 O_k 对收到的 n 个密文的签名进行批量验证. 针对每个密文，随机选取一个 $\rho_i\in Z_p^*$，若有：

$$\prod_{i=1}^{n}\hat{e}(S_{i,j},u_iv_i^{r_{i,j,2}}\cdot g^{H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j})})^{\rho_i}=\hat{e}(g,g)^{\sum_{i=1}^{n}\rho_i} \tag{1}$$

成立，则这 n 个智能电表的密文信息通过真实性和完整性的验证. 当所有的电表密文数据通过验证之后，收集器 O_k 随机选取一个 $r_{k,j,2}\in Z_p^*$，将收集到的 n 个电表密文 $CT_{i,j}$ 聚合成为一个新的密文数据包 $CT_{k,j}$ 并签名 $(S_{k,j},r_{k,j,2})$，发送给电力服务中心. 其中：

$$CT_{k,j}=(\hat{C}_{k,j,1},\hat{C}_{k,j,2})=(\prod_{i=1}^{n}c_{i,j,1},\prod_{i=1}^{n}c_{i,j,2})$$

$$S_{k,j}=g^{1/(x_k+y_kr_{k,j,2}+H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j}))}$$

当收集器 O_k 收到第 i 个智能电表发送的一对密文 $CT_{i,j}$ 和签名 $(S_{i,j},r_{i,j,2})$ 时，对这对密文和签名单独进行签名验证. 若有等式：

$$\hat{e}(S_{i,j},u_iv_i^{r_{i,j,2}}\cdot g^{H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j})})=\hat{e}(g,g) \tag{2}$$

成立，则第 i 个智能电表的密文信息通过真实性和完整性的验证.

Decryption：当电力服务中心收到收集器 O_k 发送的聚合密文 $(CT_{k,j},(S_{k,j},r_{k,j,2}))$ 之后，先验证其真实性和完整性. 若有：

$$\hat{e}(S_{k,j},u_kv_k^{r_{k,j,2}}\cdot g^{H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j})})=\hat{e}(g,g) \tag{3}$$

成立，则验证通过，电力服务中心开始对第 k 个聚合密文进行解密. 其中：

$$M_{k,j}=\hat{C}_{k,j,2}/\hat{e}(g^{x_{mon}},\hat{C}_{k,j,1})^{x_{esp}} \tag{4}$$

电力服务中心得到聚合之后的数据信息，通过计算以 g_t 为底的 $M_{k,j}$ 的对数，得到第 k 个用电区域的所有智能电表用户端的详细数据信息.

当电力服务中心同时收到 m 个收集器发送的聚合密文 $(CT_{k,j},(S_{k,j},r_{k,j,2}))$ 时，需要逐一验证其真实性. 为提高验证效率，电力服务中心对收到的 m 个聚合密文进行批量验证. 针对每个聚合密文，随机选取一个 $\gamma_k\in Z_p^*$，若有：

$$\prod_{k=1}^{m}\hat{e}(S_{k,j},u_kv_k^{r_{k,j,2}}\cdot g^{H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j})})^{\gamma_k}=\hat{e}(g,g)^{\sum_{k=1}^{m}\gamma_k} \tag{5}$$

成立，则这 m 个收集器的聚合密文通过真实性和完整性的验证.

Arbitration：当第三方仲裁机构收到收集器 $O_{k,j}$ 发送的聚合密文 $CT_{k,j}$ 之后，先验证其真实性和完整性，若有式(3)成立，则验证通过，第三方开始重新解密. 其中：

$$M_{k,j}=\hat{C}_{k,j,2}/\hat{e}(g^{x_{esp}},\hat{C}_{k,j,1})^{x_{mon}} \tag{6}$$

第三方得到聚合之后的数据信息，通过计算以 g_t 为底的 $M_{k,j}$ 的对数，得到第 k 个用电区域的所有智能电表用户端的详细数据信息. 然后对发生纠纷的信息交流活动进行合法性验证，解决纠纷，提出仲裁.

当第三方仲裁机构同时收到 m 个收集器发送的聚合密文 $(CT_{k,j},(S_{k,j,1},r_{k,j,2}))$ 时，需要逐一验证其真实性. 为提高验证效率，第三方对收到的 m 个聚合密文进行批量验证. 针对每个聚合密文，随机选取一个 $\eta_k\in Z_p^*$，若有：

$$\prod_{k=1}^{m}\hat{e}(S_{k,j},u_kv_k^{r_{k,j,2}}\cdot g^{H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j})})^{\eta_k}=\hat{e}(g,g)^{\sum_{k=1}^{m}\eta_k} \tag{7}$$

成立，则这 m 个收集器的聚合密文通过真实性和完整性的验证.

5 方案分析

5.1 正确性和安全性分析

本节对 SDA 方案的正确性和安全性进行证明和分析.

定理 1 上述 SDA 方案是正确的.

证明

(1) 智能电表 U_i 生成的一对密文和签名 $(CT_{i,j},(S_{i,j},r_{i,j,2}))$ 满足 Aggregation 算法中等式(2)的验证.

$$\begin{aligned}&\hat{e}(S_{i,j},u_iv_i^{r_{i,j,2}}\cdot g^{H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j})})\\&=\hat{e}(g^{1/(x_i+y_ir_{i,j,2}+H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j})},g^{x_i+y_ir_{i,j,2}+H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j})})\\&=\hat{e}(g,g)\end{aligned}$$

因此，收集器可验证电表 U_i 的数据 $m_{i,j}$ 的真实性和完整性.

(2) 任意时间段内智能电表 U_i 生成的一组密文和签名 $(CT_{i,j},(S_{i,j},r_{i,j,2}))$ 满足 Aggregation 算法中等式(1)的批量验证.

$$\begin{aligned}&\prod_{i=1}^{n}\hat{e}(S_{i,j},u_iv_i^{r_{i,j,2}}\cdot g^{H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j})})^{\rho_i}\\&=\prod_{i=1}^{n}\hat{e}(g^{1/(x_i+y_ir_{i,j,2}+H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j})},g^{x_i+y_ir_{i,j,2}+H(c_{i,j,1}\|c_{i,j,2}\|T_{i,j})})^{\rho_i}\\&=\hat{e}(g,g)^{\sum_{i=1}^{n}\rho_i}\end{aligned}$$

因此，收集器可批量验证所在区域的所有电表数据的真实性和完整性.

(3) 收集器 O_k 生成的一对合法聚合密文 $(CT_k,$

$(S_{k,j},r_{k,j,2})$)满足电力服务中心的签名验证,即通过等式(3)的验证.

$$\begin{aligned}&\hat{e}(S_{k,j},u_k v_k^{r_{k,j,2}}\cdot g^{H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j})})\\&=\hat{e}(g^{1/(x_k+y_k r_{k,j,2}+H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j}))},g^{x_k+y_k r_{k,j,2}+H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j})})\\&=\hat{e}(g,g)\end{aligned}$$

因此,电力服务中心可以验证收集器生成的合法聚合密文的真实性和完整性.

(4)收集器 O_k 生成的一组合法聚合密文($CT_{k,j}$,$(S_{k,j},r_{k,j,2})$)满足电力服务中心的批量验证,即通过等式(5)的验证.

$$\begin{aligned}&\prod_{k=1}^{m}\hat{e}\,(S_{k,j},u_k v_k^{r_{k,j,2}}\cdot g^{H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j})})^{\gamma_k}\\&=\prod_{k=1}^{m}\hat{e}\,(g^{1/(x_k+y_k r_{k,j,2}+H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j})},g^{x_k+y_k r_{k,j,2}+H(\hat{C}_{k,j,1}\|\hat{C}_{k,j,2}\|T_{k,j})})^{\gamma_k}\\&=\hat{e}(g,g)^{\sum_{t=1}^{m}\gamma_k}\end{aligned}$$

因此,电力服务中心可批量验证整个智能电网区域中的收集器生成的合法聚合密文的真实性和完整性.

同理,收集器 O_k 生成的一组合法聚合密文($CT_{k,j}$,$(S_{k,j},r_{k,j,2})$)满足第三方仲裁机构的批量验证,即通过等式(7)的验证. 因此,第三方仲裁机构可批量验证整个智能电网区域中的收集器生成的合法聚合密文的真实性和完整性.

(5)收集器 O_k 生成的合法聚合密文和签名($CT_{k,j}$,$(S_{k,j},r_{k,j,2})$)可以通过 Decryption 算法中的等式(4)解密,恢复得到电表总数据 M.

$$\begin{aligned}\hat{C}_{k,j,2}/\hat{e}\,(g^{x_{mon}},\hat{C}_{k,j,1})^{x_{esp}}&=\frac{\prod_{i=1}^{n}(g_t^{m_{i,j}}\cdot\hat{e}\,(g^{x_{esp}},g^{x_{mon}})^{r_{i,j,1}})}{\hat{e}\,(g^{x_{mon}},\prod_{i=1}^{n}g^{r_{i,j,1}})^{x_{esp}}}\\&=\frac{\prod_{i=1}^{n}g_t^{m_{i,j}}\prod_{i=1}^{n}\hat{e}\,(g^{x_{esp}},g^{x_{mon}})^{r_{i,j,1}}}{\prod_{i=1}^{n}\hat{e}\,(g^{x_{mon}},g^{r_{i,j,1}})^{x_{esp}}}\\&=g_t^{\sum_{i=1}^{n}m_{i,j}}=M_{k,j}\end{aligned}$$

(6)当智能电表用户和电力服务中心出现纠纷时,收集器生成的合法聚合密文和签名($CT_{k,j}$,$(S_{k,j},r_{k,j,2})$)可以通过 Arbitration 算法中的等式(6)解密,恢复得到电表总数据 $M_{k,j}$.

$$\begin{aligned}\hat{C}_{k,j,2}/\hat{e}\,(g^{x_{esp}},\hat{C}_{k,j,1})^{x_{mon}}&=\frac{\prod_{i=1}^{n}(g_t^{m_{i,j}}\cdot\hat{e}\,(g^{x_{esp}},g^{x_{mon}})^{r_{i,j,1}})}{\hat{e}\,(g^{x_{esp}},\prod_{i=1}^{n}g^{r_{i,j,1}})^{x_{mon}}}\\&=\frac{\prod_{i=1}^{n}g_t^{m_{i,j}}\prod_{i=1}^{n}\hat{e}\,(g^{x_{mon}},g^{x_{esp}})^{r_{i,j,1}}}{\prod_{i=1}^{n}\hat{e}\,(g^{x_{esp}},g^{r_{i,j,1}})^{x_{mon}}}\\&=g_t^{\sum_{i=1}^{n}m_{i,j}}=M_{k,j}\end{aligned}$$

定理 2　本文方案可保证电表数据的隐私性,即在 DBDH 难题假设下,SDA 方案中的电表数据是 ε-IND-CPA 安全的.

本文 SDA 方案中密文电表数据 $CT_{i,j}$和文献[21]中的密文数据具有相近的形式,主要区别在于 SDA 方案生成密文电表数据 $CT_{i,j}$需要同时利用电力服务中心和第三方仲裁机构的公钥,而文献[21]生成密文电表数据使用了系统公开参数和电力服务中心的唯一身份. 因此,定理 2 的证明过程与文献[21]中定理 1 类似,即本文的 SDA 方案可确保电表数据在 DBDH 难题假设下是 IND-CPA 安全的.

定理 3　本文提出的 SDA 方案可保证电表数据的完整性,即在 q-SDH 难题假设下,SDA 方案中的电表数据是 EU-CMA 不可伪造的.

本文 SDA 方案对密文数据的签名部分采用了 BB 签名方案文献[28],因此,定理 3 的证明过程与文献[28]中定理 8 类似,即本文的 SDA 方案可确保电表数据在 q-SDH 难题假设下是 EU-CMA 不可伪造的.

5.2　功能分析与比较

本节从功能上对本文的 SDA 方案与 Wang[21] 的方案进行详细对比. 两个方案均利用收集器采集并聚合来自用户端的电表数据,发送给电力服务中心. 而且,两个方案均支持收集器通过批量验证密文的真实性来提高计算效率. 在 Decryption 阶段,本文方案实现了电力服务中心批量验证聚合密文的功能,有助于提高智能电网内部数据处理的效率. 而 Wang[21] 的方案不支持电力服务中心执行批量验证操作.

在 Arbitration 阶段,本文方案引入的第三方仲裁机构能够为电网内部的信息纠纷提供仲裁服务,这在 Wang[21] 方案中没有进行考虑. 此外,本文方案还支持第三方仲裁机构执行批量验证操作,进一步提高解决纠纷的效率.

5.3　效率分析与比较

本节首先针对智能电表生成密文和签名,收集器验证签名、批量验证签名和聚合密文,以及 ESP 和第三方解密等六个阶段进行分析,将本文的 SDA 方案与 Wang[21] 的基于身份的聚合方案进行效率对比;其次,本节给出电力服务中心和第三方仲裁机构在收到相等数量聚合密文的情况下,批量验证与逐一验证两种方式的效率对比. 如表 1 所示,在理论分析比较两个方案在各阶段所需的运算成本时,仅考虑比较耗时的指数运算(记作 E)和双线性对运算(记作 B),其中,E_G 表示在群 G 上的指数运算,E_{G_T}表示在群 G_T 上的指数运算.

在生成密文阶段,本文的 SDA 方案和 Wang[21] 的方案包含相同的计算复杂度,即需要进行一次群 G 上的

指数运算,两次群 G_T 上的指数运算,以及一次双线性对运算. 在生成签名阶段,本文的 SDA 方案和 Wang[21] 的方案分别需要在群 G 上进行一次指数运算. 而在验证签名阶段,本文的 SDA 方案只需要进行一次双线性对运算和一次群 G 上的指数运算,Wang[21] 的方案则需要进行三个双线性对运算两次群 G 上的指数运算. 对一个包含 n 个智能电表的智能电网环境,SDA 方案只需要进行 $(n+1)$ 个双线性对运算,n 个群 G 上的指数运算和 n 个群 G_T 上的指数运算来处理批量验证签名. 而 Wang[21] 的方案则需要进行 $(n+2)$ 个双线性对运算和 $3n$ 个在群 G 上的指数运算. 在聚合密文和解密两个阶段,SDA 方案和 Wang[21] 包含相同的计算复杂度. 在聚合密文阶段,两个方案需要在群 G 和群 G_T 上分别进行一个指数运算. 在解密阶段,两个方案需要分别进行一个双线性对运算和一个在群 G_T 上的指数运算.

表 1 理论分析及对比

	密文生成	签名生成	签名验证	批量验证签名	密文聚合	解密
方案[21]	$1E_G+2E_{G_T}+1B$	$1E_G$	3B	$(n+2)B+3nE_G$	$1E_G+1E_{G_T}$	$1B+1E_{G_T}$
本文方案	$1E_G+2E_{G_T}+1B$	$1E_G$	$1B+1E_G$	$(n+1)B+nE_G+(n+1)E_{G_T}$	$1E_G+1E_{G_T}$	$1B+1E_{G_T}$

在进行实验分析时,实验代码基于 Pairing-based Cryptography Library (PBC-0.5.12) 进行开发,仿真系统运行于 64 bit Windows 10 操作系统,系统硬件配置为 Intel(R) Core(TM) i5-7500 CPU(3.4 GHz)和 12GB 内存. 表 2 分别给出了两个方案执行一次的加密、签名、签名验证以及解密消耗的时间,其中加密和签名过程由智能电表执行,签名验证由收集器执行,解密过程由 ESP 和第三方实体执行. 可以看出,两个方案在加密和解密阶段的运行效率基本相同;而在签名和签名验证阶段,本文的 SDA 方案比方案[21]具有更高的计算效率.

表 2 单次加密、签名、签名验证以及解密时间对比

	加密	签名	签名验证	解密
方案[21]	0.015s	0.008s	0.015s	0.188s
本文方案	0.015s	0.003s	0.010s	0.188s

在批量验证签名阶段两个方案消耗的时间如图 2 所示,可以看出,当智能电网所在区域包含的电表数目相等时,本文方案在批量验证阶段的运行时间近似保持为方案[21]的 62%. 随着电表数目的增加,两个方案均呈现出良好的线性属性. 因此,本文的 SDA 方案在批量验证阶段具有更高的运行效率.

图 3 给出两个方案在聚合电表密文阶段的时间对比,可以看出,当智能电网所在区域包含的电表数目相等时,本文方案在密文聚合阶段的运行时间与方案[21]的运行时间近似,且运行时间与电表数目呈现出较好的线性属性. 随着电表数目增加,两个方案的聚合时间与电表数目呈现的线性增长关系没有较大变化,因此,两个方案在密文聚合阶段的计算效率是相近的.

当电力服务中心收到聚合密文时,需要首先验证其真实性. 对于收到多个聚合密文的情况,批量验证与逐一的效率对比结果如图 4 所示,可以看出,当聚合密文的数量相同时,批量验证所需的运行时间比逐一验证所需的时间少,而且随着聚合密文数量的增加,批量验证所需的时间与聚合密文的数量呈现出良好的线性关系. 同电力服务中心类似,当第三方仲裁机构收到聚合密文时,也需要首先验证其真实性. 当收到多个聚合密文,批量验证与逐一验证的效率对比结果如图 5 所示,可以看出,当聚合密文的数量相同时,批量验证所需的运行时间比逐一验证所需的时间少,且批量验证所需的时间与聚合密文的数量呈现良好的线性关系.

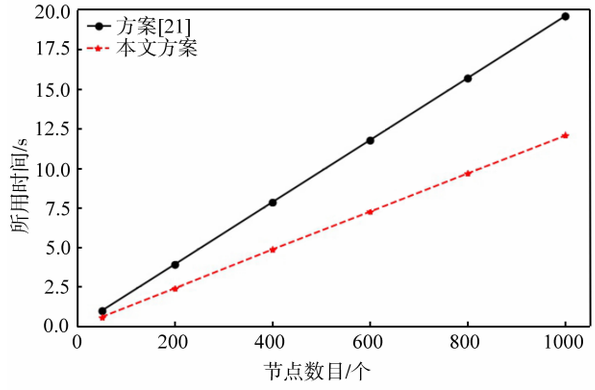

图2 批量验证n个签名的时间对比图

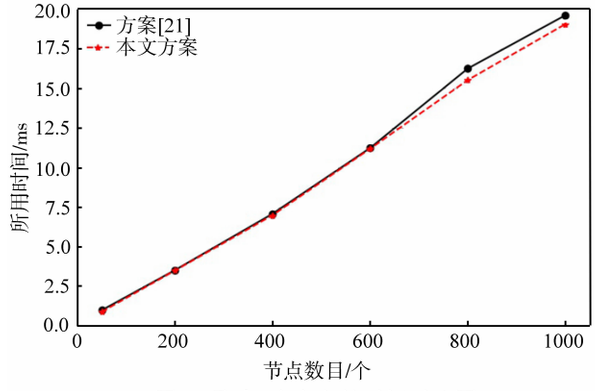

图3 聚合n个密文的时间对比图

通过上述分析可以看出,本文的 SDA 方案不但可

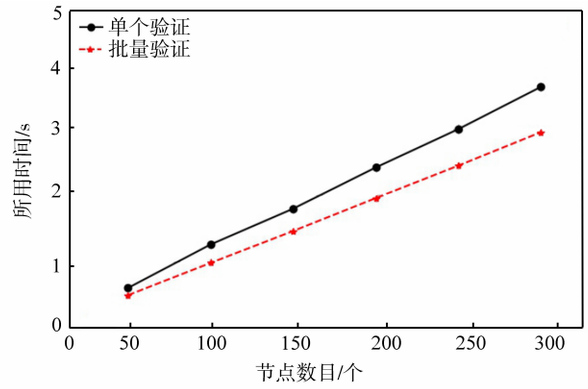

图4　电力服务中心验证n个聚合密文的时间对比图

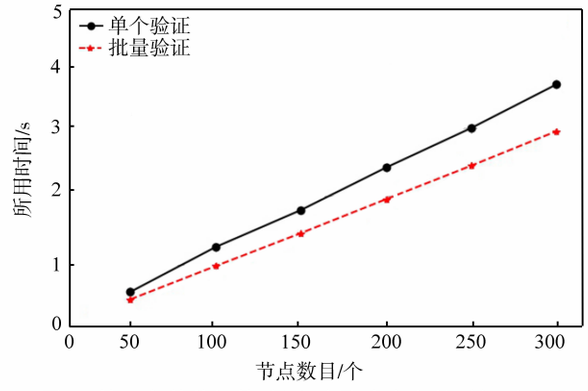

图5　第三方仲裁机构验证n个聚合密文的时间对比图

以保证智能电表数据的安全性和隐私性,而且具有较高的运行效率. 和现有方案相比,降低了数据收集与聚合阶段的计算开销和通信成本,提高了效率.

6　结束语

针对智能电网中的用户电表数据安全和隐私保护问题,本文提出了一个在标准模型下能够抵抗选择明文攻击的数据安全聚合方案. 该方案引入第三方仲裁机构,允许其解密聚合数据包来处理电表用户与电力服务中心的纠纷. 此外,本文方案中的收集器、电力服务中心和第三方仲裁机构都具有批量验证的功能,提升了智能电网系统中数据处理的效率. 经过理论分析与实验比较表明,本文的 SDA 方案不但能够有效保护用户电表数据的隐私和安全,并且比现有技术具有更高的执行效率.

参考文献

[1] 张东霞,苗新,刘丽平,等. 智能电网大数据技术发展研究[J]. 中国电机工程学报,2015,35(1):2 – 12.
Zhang Dong-xia, Miao Xin, Liu Li-ping, et al. Research on development strategy for smart grid big data[J]. Proceedings of the Csee, 2015, 35(1): 2 – 12. (in Chinese)

[2] SKOPIK F. Security is not enough! On privacy challenges in smart grids[J]. International Journal of Smart Grid and Clean Energy, 2012, 1(1): 7 – 14.

[3] 石沙沙,孙文红,江明建,等. 基于分布式数据聚合的智能电网隐私保护协议研究[J]. 信息网络安全,2015,15(12):59 – 65.
Shi Sha-sha, Sun Wen-hong, Jiang Ming-jian, et al. Research on smart grid privacy protocol based on distributed data aggregation[J]. Netinfo Security, 2015, 15(12): 59 – 65. (in Chinese)

[4] 李增鹏,等. 一种基于全同态加密的智能电网数据交换隐私保护方案[J]. 信息网络安全,2016,16(3):1 – 7.
Li Zeng-peng, et al. A privacy preservation scheme for data exchange of smart grid based on homomorphic encryption [J]. Netinfo Security, 2016, 16(3): 1 – 7. (in Chinese)

[5] Mcdaniel P, Mclaughlin S. Security and privacy challenges in the smart grid[J]. IEEE Security & Privacy, 2009, 7(3): 75 – 77.

[6] Sand G, Tsitouras L, Dimitrakopoulos G, et al. A big data aggregation, analysis and exploitation integrated platform for increasing social management intelligence[A]. Proceedings of the IEEE International Conference on Big Data [C]. USA: IEEE, 2014. 40 – 47.

[7] Cost P, Donnelly A, Rowstron A I, et al. Camdoop: exploiting in-network aggregation for big data applications[A]. Proceedings of the 8th USENIX Conference on Networked Systems Design and Implementation[C]. USA: USENIX, 2012. 3 – 3.

[8] Efthymiou C, Kalogridis G. Smart grid privacy via anonymization of smart metering data[A]. Proceedings of the IEEE International Conference on Smart Grid Communications[C]. USA: IEEE, 2010. 238 – 243.

[9] Fan C N, Huang S Y, Lai Y, et al. Privacy-Enhanced data aggregation scheme against internal attackers in smart grid [J]. IEEE Transactions, 2014, 10(1): 666 – 675.

[10] Yu C, Chen C, Kuo S, et al. Privacy-preserving power request in smart grid networks[J]. IEEE Systems Journal, 2014, 8(2): 441 – 449.

[11] 张木玲. 智能电网中若干安全和隐私问题的研究[D]. 上海:上海交通大学,2014. 43 – 56.
Zhang Mu-ling. Security and privacy issues in smart grid [D]. Shanghai: Shanghai Jiaotong University, 2014. 43 – 56. (in Chinese)

[12] 夏卓群,等. 一种基于虚拟环架构的电力用户隐私保护方法研究[J]. 信息网络安全,2018,18(2):48 – 53.
Xia Zhuo-qun, et al. Research on a privacy protection method for power users based on virtual ring architecture [J]. Netinfo Security, 2018, 18(2): 48 – 53. (in Chinese)

[13] 王晓晗,李雄伟,张阳,等. 一种基于故障注入的硬件木马设计[J]. 军械工程学院学报,2015,27(5):57 – 61.
Wang Xiao-han, Li Xiong-wei, Zhang Yang, et al. Hardware Trojan design based on fault injection[J]. Journal of Ordnance Engineering College,2015,27(5):57 – 61. (in Chinese)

[14] Wang Y J, Pang H H, Deng R H, et al. Securing messaging services through efficient signcryption with designated equality test[J]. Information Sciences,2019,490(3):146 – 165.

[15] Wang Y J, Ding Y, Wu Q H, et al. Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs[J]. IEEE Transactions on Information Forensics and Security,2019,14(7):1779 – 1790.

[16] 曹波,朱祝英,吴峥,等. 智能电网下隐私保护技术研究与应用[J]. 计算机与数字工程,2017,45(9):1809 – 1813.
Cao Bo, Zhu Zhu-ying, Wu Zheng, et al. Research and application of privacy protection technology in smart grid [J]. Computer & Digital Engineering,2017,45(9):1809 – 1813. (in Chinese)

[17] 龚凡. 基于群签名的智能电网用电量统计及电费的缴纳方案[D]. 西安:西安电子科技大学,2013. 29 – 37.
Gong Fan. Colletcing consumption data and dynamic billing system based on group signature[D]. Xi'an: Xidian University,2013. 29 – 37. (in Chinese)

[18] 陈明. 标准模型下可托管的基于身份认证密钥协商[J]. 电子学报,2015,43(10):1954 – 1962.
Chen Ming. Escrowable identity-based authenticated key agreement in the standard model[J]. Acta Electronica Sinica,2015,43(10):1954 – 1962. (in Chinese)

[19] Wang X F, Mu Y, Chen R M, et al. An efficient privacy-preserving aggregation and billing protocol for smart grid [J]. Security and Communication Networks, 2016, 9(17):4536 – 4547.

[20] 余勇,叶云,黄刘生,等. 一种面向智能电网的隐私保护数据聚合协议[J]. 小型微型计算机系统,2016,37(5):1097 – 1101.
Yu Yong, Ye Yun, Huang Liu-sheng, et al. Privacy preserving data aggregate protocol for smart grid[J]. Journal of Chinese Computer Systems,2016,37 (5):1097 – 1101. (in Chinese)

[21] Wang Z W. An identity-based data aggregation protocol for the smart grid[J]. IEEE Transactions on Industrial Informatics,2017,13(5):2428 – 2435.

[22] Ding Y, Wang B Y, Wang Y J, et al. Privacy and integrity protection of metering data in smart grid[A]. Proceedings of the 14th Asia Joint Conference on Networked Systems Design and Implementation [C]. Japan: IEEE, 2019. 40 – 47.

[23] 张思佳,顾春华,温蜜. 智能电网中的数据聚合方案分类研究[J]. 计算机工程与应用,2019,55(12):83 – 89.
Zhang Si-Jia, Gu Chun-hua, Wen Mi. Analysis and research on data aggregation scheme in smart grid [J]. Computer Engineering and Applications,2019,55(12):83 – 89. (in Chinese)

[24] He D, Kumar N, Lee J, et al. Privacy-preserving data aggregation scheme against internal attackers in smart grids [J]. Wireless Networks,2016,22(2):491 – 502.

[25] He D, Kumar N, Zeadally S, et al. Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries [J]. IEEE Transactions on Smart Grid,2017,8(5):2411 – 2419.

[26] Shi Z G, Sun R X, Lu R X, et al. Diverse grouping-based aggregation protocol with error detection for smart grid communications[J]. IEEE Transactions on Smart Grid, 2015,6(6):2856 – 2868.

[27] Guan Z, Si G. Achieving privacy-preserving big data aggregation with fault tolerance in smart grid[J]. Digital Communications and Networks,2017,3(4):242 – 249.

[28] Boneh D, Boyen X. Short signatures without random oracles and the SDH assumption in bilinear groups[J]. Journal of Cryptology,2008,21(2):149 – 177.

作者简介

丁 勇 男,1975 年生,重庆潼南人. 博士,博导,鹏程实验室研究员,桂林电子科技大学计算机与信息安全教授,主要研究方向为非对称加密、隐私保护和大数据等.
E-mail:stone_dingy@126.com

王冰尧 女,1994 年生,河南洛阳人. 桂林电子科技大学在读研究生,主要研究方向为应用密码学.
E-mail:1592194691@qq.com

王玉珏(通讯作者) 男,1981 年生,安徽宿州人,博士,硕导,桂林电子科技大学计算机与信息安全学院副教授,主要研究方向为应用密码学、云计算和系统安全.
E-mail:yjwang@guet.edu.cn