

文章编号:1000-5641(2015)05-0046-15

面向智能电表的隐私保护技术综述

田秀霞¹, 李丽莎², 孙超超¹, 刘大明¹

(1. 上海电力学院 计算机与信息工程学院, 上海 200090;

2. 上海电力学院 电子与信息工程学院, 上海 200090)

摘要: 随着智能电网和通信技术的发展,智能电表的普及应用受到越来越多的重视.一方面,智能电表为用户合理用电和电力公司有效供电、高效收费带来了便利,而另一方面细粒度的智能电表数据泄露用户用电行为等敏感信息,用户隐私泄露也成为最大的安全威胁.主要从智能电表端的身份隐私保护技术和数据隐私保护技术两个方面来综述国内外相关研究.对比分析了现有隐私保护技术的隐私保护强度、计算开销、传输开销等;提炼了智能电表仍然面临的安全与隐私挑战,并探讨了该领域未来的研究趋势与方向.

关键词: 智能电表; 隐私保护; 身份隐私; 数据隐私

中图分类号: TP309 **文献标识码:** A **DOI:**10.3969/j.issn.1000-5641.2015.05.004

Review on privacy protection approaches in smart meter

TIAN Xiu-xia¹, LI Li-sha², SUN Chao-chao¹, LIU Da-ming¹

(1. College of Computer and Information Engineering, Shanghai University of
Electric Power, Shanghai 200090, China;

2. College of Electronic and Information Engineering, Shanghai University of
Electric Power, Shanghai 200090, China)

Abstract: With the development of the smart grid and communication technologies, smart meters have attracted increasing attentions. On the one hand, smart meters brought considerable convenience for users with better electricity consumption management and power companies' effective power supply and efficient billing; on the other hand, it raised security threat that fine-grained smart meter data could reveal users' private information. This paper conducted a thorough survey on existing solutions mainly from identity privacy protection approach and data privacy protection approach. We deeply compared their privacy-related factors, such as the strength of privacy protection, computational overhead, transmission overhead. Finally, we investigated the remaining challenges to protect user privacy in smart meter and discussed plausible and promising trends and directions for future research.

Key words: smart meter; privacy protection; identity privacy; data privacy

收稿日期:2015-06

基金项目:国家重点基础研究发展计划(973)(2010CB328106);国家自然科学基金(61202020);上海市自然科学基金(12ZR1411900)

第一作者:田秀霞,女,博士,教授,研究生导师,研究方向为数据库安全、隐私保护和基于密码学的访问控制,以及面向电力用户侧的安全计算. E-mail: xxtian@shiep.edu.cn.

0 引 言

智能电网^[1],或称未来电网,旨在为电力用户提供更稳定,更可靠的电能.随着智能电网和通信技术的发展,电力用户与电力公司间的双向通信成为可能,而用户侧的智能电表是双向通信中的关键部件.智能电表实时监测智能电器用电情况,使电力用户更经济有效的管理他们的用电量.由于智能测量技术,即 AMI(Advanced Metering Infrastructure)^[2]越来越成熟,电力公司也越来越多的采用远程实时监测和采集智能电表的电量数据,不仅有效提高了抄表质量、抄表效率和经济效益^[3],而且能够有效调整电力供应,满足电力用户实时用电需求及避免多余发电.

然而,智能电表为电力用户和电力企业带来便利的同时,也同样给电力用户带来了隐私威胁^[4].细粒度的智能电表数据泄露人们生活习性等隐私信息,一旦被攻击者掌握,将会给电力用户造成难以估量的损失.欧盟信息保护监督组织主任助理 Giovanni Buttarelli 说:“智能电表数据对于分析能源使用情况十分有用,但与此同时,也可能被一些别有用心的人用来进行市场销售、广告推销或差别定价等.”英联合王国能源主任 Christine McGourty 指出,解决智能电表数据保护和用户隐私问题是重中之重.国际隐私权组织的 Anna Fielder 指出,消费者对智能电表的实时监测感到不安,人们不想在被人监视之下生活.2010 年,美国的斯科茨谷市发生了一起“Stop Smart Meter”的游行示威,人们对智能电表的“不信任感”达到高潮.2013 年,泸州查处首例智能电表窃电行为,窃电 4032 度.英国《卫报》称,到 2019 年智能电表将普及所有英国家庭,这将会涉及到更多的个人隐私问题.越来越多的事实表明,面向智能电表的隐私保护问题是亟待解决的,因此近年来研究人员一直致力于寻求在最少泄露个人隐私信息的情况下享受智能电表带来便利的方法.

面向智能电表隐私保护技术主要包括智能电表身份隐私保护技术和智能电表数据隐私保护技术.在给出两种隐私保护技术定义之前,我们先介绍智能电表的三个主要因素:智能电表身份、智能电表实时(细粒度)电量数据和智能电表总电量数据.智能电表实时电量数据泄露用户隐私信息,而智能电表总电量,即计费周期内的总电量,几乎不会泄露用户隐私信息;攻击者只有掌握智能电表身份及其实时电量数据才能对具体用户实施攻击,掌握任何其他单一因素或两两组合因素均不能对用户产生隐私或安全威胁.因此,智能电表身份隐私保护技术是指保护智能电表身份不被攻击者知晓;若攻击者知晓智能电表实时电量数据,但不知智能电表身份,其所掌握的隐私信息就无法定位到具体某个用户.智能电表数据隐私保护技术是指保护智能电表实时电量数据不被攻击者知晓;若攻击者知晓智能电表身份,但其不知晓智能电表用户隐私信息,其就无法实施攻击.本文将针对智能电表身份隐私保护技术和智能电表数据隐私保护技术两方面内容对现有工作进行总结.

1 系统模型

图 1 为智能电网通信网的一般模型,其中主要涉及 4 个实体:智能电器、智能电表、集中器和电力公司,下面依次介绍每个实体的功能和作用.

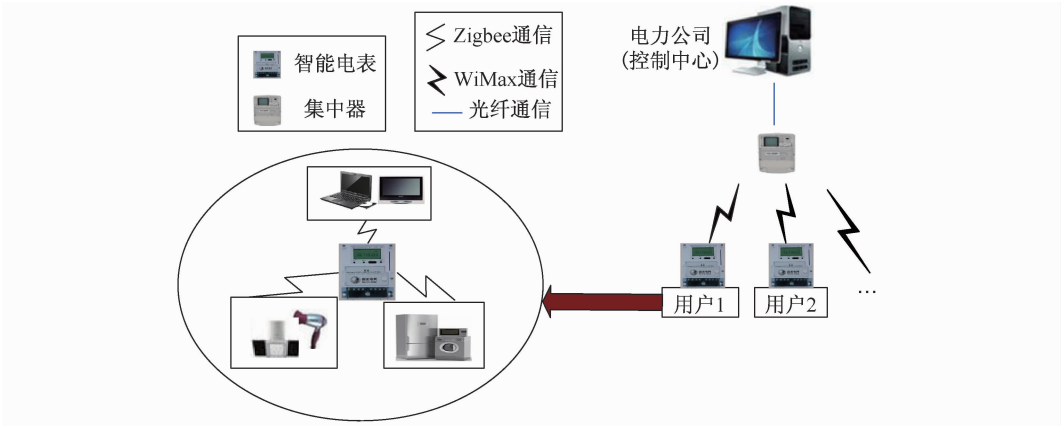


图 1 智能电网通信网框架图

Fig. 1 Framework of communication network in smart grid

1.1 智能电器

智能电器(如电视、洗衣机等),在智能电网中各自有一个 IP 地址,其用电数据通过 Zig-Bee 无线网实时传送给智能电表(见图 1). ZigBee,功率要求低、网络配置和管理规定简单,优于其他短距离无线通信(如 WiFi),被选为智能电器与智能电表间的通讯工具^[5-6].

1.2 智能电表

智能电表是智能电网的智能终端,有很多身份属性^[7],如电表编号、URI(Uniform Resource Identifier)等,这些身份属性用于身份认证或其他目的,本文将用户和智能电表看成一个整体,即用户的身份与智能电表的身份一致. 智能电表以双向多种费率计量、双向数据通信和防窃电等功能为特征,实时监测^[8]智能电器的用电情况,为用户提供详细的用电信息,使用户更好的管理他们的用电量^[9]. 智能电表数据可以通过有线网,如 RS485、M-BUS 或电力线载波^[3,10]也可以通过无线网,如 WiMax(Worldwide Interoperability for Microwave Access)、3G 等其他无线宽带技术^[5-6],实时传送到集中器,图 1 显示为其中一种通信方式.

1.3 集中器

集中器是连接终端、计算机或通信设备的中心连接点设备,用来抄写智能电表数据并定时把电表数据通过有线网,如 LAN(Local Area Network)、光纤^[5-6],或无线网,如 GPRS(General Packet Radio Service)、CDMA(Code Division Multiple Access)^[3]等通信方式传送给电力公司(控制中心),实现智能电表与控制中心的实时在线连接. 集中器使得远程抄表的效率、费用以及数据完整率、数据共享等方面得到很大改善.

1.4 电力公司

电力公司是智能电表数据的处理中心,也是供配电的控制中心. 电力公司采集智能电表数据有两个目的:一是计收电费;二是分析数据,根据数据分析调整电量供应,避免多余发电和促进电力有效可靠传输.

2 攻击模型

攻击类型分为两种:内部攻击和外部攻击.

2.1 内部攻击

内部攻击者包括恶意用户、semi-honest 电力公司和恶意中间实体。

恶意用户:恶意用户可能窥探其他用户的用电数据,试图获取他人隐私信息实施恶意的,如报复;恶意用户也可能抵赖其用电量,企图少交甚至不交电费。

semi-honest 电力公司:电力公司的 semi-honest 性是指电力公司内部可能有恶意的员工。电力公司需要知道用户用电信息计收电费,如总用电量一均一电价计费,实时用电量一分时电价计费,但恶意员工可能根据智能电表身份及其细粒度的电量数据,窥探用户隐私。

恶意中间实体:智能电表与电力公司通信途径的中间实体^[11],可能是恶意的,它可能根据其知道的背景信息,窥探用户隐私。

2.2 外部攻击

外部攻击者包括窃听者(Eavesdropper)和截获者(Interceptor). 窃听者意图通过窃听智能电表与电力公司间的通信,获取智能电表数据信息进而窥探用户隐私. 截获者妄图截获智能电表与电力公司的通信内容,并利用一些数据分析技术(如数据挖掘)获取智能电表用户隐私信息。

针对上述攻击模型,主要有两种解决方法:①身份隐私保护技术,使电力公司只知晓智能电表电量数据不知晓其身份,但同时支持智能电表的身份认证;②数据隐私保护技术,使电力公司只知智能电表身份不知其电量数据,但同时保证智能电表数据无法被外部攻击者窃听或截取. 表 1 是智能电表隐私保护技术中所用字符的含义。

表 1 字符含义
Tab.1 Notations

字符	含义
PC	电力公司
Pub_R	实体 R 的公钥
$E_{Pub_R}(J)$	表示用实体 R 的公钥加密信息 J
$Sig(\cdot)$	表示签名
$J Q$	表示信息 J 和信息 Q 的连接,无实质意义

3 智能电表身份隐私保护技术

根据技术划分,智能电表身份隐私保护技术可以分为三类:基于签名的身份隐私保护技术,基于证书的身份隐私保护技术和基于零知识证明的身份隐私保护技术. 表 2 对比分析了三类技术的隐私保护强度、计算消耗、传输消耗及占用内存大小。

表 2 身份隐私保护技术性能对比

Tab.2 Performance comparisons of identity privacy protection

身份隐私保护技术	隐私保护强度	计算开销	传输消耗	内存占用
签名	盲签名	强	中	中
	环签名	强	大	小
	HMAC	中	小	中
	承诺方案	弱	小	中
证书	中	中	中	中
零知识证明	中	小	大	大

3.1 基于签名的身份隐私保护技术

基于签名的身份隐私保护技术一般情景是,智能电表利用一些签名方法(如盲签名)实现身份认证的同时使电力公司无法知晓智能电表的真实身份 ID. 根据所采用的签名技术,基于签名的身份隐私保护技术又可分为盲签名、环签名、哈希信息验证码(Hash-based Message Authentication Code, HMAC)和承诺方案(Commitment Scheme)四类.

3.1.1 盲签名

Jeanno 等^[12]采用盲签名^[13]实现身份认证的同时保护了智能电表身份隐私. 盲签名旨在使签名者不知其所签信息的具体内容.

假设有两方 Alice 和 Bob. Alice 的公钥/私钥对,即 $(e, n)/(d, n)$,基于 RSA 公钥加密生成. Bob 生成的消息 M ,需要 Alice 签名. 在签名之前, Bob 用随机盲因数 F 盲化消息 M ,即 $X = (MF^e) \bmod n$,然后将 X 发送给 Alice. Alice 对 X 进行签名,即 $Sig(X) = X^d \bmod n$,但其不知所签的真实信息 M ,然后其将 $Sig(X)$ 发送给 Bob. Bob 做计算得到真实消息 M 的签名 $Sig(M)$,计算过程如下: $Sig(X) \times F^{-1} = X^d \bmod n \times F^{-1} = (M^d F^{ed}) \bmod n \times F^{-1} = X^d \bmod n = Sig(M)$,其中 $F^{ed} = 1$.

在 Jeanno 等的方案中,电力公司签名的是包含定值电量信息的凭证 $C_i(CID, date, value)$,其中 CID 是凭证标识符, $date$ 是签发日期, $value$ 是定值电量;智能电表将每个 CID 盲化,然后提交盲化因数证明 $value$ 的有效;智能电表凭借已签名的凭证实时向电力公司提交电量,在此过程中电力公司不知智能电表身份;在计费阶段,智能电表发送未使用的签名凭证和身份给电力公司,电力公司根据该智能电表总的签名凭证与未使用的签名凭证得到该智能电表用户总的用电量.

从该方案可以看出,在电量提交阶段电力公司知道智能电表实时电量数据但不知道其身份,在计费阶段电力公司知道智能电表身份和其总电量但不知道智能电表实时电量数据,因此保护了用户隐私. 但该方案有两个明显的缺陷:一是需要预先生成大量的标有定值电量的签名凭证,在实际中很难实施;二是智能电表实时电量数值(即用户实时用电量)受到限制,不能根据负荷需要请求电量.

盲签名隐私保护效果好,其本身的算法很简单,但为了防止无效签名需要在签名之前进行多次的验证,增加了算法的计算开销和传输开销.

3.1.2 环签名

Yu 等^[14]利用环签名^[15],实现身份认证和身份隐私保护的同时避免了签名凭证的大量生成. 环签名旨在使 verifier 确信消息 M 是被团体成员中一位签名,但其无法知道具体是哪位成员的签名. 下面是环签名技术的简述.

假设 Alice 要向 Bob(verifier)发送消息 M ,需要 Alice 的签名,但 Alice 不想让 Bob 知道消息 M 是自己发送的,即不想让 Bob 知道是自己的签名. Alice 就让团体中其他 m 个成员一起对消息 M 签名. 假设每位成员的私钥为 x_i ,公钥为 $Y_i = x_i P$ (P 为较大的素数), Alice (U_u) 作如下计算:对于所有的 $i \in (1, \dots, m)$, U_u 选择随机数 a_i ,计算 $R_i = a_i P$;然后选择一个随机数 a ,计算 $R_u = aP - \sum_{i=1, i \neq u}^m H(MP, R_i) Y_i$ 和 $\sigma = [a + \sum_{i=1, i \neq u}^m a_i + x_u H(xP, R_u)] \bmod q$ (q 为较大素数且 $q \neq P$),生成环签名 $(R_1, \dots, R_m, Y_1, \dots, Y_m, \sigma)$,并将 $(MP, R_1, \dots, R_m, Y_1, \dots, Y_m, \sigma)$ 发送给 Bob. Bob 验证签名,作如下计算:对于所有的 $i \in (1, \dots, m)$,计算 $h_i = H(MP,$

R_i), 验证等式 $\sigma P = \sum_{i=1}^m (R_i + h_i Y_i)$ 是否成立, 具体的等式验证如式

$$\sum_{i=1}^m (R_i + h_i Y_i) = R_u + h_u Y_u + \sum_{i=1, i \neq u}^m (R_i + h_i Y_i) = aP + h_u Y_u + \sum_{i=1, i \neq u}^m R_i = \sigma P.$$

在 Yu 等的方案中, 智能电表用第三方密钥分发中心 KDC(Key Distribution Center)的公钥加密自己的实时电量数据, 其真实身份用电力公司公钥加密生成伪随机身份, 并利用环签名实现身份的认证. 电力公司能解密伪随机身份得到智能电表的真实身份, 但其无法解密电量信息; KDC 解密电量信息并合计电量, 为了防止电力公司关联智能电表真实身份与其电量信息, KDC 给总电量添加干扰, 即 $M'_{sum} = M_{sum} + b$ (其中, M_{sum} 为总电量, b 为一个随机数, M'_{sum} 为干扰后的总电量), 并将 M'_{sum} 发送给电力公司, KDC 知道智能电表细粒度的电量信息但其不知道智能电表真实身份, 无法窥探用户隐私. 但该方案明显的缺陷是用户上交的电费可能不是其应交的电费, 而且也无法防止 KDC 与 semi-honest 电力公司的共谋.

和盲签名相比, 环签名的优点是签名可以重复利用, 无需预先生成大量的签名, 与盲签名具有一样的隐私保护效果; 缺点是计算复杂性 (包括计算开销、内存占用)、传输开销相对较大.

3.1.3 哈希信息验证码(HMAC)

Chim 等在文献[16]中及 Fouda 等^[5-6] 利用哈希信息验证码(HMAC)生成签名实现身份认证. HMAC 技术很简单, 仍以 Alice 和 Bob 为例. Alice 向 Bob 发送消息 M 之前需对 M 作 HMAC 签名, 即 $H_s(M)$, 其中 s 是 Alice 和 Bob 双方都知道的密钥, $H(\cdot)$ 表示一个哈希函数, $H_s(M)$ 表示用密钥 s 对消息 M 实现哈希运算, 之后 Alice 发送 $(H_s(M), M)$ 给 Bob. Bob 用已知的密钥 s 及收到的消息 M 作哈希运算, 验证所得的结果与所收到的 $H_s(M)$ 是否相等, 若相等则验证成功.

在文献[16]的方案中, 每个智能电表有一个嵌入式设备, 系统初始密钥 K 预先载入智能电表嵌入式设备及集中器中; 智能电表提交实时电量数据时, 先生成伪随机身份 PID (生成方法与 Yu 等^[14] 方案中一样), 然后生成 HMAC 签名, 即 $\sigma = H_K(PID || E_{Pub_{PC}}(M) || T)$, 其中 M 为电量, T 为提交电量的时间, 并将 $(\sigma, PID, E_{Pub_{PC}}(M), T)$ 发送给集中器; 集中器用密钥 K 作初步的签名认证, 成功后将 $(PID, E_{Pub_{PC}}(M), T)$ 发送给电力公司; 电力公司用自己的私钥解密得到智能电表真实身份及其电量 M , 以此作电费计算. 该方案有两个明显的缺陷: 一是智能电表嵌入的硬件设备是方案的关键部件, 但其易毁坏; 二是电力公司知道用户实时用电信息及其智能电表身份, 可能窥探用户隐私. Fouda 等利用 PKI(Public Key Infrastructure)进行智能电表间的初始认证, 然后利用 Diffie-Hellman 技术建立 HMAC 签名进行智能电表间的安全通信, 但他们没有考虑智能电表数据被内部攻击者窃取的风险.

HMAC 的计算复杂性、传输开销较小, 但隐私保护效果较弱.

3.1.4 承诺方案(Commitment Scheme)

Chim 等在文献[17]中基于承诺方案(Commitment Scheme)实现用户用电计划制定及身份认证的同时保护用户隐私. 下面具体介绍承诺方案. 承诺方案允许一方 (如 Alice) 承诺一个值, 这个值对另一方 (如 Bob) 保密; 然后 Alice 向 Bob 揭露承诺值, 证明自己的揭露值与承诺值一样. 承诺方案一般包含两个函数: $Commit(\cdot)$, 指以一个秘密值和一个承诺钥匙为输入产生一个承诺; $CheckReveal(\cdot)$, 指以承诺、秘密值和一个解除承诺钥匙为输入产

生一个正值或负值. 假设 Alice 想向 Bob 承诺一个秘密值 X . Alice 首先生成一个承诺钥匙和一个解除承诺钥匙, 分别为 CK_A 和 DK_A ; 然后 Alice 计算 $C_A = \text{Commit}(X, CK_A)$, 并将其发送给 Bob. 需要兑现承诺时, Alice 将 C_A 、 X 和 DK_A 发送给 Bob; Bob 调用函数 $\text{CheckReveal}(C_A, X, DK_A)$ 验证 Alice 的承诺. RSA 公钥加密算法, 由于它的随机填充性^[18], 是一种常见的承诺功能的实现.

在文献[17]的方案中, 智能电表在用电之前, 需向电力公司提交近期的用电计划, 如增加用电或减少的用电量, $U_i = [u_{i0}, u_{i1}, \dots, u_{i(n-1)}]$ 表示未来各个时段内需要增加或减少的电量; 智能电表在提交 U_i 之前, 用电力公司的公钥加密 U_i 各个时段的用电计划, 即 $E_i = [e_{i0}, e_{i1}, \dots, e_{i(n-1)}]$, 其中 $e_{ix} = E_{\text{Pub}_{PC}}(u_{ix})$, 然后作哈希运算并生成承诺, 即 $H_i = h(ID_i, T, U_i)$ 、 $C_i = \text{Commit}(H_i, CK_i)$, 其中 ID_i 为智能电表身份, T 为签名生成的时间, CK_i 为承诺钥匙; 在计费阶段智能电表需提交 ID_i 、 T 、 U_i 和 C_i 验证自己的承诺, 电力公司根据智能电表承诺的用电计划与其实际用电作比较, 看是否相符. 该方案中电力公司公钥/私钥基于同态密钥体制生成, 电力公司得到的是 HAN(Home Area Network)内所有用户的用电计划, 无法知道每户的用电计划, 但电力公司知道每户的实际用电情况, 存在隐私泄露的风险.

承诺方案明显的缺点是承诺兑现时用户隐私随之泄露.

3.2 基于证书的身份隐私保护技术

基于证书的身份隐私保护技术一般情景是, 可信第三方或电力公司向智能电表颁发证书, 智能电表凭借证书提交电量, 电力公司依据证书计收电费.

Lee 等^[19]引入可信第三方 CA(Certificate Authority)颁发证书给智能设备(智能电表和智能电器)实现智能设备间的相互认证, 但没有考虑智能电表和电力公司间的认证. Efthymiou 等^[20]假设每个智能电表有两个 ID, 即 HFID(High-Frequency ID)和 LFID(Low-Frequency ID). HFID 是匿名的, 用于传输敏感信息, 即智能电表实时电量数据; LFID 具有归属属性, 用于传输非敏感信息, 即智能电表在计费周期(如一周或一个月)内请求的总电量. 电力公司颁发智能电表传输总电量的证书 CDP(Client Data Profile), 其中包含 LFID; CDP 生成后, 相隔足够长的时间(以避免电力公司关联两个证书)智能电表生成传输实时电量的证书 ADP(Anonymous Data Profile), 其中包含 HFID, 然后智能电表将 CDP 和 ADP 发送给可信第三方(如电表制造商), 第三方关联两个证书后智能电表可凭借 ADP 实时提交电量. 该方案明显的漏洞是第三方知道关键性信息, 即 HFID 和 LFID 的关联信息, 造成隐患.

相比基于签名的身份隐私保护技术, 基于证书的身份隐私保护技术优点是算法简单, 计算消耗及传输消耗较小; 缺点是隐私保护强度弱, 内存占用较大, 大多依赖可信第三方.

3.3 基于零知识证明的身份隐私保护技术

基于零知识证明(Zero-knowledge Proofs)的身份隐私保护技术一般情景是, 用户根据自家智能电表的电量信息和电费定价政策计算电费, 然后利用零知识证明协议向电力公司证明身份及电费计算的准确性. 零知识证明是一种涉及双方的协议, 即 prover 向 verifier 证明并使其相信自己知道或拥有某项任务的一个解决方法 solution, 但证明过程不能向 verifier 泄漏关于 solution 的机密信息. 零知识证明^[21]具有以下重要性能: ① 一个有效的 prover, 其拥有某项任务的一个解决方案 solution, 几乎能够完全取信于 verifier; ② 一个无效的 prover, 其不知道该项任务的任何 solution, 几乎完全不能取信于 verifier; ③ verifier 无法获得有关 prover 所知的 solution 的任何有用信息.

Markham 等^[22]将设定好的 solution,即伪随机标签 $\{r_i\}$ 和密钥集 $\{k_j\}$,预先载入智能电表和电力公司的服务器. 智能电表每次提交的电量标有不同的伪随机标签. 在电费计量阶段,用户根据电费定价政策及电量信息计算电费 E ,并将 E 提交给电力公司,接着用户提交 $\{r_i\}$ 和 $\{k_j\}$ 证明身份和电费计算的正确性. 该方案明显的缺陷是智能电表需长期存储大量的伪随机标签,造成存储压力且伪随机标签易泄露. Rial 等^[23]指出离散对数知识证明^[24]、一些元素在不同表示中平等的知识证明^[25]、时间间隔检查证明^[26]、范围证明^[27]及任何先前的两个元素分离或结合的证明^[28],其 Σ -协议的结果可以通过 Fiat-Shamir 启发式^[29]转化为随机语言模型的零知识证明. Rial 等利用承诺方案制定不同的定价政策实现零知识的身份认证和 TOU(Time of Use)计费.

基于零知识证明的身份隐私保护技术算法简单,计算消耗较小,但内存占用较大,隐私保护效果一般.

4 智能电表数据隐私保护技术

智能电表数据隐私保护技术的关键思想是干扰智能电表数据,模糊用户用电模式. 干扰智能电表数据主要采用基于数据聚合技术和基于充电电池技术实现. 表 3 对比分析了两类技术的隐私保护强度、计算消耗、成本大小的特点.

表 3 数据隐私保护技术性能对比

Tab. 3 Performance comparisons of data privacy protection

数据隐私保护技术		隐私保护强度	计算开销	成本
数据聚合	同态加密	弱	中	低
	同态加密 + 密钥共享	强	大	中
	掩蔽式	强	中	低
	充电电池	强	小	高

4.1 基于数据聚合技术

基于数据聚合技术^[30]是指利用加密方法使得电力公司能够计算多个用户的总电量而不知道每个用户的用电量,即模糊用户用电模式,实现电力公司分析数据的目的.

4.1.1 同态加密

同态加密的主要思想是接收者不需要解密每个密文,而对所有密文进行某种运算,最后只需解密一次便得到想要的结果. 我们以常见的 Paillier 密码体制为例^[31]作说明. 例如, Alice 想知道 Bob 和 David 发送的数据之和,假设 Alice 的公钥为 $Pub_A = (n, g)$. Bob 和 David 要发送的数据分别为 x_1, x_2 ,在发送之前,他们分别用 Alice 的公钥加密自己的数据,即 $E_{Pub_A}(x_1) = g^{x_1} r_1^n \bmod n^2$ 和 $E_{Pub_A}(x_2) = g^{x_2} r_2^n \bmod n^2$,其中 r_1 和 r_2 是随机数,然后分别将密文发给 Alice; Alice 计算 $g^{x_1} r_1^n \times g^{x_2} r_2^n = g^{x_1 + x_2} (r_1 r_2)^n = E_{Pub_A}(x_1 + x_2)$,然后用自己的私钥解密一次得到 x_1, x_2 之和.

Li 等^[11]以智能电表为子节点,电力公司为根节点,根据网络拓扑创建广度优先的虚拟聚合树. 在虚拟聚合树中,子节点层智能电表用电力公司的公钥加密自己的数据后上传给父节点层的智能电表,父节点层的智能电表将自己的数据用电力公司公钥加密后与子节点上传的数据做乘法并将其结果上传,最终数据上传到电力公司,电力公司用自己的私钥解密一次得到所有节点的数据总和. 在 Li 等的方案中,所有智能电表用一样的密钥加密,隐私保护

效果较弱. Erkin 等^[32]对同态加密作了改进,他们将模 n 分成若干份,每份分发给一个智能电表.以 Alice、Bob 和 David 三个用户为例,假设他们分别拥有随机数 n_1 、 n_2 和 n_3 ,其中 $n_1 + n_2 + n_3 = n$. 他们分别对自己的电量作如下加密,

$$\begin{aligned} \text{Alice: } E_{Pub_A}(m_{1,t}) &= g^{m_{1,t} r^{n_1}} \bmod n^2, \\ \text{Bob: } E_{Pub_A}(m_{2,t}) &= g^{m_{2,t} r^{n_2}} \bmod n^2, \\ \text{David: } E_{Pub_A}(m_{3,t}) &= g^{m_{3,t} r^{n_3}} \bmod n^2. \end{aligned}$$

电力公司得到聚合数据为

$$\prod_i E_{Pub_A}(m_i) = g^{\sum_i m_{i,t} r^{\sum_i n_i}} \bmod n^2 = g^{\sum_i m_{i,t} r^n} \bmod n^2 = E_{Pub_A}(\sum_i m_{i,t}).$$

Erkin 等的方案相当于每个智能电表用不同的密钥加密自己的电量,隐私保护效果得到了改善.但在该方案中若有一个用户未提交自己的电量,电力公司将无法得到所有用户总电量.

4.1.2 同态加密与密钥共享相结合

Garcia 等^[33]提出一个基于密钥共享的隐私保护协议.在协议中,每个用户将自己的电量分成若干份,然后将每份分发给不同的用户,具体如下,

$$\begin{aligned} \text{Alice: } m_{1,t} &= [m_{1,t}(1) + m_{1,t}(2) + m_{1,t}(3)] \bmod \varphi, \\ \text{Bob: } m_{2,t} &= [m_{2,t}(1) + m_{2,t}(2) + m_{2,t}(3)] \bmod \varphi, \\ \text{David: } m_{3,t} &= [m_{3,t}(1) + m_{3,t}(2) + m_{3,t}(3)] \bmod \varphi. \end{aligned}$$

以 Alice、Bob 和 David 三个用户为例,其中 φ 为较大的素数, $m_{1,t}$ 、 $m_{2,t}$ 和 $m_{3,t}$ 分别表示 Alice、Bob 和 David 在 t 时刻的电量. Alice 将 $m_{1,t}(1)$ 自己保存,将 $m_{1,t}(2)$ 、 $m_{1,t}(3)$ 分别用 Bob、David 公钥加密之后发送给电力公司,需要指出的是用户的公钥均具有同态性. Bob 和 David 与 Alice 的做法一样. 电力公司收到后,将用相同密钥加密的数据相加,计算如下:

$$E_{Pub_i}(m'_{i,t}) = \prod_{j \neq i} E_{Pub_j}(m_{j,t}(t)) = E_{Pub_i}(\sum_{j \neq i} m_{j,t}(t)).$$

其中, Pub_1 、 Pub_2 和 Pub_3 分别是 Alice、Bob 和 David 的公钥. 然后电力公司发送 $E_{Pub_1}(m'_{1,t})$ 给 Alice. Alice 用自己的私钥解密得 $m'_{1,t}$ 并加上 $m_{1,t}(1)$, 得 $m_{1,t}(1) + m_{2,t}(1) + m_{3,t}(1)$ 并将其发送给电力公司. 仍然, Bob 和 David 与 Alice 的做法一样. 这样电力公司得到 Alice、Bob 和 David 在 t 时刻的总电量,无法得到每个用户的用电量,且每个用户也无法获知其他用户的电量.

相比于同态加密,此种方法隐私保护效果较好,但由于引入共享密钥方案,增大了计算开销.

4.1.3 掩蔽式技术

掩蔽(masking)式方法是指给用户电量添加掩蔽随机数,即 $E(M) = (m + k) \bmod n$,其中 m 表示电量, k 表示掩蔽随机数, n 为较大的素数.

Kursawe 等^[34]提出两种协议. 第一种是聚合协议:每个用户使用掩蔽随机数 x_i 掩蔽自己的用电量,即 $m_{i,t} + x_i$,所有用户加密后的数据相加能自动消除掩蔽随机数,即协议的输出为 $\sum m_{i,t}$. 第二种是比较协议:每个用户输出 $g_j^{m_{i,t} + x_i}$,其中 $g_j = H(j)$, $H(\cdot)$ 为哈希函数, j 为每次测量计算的标识符, x_i 为掩蔽随机数,电力公司得到聚合量如式

$$\prod_{i=1}^3 g_j^{m_{i,t} + x_i} = g_j^{\sum_{i=1}^3 m_{i,t} + x_i} \bmod p.$$

以 Alice、Bob 和 David 三个用户为例,其中 p 为较大的素数. 由于 discrete-log 问题^[34], 电力公司无法得到聚合量的真实值,但其知晓 g_j 和聚合量的估计值 $\tilde{m}_{total,t}$. 电力公司计算 $g_j^{\tilde{m}_{total,t}}, g_j^{\tilde{m}_{total,t}-1}, g_j^{\tilde{m}_{total,t}+1}, \dots$, 直到找到与所接收的聚合量值相近或相等为止.

聚合协议的算法简单,计算开销小,但隐私保护强度弱;而比较协议算法复杂,计算开销大,无法得到聚合量真实值,但隐私保护效果好.

Kursawe 等提出四种生成掩饰随机数的方法:一种基于密钥共享,其他三种基于 D-H 协议. 但这些方法计算开销较大. 这里我们只概述一种基于 D-H 协议的掩饰随机数生成方法,具体如下:假设每个智能电表的身份为 ID_i , 私钥为 X_i , 公钥为 $g_j^{X_i}$, 每个智能电表将其公钥发送给其它所有智能电表;智能电表验证其它智能电表的公钥后,计算 $g_j^{x_i} = \prod_{k \neq i} (g_j^{X_k})^{(-1)^{k < j} X_i}$, 其中检索值 $k < i$ 的结果为 1, 否则为 0, x_i 为每个智能电表要生成的掩饰随机数,显然 x_i 之和为 0, 即 $\sum_i x_i = \sum_i \sum_{k \neq i} (-1)^{k < j} X_k X_i = 0$.

在 Ács 等^[35]的方案中,掩饰随机数的生成没有规则限制,利用简单的加法实现数据聚合和隐私保护的同时大大减少了计算量,但该方案抵抗外部攻击的能力较弱. 仍以 Alice、Bob 和 David 三个用户为例概述 Ács 等的聚合方案. 首先每个用户随机地选择其他几个用户作为交换掩饰随机数的对象,智能电表间的耦合是双向定向的,即 Alice 选择了 Bob 和 David, 则 Bob 和 David 也就选择了 Alice. 一旦 Alice 和 Bob 相互选定,他们生成一个掩饰随机数 x_{12} 作为他们的共享密钥. Alice 将自己的电量加上 x_{12} , Bob 将自己的电量减去 x_{12} . Alice 与 David 生成另一个掩饰随机数 x_{13} , 并将其加到自己电量. 最后 Alice 再用与电力公司间共享的密钥 K_{1A} 加密, 结果为

$$\text{Alice: } E_{K_{1A}}(\tilde{m}_{1,t}) = (m_{1,t} + x_{12} + x_{13} + K_{1A}) \bmod p.$$

同样, Bob 和 David 加密自己的电量得

$$\text{Bob: } E_{K_{2A}}(\tilde{m}_{2,t}) = (m_{2,t} - x_{12} + x_{23} + K_{2A}) \bmod p,$$

$$\text{David: } E_{K_{3A}}(\tilde{m}_{3,t}) = (m_{3,t} - x_{13} - x_{23} + K_{3A}) \bmod p.$$

其中 K_{2A} 、 K_{3A} 分别为 Bob 与电力公司, David 与电力公司间的共享密钥. 然后 Alice、Bob 和 David 分别将加密后的电量发送给电力公司. 电力公司将所有密文直接加和, 掩饰随机数自动消除, 然后电力公司减去与三人共享的密钥, 得到聚合量的真实值.

文献[35]还提到一种方法,即利用 Laplace 噪音生成掩饰随机数,该方法可以依据用户需求设置数据的隐私保护水平,但电力公司无法得到聚合量的真实值. 电力公司收到的聚合数据为 $\sum m = \sum_i m_{i,t} + Lab(a)$, 其中 $Lab(a)$ 为 Laplace 噪音^[36], $\sum m$ 有 ϵ -差分隐私^[37]保护效果. 文献[35]利用服从伽马分布的随机变量生成 Laplace 噪音,即每个智能电表提交数据之前给自己的电量数据添加伽马随机变量,即 $m_{i,t} + g_1(i, a) - g_2(i, a)$, 其中 $g_1(i, a)$ 、 $g_2(i, a)$ 为伽马随机变量,且 $\sum_i (g_1(i, a) - g_2(i, a)) = Lab(a)$. Rastagi 等^[38]根据定理 $Z = Y_1^2 + Y_2^2 - Y_3^2 - Y_4^2$ (其中 Z 是服从 $Lap(2b^2)$ 的随机变量, $Y_j \sim N(0, b)$ ($j = 1, 2, 3, 4$) 是高斯随机变量), 利用高斯分布随机数据生成 Laplace 噪音实现噪音随机数的分布式聚合.

表 4 汇总了以上掩饰随机数生成技术.

表 4 掩蔽随机数生成技术汇总

Tab. 4 Summary of the generation of masking-random number

掩蔽随机数生成技术	掩蔽随机数生成	
	规则	计算开销
Kursawe ^[34]	加和为零	大
$\hat{A}cs^{[35]}$ (加法)	任意生成	小
$\hat{A}cs^{[35]}$ (噪音)、Rastagi ^[38]	满足 ϵ -差分隐私水平	中

4.2 基于充电电池技术

Varodayan 等^[39]、Kalogridis 等^[40]使用充电电池来保护家庭用电信息. 基于充电电池的电网基本结构如图 2 所示. 信息流从智能电器到电力公司: 电池输入负荷为用户侧智能电器总负荷; 电池的输入负荷, 即智能电表向电力公司提交的电量数据, 受智能电器总负荷和电池充放电的共同影响. 电力流从电力公司经充电电池输送到用户侧智能电器. 充电电池有三个基本功能: ①将来自电力公司的电能传送给智能电器; ②存储来自电力公司的电能以备; ③将存储的电能传送给智能电器. 这样, 充电电池和电力公司可以单独或同时向智能电器供电, 智能电表数据就不能直接反映智能电器的用电信息, 模糊了用户用电模式, 保护了用户的隐私信息.

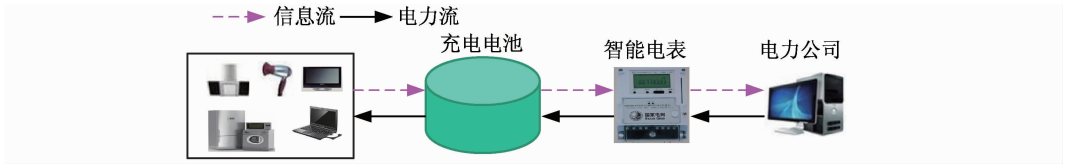


图 2 充电电池电网基本机构

Fig. 2 Framework of communication network with Rechargeable Battery

Varodayan 等假设充电电池的输入负荷 X 、输出负荷 Y 为随时间变化的二进制序列, 分别以 $\{x_1, x_2, \dots\}$ 、 $\{y_1, y_2, \dots\}$ 表示. 充电电池有两种状态: 0 为放电, 1 为充电. 在任意离散的时间, 智能电器消耗 0 或 1 单元的电量, 电力公司提供 0 或 1 单元的电量. 若知道 t 时刻的电池状态 b_t , 则在 $t + 1$ 时刻电池状态 b_{t+1} 、电器消耗状态、电池输入负荷 x_{t+1} 及其输出负荷 y_{t+1} 有三种可能的组合情况, Varodayan 等假设每一种情况的发生具有一定的概率并对此制定出两种随机电池政策, 利用仿真技术^[41]定量分析了两种电池政策信息泄露速率, 结果表明随机电池政策信息泄露速率相对较低, 有很好的隐私保护效果. Kalogridis 等利用电力路由调整充电电池的充放电以抵消负荷电量的变化, 这样用户负荷基本保持不变, 攻击者无法根据用户负荷变化来窥探用户隐私.

相比于数据聚合方法, 充电电池方法的优点是计算开销小; 缺点是成本高, 隐私保护强度相对较弱.

5 智能电表隐私保护技术小结

本节根据第 2 节的攻击模型对现有工作中两类隐私保护技术进行抗攻击能力汇总, 如表 5 所示, 每种隐私保护技术都有其不同的抗攻击能力, 其中“√”表示具备某种抗攻击能力, “×”表示不具备某种抗攻击能力.

表 5 隐私保护技术汇总
Tab. 5 Summary of privacy protection

类别		隐私保护技术	内部攻击				外部攻击	
			恶意用户	Semi-honest 电力公司	恶意中间 实体	第三方	窃听器	截获者
身份隐私	盲签名	Jeanno ^[12]	✓	✓	✓	✓	✓	✓
	环签名	Yu ^[14]	✓	✓	✓	✓	✓	✓
	HMAC	Chim ^[16]	✓	×	✓	✓	✓	✓
		Fouda ^[5,6]	×	×	×	✓	✓	✓
	承诺方案	Chim ^[17]	✓	×	✓	✓	✓	✓
	证书	Lee ^[19]	×	×	✓	×	✓	✓
		Efthymiou ^[20]	✓	✓	✓	×	✓	✓
	零知识证明	Markham ^[22]	✓	✓	✓	✓	✓	✓
		Rial ^[23]	✓	✓	✓	✓	✓	✓
	数据隐私	同态加密	Li ^[11]	×	✓	✓	✓	✓
Erkin ^[32]			×	✓	✓	✓	✓	✓
同态加密 + 密钥共享		Garcia ^[33]	✓	✓	✓	✓	✓	✓
掩蔽式		Kursawe ^[34]	×	✓	✓	✓	✓	✓
		Ács ^[35]	✓	✓	✓	✓	✓	✓
		Rastagi ^[38]	×	✓	✓	✓	✓	✓
充电电池		Varodayan ^[39]	×	✓	✓	✓	✓	✓
		Kalogridis ^[40]	×	✓	✓	✓	✓	✓

6 存在的问题和挑战

前面总结的各种研究成果从不同方面解决了智能电表中隐私保护问题,但仍存在以下问题和挑战:

(1)提出的智能电表隐私保护技术没有考虑恶意电表用户带来的隐私威胁. 恶意电表用户有可能出于好奇或某种利益,甚至是报复心理,利用智能电网的便利窥探其他用户智能电表数据信息进而实施不法目的;另外,恶意用户有可能抵赖其用电量意图少缴纳甚至不缴纳电费,这将造成电力公司亏损,因此恶意用户不能忽视.

(2)提出的智能电表数据隐私保护技术有充电电池技术和数据聚合技术,而数据注入技术——向智能电表数据注入一些新数据,干扰智能电表数据,模糊用户用电模式——也是智能电表隐私保护的一个研究方向.

(3)随着智能电表的普及,智能电网进入了大数据时代. 海量的实时采集智能电表数据的存储^[42]与计算使得智能电网与云计算的结合成为必然. 但在云计算环境下,如何保护用户隐私不泄露的同时实现智能电表数据的存储与查询是亟待解决的问题. 目前只有极少数文献在做这方面的研究. 文献[43]采用数据分块存储的方式,利用分块关系和混淆技术保护用户隐私.

(4)根据中国电网的现状,电网互联是一个必然趋势^[44]. 国家电力公司称将在 2015 年建成全国统一的联合电网. 随着联合电网平台的搭建,智能电表用户需要访问^[45]众多的电力公司以寻求最宜(如电价优惠或服务周到)的供电部门. 传统意义上,智能电表需要向每个电力公司注册一个身份,用来进行身份认证,则智能电表每访问一个电力公司就需要进行一次身份认证,造成智能电表频繁的身份认证. 如何实现智能电表身份的联合管理^[7],或者说

智能电表只需向一个电力公司进行身份认证,成功后则可访问其他的电力公司而无需再次身份认证,这将是新的研究挑战。

(5)智能电表参数(如尖峰平谷时段),也应该得到安全保护。分时电价在尖峰平谷时段的价位有差异,改变某个时段的时间长度,变会影响用户所缴纳的电费。如,用户可以通过新一代智能型 Web-based 电表集中器 PMC-5151^[46],操作网页浏览器进行前端智能电表的参数设定。而目前关于智能电表参数安全保护的文献极少。

7 总结与展望

本文主要从智能电表身份隐私保护技术和智能电表数据隐私保护技术两个方面回顾了最近几年来国内外在智能电表隐私保护领域的主要研究成果。身份隐私保护技术主要从基于签名的身份隐私保护技术、基于证书的身份隐私保护技术和基于零知识证明的身份隐私保护技术展开分析;数据隐私保护技术主要从数据聚合技术和充电技术展开分析。最后归纳总结了智能电表隐私保护领域中目前存在的问题和挑战。相信随着智能电表隐私保护问题的解决,智能电表将普及每个家庭并有效调节用户用电习惯。

[参 考 文 献]

- [1] GELLINGS C W. The smart grid: enabling energy efficiency and demand response[M]. Lilburn GA: Fairmont Press, 2009.
- [2] 路保辉,马永红. 智能电网 AMI 通信系统及其数据安全策略研究[J]. 电网技术, 2013, 37(8): 2244-2249.
- [3] 厦门毅仁信息技术有限公司. 智能小区水表、电表、气表、热力表能耗计量远程集中抄表系统[R/OL]. (2014-03-23)[2015-06-01]. <http://www.gongkong.com/webpage/news/201403/2014032309333700001.htm>
- [4] 田秀霞,高明,王晓玲,等. 数据库服务——安全与隐私保护[J]. 软件学报, 2010, 21(5): 991-1006.
- [5] FOUDA M M, FADLULLAH Z M, KATO N, et al. A lightweight message authentication scheme for smart grid communications[J]. IEEE Transactions on Smart Grid, 2011, 2(4): 675-685.
- [6] FOUDA M M, FADLULLAH Z M, KATO N, et al. Towards a light-weight message authentication mechanism tailored for smart grid communications[C]//Proceedings of the IEEE International Conference on Information Networking. Shanghai, 2011: 1018-1023.
- [7] ELISA B, KENJI T. Identity management concepts, technologies, and systems[M]. Boston: Artech House, 2011.
- [8] 刘薇. 智能电表数据安全保护技术探讨[J]. 电源技术应用, 2013(6): 404.
- [9] 王耀辉,金海燕,朱莉. 基于用户隐私保护的智能电表设计[J]. 黑龙江科技信息, 2014(7): 73-75.
- [10] 春波绿影. 电力线载波自动抄表系统-智能电表之自动抄表主流方案盘点[R/OL]. (2013-01-28)[2015-06-01]. http://www.elecfans.com/dianyuan/306612_4.html
- [11] LI F, LUO B, LIU P. Secure Information Aggregation for Smart Grids Using Homomorphic Encryption[C]//Proceedings of the 1st IEEE International Conference on Smart Grid Communication. Gaithersburg, MD, 2010: 327-332.
- [12] CHEUNG J C L, CHIM T W, YIU S M, et al. Credential-based privacy-preserving power request scheme for smart grid network[C]//Proceedings of the IEEE Global Telecommunications Conference. Houston, 2011: 1-5.
- [13] CHAUM D. Blind signatures for untraceable payments[C]//Proceedings of CRYPTO'82 Conference on Advances in Cryptology. California USA: Springer Berlin Heidelberg, 1982: 199-203.
- [14] YU C M, CHEN C Y, KUO S Y, et al. Privacy-preserving power request in smart grid networks [J]. IEEE Systems Journal, 2014, 8(2): 441-449.
- [15] LIN X, LU R, ZHU H, et al. ASRPAKE: An anonymous secure routing protocol with authenticated key ex-

- change for wireless ad hoc networks[C]//Proceedings of the IEEE ICC. Glasgow, 2007: 1247-1253.
- [16] CHIM T W, YIU S M, LUCAS C K, et al. PASS: Privacy-preserving authentication scheme for smart grid network[C]//Proceedings of the IEEE International Conference on Smart Grid Communications. Brussels, 2011: 196-201.
- [17] CHIM T W, YIU S M, HUI L C K, et al. PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart Grid[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(1): 85-97.
- [18] KALISKI B, STADDON J. RSA Cryptography Specifications Version 2.0[M]. [s.l.]: The Internet Society, 1998.
- [19] LEE S, BONG J, SHIN S, et al. A security mechanism of smart grid AMI network through smart device mutual authentication[C]//Proceedings of 2014 IEEE International Conference on Information Networking. Phuket, 2014: 592-595.
- [20] EFTHMIOU C, KALOGRIDIS G. Smart grid privacy via anonymization of smart metering data[C]//Proceedings of the 1st IEEE International Conference on Smart Grid Communications. Gaithersburg, MD, 2010: 238-243.
- [21] BELLARE M, GOLDREICH O. On defining proofs of knowledge[C]//Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer Berlin Heidelberg, 1992: 390-420.
- [22] MARKHAM M M, SHENOY P, FU F, et al. Private memoirs of a smart meter[C]//Proceedings of the 2010 ACM BuildSys International Conference on Embedded Systems for Energy-Efficient Buildings. Zurich: ACM, 2010: 61-66.
- [23] RIAL A, DANEZIS G. Privacy-Preserving Smart Metering[C]//Highlights of the Information Security Solutions Europe 2012 Conference. Europe: Springer Berlin Heidelberg, 2012: 105-115.
- [24] SCHNORR C. Efficient signature generation for smart cards[J]. Journal of Cryptology, 1991, 4(3):239-252.
- [25] CHAUM D, PEDERSEN T. Wallet databases with observers[C]//Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. California, USA: Springer Berlin Heidelberg, 1993:89-105.
- [26] OKAMOTO T. An efficient divisible electronic cash scheme[C]//Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology. California, USA: Springer Berlin Heidelberg, 1995: 438-451.
- [27] BOOUDOT F. Efficient proofs that a committed number lies in an interval[C]//Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. Bruges, Belgium: Springer Berlin Heidelberg, 2000: 431-444.
- [28] CRAMER R, DAMGARD I, SCHOENMAKERS B. Proofs of partial knowledge and simplified design of witness hiding protocols[C]//Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology. California, USA: Springer Berlin Heidelberg, 1994: 174-187.
- [29] FIAT A, SHAMIR A. How to prove yourself: Practical solutions to identification and signature problems[C]//Proceedings of the Advances in Cryptology. [s.l.]: Springer Berlin Heidelberg, 1987: 186-194.
- [30] ERKIN Z, TRONCOSPASTORIZA J R, LAGENDIJK R L, et al. Privacy-preserving data aggregation in smart metering systems: an overview[J]. IEEE Signal Processing Society, 2013, 30(2): 75-86.
- [31] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Proceedings of the 17th International Conference on Theory Application Cryptographic Techniques. Prague, Czech Republic: Springer Berlin Heidelberg, 1999: 223-238.
- [32] ERKIN Z, TSUDIK G. Private computation of spatial and temporal power consumption with smart meters[C]//Proceedings of the International Conference on Applied Cryptography and Network Security. Singapore: Springer Berlin Heidelberg, 2012: 561-577.
- [33] GARCIA F D, JACOBS B. Privacy-friendly energy-metering via homomorphic encryption[C]//Proceedings of the 6th Workshop on Security and Trust Management. Athens, Greece: Springer Berlin Heidelberg, 2010: 226-238.
- [34] KURSAWE K, DANEZIS G, KOHLWEISS M. Privacy-friendly aggregation for the smart-grid[C]//Proceedings

- of the 11th International Symposium on Privacy Enhancing Technologies. Waterloo, Canada: Springer Berlin Heidelberg, 2011: 175-191.
- [35] ÁCS G, CASTELLUCCIA C. I have a DREAM! (differentially private smart metering)[C]//Proceedings of the 13th international conference on Information hiding. [s.l.]: Springer Berlin Heidelberg, 2011: 118-132.
- [36] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis[C]//Proceedings of the 3rd Theory of Cryptography Conference. New York: Springer Berlin Heidelberg, 2006: 265-284.
- [37] DWORK C. Differential privacy: A survey of results[C]//Proceedings of the 3rd International Conference on Theory and Applications of Models of Computation. Xi'an China: Springer Berlin Heidelberg, 2008: 1-19.
- [38] RASTAGI V, NATH S. Differentially private aggregation of distributed time-series with transformation and encryption[C]//Proceedings of the 2010 ACM SIGMOD International Conference on Management of data. Indiana: ACM, 2010: 6-11.
- [39] VARODAYAN D, KHISTI A. Smart meter privacy using a rechargeable battery: minimizing the rate of information leakage[C]//Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing. Prague; Czech Republic, 2011: 1932-1935.
- [40] KALOGRIDIS G, EFTHYMIOU C, DENIC S, et al. Privacy for smart meters: towards undetectable appliance load signatures[C]//Proceedings of the IEEE International Conference on Smart Grid Communications. Gaithersburg, MD, 2010: 232-237.
- [41] ARNOLD D M, LOELIGER H A, VONTOBEL P O, et al. Simulation-based computation of information rates for channels with memory[J]. IEEE Transactions on Information Theory, 2006, 52(8): 3498-3508.
- [42] TIAN X X, SHA C F, WANG X L, et al. Privacy preserving query processing on secret share based data storage [C]//Proceedings of the 16th International Conference on Database Systems for Advanced Applications(DASFAA 2011). Hong Kong China: LNCS6587, 2011: 108-122.
- [43] 任梦吟,毛琪琦,马婷,等. 基于云计算的智能电表用户表单隐私保护. 智能电网, 2014(4): 123-128.
- [44] 国家电力公司称将在 2015 年建成全国统一的联合电网[J]. 中国石油和化工, 2001, (3):11.
- [45] TIAN X X, HUANG L, WANG Y, et al. DualAcE: fine-grained dual access control enforcement with multi-privacy guarantee in DaaS[J]. Security and Communication Networks, 2014, 8(8): 1494-1508.
- [46] 林稼弘. 泓格发表新式智能型 Web-Based 电表集中器[R/OL]. (2014-02-19)[2015-06-01]. [http://gb-www.digitimes.com.tw/tw/iac/shwnws.asp? cat = 10&cat1 = 10&cnlid = 19&id = 368253](http://gb-www.digitimes.com.tw/tw/iac/shwnws.asp?cat=10&cat1=10&cnlid=19&id=368253).

(责任编辑 李万会)