Chapter 15
Techniques, Taxonomy, and Challenges of Privacy Protection in the Smart Grid

Suleyman Uludag, Sherali Zeadally and Mohamad Badra

15.1 Introduction

The scope of the rights of individuals has been constantly evolving. It has long been established that the full protection of life and property falls within the individual rights coverage for most cultures throughout the human history. While the early boundaries of the "right to property" have only incorporated the tangible dimension, the intangible portion has been expanding [1] rapidly since the industrial revolution. One important component of the intangible part is defined by the right to privacy, coined by Warren and Brandeis in 1890 [1].

A strong positive correlation between technological development and privacy concerns is almost universally agreed [2]. In Warren and Brandeis' terminology, "the right to be left alone" has expanded to include other personally associable phenomena such as audio, photographs, video, data, and more recently biometric identification and genetic data) rather than mere physical property. Computerization, automation, transmission, and storage of data, enabled by recent advances in telecommunications, Internet technologies, and mobile and cloud computing services, have increased the importance and relevance of the term "privacy".

S. Uludag (✉)
The University of Michigan—Flint, Michigan, USA
e-mail: uludag@umich.edu

S. Zeadally
College of Communication and Information, University of Kentucky,
Lexington, KY, USA
e-mail: szeadally@uky.edu

M. Badra
Zayed University, Dubai 19282, UAE
e-mail: mohamad.badra@zu.ac.ae

S. Zeadally and M. Badra (eds.), *Privacy in a Digital, Networked World*,
Computer Communications and Networks,
DOI 10.1007/978-3-319-08470-1_15

In spite of its wide usage, the term privacy does not have a universally-agreed-upon definition [3].[1] It is quite remarkable that such an important concept has evaded a formal definition. The concept of privacy has a long history of discussions of importance, from Greek philosophers including Aristotle (public sphere of political activity versus private sphere [3]) and Socrates, to Biblical and Quranic passages [5]. Allen West in his landmark work [2] defines privacy in terms of self-determination as follows:

> Privacy, now, is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Another important document about the principles of privacy protection was developed in 1981 by the Organization for Economic Co-operation and Development (OECD) [6][2] and was later updated in 2013 [7]. Yet, even these guidelines are not observed by many countries. For example, while the European Union seems to be following them, the United States does not.

Widespread adoption of privacy protection mechanisms depends on the political will, which seems to be prioritizing other concerns such as public safety, especially since September 11, 2001. However, the awareness and demand of the public for a stronger adoption and enforcement of the privacy regulations has been increasing unabated. Many recent developments and news such as Wikileaks, US NSA leaks by Edward Snowden, Facebook's recent disclosure of Emotion Experiment, EU's recent ruling on "right to be forgotten," have been keeping the topic of privacy discussions current and fresh in the public sphere, thereby increasing demand for more action.

In line with technological developments, the ever-changing field of ubiquitous applications, and high-level penetration of mobile and other electronic devices, the potential for privacy violation has been increasing in scope. While there is a perceived clash between the technology and privacy protection, there are also many efforts to put the use of technology in its defense. One pioneering work that has spawned quite a lot of attention, interest, and follow-up studies is Chaum's paper [8] in 1985 on providing privacy to individuals and organizations bi-directionally in a secure fashion. He argues for embedding privacy-providing mechanisms in the design and development of the technology by means of cryptography. Chaum's ideas are further developed and formalized under the term of privacy-enhancing technologies (PET) in 1995 [9] and then in 2003 [10]. PET is defined in [10]:

> PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system.

Our work in this chapter is line with the notion of PET, which we use to provide an understanding and awareness of privacy issues, challenges, and threats in the

[1] Some technology company executives have gone so far to declare privacy irrelevant, dead, or even defunct. A more elaborate debunking of these myths can be found in [4].

[2] http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Smart Grid (SG), the next generation of the traditional Power Grid enhanced with state-of-the-art computing and communications technologies. Just as is the case with many engineering and technical decisions, the touted benefits of the SG initiative comes with many risks and trade-offs. The deployment and adoption of Smart Grid technologies have opened up several security issues at the levels of the consumer, the communication, and the energy provider. Security aspects such as confidentiality, authentication, authorization, integrity, and non-repudiation have been extensively investigated and various innovative solutions have been proposed in the literature. There are many publications on SG security, including survey style articles and books, such as [11–36]. While some of these address privacy, explicitly or implicitly, there is a need for an up-to-date coverage of SG privacy techniques. In contrast to most previous works with the SG security focus, our main motivation in this chapter is to review, classify, discuss, and analyze recent SG privacy solutions that have been proposed in the literature. In addition, we also provide a comprehensive treatment of the approaches, mechanisms, and cryptographic tools used in the SG to support the use and design of privacy enforcing techniques.

15.1.1 Contributions

In this chapter, we provide a novel taxonomy of privacy provisioning and protection techniques in the SG. The comprehensive survey, explanations, and discussions of the various privacy schemes are expected to serve as a good reference for those interested in working on privacy issues in the SG environment. The rest of the chapter is organized as follows. Section 15.2 presents a brief SG overview. Section 15.3 discusses the privacy-related problems within the SG environment and explains why privacy is crucial in the overall success of the SG paradigm. Section 15.4 presents a novel taxonomy of recently proposed privacy-preserving solutions for the SG. Section 15.5 explores outstanding challenges that must be addressed in the future and opportunities for new research directions. Section 15.6 concludes the chapter.

15.2 Background on Smart Grid

In this section, we present the main features of the traditional Power Grid followed by the SG vision.

15.2.1 Traditional Power Grid

The current traditional electric Power Grid is considered to be the largest man-made machine in the world. Its infrastructure and operations have not changed

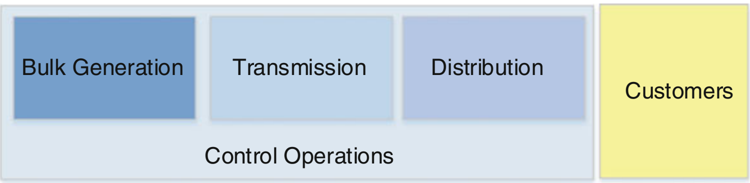


Fig. 15.1 Architecture of the traditional electric power grid

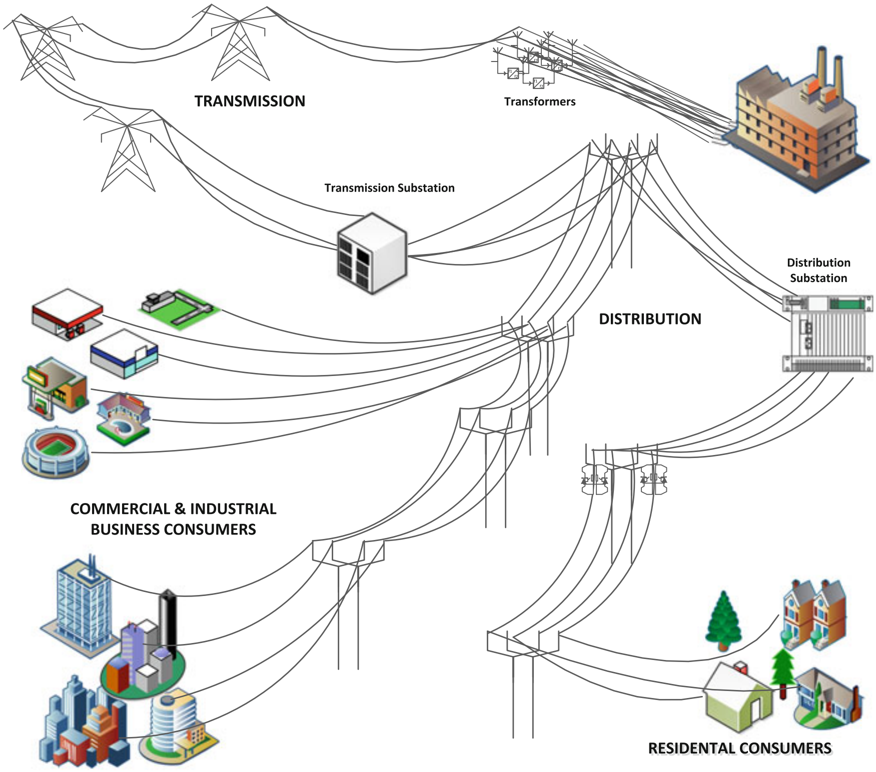


Fig. 15.2 A high-level structure of the current power grid

significantly over the past century. Its architecture mainly consists of four sections, as shown in Fig. 15.1: generation,[3] transmission, distribution, and consumption. A high-level structure of its topology and its components are displayed in Fig. 15.2. The generation of energy is highly centralized and is carried out in bulk mode, such as nuclear systems, hydroelectric systems, wind farms, and others. The high-voltage

[3] We use the terms *generation* and *production* interchangeably.

electricity is relayed in the transmission subsystem over long distances. When handed off to the distribution subsystem, the energy is converted into medium voltage. Through the distribution subsystem substations, the voltage is reduced to lower values and then distributed to a variety of end-users, from commercial, industrial, business, to residential areas. The energy production and distribution schema are supervised by a centralized control system, known as Supervisory Control and Data Acquisition (SCADA) systems, in charge of mapping and visualizing any operational activity in the field as well as controlling the storage and demand of power. In fact, SCADA systems can remotely and locally control the power transmission and distribution based on the current demand and peak loads thereby minimizing unnecessary power generation.

15.2.2 The Smart Grid Vision

SG is a term generally used to refer to an enhancement of the traditional Power Grid, especially, in terms of the computing and communications technologies. SG can be defined as follows [37, 38]:

> The SG can be regarded as an electric system that uses information, two-way, cyber-secure communication technologies, and computational intelligence in an integrated fashion across electricity generation, transmission, substations, distribution and consumption to achieve a system that is clean, safe, secure, reliable, resilient, efficient, and sustainable.

"System of Systems" is a term generally used to qualify the SG in the literature to emphasize its heterogeneity.

Economic development and its sustainability are closely coupled with the effective, efficient, and robust use of the energy. The energy sector, and especially the grid infrastructure, has traditionally focused on the reliable provisioning. Until recently, communications and flow of information have been considered only with extraneous significance. Under an aging and ineffective energy distribution system, unprecedented initiatives have recently been instituted in many countries to improve the Power Grid with the SG. The key facilitators of the SG are two-way energy and information flows between the suppliers and consumers. The conventional supply chain of the energy is being expanded to include alternative sources of energy, such as solar, wind, tidal, biomass, and so on. from a variety of distributed small and large energy producers. The consumers are becoming more active participants by means of such devices as smart meters, smart thermostats, smart appliances. The grand vision of an autonomic, self-healing SG with a dynamic demand response model with pricing still has many challenges, not the very least from the perspective of the networking infrastructure and distributed computing. Demand Response (DR) is defined by the US Department of Energy as follows [39]:

> Changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed

> to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized.

The sheer size of the contemplated SG of the future is to rival the Internet in the number of participants. Smarter generation, transmission, distribution, and consumption of electricity are essential to achieve a reliable, clean, safe, resilient, secure, efficient, and sustainable power system [37].

Some of the noteworthy standardization efforts, high-level conceptual reference models, and roadmaps for the SG are given by the NIST Framework and Roadmap for SG Interoperability Standards [40], IEC SG Standardization Roadmap [41], CEN/CENELEC/ETSI Joint Working Group on Standards for SGs [42], and IEEE P2030 [43]. A conceptual view of the NIST's SG reference model is depicted in Fig. 15.3 with seven domains: customers, markets, service providers, operations, generation, transmission, and distribution. As compared to Fig. 15.2, the generation is no longer in bulk; it also includes the distributed and renewable energy sources as well. It is also worth noting from Fig. 15.3 the bi-directional electricity and information flows and the integration of the renewables. Another important conceptualization is the addition of third-party services to enhance the energy consumption experience of the end-users by means of open markets. The financial gears are also in place: global investment on SG had exceeded $15 billion as of 2013, more than a four-fold increase from 2008 levels [44].

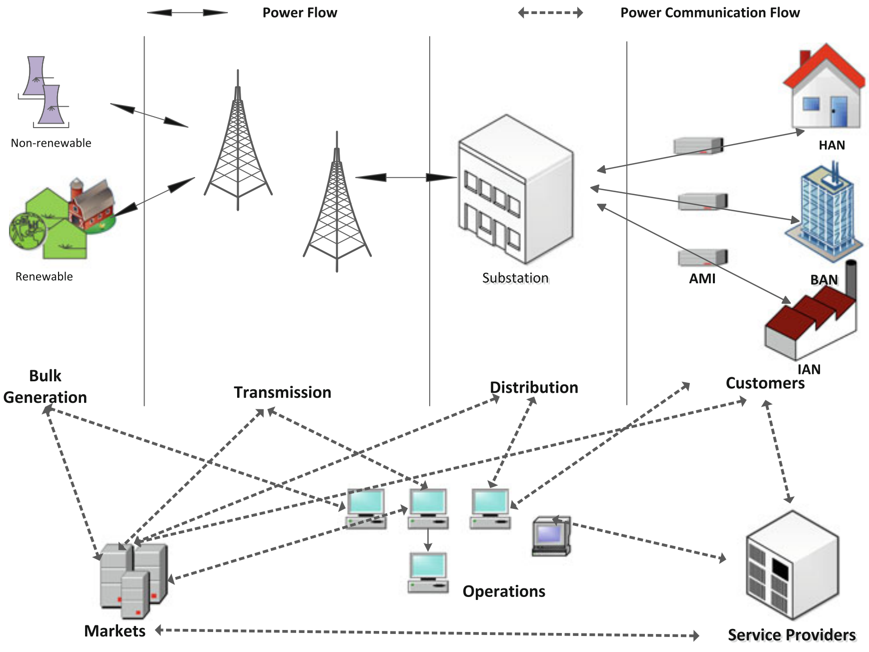


Fig. 15.3 NIST's 7-domain smart grid conceptual model

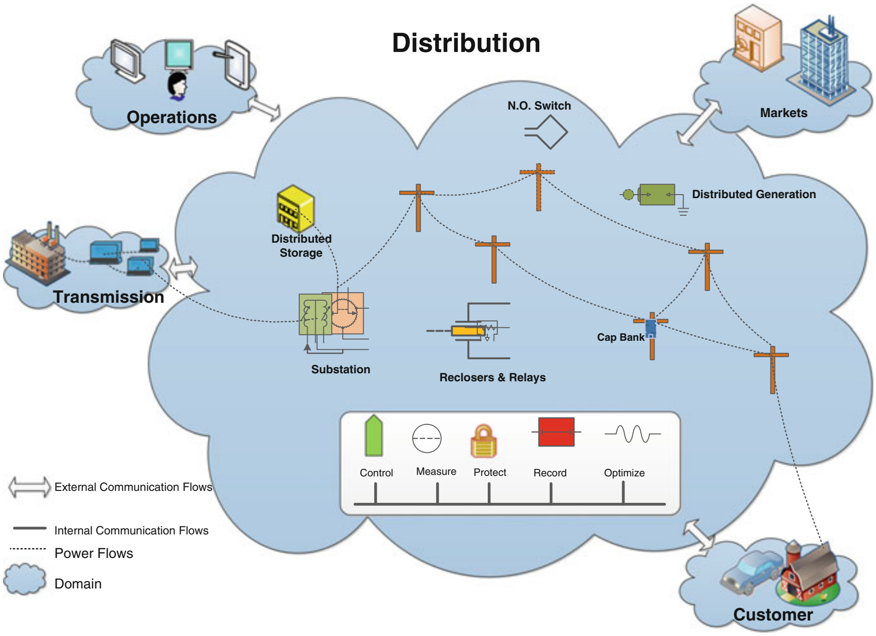


Fig. 15.4 Distribution domain of NIST's smart grid conceptual model

The most relevant domain of the NIST Conceptual Model for this chapter is the Distribution Domain (as depicted in Fig. 15.4), because it is the main physical interface between the end-user and the SG and it is the center of almost all of the potential privacy violations. Note that it is also the Distribution Domain that is responsible for achieving the most widely-cited benefits of the SG which include control, measurement, sensing, data collection and storage, and optimization of operations that take place in or for it.

The anticipated benefits [40] of the SG include:

- Increased power reliability and quality.
- Optimized resources to smoothen the power demand to avoid using expensive peaker capacity.
- Improved resilience to disruption by natural disasters and attacks.
- Automated systems to enable self-healing responses to system disturbances.
- Incorporation of distributed and/or renewable energy sources.
- Reduction of greenhouse emissions.
- Actionable and timely energy usage information to customers.
- Facilitation of plug-in electric vehicles and new energy storage options.

15.2.3 Smart Meters and AMI

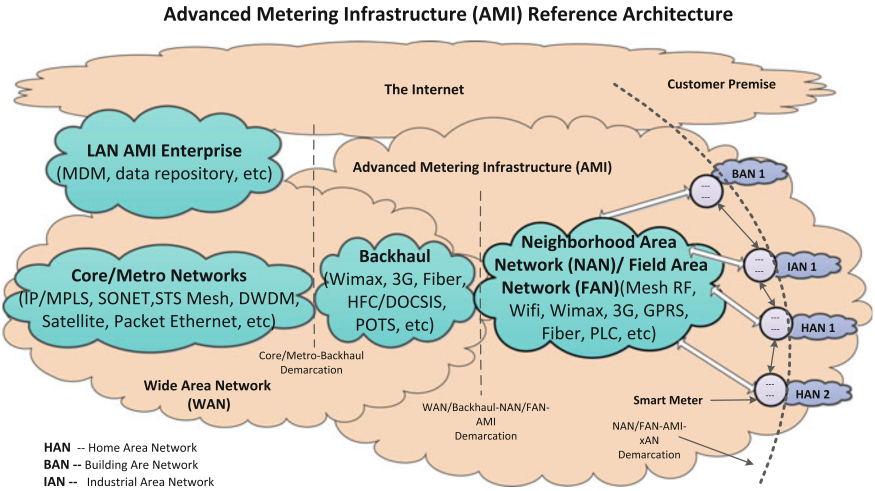
In transitioning from the Power Grid to the SG, Automatic Meter Reading (AMR) has provided a stepping stone functionality. AMR provides automatic collection of data from the energy metering devices and transmission of them to a central location for further processing and analysis.

In the SG, AMR is replaced by Advanced Metering Infrastructure (AMI) which enables bidirectional data transfer between the meter and the grid. The meter that provides such functionality in the SG is usually referred to as a *Smart meter*. Smart meters can read real-time energy consumption information as well as other operationally needed data, such as voltage values, phase angle and the frequency, and so on. Smart meters are solid state programmable devices that can perform many functions allowing users to perform intended tasks by inputting a sequence of instructions into their processing unit and memory. Among some of the tasks that a smart meter can do are [45]: time-based pricing, collecting consumption data for consumer and utility, net metering, loss of power (and restoration) notification, better access and data to manage energy, decision and selection of rate options, remote turn on/turn off operations, load limiting for *bad pay* or demand response purposes, energy prepayment, power quality monitoring, meter tampering and energy theft detection, costs reduction in wrong estimations of billings, service and operational reduction in traditional tasks of metering reading, or communications with other intelligent devices or appliance devices in the home. Although all these tasks may not be supported by a particular meter and there might be other tasks that it can do, the overall idea is that smart meters make it possible to add some kind of intelligence to the network and individual features of each residential consumer.

There are several technologies and applications that have been integrated to perform as one in an AMI system [45] including: smart meters, wide-area communications infrastructure, Home (local) Area Networks (HANs), Meter Data Management Systems (MDMS), and operational gateways working as main collectors. Figure 15.5 shows a model of AMI system as envisioned by NIST from the perspective of computer networking terminology by means of interconnected nodes and clouds to emphasize the bidirectional nature of the communication enabled by AMI.

Another abstraction of the AMI network is presented in Figs. 15.6 and 15.7 that show the concepts of HAN, Building Area Network (BAN), Industrial Area Network (IAN), Neighborhood Area Network (NAN), and Field Area Network (FAN).

There is some notion of hierarchy in AMI when data are collected, processed, and analyzed to optimize the energy use and bring about the benefits of the SG. Such a hierarchy of the communications architecture is depicted in Fig. 15.8. Smart meters span out from feeders, which may also serve as natural data aggregation points. Feeders are controlled by the distribution substations, which are in turn connected to the transmission substations. NIST domains interact with this hierarchy to provide a new level of experience and service as part of the SG.



Advanced Metering Infrastructure (AMI) Reference Architecture
The Internet
Customer Premise
LAN AMI Enterprise
(MDM, data repository, etc)
Advanced Metering Infrastructure (AMI)
BAN 1
Neighborhood Area Network (NAN)/ Field Area Network (FAN)(Mesh RF, Wifi, Wimax, 3G, GPRS, Fiber, PLC, etc)
IAN 1
Backhaul
(Wimax, 3G, Fiber, HFC/DOCSIS, POTS, etc)
Core/Metro Networks
(IP/MPLS, SONET,STS Mesh, DWDM, Satellite, Packet Ethernet, etc)
HAN 1
Core/Metro-Backhaul Demarcation
Wide Area Network (WAN)
WAN/Backhaul-NAN/FAN-AMI Demarcation
Smart Meter
HAN 2
NAN/FAN-AMI-xAN Demarcation
HAN -- Home Area Network
BAN -- Building Are Network
IAN -- Industrial Area Network

Fig. 15.5 Smart grid advanced metering infrastructure reference architecture

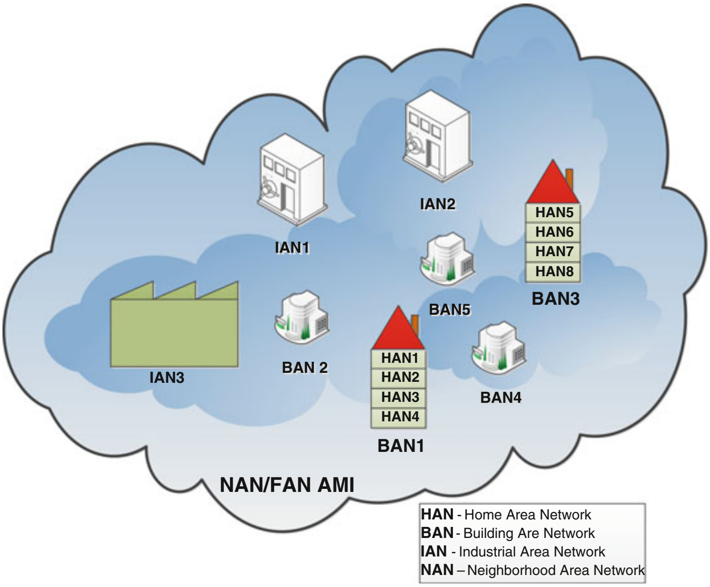


Fig. 15.6 Smart grid advanced metering infrastructure

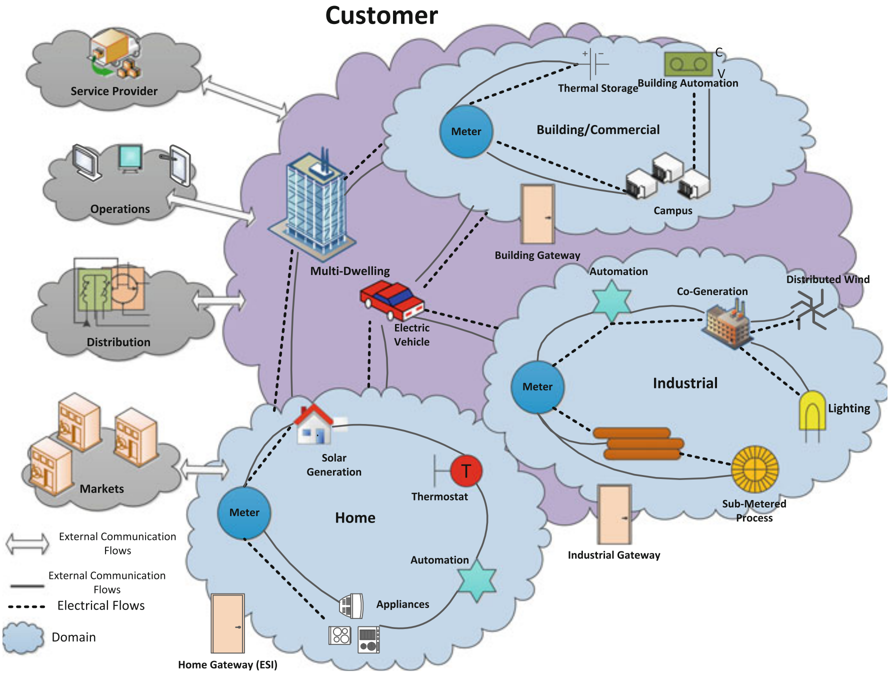


Fig. 15.7 Details of HAN, BAN, and IAN

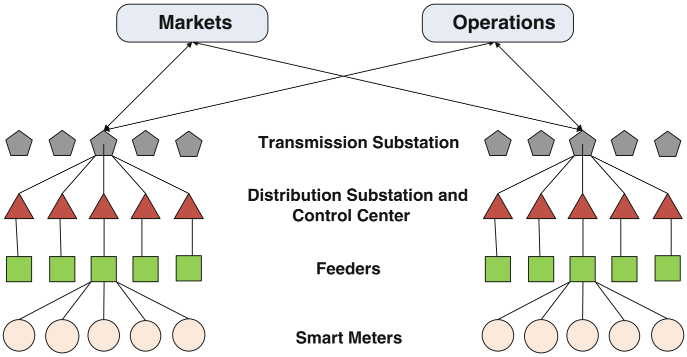


Fig. 15.8 SG communications architecture

15.2.4 Microgrids

One of the many new mechanisms of the SG for power delivery is *microgrids* [46–48]. As a low voltage distribution network, microgrids[4] are autonomous energy

[4] Microgrids are referred to as Distributed Resource Island Systems in IEEE 1547 terminology.

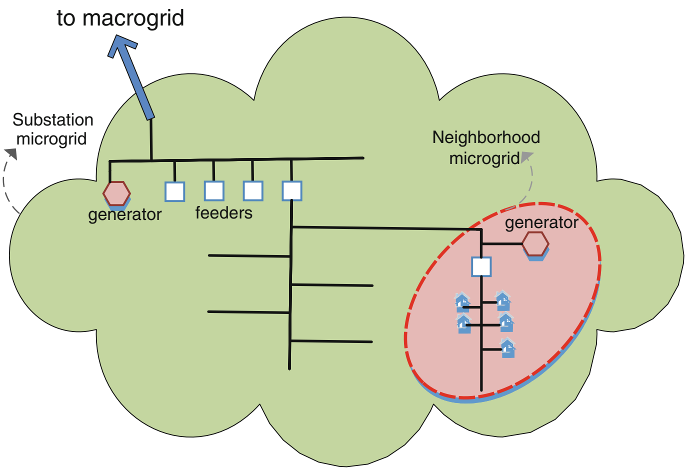


Fig. 15.9 A microgrid model

management systems under the control of a single administrative authority that is capable of operating in parallel to or in intentional or accidental islanded mode from the existing Power Grid. They usually include distributed and renewable energy sources as well as some level of energy storage subsystems. A representation of a microgrid model is shown in Fig. 15.9.

15.3 Smart Grid Privacy Issues

Demand Side Management (DSM) is one of the most important components of the grid of the future [49]. The overarching goal of DSM is to improve the efficiency and effectiveness through energy consumption scheduling. DSM tries to shift and/or reduce the load to achieve its objective by reducing the Peak-to-Average Ratio (PAR), cost, and so on. In [50], energy-cost and PAR minimization are performed with the help of an energy consumption scheduler and a Linear Programming (LP) formulation. Joint energy payment and waiting time minimization are studied in [51]. A game theoretic approach is proposed to maximize the utility function in [52]. In [53], a consumption scheduling algorithm based on Integer Linear Programming (ILP) and game theory is applied to minimize load. In contrast to the current grid, one of the key features of the future grid is to adjust loads dynamically, turning them on or off as needed. This is called *load shedding*. In [54], an optimization framework is proposed to find the minimum amount of load to shed while satisfying load-balancing and shedding constraints. Dynamic load-shedding schemes have been studied in the presence of large disturbances accounting system dynamics [55, 56]. Du and Nelson [57] presents a two-step algorithm for the optimal load shedding in an intentional island.

Given the information collected by smart meters in the SG environment, privacy issues become a vital concern for the success of SG initiatives. In the SG AMI, the privacy goes beyond anonymity to include undetectability of operational status of individual residential appliances. It has been well-known for quite a while that it is trivial to determine sophisticated usage patterns from the smart meter data by using rather simple statistical methods [58, 59]. Prevention of this kind of violation is the main aspect of privacy that we are addressing in this chapter.

The privacy-related issue here is that for proper functioning of the AMI system, very detailed and often precise information about users' electricity usage is needed. Hence, while this smart system could offer many great benefits, it takes away a significant level of privacy a user may like to have. In the rest of this section, we first elaborate on the general notion of privacy and then delve into some details as to why we need to address the privacy concerns explicitly and convincingly.

15.3.1 Basic Privacy Concepts

Privacy may be defined as the claim of individuals, groups, or institutions to determine when, how, and to what extent information about themselves is communicated to others [2]. The notion of privacy may vary from person to person, and from culture to culture. It could also be defined as the right to informational self-determination, that is, individuals must be able to determine for themselves when, how, to what extent, and for what purpose information about them is communicated to others [60]. This term is often related to an entity's (individual, group, or institution) identity or anonymity. As human beings, each of us likes to keep certain information about ourselves confidential while we like to express some information to draw a distinct line with others or to make a presence in the society that we live in. Similarly, a group or institution may have some information for disclosure to the public while sensitive information must be protected from being disclosed to unwanted parties. The unwanted parties may include individuals who are not members of the group or institution, other groups or institutions, a person with short-term membership, or a deliberate intruder (attacker) attempting to retrieve information illegitimately.

The definition and boundaries of privacy tend to vary among different societies and cultures and as such, there is no clear list of categories of privacy that can be applicable for all. However, four major types of privacy are generally recognized:

- **Personal privacy**. This includes mainly body privacy and territorial privacy. Body privacy varies among individuals in terms of the types of clothing one wears to protect the body. Territorial privacy means making a boundary or to create a barrier between the person and others. This can be implemented by erecting walls, fences, or screens, by using cathedral glass/partitions, by maintaining a distance, among other things.

- **Information privacy**. This kind of privacy is mainly related to passing of information over various media and could also be called communications privacy. Some of the notable information privacies are:
  - *Internet privacy*. The ability to determine the kind of information one reveals or withholds about oneself over the Internet, who has access to such information, and for what purposes one's information may or may not be used.
  - *Financial information privacy*: information about own bank account, amount of money, transaction details, debt, and so on.
  - *Medical privacy*: information about a persons health conditions.
  - *Political privacy*: political stance such as who a person may have voted for.

  Information privacy also means how someone expresses matters about him- or herself in any field. People are sometimes willing to give up information about themselves not because they are ignorant or because they are being tricked by evil corporations, but because it can sometimes be in their best interests to do so [61, 62]. Such information can be posted on the Internet or via social networks or other channels the person is involved with. So, in such a case, a person may judge the benefit of exposing such information, which he or she may like others to know but not through him- or herself directly, to be avoiding the accountability or responsibility of such apparent "leak" of information.
- **Organization privacy**. this includes the confidential information about an organization such as business strategies, loss and profit statistics, current trend in the market, future products, potential customers, transaction details, and similar information. An organization may put some information in the public arena for transparency (which will show the ethical standard of the organization, commonly accessible by anybody) and declares certain information as classified, which is a categorization applied to information that a government or a group claims as sensitive. Prominent examples of organizational security could be often associated with trade secrets and national security.
- **Spiritual and intellectual privacy**. This kind of privacy includes a person's spiritual nature, of his or her feelings and intellect. A person may have certain religious beliefs but may not like to express these to others. It may be because of the adverse or hostile environment. Also, a highly intelligent person may act as dumb or may not like to show his or her intelligence in all gatherings. For example, a person working in a research group may restrain from showing all his or her talents to others so that others may not take his or her ideas away without giving proper credit, or it may be that the person is selfish or may like not to actually get involved in intellectual contribution in the group for some personal reasons.

As the meanings of privacy are different in various scenarios, there are other ways of looking at it. [63, 64] described six types of privacies related to a mans personality: (1) solitude, (2) isolation, (3) anonymity, (4) reserve, (5) intimacy with friends, and (vi) intimacy with family. Solitude is the most complete state of privacy that individuals can achieve. It is a type of privacy in which the individual is alone and unobserved. Pedersen [63] differentiates between isolation termed as alone and away from others and solitude defined as alone by oneself and free from observation by others. Anonymity is a type of privacy that occurs when it is possible to move around in public or, for example, browsing through the Internet without being recognized or being the subject of attention. Reserved behavior includes examples of low self-disclosure. Finally, any kind of intimacy is a type of privacy that relates to an individual's or group's desire to promote close personal relationships. All of these personal traits of human beings need to be studied and thoroughly understood while making any policy related to privacy in any sector, because the same human beings are the beneficiaries or users of these systems.

15.3.2 The Need for Privacy in the Smart Grid

In a SG network, key questions regarding setting the policies on user data privacy are [65]:

- Who owns the data of the customer?
- How is the access to and use of customer data regulated?
- Who guarantees privacy and security of customer data (e.g., against risk of surveillance or criminal activity)?
- Will sale or transfer of customer data be allowed, and under what terms and to whose benefit?
- In jurisdictions with retail choice, are measures needed to ensure competing electricity providers have access to customer data on the same terms as the incumbent utility?

In fact, rival electricity providers may compete to dominate the market, and their access to users electricity usage patterns and behavioral information could be very crucial. The electricity providers or provider agents may use the user data to determine their business strategies and special packages or offers. In an open market environment, such data could be partially collected after the offers are made public and some information is available for all, but if privacy is breached beforehand and specific user data is available to some parties, then these electricity providers may have unfair gains. Appropriate privacy policies may restrict, mitigate, or resolve such use of unfair means in setting business strategies. All these issues explain why the privacy of data of SG users is a very critical issue both for users and the electricity providers.

The privacy of SG users is a very important issue. The strong integration of Information and Communication Technologies (ICTs) for the SGs operation introduces different types of privacy concerns. Depending on how the consumer (or user) uses electricity and recharges it, the privacy of the user can be affected by two usage scenarios namely:

- **The user recharges electricity balance via personal interaction (private mode)**. For instance, the user goes in person to the electricity providers agent and recharges his “smart electricity card” similar to a credit or debit card that can be reloaded and placed into the electricity meter. The other personal interaction may happen via the phone or in person by going to the agent and getting a new recharge or reload number, similar to that used in many places for pre-paid mobile phone balance or validity extension. The customer can also obtain a recharging number obtained from a pre-paid card. This method does not reveal the identity of the person who has purchased the card, which is later used in the electrical meter to do the reloading task. It is worth pointing out that the authorization number will need to be validated and authenticated before electricity consumption. When this number is entered from any home or building (connected to the SG), it passes through an authentication process during which information could be stored by the utility company or one of its designated agents. This information needs privacy protection measures in place.

- **The users recharge their electricity balance via the Internet (public mode)**. If any website or online system is used and the balances are adjusted via payment through some bank account or other payment methods, then all the cybersecurity-related privacy issues must be considered. When a web interface is used and there is a back-end database, web attacks (such as Structured Query Language (SQL) injection [66]) could affect the privacy of the user by disclosing not-to-be-exposed data from the back-end database. The web-based (i.e., online) form to recharge the user’s electricity balance could be made as simple as requiring a single identification number from the user. The privacy issue in this process is whether the user wants to be known at the time of recharging a balance for future electricity usage. In fact, user’s information can be used by different departments or branches of the electricity provider. The user may choose who can access the information and who can not. An instance of personal preference can be the option of receiving company related news, updates, or offers of newly introduced packages or benefits from the electricity supplier company to the user’s email address. For managing user’s own preferences, agent technology [67] could be used, in which each subscriber or user is assigned an agent representing the user’s interests. Each service can also be assigned an agent to reap the most benefit. A service agent could negotiate with subscriber agents about information and authorizations versus the quality of the offered service.

The level of personal information involved and used will dramatically increase with the modernization of the grid. Smart meters and smart appliances could lead to a data explosion of intimate details of daily life. However, at this point, it is quite unclear as to who will gain access to this information, besides the customer’s utility provider, and control utilities. With the deployment of the SG, energy measurements can take place at much shorter intervals (unlike at the end of the billing cycle as in conventional methods).

Currently, there are several types of concerns related to the privacy and security of data associated with the SG. In this chapter, we focus on the issue of privacy linked with consumer information. Potential privacy concerns of SG consumers include: how the required information is going to be collected, used, and disclosed; how customer information is expected to be safeguarded and how it may be used for or against the consumers; how permissions will be granted for the collected data to be shared with multiple agencies; and the liabilities related to any breaches of consumer information. It is also worthwhile exploring how the SG will know about individuals. For example, the energy fluctuation pattern of home appliances is so unique that it may be possible to infer, for example, the model applied for a user's refrigerator. It is also worth noting that many times data that is harmless when collected in isolation may become a privacy threat when combined with other types of data, or examined by a third party for a pattern.

Even when the data about electricity consumption is not collected at regular intervals, information can still be collected at a slower rate through the persistent monitoring of energy consumption. As a result, private information such as how many people live in a household, their presence and absence at home, their schedules for taking showers, watching TV, frequency of microwave use, and their sleeping patterns can be collected or deduced. For many individuals, the collection of this type of information represents an invasion of the "sanctity of the home", and one may argue that such intimate details of someone's daily life should not be accessible. The user's data could disclose their usage pattern of electric devices, and very intimate details of household equipment, even their possible locations (e.g. if the SG concept also is combined with the smart home concept where, when a person leaves a room the lights and electric equipment are automatically turned on or off). In such a case, even the movement pattern of the user within his or her own home could be deduced!

The privacy concerns discussed here are further confirmed by a study called Privacy Impact Assessment (PIA) [12] conducted in September 2009 by the Privacy Sub-Group of the Cyber Security Working Group. The report has identified the following issues and concerns related to consumer-to-utility information exchanges in the US SG:

- There is no clear understanding of the privacy issues on the SG.
- There are a lack of standards, privacy policies, or procedures by the entities involved in the SG and the collection of information.
- Definitions of personally identifiable information are inconsistent in the utility industry.
- Smart meters and distributed energy systems may reveal information about residential consumers and activities within the house.
- Roaming SG devices (e.g., electrical vehicle recharging at other charging stations such as a friend's house) may generate more personal information.
- Even though the National Association of Regulatory Utility Commissioners adopted the 2000 resolution[5] urging the adoption of privacy principles, only a few state utility level commissions have begun to assess privacy issues associated with the SG. This is the case with the state of California through its eight

[5] http://www.naruc.org/Resolutions/privacy_principles.pdf.

Fair Information Practice (FIP) principles[6] such as transparency, right to access information collected (individual participation), individual access to see and copy information stored on an individual, limited types of information that may be collected on an individual (collection limitation), limited internal use of information about an individual, data quality and integrity, data security, accountability, and auditing.

15.3.3 Load-Monitoring Techniques

As we mentioned previously, the possibility of learning information about individuals' behaviors, personal habits, and lifestyle raises concerns. This becomes an important issue when this information can be used for other purposes besides delivering electricity. Electric utilities and other providers may have access to information about the in-house activities of customers, the times when they are using various devices and appliances, as well as the type of devices being used. The initial goal of collecting electricity usage information to generate an electricity profile has now become a source of behavioral information with an immense potential. The most serious threats related to the privacy deterioration of SG consumers include: cyber-attack and intrusion, identity theft, tracking and observing the behavioral patterns of the consumers and the appliances being used, and real-time spying and surveillance. In intrusive load monitoring (ILM), there is an individual monitor for each appliance to acquire the aggregate energy consumption of household electric devices. An alternative technique for deducing the appliance usage characteristics is called non-intrusive load monitoring (NILM), or non-intrusive appliance load monitoring (NIALM), where only one individual monitor is enough to decide the energy usage from the aggregate data. NILM was first reported in 1992 [68]. Since then, various other techniques have been developed for NILM that separate individual appliance power consumption levels from from single, aggregated measurements. Recent surveys about NILM can be found in [59, 69]. An illustration of the concept is presented in [70], where a behavior extraction algorithm implemented in Matlab is used. DSM and Demand response systems provide sufficient power usage information to reveal in-home activities that might be disturbing for the privacy of the households. It is worth noting that NILM can be easily implemented using off-the-shelf hardware and software without much technical expertise.

[6] Senate Bill 1476 was passed in 2010 to protect the privacy and security of customer data generated by advanced meters. The California Public Utilities Commission (CPUC) subsequently issued Decision (D.)11-07-056 on July 28, 2011 to implement SB 1476. See http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf for more details.

As a result, privacy concerns, coupled with a degree of security related issues, may lead to any of the following unintended consequences [31, 71, 72], or some other vulnerabilities not currently identified:

- Hackers could manipulate power consumption and billing.
- Cyber-terrorists might fake power consumption data on a large scale to attack the power system.
- Attackers may take control of the smart meters for manipulation at will.
- Direct marketers, criminals, law enforcement agencies may use the energy consumption data without prior approval or notification.
- Energy consumption patterns of individual appliances can be identified with high accuracy.

Thus, privacy is the Achilles' heel for the success of the SG and needs to be carefully investigated and addressed.

15.4 Privacy Solutions

In this section, we present a novel taxonomy of the privacy techniques proposed for the SG domain, and we provide a synopsis of each category with references, and compare and contrast them.

15.4.1 Taxonomy of Privacy Techniques

A comprehensive and novel taxonomy of the SG privacy-protection mechanisms and approaches is given in Fig. 15.10. We divide the SG approaches into *spatial*

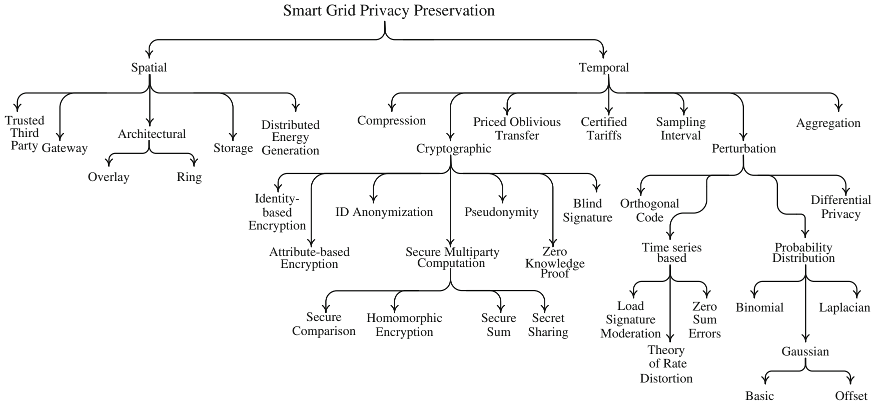


Fig. 15.10 Privacy-preservation techniques used in the SG

and *temporal* broad categories. The former include those that devise privacy into the system by means of a physical device or entity while the latter incorporates privacy into the system by means of logical extensions. We note that the individual categories identified in Fig. 15.10 do not necessarily indicate an exclusive technique. In fact, a privacy preservation proposal reported in the literature may, and usually does, implement a combination of them. The categorization of Fig. 15.10 is to provide a delineation of identifiably distinguishable techniques to provide a smoother and clear explanation in what follows. A different approach has been taken in [73] where privacy preservation techniques are presented with a combination of methods from parts of Fig. 15.10 on a per paper basis.

Next, we provide a discussion of the spatial and temporal categories along with their subclasses.

15.4.2 Spatial Privacy Techniques

There are five main categories of spatial privacy-protection mechanisms proposed in the literature for the SG, as shown in Fig. 15.11, together with the cited references.

15.4.2.1 Trusted Third Party

A trusted third party (TTP) in cryptography is an independent entity that acts as a liaison between two or more collaborating organizations; which, in our case, is between the end-user and the power utility [74–76]. The TTP has to be completely trusted by all participants with respect to its intentions, technical competence, and so on, so mutual trust can be achieved. In the literature, TTP is also referred to as the third party escrow service [75].

In what follows, we elaborate on the approach in [75] as one example in this category: [75] provides a mechanism for anonymizing high-frequency energy

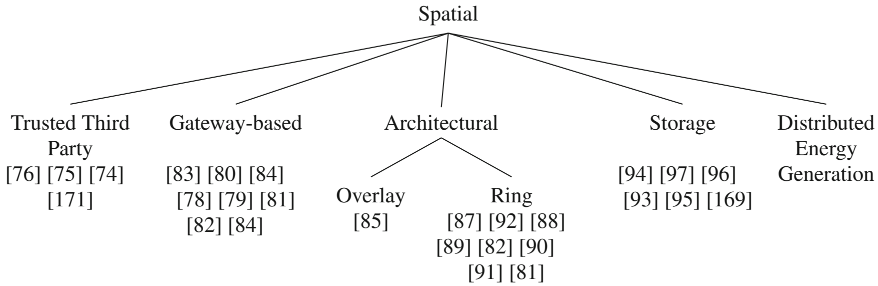


Fig. 15.11 Spatial privacy-provisioning techniques for the smart grid

measurement data (such as usage patterns of specific electrical appliances) through the use of a Pseudonymous Identity (PID). The anonymous meter readings are difficult to associate with a particular smart meter or customer, thus offering a higher level of privacy to the SG user.

The distinguishing feature of the Escrow smart meter is that it has two separate IDs, rather than a single ID as is the case with standard smart meters. The two IDs are the high-frequency ID (HFID) which is anonymous, and the low-requency ID (LFID) [77], which can be related to a specific customer or smart meter. The main idea of the scheme is to provide anonymity of the HFID messages. The anonymity is implemented by not disclosing the HFID to the utility or the smart meter installer. The HFID is 'hidden' inside the smart meter, or hard-coded to be used for all HFID-related messages. In order for the utility to verify the legitimacy of the HFID, a third party Escrow mechanism is implemented. The third-party can be the manufacturer of the smart meter itself or some other trusted third-party, which has been given access to this information. The manufacturer can assign two unique IDs to each smart meter that is produced, only one of which (LFID) is visible to the utility, both during the procurement and deployment procedures. Essentially, the manufacturer (or the Escrow service) is the only party that is aware (and has a record) of the connection between a valid HFID or LFID pair. The Escrow is required to comply with a strong data privacy policy. For example, the Escrow may not be expected to access, process, or store smart metering data—it will only know about the relationship between a valid HFID and LFID.

15.4.2.2 Gateway-Based Approaches

In the gateway-based approach, an external entity outside of the customer premises acts on behalf of the end-users to obfuscate the relationship between the data and the owner [78–84].

The Smart Energy Gateway (SEG) architecture [83] is deployed at users' premises and uses a privacy manager, which is designed as a software component running on SEG, deployed at users' premises. The idea behind the architecture is to provide user-centric privacy, which means that the user could be in control of his or her own privacy parameters. The proposed privacy manager has the ability to specify privacy conditions and obligations with respect to the handling of users' private data, and to rely on SEG security architecture features such as application isolation, mandatory access control, pseudonymity, and secure storage to reliably enforce the users' specified privacy constraints. The main features of the privacy manager include:

- **Customer privacy preference specification and enforcement**. The energy customer would express how personal information disclosed should be handled and the utility or service provider would express how customer's information will be treated. Privacy policies enforcement: each SEG application policy is bound to a smart software agent and has to be validated against the SEG platform integrity policy both during the installation and at runtime. This ensures that SEG only hosts and runs smart software agents that meet pre-defined gateway security requirements (e.g., that the former will not access locally-stored energy usage data collected at this particular premise).

- **Secure storage and data masking**. The secure storage will guarantee the confidentiality and accuracy of locally-stored energy usage data. Only trusted and legitimate applications (e.g., billing provider software agent) can access the metered data repository.
- **Pseudonymity**. Enables the customer to use SG resources or related services without revealing their respective identities but remaining accountable for their transactions.
- **Privacy feedback**. Allows the display of feedbacks to the energy customer regarding the handling of its personally identifiable information.

15.4.2.3 Architectural Schemes

Architectural schemes arrange the topology of the smart meters in order to implement privacy protection. Two distinct categories are considered:

1. **Overlay**. Randomly organized smart meters form peer-to-peer groups in [85] using Chord algorithm [86]. Peer anonymization algorithm together with in-network aggregation enhance the privacy protection capabilities of the proposed approach.
2. **Ring topology**. A few proposed approaches [81, 82, 87–92] take advantage of imposing some form of a ring architecture for the SG meters. For example, a virtual ring architecture is proposed in [87] to provide a privacy protection solution using symmetric or asymmetric encryption of customers' requests belonging to the same group.

15.4.2.4 Storage-Based Mechanisms

As the name implies, a type of energy storage infrastructure is employed for the privacy protection in this category [93–97]. For example, the authors in [94, 95] assume that future smart homes will contain several energy storage and energy generation devices, and thus *electrical power routing* will be feasible. More details of this are given in Sect. 15.4.3.6, under Time series-based privacy.

15.4.2.5 Privacy with Distributed Energy Generation

The main idea behind privacy protection using Distributed Energy Generation (DEG or a.k.a. Distributed Energy Resources or DER) relies on the intermittent and stochastic energy values provided by DEG to mask the actual energy consumption from the disclosed values assuming that DEG is private to the end-user.

15.4.3 Temporal Privacy Techniques

A second major category of privacy preservation techniques we consider includes those that implement techniques over time without relying on an external tangible entity. We describe some of these techniques in this category.

15.4.3.1 Compression-Based Approach

As the name implies, the energy consumption data is transformed using compression techniques to protect the privacy [98, 99]. Compression alone may not be strong enough and thus [99] uses it in combination with other techniques.

Li et al. [98] makes use of the technique of *compressed sensing* from signal processing to provide privacy protection. Compressed sensing [100–102], also known as sparse sampling, assumes the smart meter data is sparse with uniform delay and uses a secret random sequence so that the original data can be reconstructed at the receiving end.

15.4.3.2 Cryptographic

There are various cryptographic techniques reported in the literature that are used to provide privacy in the SG as shown in Fig. 15.12. We divide the cryptographic temporal privacy-protection techniques into seven categories and discuss them here.

Privacy Through Identity-Based Encryption

An identity-based encryption (IdBE) scheme is a public-key cryptosystem where the key may be selected to be any string, such as email addresses, dates, and so on. It was first introduced as a problem in [103] with solutions in [103–105]. IdBE may be used for privacy in the SG as discussed in [106].

Privacy Through Attribute-Based Encryption

In the attribute-based encryption (AbE) [107], ciphertexts are associated with sets of attributes. Private keys are coupled with access structures to control which ciphertexts can be used to decrypt them. AMI is an important component of the

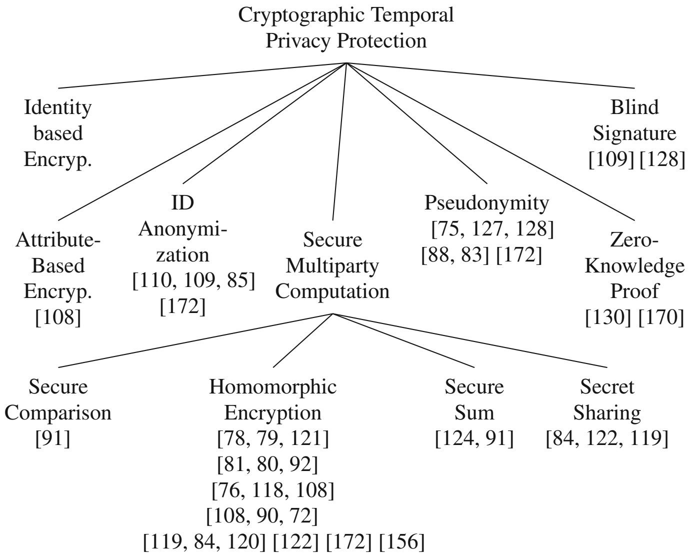

Cryptographic Temporal Privacy Protection
Identity based Encryp.
Blind Signature [109] [128]
Attribute-Based Encryp. [108]
ID Anonymi-zation [110, 109, 85] [172]
Secure Multiparty Computation
Pseudonymity [75, 127, 128] [88, 83] [172]
Zero-Knowledge Proof [130] [170]
Secure Comparison [91]
Homomorphic Encryption [78, 79, 121] [81, 80, 92] [76, 118, 108] [108, 90, 72] [119, 84, 120] [122] [172] [156]
Secure Sum [124, 91]
Secret Sharing [84, 122, 119]

Fig. 15.12 Cryptographic temporal privacy-protection techniques for the smart grid

overall DR system, as defined before in Sect. 15.2.2. In [108], the authors propose to protect multicast communications involving crucial DR messages from the control center to the smart meters by means of an AbE implementation.

Privacy Through ID Anonymization

Anonymization is a general term that decouples a message from its originator. Several proposals in the literature take advantage of the anonymization techniques for the SG privacy [15, 85, 109, 110].

Secure Multiparty Computation

Secure multiparty computation (SMC) has been developed as an alternative to the TTP approach. SMC is a set of techniques to compute a function collectively with the assurance that at the end of the multiparty computation, no participant can learn anything except its own input and the result. Then intended information should be inferable only from these two pieces of information. Historically, SMC was initiated to address Yao’s Millionaire Problem [111] where two parties can know which of them is richer without disclosing their actual wealth. Yao’s two-party solution was extended to multiple parties in [112].

1. **Secure comparison**. This is an implementation of the Yao's Millionaire Problem [111], as described above. [91] used secure comparisons algorithms as part of the overall SMC approach for smart meter data processing.
2. **Homomorphic encryption**. One of the most common methods to ensure privacy in the SG has been the homomorphic encryption technique, which dates back to the first problem formulation in 1978 [113]. A partial homomorphic encryption that preserves the structure of multiplication or division, but not both, has been used until recently. The solution has been elusive until the formulation of the first fully homomorphic encryption scheme in 2009 [114]. Homomorphic encryption enables computation on the encrypted data without revealing the plaintext. Given a homomorphic encryption function E(), and two messages x, y, the following relationship is guaranteed:

   $$\mathrm{E}(x \odot y) = \mathrm{E}(x) \bigstar \mathrm{E}(y), \tag{15.1}$$

   without knowing the plaintext x, y, and the private key. Paillier cryptosystem [115, 116] is an example of an additive homomorphic encryption, where with respect to Eq. 15.1, $\odot$ is multiplication and $\bigstar$ is addition. In other words, the sum of plaintext is calculated from multiplication of the ciphertext. Another commonly used additive homomorphic encryption is the Boneh-Goh-Nissim (BGN) cryptosystem [117], which is based on Paillier but with bilinear groups.

   Implementation of homomorphic encryption techniques for privacy preservation in the Smart grid are given in [72, 76, 78, 79–81, 84, 90, 92, 108, 118–120, 121, 122]. For example, the authors of [121] propose an Energy Privacy Preserving Aggregation (EPPA) scheme for secure SG communications. EPPA uses a multi-dimensional data aggregation approach based on the homomorphic Paillier cryptosystem [116], which is composed of three algorithms namely, key generation, encryption, and decryption. The proposed technique is based on composite residuosity classes, whose computation is believed to be computationally difficult. It is a probabilistic asymmetric algorithm for public key cryptography and inherits additive homomorphic properties [113]. Homomorphic encryption allows specific types of computations to be carried out on ciphertext and obtain an encrypted result. For example, one user could add two encrypted numbers and then another user could decrypt the result, without either of them being able to find the value of the individual numbers. Homomorphic encryption schemes are malleable by design. Another homomorphic encryption system for the privacy-preserving data collection and aggregation is proposed in [84, 122] based on the Lite Cramer-Shoup Scheme [123].
3. **Secure sum**. One way to implement the secure sum is by means of Paillier cryptosystem, as proposed in [91]. Another secure sum technique is used in [124] based on the algorithm in [125]. The basic idea of this algorithm is shown in Figs. 15.13, 15.14, 15.15, 15.16, 15.17 and 15.18. Bob, Alice, and Charlie have their own secrets, as shown in Fig. 15.13, and they would each like to compute the sum without revealing their own secret values. Any arbitrary

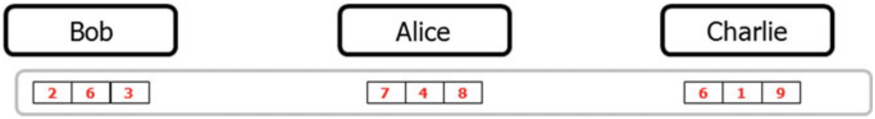


Fig. 15.13 Secrets of Bob, Alice, and Charlie

initiator may start the process. Let Bob initiate it in our example by generating a random profile, as shown in Fig. 15.14. Bob adds the random secret profile to its secret profile, shown in Fig. 15.15.

Bob sends its secret plus random secret to Alice. Note that Alice cannot break up the totals to find out Bob's secret. Alice adds her own secrets to the values received from Bob, as shown in Fig. 15.16. Figure 15.17 show that Charlie gets Alice's transmission and adds his values. Bob receives the profile from Charlie,

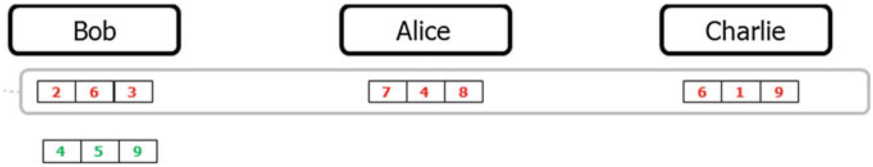


Fig. 15.14 Bob's secret random values

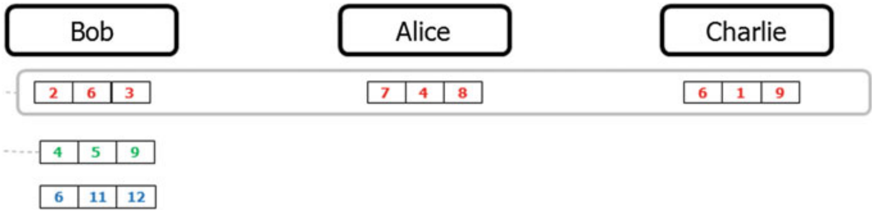


Fig. 15.15 Bob's secret random values added to his own secret

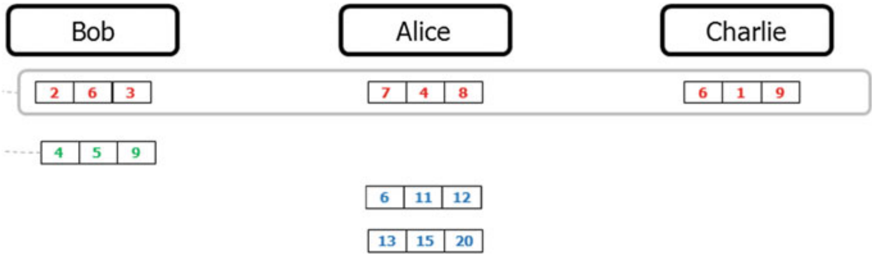


Fig. 15.16 Alice receives Bob's transmission

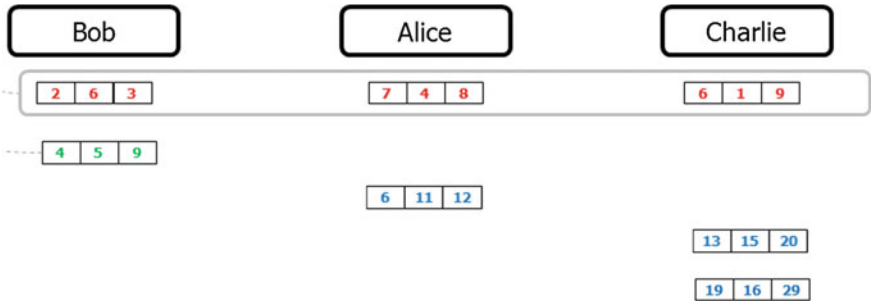


Fig. 15.17 Charlie receives Alice's transmission

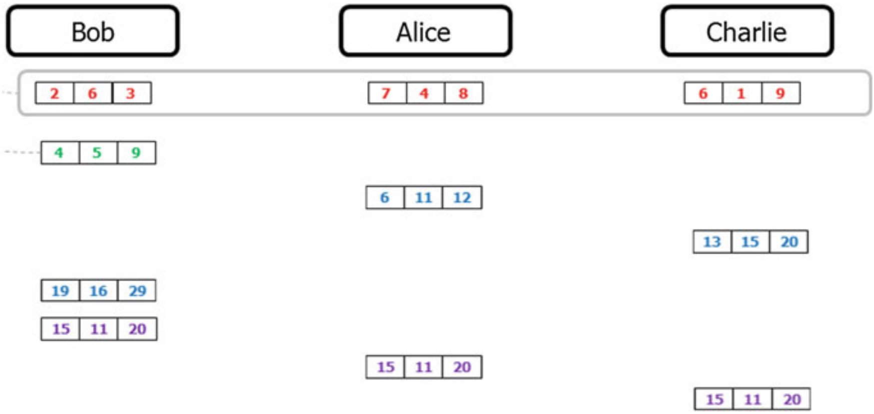


Fig. 15.18 Bob receives Charlie's transmission and computes the sum

subtracts the random secret only known to him and reaches the sum, without knowing either Alice's or Charlie's values and disseminates it to the others, as shown in Fig. 15.18.

4. **Secret sharing**. The basic idea of secret sharing is to break up a message M into k parts before transmission in such a division that the original message M can be assembled together from these n pieces while even access to $n - 1$ parts will not be sufficient to infer M. The techniques for such a goal have been introduced by Shamir in [126]. Secret sharing has been exploited in [84, 122] to develop a secure and distributed protocol with privacy-preserving aggregation of SG metering data.

Pseudonymity

Unlike anonymity, where identity is hidden and/or decoupled from the message, in pseudonymity, fictitious names are used to represent messages. The real identity to the fictitious mapping must be kept secret. Examples of this approach are proposed in [75, 88, 83, 127, 128]. We provide some details of one these here.

The privacy-preserving authentication scheme for an SG network (PASS) [127] involves the use of a smart appliance (located at customers homes) attached to a tamper-resistant device for generating pseudo identities and signatures on messages. A customer is given this device when he or she opens an account or registers a newly purchased smart appliance. The characteristic features of the PASS architecture are as follows:

- Message authentication: before a smart appliance transmits a request message to the control center, it has to include a hash-based message authentication code (HMAC) signature on the message using the regional system key. This regional system key is only known by the control center, the substation, and all tamper-resistant devices within the region. Hence, an outside attacker (who does not belong to the region or is not a registered smart appliance) does not know how to generate a valid HMAC signature. Thus, the PASS scheme protects from outsider attacks.
- Identity privacy: in all request messages sent by a smart appliance, real identities are used instead of pseudo identities.
- Request message confidentiality: the amount of electricity required by a smart appliance is encrypted using the public key of the control center. Thus, except for the control center, no one can decrypt the value representing the electricity amount. On the other hand, the encryption feature in the PASS architecture allows a substation to aggregate request messages sent by smart appliances within its region but the substation does not need to know about those individual amount values.

Zero-Knowledge Proof

Zero-knowledge proofs are those convincing assertions that yield nothing but their validity [129]. In other words, one party proves to another without revealing any information besides a statement of affirmation or decline. The authors of [130] deal with preserving the privacy of metered data. The authors propose a set of privacy-preserving protocols amongst a provider, a user agent, and a simple tamper-evident meter by taking advantage of a zero-knowledge proof. This work considers a scenario where the privacy of the metered data is preserved by employing encryption mechanisms along with certification techniques. Within the boundary of a home environment, plaintext is used, but when sending or communicating with entities outside the home boundary, certification, and encryption techniques are used. The authors argue that their scheme can be applied to all types of smart metering including electricity, waters and gas metering, and can be extended for other future smart meter-based systems. The main contribution of this work can be summarized as follows: the meter produces certified readings of measurements and transmits them to the user via a secure communication channel.

For billing, the user combines those readings with a certified tariff policy to produce a final bill. The bill is then transmitted to the provider alongside a zero-knowledge proof that ensures the calculation to be correct and leaks no additional information. A zero-knowledge proof of knowledge [131] is a two-party protocol between a prover and a verifier. The prover demonstrates to the verifier its knowledge of some secret input (witness) that fulfills some statements without disclosing this input to the verifier. The protocol should meet two properties: (1) it should be a proof of knowledge, which means that a prover without knowledge of the secret input convinces the verifier with negligible probability, and (2) it should be zero-knowledge, that is, the verifier learns nothing but the truth of the statement. The fact that a witness is not distinguishable from active participants is a weaker property which requires that the proof does not reveal the witness (among all possible witnesses) used by the prover.

Blind Signature

In [109], the authors consider an SG network as three basic layers: at the highest layer, there is a control center maintained by the power operator, the second layer has substations inside the distribution network and each substation is responsible for the power supply of an area, and the lowest layer has the smart meters which are placed at the users' premises as shown in Fig. 15.19.

The proposed anonymous credential architecture [109] preserves users' privacy information, including their daily electricity usage pattern from third parties as well as from the power operator. The scheme is based on *blind signatures* [132]. Blind signature is a method that allows the first party (Party 1) to sign a message generated by a second party (Party 2), without knowing its actual content. When a third party (Party 3) receives the signed message, it can verify that the message is signed by Party 1. The anonymous credential scheme uses the blind signature technique to allow the control center (Party 1) to sign a credential generated by a customer (Party 2) without knowing its actual content. At a later time, the control center itself

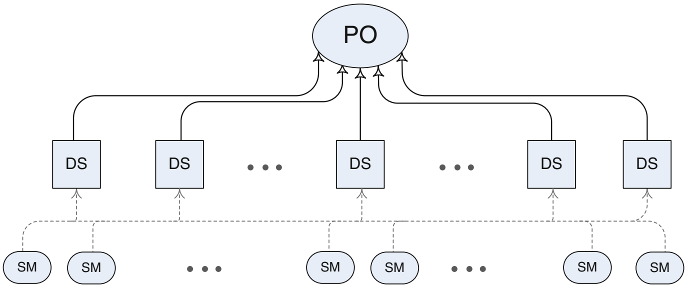


Fig. 15.19 A three-layer smart grid architecture. *PO* power operator, *DS* distribution substation, *SM* smart meter

(Party 3) can verify that the credential is indeed signed by Party 1 without knowing who requested the signature or when the signature was generated. The use of the blind signature technique in this scheme is as follows: the customers prepare a set of credentials, each stating the amount of electricity requested, and request the control center to sign them blindly so that the customer can submit any of these credentials for the request of electricity. Since Party 1 does not know the actual content of the message sent by Party 2, the message is verified using a special technique which is widely adopted in e-cash schemes. Party 2 generates n messages using different blinding factors. It then blinds the n messages and sends them to Party 1. Next, Party 1 randomly chooses m messages ($m < n$) and challenges Party 2 to reveal them by providing the m blinding factors. If the m blinding factors are correct, Party 1 accepts the signature request and signs the remaining ($m - n$) messages. The scheme assumes that any smart meter can communicate with the control center via a secure communication channel (such as one using the advanced encryption standard (AES) and third parties cannot read the contents without the key concerned).

When a customer presents a credential anonymously, the control center cannot tell which customer is making the request, yet it can verify the signature to confirm that it is from a valid customer (since only valid customers can request blind signatures). The four phases involved in the Anonymous Credential scheme are as follows:

- **Setup phase**. The control center assigns a Ron Rivest, Adi Shamir and Leonard Adleman (RSA) public and private key pair for signing credentials.
- **Registration phase**. Carried out at the beginning of each month. This phase is not anonymous. Customers need to be authenticated using their real identities via an authenticated channel.
- **Power requesting phase**. Can be executed at any time during the month when the smart meter of a customer finds that it needs more power to support all the electric appliances. This phase is anonymous. Customers are validated via anonymous credentials.
- **Reconciliation phase**. Carried out at the end of each month. This phase is not anonymous. The smart meter sends the unused credentials back to the control center to evaluate the amount of power requested so far.

Another approach based on the fair blind signature [133] method is reported in [128] for the vehicle-to-grid (V2G) system, involving both charging and discharging of battery vehicles (BVs). Fair blind signature is an extension of the basic blind signature scheme where misuse of the system against black-mailing and money laundering is prevented by means of an embedded property to remove anonymity via a trusted entity. In our case, it is used to ensure proper billing.

15.4.3.3 Priced Oblivious Transfer

Oblivious transfer, introduced in 1981 in [134], is a protocol in which the sender remains unaware of what has been transmitted out of the potentially transferable many pieces. Using oblivious transfer protocol, a protocol is developed in [135], called priced oblivious transfer, to enable buyers purchase digital goods from vendors without letting the seller learn *what*, and to the extent possible, *when* and *how much*. Priced Oblivious protocol is used in [136] to propose a privacy preserving billing protocol which guarantees the power operator gets the correct amount of money without learning the current energy consumption of each customer.

15.4.3.4 Certified Tariffs

As explained in Sect. 15.4.3.2 (the subsection on Zero-knowledge proof) from [130], the energy provider cannot gather any fine-grained readings. The provider is guaranteed that the correct fee is calculated based on the actual readings and time-of-use tariffs without learning.

15.4.3.5 Sampling Interval

Smart meters in the AMI system provide sampling of measurements and potentially other useful information and report them back to the power operator or other third parties. The sampling process is the center of privacy concerns as it transmits potentially sensitive information. The authors in [137] consider sampling as a design parameter in the performance of DR schemes to explore some trade-offs between performance and privacy. An optimization problem is considered to find the right sampling interval given a set of performance goals and desired privacy level.

15.4.3.6 Perturbation

Another technique for privacy preservation that has gained a considerable attention is a set of techniques collectively known under the term *perturbation*. A taxonomy with the cited work is depicted in Fig. 15.20. A common theme in these techniques is the transformation of the energy consumption data from what gets disclosed out of the customer premises. We provide details of this category with its subclasses in what follows.

Privacy Using Orthogonal Code

The work in [138] analyzes security and privacy in the SG and specifically emphasizes the privacy aspects. The authors propose a secure and efficient in-network data aggregation and dispatch scheme for AMI in home area networks for the SG. In-network aggregation is the process of collecting content from multiple sources or devices in a network. With this mechanism, the authors propose the use of Walsh function [139] based on Hadamard code [140] to generate mutual orthogonal chip codes to be used in the secure in-network data aggregation and

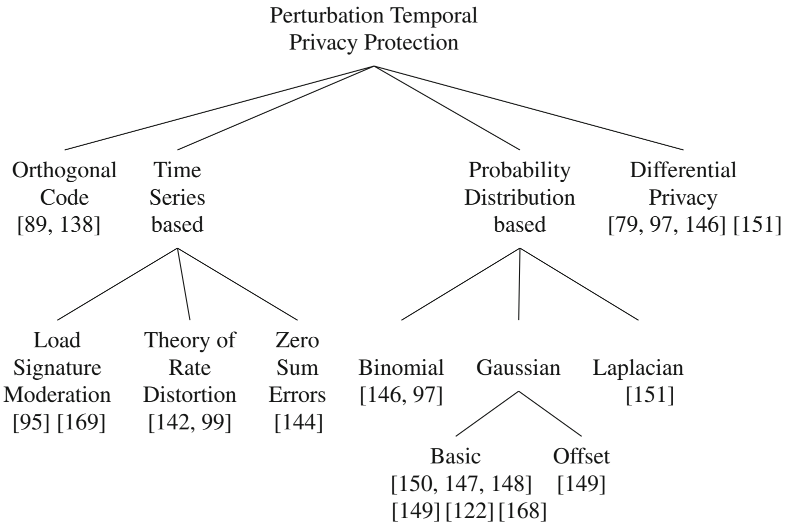

Perturbation Temporal Privacy Protection
Orthogonal Code [89, 138]
Time Series based
Probability Distribution based
Differential Privacy [79, 97, 146] [151]
Load Signature Moderation [95] [169]
Theory of Rate Distortion [142, 99]
Zero Sum Errors [144]
Binomial [146, 97]
Gaussian
Laplacian [151]
Basic [150, 147, 148] [149] [122] [168]
Offset [149]

Fig. 15.20 Perturbation-based temporal privacy-provisioning techniques for the smart grid

dispatch scheme. The use of orthogonal code allows multiple users to communicate simultaneously over a single frequency. This is achieved by the use of spreading codes whereby a single data bit is “spread” over a longer sequence of transmitted bits. These codes, also known as chip sequences, must be carefully chosen so that the data may be correctly “de-spread” at the receiver. Such codes are known as orthogonal codes. The Hadamard code [140] is an error-correcting code that is usually used for error detection and correction when transmitting messages over very noisy or unreliable channels. In their work, the authors apply these techniques envisioning that the smart meter works as an authentication server that is connected with multiple smart devices and each smart device contributes to the formation of confidential data, which can be regenerated at the smart meter. This work describes the coding techniques and the steps on how the original data readings are spread and then mixed up with the spreading code of other smart devices. The smart meter can reconstruct the original reading data from the mixed data using the chip code established with smart devices during their initialization procedure through mutual authentications.

Another work that encrypts measured data by orthogonal codes by using Walsh code is reported in [89], which uses a ring communication architecture.

Time Series-Based Privacy

One way to look at the measurements coming out of the smart meters is a series of data giving way to a wealth of methods that can be invoked from the field of time series. We present a survey of some of these methods here.

1. **Load signature moderation**: Load signature moderation (LSM) [95] scheme suggests that the home electrical power routing can be used to moderate the home's load signature in order to hide appliance usage information. Load signature is defined as a series of time-stamped average power loads $p(t)$ derived from cumulative energy values $e(t)$ metered at interval Δt:

$$p(t) = \frac{e(t) - e(t - \Delta t)}{\Delta t} \tag{15.2}$$

A *home load signature* is the sum of all home appliance loads. To perform load signature moderation, the authors assume that future smart homes will contain a variety of energy storage and energy generation devices, and thus electrical power routing will be feasible. Electrical power routing means the selective control and power mixing of a number of electricity sources to route electricity to a number of consumers. For instance, a kettle drawing 2 kW of power when switched on; the power router could be configured so that 1 kW is supplied from a solar panel, 0.5 kW from a battery, and 0.5 kW from the main electricity supply. The basic contribution of this approach is that it presents the idea how to provide sufficient privacy for the user by including privacy mechanisms for the smart meters which is supposed to record the usage. The authors also propose a power management model using a rechargeable battery, a power mixing algorithm, and evaluate its protection level by proposing three different privacy metrics: an information theoretic (relative entropy), a clustering classification, and a correlation/regression one. We will briefly review these metrics:

- *Relative entropy*: the relative entropy or Kullback Leibler distance [141] is a well-known information theoretic quantity which can be used to compare two sources of information. The distance here is not the mathematical meaning of distance but rather it quantifies the relation between probability densities. If p_0 and p_1 are two probability densities, the Kullback-Leibler distance is defined to be,

$$D(p_0||p_1) = \int_{xmin}^{xmax} p_1(x) log \frac{p_1(x)}{p_0(x)} dx \tag{15.3}$$

  where p_0 and p_1 are the probability density functions of p_0 and p_1, respectively.
  Relative entropy is always positive, and for identical p_0 and p_1, it is zero. Hence, the authors in [95] state that the level of privacy protection offered by a mapping $\emptyset$ can be measured by the relative entropy, $D_{\emptyset}(p_0||p_1)$ such that the higher the level of protection offered by $\emptyset$, the larger the relative entropy.
- *Clustering classification*: the authors propose using any of the available clustering classification mechanisms which takes a set of data with a distance metric and groups them into n clusters that minimize the distance between points. The distance metric here is the difference between power consumption

values. They propose to use a simple method of trace analysis that aims to recover information about device power usage from a small amount of information sent via the signals.

- *Regression analysis*: as a third metric, the work described in [132] quantifies privacy by combining cross correlation and regression procedures, which can be termed as regression analysis. In statistics, regression analysis includes many techniques for modeling and analyzing several variables, when the focus is on the relationship between a dependent variable and one or more independent variables. A dependent variable is what is measured in an experiment and what is affected during the experiment. This kind of variable responds to the independent variable. It is termed so because it depends on the independent variable. In a scientific experiment, there cannot be a dependent variable without an independent variable. Just as an example, if someone is interested to find out how time spent on studying changes "test score", then it is understood that the test score does not change the time spent, as that had happened earlier. In this case, "studying time" is the independent variable and "test score" is the dependent variable. Based on these foundations and ideas, the authors in this work apply regression analysis on the received signals to recover information by comparing them over time.

This work can be extended to include other types of privacy metrics, such as mutual entropy or equivocation. In addition, smarter battery privacy algorithms may be designed, which the authors have left as future works.

2. **Theory of rate distortion**: Rate-distortion theory is a subfield of information theory that addresses the problems of lossy compression. It analyzes the theoretical fundamentals of determining the bit rate to be communicated over a communications channel in order for the original data to be reconstructed at the receiver subject to a distortion level.

   Information theoretic approaches to SG privacy have been proposed in a few studies [99, 142, 143] by means of the rate-distortion theory. Rate-distortion theory has been used to provide SG privacy in a few recent studies [99, 142, 143]. Rajagopalan et al. [99] and Sankar et al. [143] attempt to quantify privacy in order to gain insight into the tradeoff between sharing information (utility) and hiding it (privacy). The utility is represented by means of square error (distortion D)

$$D = \frac{1}{n}\sum_{k=1}^{n}\mathbb{E}[(X_k - \hat{X}_k)^2] \tag{15.4}$$

   where X_k is the actual measurement, $\hat{X}_k$ is the exposed value; while privacy is represented by information leakage:

$$L = \frac{1}{n}\mathscr{I}(Y_n; \hat{X}_n) \tag{15.5}$$

where Y_n represents the inferred data as a random variable correlated with the measurement variable X. Some examples of interference sequence Y_n include the known appliance signatures that are provided by NILM techniques discussed earlier in Sect. 15.3.3. The proposed algorithm, interference-aware reverse waterfilling solution, exposes high power but less private appliance information and filters out components with lower power to a distortion threshold. However, this proposal is only limited to a framework proposal and an algorithmic approach is not detailed enough to implement it.

Another rate-distortion theory based approach is given in [142]. However, similar to the previous ones, it also suffers from unrealistic assumptions and the approach is complex. For instance, the assumption about binary input and output loads are unrealistic.

3. **Zero-Sum Errors**. The authors of [144] propose a cooperative state vector estimation technique that preserves the privacy of the personal behavior of the user. Unlike most other privacy preservation techniques for the SG where energy consumption information is the focus, the authors here provide privacy protection for phase angle measurements. Thus, they take advantage of the state estimation methodology [145]. The key objectives are to ensure mainly two things: (1) the power measurement is well obfuscated such that users do not fully disclose their private behavioral information, and (2) the obfuscated data retains the necessary or basic information such that the state vector (a column vector whose components are the state variables of the system) can be accurately estimated from the perturbed data. "Perturbed data" are the original measurement data that are modified to conceal the information and to make it difficult to infer the original data. Another significant contribution of this work is that the authors evaluated the performance of the proposed data obfuscation scheme with 1,349 measurement data sets. For this, they used the data sets as if they are connected to five different IEEE test systems that are portions of the Middlewestern US Electric Power Grids. They also evaluated the illegibility to human inspectors, resilience to automated data mining attackers, and communication overhead.

Privacy with Probability Distribution Functions

Another method of transforming the exposed measurement data is by means of adding noise from probability distribution functions.

1. **Binomail**. Binomial distribution is proposed in [97, 146].
2. **Gaussian**.
   a. Basic: straight Gaussian distribution is used to determine the magnitude of the noise in [147–150].
   b. Offset: [149] proposed a noise canceling mechanism by using a technique which is based on the Central Limit Theorem. In the offset method, the

margin caused by noises in previous time slots is compensated to achieve zero error in billing computation.

3. **Laplacian**. Laplace distribution is the basis for computing the noise in [151]. Chen et al. [79] employs symmetric geometric distribution, which can be regarded as a discrete approximation of Laplace distribution. The use of geometric distribution for the noise was pioneered by [152].

Differential Privacy

The notion of differential privacy is coined in [153, 154]. Differential privacy has emerged from the field of database queries where the goal is to answer queries in an accurate way while preserving the privacy of individuals. Differential privacy yields plausible deniability to blur the data hidden behind. It is about an information-releasing algorithm with a mathematical underlying model. Differential privacy boils down to distorting the answers to the database queries by means of adding a predefined noise so that the intended receiver filters it out to reach an almost accurate answer. As can be seen from the problem definition, this is applicable to the SG privacy case as well. Differential privacy-based mechanisms have been proposed in [79, 97, 146, 151].

15.4.3.7 Aggregation

To secure the data-collection task, there are two major approaches: one is to ensure the protection of the data content directly without regard to the data semantics. The approach presented in [60] is based on symmetric cryptography to provide data confidentiality and authentication between sensors and the base station. [155] describes a protocol for data collector (DC) to collect data from a measurement device (MD), but direct communication between the DC and the MD is assumed. Another category for providing security exploits the *aggregate* statistics of the sensed data, such as summation, average, minimum, maximum, and so on. These approaches take advantage of in-network data processing (also referred to as *aggregation*) to apply some obfuscating operations on the transmitted data [72, 122, 138, 156–162]. A few common examples in this category include cluster-based private data aggregation [159] and its integrity enhanced version [160], secret perturbation [157], *k*-indistinguishable privacy-preserving data aggregation [158], a centralized authentication server based in-network aggregation for AMI [138, 161], homomorphic encryption-based aggregation [72, 78, 80], a secure architecture for distributed secure hierarchical data collection aggregation of additive data [84, 122], a secure and scalable data collection protocol for smart meter data [163, 164], multifunctional, privacy-protecting aggregation [79], and a network coding-based encryption between smart meters and aggregators [162]. Another one is reported in [121]. Many of the existing data aggregation schemes collect information as one-dimensional information. However, smart meter data could be considered as multi-dimensional in nature, because, these include including various aspects of the information such as the amount of energy consumed, the time it was consumed, the purpose of the consumption, and so on. Considering the high data collection frequency, multi-dimensional information and the large number of users, current data aggregation schemes generate not only huge communication costs but also impose overwhelming processing load on local gateways. In contrast to traditional one-dimensional data aggregation methods, Energy Privacy Preserving Aggregation (EPPA), as discussed earlier in "Secure Multiparty Computation", is shown to greatly reduce computational cost and significantly improve communication efficiency while satisfying the real-time high-frequency data collection requirements in SG communications. The main drawback of the work is that it is highly theoretical and it does not really provide enough details on how such an approach can be deployed in practice.

15.5 Challenges and Opportunities

The preservation of privacy in the SG environment has many fundamental open challenges that still need to be solved. As our literature survey shows, several research projects have been investigating privacy-preserving techniques for the SG environment in the last few years. We found that there is need for privacy to be comprehensively regulated through legal and regulatory frameworks for enhancing users' confidence and for reinforcing individual's privacy rights. These frameworks should provide a comprehensive view of both the challenges and limitations related to personal data protection rights as they pertain to the SG technology.

In recent years, a lot of work has been undertaken on designing privacy-preserving methods using various technical approaches, which vary according to the context and the architecture in use. Throughout this chapter, various SG privacy solutions aimed at preserving smart meters' privacy have been discussed. As we have pointed out earlier, most of the recently proposed SG solutions have limitations and they do not always follow the recommendations being made by standardizations entities and governmental agencies [40]. Although it is not mandatory to follow the recommended guidelines made by standardization bodies, for future interoperability and scalability, SG privacy solutions should nevertheless take these recommendations into consideration. We discuss here some of the challenges that still need to be addressed in the future by researchers and designers working in the area of SG privacy.

- **Third party issue**

  The privacy issues in the SG are particularly magnified by the large-scale infrastructures, the diversity of communication technologies, the number data sources, and the high volume of data generated. In the past, most of the SG services were basically limited to governments or large enterprises, which have traditionally built by proprietary and isolated infrastructures (e.g., electrical power network) to provide services to customers. However, third parties can actually offer their infrastructures and services with limited control from governments and, hence, concerns have arisen about third-party access to the customer's personal information.

- **Privacy and authentication**
  Privacy is often closely linked with authentication. The issue of trade-off between privacy rights of entities and the need to authenticate them needs to be explored further. Unfortunately, authentication leads to personal information becoming available. However, authentication is a very important security service that may help to eliminate some of the cyber attack classes such as man-in-the-middle attacks and false data injection attacks. The latter consists of forging and manipulating the quantities of energy supply and requests. It is worth noting that authenticated nodes may also inject false data without being detected as is the case with recently proposed homomorphic encryption-based solutions [87, 165].
- **Privacy and forensics**
  Privacy solutions are also closely linked with verifiability requirements [166] and with tractability as well as forensic techniques. We should formulate threat models to detect cyber attacks and data leakage scenarios [166] such as infrastructure attacks and rogue nodes. In particular, a privacy-preserving solution should provide a well-maintained log that may help in preventing fraud and in resolving disputes. Traceability and forensic techniques should be taken into consideration during service design and the development of service architectures [167]. In the context of the SG and real-time ecosystems, we should not only cover the effectiveness of privacy-preserving methods, but also have the ability to monitor and detect anomalies in real-time and analyze the data collected and aggregated from the different sources. The challenge here is to define an effective method to identify legitimate traffic, to enable forensic investigation on subversive and illegal activities, and to mitigate any possible insider attacks against the infrastructure. In fact, security and forensics techniques are fundamental, especially when an adversary tampers with a device from which data are collected or aggregated or when the same adversary successfully performs cloning attacks.

Multi-disciplinary research approaches which consider training, legal, and technological aspects should be developed to address the privacy issues that arise with the SG environment. Future SG privacy solutions should include the design and development of architectures that prevent unnecessary linking between the user identity and the SG services, while guaranteeing traceability and accountability in the presence of an important set of interconnected engineering resources and nodes. We argue that a holistic approach is needed to identify and address privacy challenges throughout the engineering phase of the SG in order to ensure SG solutions that maintain privacy and are also secure, scalable, and cost-effective.

15.6 Conclusion

Over the past several years we have witnessed huge investments and interests from industry and governments in SG technologies. Various stakeholders (residential/commercial customers, local government, utility operators, etc.) are expected to reap several benefits associated with the SG including improved energy efficiency, increased reliability, reduced energy costs, greater flexibility in energy consumption, better safety and security, and an improved environment (through renewable, renewable non-variable, non-renewable/non-variable energy sources). The deployment of SG technologies has also raised considerable concerns in data privacy issues of SG users, as we have discussed in this chapter. The privacy concerns are mostly related to the collection and use of energy consumption data. In this context, we have discussed various SG privacy issues and we have presented SG privacy architectures and approaches that have been recently proposed in the literature. A unique taxonomy of the various privacy protection mechanisms proposed in the literature has been developed. We also identified the various strengths and weaknesses of these privacy solutions. The success of SG technology and its wide acceptance rely on gaining the trust and confidence of customers, which in turn depends on assurances regarding the protection of their privacy.

References

1. Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev 4(5):193–220. doi:10.2307/1321160, url:http://www.jstor.org/stable/1321160
2. Westin AF (1967) Privacy and freedom. Atheneum
3. DeCew J (2013) Privacy. In: Zalta EN (ed) The Stanford encyclopedia of philosophy, fall 2013 edn, url:http://plato.stanford.edu/entries/privacy/
4. Richards NM (2014) Four myths of privacy. In: Sarat A (ed) A world without privacy?, April 2014 edn, url:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427808
5. Holvast J (2007) 27—history of privacy. In: Leeuw KD, Bergstra J (eds) The history of information security. Elsevier Science B.V., Amsterdam, pp 737–769. doi:http://dx.doi.org/10.1016/B978-044451608-4/50028-6, url:http://www.sciencedirect.com/science/article/pii/B9780444516084500286
6. OECD, for Economic Co-operation, O., Development (1981) Guidelines on the protection of privacy and transborder flows of personal data. Organisation for Economic Co-operation and Development; OECD Publications and Information Center Paris, Washington, D.C, url: http://oe.cd/privacy, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
7. OECD (2013) Guidelines on the protection of privacy and transborder flows of personal data. Organisation for Economic Co-operation and Development; OECD Publications and Information Center Paris, Washington, D.C, url:http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
8. Chaum D (1985) Security without identification: transaction systems to make big brother obsolete. Commun ACM 28(10):1030–1044. doi:10.1145/4372.4373, url:http://dl.acm.org/citation.cfm?id=4372.4373

9. van Rossum H, Gardeniers H, Borking J, Cavoukian A, Brans J, Muttupulle N, Magistrale N (1995) Privacy-enhancing technologies: the path to anonymity. Information and Privacy Commissioner/Ontario, Canada & Registratiekamer, Den Haag, The Netherlands
10. Blarkom GV, Borking J, Olk J (2003) Handbook of privacy and privacy-enhancing technologies. Privacy incorporated software, pp 42–50, url:http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf
11. DRAFT NISTIR 7628 Revision 1 (2013) Guidelines for smart grid cyber security. Supportive analyses and references, vol 3. Smart Grid Interoperability Panel (SGIP), Smart Grid Cybersecurity Committee, url:http://csrc.nist.gov/publications/drafts/nistir-7628-r1/draft_nistir_7628_r1_vol3.pdf
12. DRAFT NISTIR 7628 Revision 1 (2013) Guidelines for smart grid cybersecurity. Privacy and the smart grid, vol 2. Smart Grid Interoperability Panel (SGIP), Smart Grid Cybersecurity Committee, url:http://csrc.nist.gov/publications/drafts/nistir-7628-r1/draft_nistir_7628_r1_vol2.pdf
13. DRAFT NISTIR 7628 Revision 1 (2013) Guidelines for smart grid cybersecurity: smart grid cybersecurity strategy, architecture, and high-level requirements, vol 1. Smart Grid Interoperability Panel (SGIP), Smart Grid Cybersecurity Committee, url: http://csrc.nist.gov/publications/drafts/nistir-7628-r1/draft_nistir_7628_r1_vol1.pdf
14. Asghar M, Miorandi D (2013) A holistic view of security and privacy issues in smart grids. In: Cuellar J (ed) Smart grid security. Lecture notes in computer science, vol 7823. Springer, Berlin, pp 58–71, url:http://dx.doi.org/10.1007/978-3-642-38030-3_4
15. Barenghi A, Pelosi G (2011) Security and privacy in smart grid infrastructures. In: Proceedings—international workshop on database and expert systems applications, DEXA, pp 102–108. doi:10.1109/DEXA.2011.74
16. Hauser CH, Bakken DE, Dionysiou I, Gjermudød KK, Irava VS, Helkey J, Bose A (2007) Security, trust and QoS in next-generation control and communication for large power systems. Int J Crit Infrastruct 4:3–16
17. Chen TM (2010) Survey of cyber security issues in smart grids. doi:10.1117/12.862698, url: http://dx.doi.org/10.1117/12.862698
18. Cleveland FM (2008) Cyber security issues for advanced metering infrastructure (AMI). In: Power and energy society general meeting—conversion and delivery of electrical energy in the 21st century, 2008 IEEE, pp 1–5. doi:10.1109/PES.2008.4596535
19. Das SK, Kant K, Zhang N (2012) Handbook on securing cyber-physical critical infrastructure. Elsevier Science, url:http://books.google.com/books?id=MftTeQivgA0C
20. Fleury T, Khurana H, Welch V (2009) Towards a taxonomy of attacks against energy control systems, pp 71–85. Springer. doi:10.1007/978-0-387-88523-0_6, url:http://www.springerlink.com/content/d38w8553g6211838/
21. For E, Chan AC, Zhou J (2013) On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. Commun Mag, IEEE 51(1):58–65. doi:10.1109/MCOM.2013.6400439
22. Fries S, Falk R, Sutor A (2013) Smart grid information exchange securing the smart grid from the ground. In: Cuellar J (ed) Smart grid security. Lecture notes in computer science, vol 7823. Springer, Berlin, pp 26–44, url:http://dx.doi.org/10.1007/978-3-642-38030-3_2
23. Hahn A, Govindarasu M (2011) Cyber attack exposure evaluation framework for the smart grid. IEEE Trans Smart Grid 2(4):835–843. doi:10.1109/TSG.2011.2163829
24. Hull J, Khurana H, Markham T, Staggs K (2012) Staying in control: cybersecurity and the modern electric grid. Power Energy Mag, IEEE 10(1):41–48. doi:10.1109/MPE.2011.943251
25. Jokar P, Arianpoo N, Leung VCM (2012) A survey on security issues in smart grids. Secur Commun Netw. doi:10.1002/sec.559, url:http://dx.doi.org/10.1002/sec.559
26. Li X, Liang X, Lu R, Shen X, Lin X, Zhu H (2012) Securing smart grid: cyber attacks, countermeasures, and challenges. Commun Mag IEEE 50(8):38–45. doi:10.1109/MCOM.2012.6257525

27. Liu J, Xiao Y, Li S, Liang W, Chen CLP (2012) Cyber security and privacy issues in smart grids. Commun Surv Tutor IEEE 14(4):981–997. doi:10.1109/SURV.2011.122111.00145
28. McBride AJ, McGee AR (2012) Assessing smart grid security. Bell Labs Tech J 17(3):87–103. doi:10.1002/bltj.21560, url:http://dx.doi.org/10.1002/bltj.21560
29. Mo Y, Kim TH, Brancik K, Dickinson D, Lee H, Perrig A, Sinopoli B (2012) Cyber-physical security of a smart grid infrastructure. Proc IEEE 100(1):195–209. doi:10.1109/JPROC.2011.2161428
30. Nordell DE (2012) Terms of protection: the Many faces of smart grid security. Power Energy Mag IEEE 10(1):18–23. doi:10.1109/MPE.2011.943194
31. Systems S, McDaniel P, McLaughlin S (2009) Security and privacy challenges in the smart grid. Secur Priv IEEE 7(3):75–77. doi:10.1109/MSP.2009.76
32. Wang W, Lu Z (2013) Cyber security in the smart grid: survey and challenges. Comput Netw 57(5):1344–1371. doi:http://dx.doi.org/10.1016/j.comnet.2012.12.017 , url:http://www.sciencedirect.com/science/article/pii/S1389128613000042
33. Wang Y, Ruan D, Gu D, Gao J, Liu D, Xu J, Chen F, Dai F, Yang J (2011) Analysis of smart grid security standards. In: 2011 IEEE international conference on computer science and automation engineering (CSAE), vol 4, pp 697–701. doi:10.1109/CSAE.2011.5952941
34. Xiao Y (2013) Security and privacy in smart grids. Taylor & Francis, url:http://books.google.com/books?id=QQ2oY0IrRM8C
35. Yan Y, Qian Y, Sharif H, Tipper D (2012) A survey on cyber security for smart grid communications. Commun Surv Tutor IEEE 14(4):998–1010. doi:10.1109/SURV.2012.010912.00035
36. Zhou L, Chen S (2012) A survey of research on smart grid security. In: Lei J, Wang F, Li M, Luo Y (eds) Network computing and information security. Commun Comput Inf Sci 345:395–405 (Springer, Berlin, url:http://dx.doi.org/10.1007/978-3-642-35211-9_52
37. Fang X, Misra S, Xue G, Yang D (2012) Smart grid the new and improved power grid: a survey. IEEE Commun Surv Tutor 14(4):944–980. doi:10.1109/SURV.2011.101911.00087, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6099519
38. Gharavi H, Ghafurian R (2011) {Smart grid}: the electric energy system of the future. Proc IEEE 99(6):917–921. doi:10.1109/jproc.2011.2124210, url:http://dx.doi.org/10.1109/jproc.2011.2124210
39. US Department of Energy (2006) Benefits of demand response in electricity markets and recommendations for achieving them—a report to the United States Congress Pursant to Section 1252 of the Energy Policy Act of 2005, pp 122
40. National Institute of Standards and Technology (2013: NIST framework and roadmap for smart grid interoperability standards, Release 2.0. smart grid interoperability panel (SGIP), url:http://j.mp/1rs1tKs http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/IKBFramework/NIST_Framework_Release_2-0_corr.pdf
41. International Electrotechnical Commission (2010) IEC Strategic Group 3, Smart grid standardization roadmap, url:http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf
42. European Committee for Electrotechnical Standardization (2011) Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids
43. IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS) (2011) End-use applications, and loads. IEEE Std 2030-2011, pp 1–126. doi:10.1109/IEEESTD.2011.6018239
44. International Energy Agency (2013) Tracking clean energy progress 2013. IEA input to the clean energy ministerial, url:http://www.iea.org/publications/TCEP_web.pdf
45. National Energy Technology Laboratory, the U.S. Department of Energy, D.O.E., Office of Electricity Delivery and Energy Reliability (2008) Advanced metering infrastructure. White Paper
46. Kroposki B, Pink C, Basso T, DeBlasio R (2007) Microgrid standards and technology development. In: Power engineering society general meeting, 2007, pp 1–4. IEEE. doi:10.1109/PES.2007.386053

47. Lasseter RH (2002) MicroGrids. In: Power engineering society winter meeting, vol 1, pp 305–308. IEEE. doi:10.1109/PESW.2002.985003
48. Vaccaro A, Popov M, Villacci D, Terzija V (2011) An integrated framework for smart microgrids modeling, monitoring, control, communication, and verification. Proc IEEE 99 (1):119–132. doi:10.1109/JPROC.2010.2081651
49. Masters GM (2004) Renewable and efficient electric power systems. Wiley, New York)
50. Mohsenian-Rad AH, Wong VWS, Jatskevich J, Schober R, Leon-Garcia A (2010) Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid. IEEE Trans Smart Grid **1**(3):320–331. doi:10.1109/TSG.2010.2089069
51. Mohsenian-Rad AH, Leon-Garcia A (2010) Optimal residential load control with price prediction in real-time electricity pricing environments. IEEE Trans Smart Grid 1(2):120–133. doi:10.1109/TSG.2010.2055903
52. Samadi P, Mohsenian-Rad AH, Schober R, Wong VWS, Jatskevich J (2010) Optimal real-time pricing algorithm based on utility maximization for smart grid. In: IEEE SmartGridComm, pp 415–420). doi:10.1109/SMARTGRID.2010.5622077
53. Zhu Z, Tang J, Lambotharan S, Chin WH, Fan Z (2011) An integer linear programming and game theory based optimization for demand-side management in smart grid. In: GLOBECOM workshops (GC Wkshps), 2011 IEEE, pp 1205–1210. doi:10.1109/GLOCOMW.2011.6162372
54. Hajdu LP, Peschon J, Tinney WF, Piercy DS (1968) Optimum load-shedding policy for power systems. IEEE Trans Power Apparatus Syst **PAS-87**(3):784–795. doi:10.1109/TPAS.1968.292194
55. Aponte EE, Nelson JK (2006) Time optimal load shedding for distributed power systems. IEEE Trans Power Syst 21(1):269–277. doi:10.1109/TPWRS.2005.857826
56. De Tuglie E, Dicorato M, La Scala M, Scarpellini P (2000) A corrective control for angle and voltage stability enhancement on the transient time-scale. IEEE Trans Power Syst 15 (4):1345–1353. doi:10.1109/59.898111
57. Du P, Nelson JK (2009) Two-step solution to optimal load shedding in a micro-grid. In: Power systems conference and exposition, 2009. PSCE ‘09. IEEE/PES, pp 1–9. doi:10.1109/PSCE.2009.4840112
58. Molina-Markham A, Shenoy P, Fu K, Cecchet E, Irwin D (2010) Private memoirs of a smart meter. In: Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building, BuildSys ‘10. ACM, New York, NY, USA, pp 61–66. doi:10.1145/1878431.1878446
59. Wang Z, Zheng G, Member S (2012) Residential appliances identification and monitoring by a nonintrusive method. IEEE Trans Smart Grid 3(1):80–92. doi:10.1109/TSG.2011.2163950
60. Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE (2002) SPINS: security protocols for sensor networks. Wirel Netw 8(5):521–534. doi:10.1023/A:1016598314198
61. Miller J (2008) Who are you, Part II: more on the trade-off between information utility and privacy. IEEE Internet Comput 12(6):91–93. doi:10.1109/MIC.2008.135, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4670125
62. Miller J (2008) Who are you? The trade-off between information utility and privacy. IEEE Internet Comput 12(4):93–96. doi:10.1109/MIC.2008.91, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4557986
63. Pedersen DM (1982) Personality correlates of privacy. J Psychol 112(1):11–14. doi:10.1080/00223980.1982.9923528, url:http://www.tandfonline.com/doi/abs/10.1080/00223980.1982.9923528
64. Brierley N (1992) The meaning and use of privacy: a study of young adults. Ph.D. thesis, The University of Arizona
65. International Energy Agency (2011) Technology roadmap: smart grids, url:http://www.iea.org/papers/2011/
66. Kindy DA, Pathan ASK (2011) A survey on SQL injection: vulnerabilities, attacks, and prevention techniques. In: 2011 IEEE 15th international symposium on consumer electronics

(ISCE), pp 468–471. IEEE. doi:10.1109/ISCE.2011.5973873, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5973873

67. Singh M (2002) Privacy for telecom services. IEEE Internet Comput 6(1):4–5. doi:10.1109/MIC.2002.978364, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=978364
68. Hart GWG (1992) Nonintrusive appliance load monitoring. In: Proc IEEE **80**(12):1870–1891. doi:10.1109/5.192069, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=192069
69. Zeifman M, Roth K (2011) Nonintrusive appliance load monitoring: review and outlook. IEEE Trans Consum Electron 57(1):76–84. doi:10.1109/TCE.2011.5735484, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5735484
70. Lisovich MA, Mulligan DK, Wicker SB (2010) Inferring personal information from demand-response systems. IEEE Secur Priv Mag 8(1):11–20. doi:10.1109/MSP.2010.40, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5403146
71. Khurana H, Hadley M, Lu N, Frincke DA (2010) Smart-grid security issues. IEEE Secur Priv 8:81–85. doi:10.1109/MSP.2010.49
72. Li FF, Luo B, Liu P (2010) Secure information aggregation for smart grids using homomorphic encryption. In: IEEE SmartGridComm, pp 327–332. IEEE. doi:10.1109/SMARTGRID.2010.5622064, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622064
73. Zeadally S, Pathan AS, Alcaraz C, Badra M (2013) Towards privacy protection in smart grid. Wirel Pers Commun 73(1):23–50. doi:10.1007/s11277-012-0939-1, url:http://dx.doi.org/10.1007/s11277-012-0939-1
74. Budka K, Deshpande J, Hobby J, Kim YJKYJ, Kolesnikov V, Lee WLW, Reddington T, Thottan M, White CCA, Choi JICJI, Hong JHJ, Kim JKJ, Ko WKW, Nam YWNYW, Sohn SYSSY (2010) GERI—Bell labs smart grid research focus: economic modeling, networking, and security & privacy. In: 2010 first IEEE international conference on smart grid communications (SmartGridComm), pp 208–213. IEEE. doi:10.1109/SMARTGRID.2010.5622043, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622043
75. Efthymiou C, Kalogridis G (2010) Smart grid privacy via anonymization of smart metering data. In: SmartGridComm, pp 238–243. doi:10.1109/SMARTGRID.2010.5622050
76. Vetter B, Ugus O, Westhoff D, Sorge C (2012) Homomorphic primitives for a privacy-friendly smart metering architecture. In: SECRYPT 2012—proceedings of the international conference on security and cryptography, pp 102–112, url http://www.scopus.com/inward/record.url?eid=2-s2.0-84867646415&partnerID=tZOtx3y1
77. Cardenas A, Safavi-Naini R (2012) Security and privacy in the smart grid. In: Das SK, Kant K, Zhang N (eds) Handbook on securing cyber-physical critical infrastructure
78. Chen L, Lu R, Cao, Z (2014) PDAFT: a privacy-preserving data aggregation scheme with fault tolerance for smart grid communications. Peer-to-peer networking and applications, pp 1–11. doi:10.1007/s12083-014-0255-5, url:http://dx.doi.org/10.1007/s12083-014-0255-5
79. Chen L, Lu R, Cao Z, AlHarbi K, Lin X (2014) MuDA: multifunctional data aggregation in privacy-preserving smart grid communications. Peer-to-peer networking and applications, pp 1–16. doi:10.1007/s12083-014-0292-0, url:http://dx.doi.org/10.1007/s12083-014-0292-0
80. Chim T, Yiu S, Li V, Hui C, Zhong J (2014) PRGA: privacy-preserving recording amp; Gateway-assisted authentication of power usage information for smart grid. IEEE Trans Dependable Secure Comput PP(99):1. doi:10.1109/TDSC.2014.2313861
81. Gómez Mármol F, Sorge C, Petrlic R, Ugus O, Westhoff D, Martnez Pérez G (2013) Privacy-enhanced architecture for smart metering. Int J Inf Secur 12(2):67–82. doi:10.1007/s10207-012-0181-6, url:http://dx.doi.org/10.1007/s10207-012-0181-6, http://link.springer.com/10.1007/s10207-012-0181-6
82. Liang X, Li X, Lu R, Lin X, Shen X (2013) UDP: usage-based dynamic pricing with privacy preservation for smart grid. IEEE Trans Smart Grid 4(1):141–150. doi:10.1109/TSG.2012.2228240

83. Phom HS, Kuntze N, Rudolph C, Cupelli M, Liu J, Monti A, Simo Fhom H (2010) A user-centric privacy manager for future energy systems. Power System, pp 1–7. doi:10.1109/POWERCON.2010.5666447, url:http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5666447, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5666447
84. Rottondi C, Verticale G, Capone A (2013) Privacy-preserving smart metering with multiple data consumers. Comput Netw 57(7):1699–1713. doi:http://dx.doi.org/10.1016/j.comnet.2013.02.018, url:http://www.sciencedirect.com/science/article/pii/S1389128613000364
85. Finster S, Baumgart I (2013) Elderberry: a peer-to-peer, privacy-aware smart metering protocol. In: Proceedings—IEEE INFOCOM, pp 3411–3416. doi:10.1109/INFCOM.2013.6567173
86. Stoica I, Morris R, Liben-Nowell D, Karger DR, Kaashoek MF, Dabek F, Balakrishnan H (2003) Chord: A scalable peer-to-peer lookup protocol for Internet applications. IEEE/ACM Trans Netw 11:17–32. doi:10.1109/TNET.2002.808407
87. Badra M, Zeadally S (2014) Design and Performance analysis of a virtual ring architecture for smart grid privacy. IEEE Trans Forensics Secur 9(2):321–329. doi:10.1109/TIFS.2013.2296441
88. Finster S, Baumgart I (2013) Pseudonymous smart metering without a trusted third party. In: Proceedings—12th IEEE international conference on trust, security and privacy in computing and communications, TrustCom 2013, pp 1723–1728. doi:10.1109/TrustCom.2013.234
89. Li S, Choi K, Chae K (2014) OCPM: ortho code privacy mechanism in smart grid using ring communication architecture. Ad Hoc Netw. doi:http://dx.doi.org/10.1016/j.adhoc.2014.05.007, url:http://www.sciencedirect.com/science/article/pii/S1570870514001024
90. Mármol F, Sorge C, Ugus O, Pérez G., Mármol FG, Pérez GM (2012) Do not snoop my habits: preserving privacy in the smart grid. IEEE Commun Mag 50(5):166–172. doi:10.1109/MCOM.2012.6194398, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6194398
91. Thoma C, Cui T, Franchetti F (2012) Secure multiparty computation based privacy preserving smart metering system. In: 2012 North American power symposium (NAPS), pp 1–6. IEEE. doi:10.1109/NAPS.2012.6336415, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6336415
92. Yu C, Chen C, Kuo S, Chao H (2014) Privacy-preserving power request in smart grid networks. Syst J IEEE 8(2):441–449. doi:10.1109/JSYST.2013.2260680
93. Ge B, Zhu WTW (2013) Preserving user privacy in the smart grid by hiding appliance load characteristics. In: Wang G, Ray I, Feng D, Rajarajan M (eds) Cyberspace safety and security. Lecture notes in computer science, vol 8300. Springer International Publishing, pp 67–80 (2013), url:http://link.springer.com/chapter/10.1007/978-3-319-03584-0_6
94. Kalogridis G, Cepeda R, Denic SZ, Lewis T, Efthymiou C (2011) ElecPrivacy: evaluating the privacy protection of electricity management algorithms. IEEE Trans Smart Grid 2 (4):750–758. doi:10.1109/TSG.2011.2160975, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6003811
95. Kalogridis G, Efthymiou C, Denic SZ, Lewis TA, Cepeda R (2010) Privacy for smart meters: towards undetectable appliance load signatures. In: 2010 first IEEE international conference on smart grid communications (SmartGridComm), pp 232–237. doi:10.1109/SMARTGRID.2010.5622047
96. Kalogridis GG, Denic SZ (2011) Data mining and privacy of personal behaviour types in smart grid. In: Proceedings—IEEE international conference on data mining, ICDM, pp 636–642. IEEE. doi:10.1109/ICDMW.2011.58, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6137440
97. Zhao J, Jung T, Wang Y, Li XY (2014) Achieving differential privacy of data disclosure in the smart grid. In: IEEE INFOCOM 2014
98. Li H, Mao R, Lai L, Qiu RC (2010) Compressed meter reading for delay-sensitive and secure load report in smart grid. In: 2010 first IEEE international conference on smart grid communications (SmartGridComm), pp 114–119. IEEE. doi:10.1109/SMARTGRID.2010.5622027, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622027

99. Rajagopalan SR, Sankar L, Mohajer S, Poor HV Smart meter privacy: a utility-privacy framework. In: 2011 IEEE international conference on smart grid communications, SmartGridComm 2011, pp 190–195. doi:10.1109/SmartGridComm.2011.6102315
100. Candes E, Romberg J, Tao T (2006) Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE Trans Inf Theory 52 (2):489–509. doi:10.1109/TIT.2005.862083, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1580791
101. Candes EJ, Tao T (2006) Near-optimal signal recovery from random projections: universal encoding strategies? IEEE Trans Inf Theory 52(12):5406–5425. doi:10.1109/TIT.2006.885507, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4016283
102. Donoho DL (2006) Compressed sensing. IEEE Trans Inf Theory 52(4):1289–1306. doi:10.1109/Tit.2006.871582, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1614066
103. Shamir A (1985) Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO 84 on advances in cryptology, pp 47–53. doi:10.1007/3-540-39568-7_5, url:http://dl.acm.org/citation.cfm?id=19478.19483
104. Boneh D, Franklin M (2003) Identity-based encryption from the weil pairing. doi:10.1137/S0097539701398521
105. Cocks C (2001) An identity based encryption scheme based on quadratic residues. Cryptogr Coding, pp 360–363. doi:10.1007/3-540-45325-3_32, url:http://link.springer.com/chapter/10.1007/3-540-45325-3_32
106. Kalogridis G, Sooriyabandara M, Fan Z, Mustafa MA (2014) Toward unified security and privacy protection for smart meter networks. Syst J IEEE 8(2):641–654. doi:10.1109/JSYST.2013.2260940
107. Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security—CCS '06. ACM Press, New York, p 89. doi:10.1145/1180405.1180418, url:http://dl.acm.org/citation.cfm?id=1180405.1180418
108. Li D, Aung Z, Williams J, Sanchez A (2014) P2DR: privacy-preserving demand response system in smart grids. In: 2014 international conference on computing, networking and communications (ICNC), pp 41–47. doi:10.1109/ICCNC.2014.6785302
109. Cheung JCL, Chim TW, Yiu SM, Hui LCK, Li VOK (2011) Credential-based privacy-preserving power request scheme for smart grid network. In: 2011 IEEE global telecommunications conference—GLOBECOM 2011, pp 1–5. IEEE. doi:10.1109/GLOCOM.2011.6134566, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6134566
110. Chim T, Yiu S, Hui L, Li V, Mui T, Tsang Y, Kwok C, Yu K (2012) Selling power back to the grid in a secure and privacy-preserving manner. In: Chim T, Yuen T (eds) Information and communications security, vol 7618., Lecture notes in computer scienceSpringer, Berlin, pp 445–452
111. Yao AC (1982) Protocols for secure computations. 23rd annual symposium on foundations of computer science (sfcs 1982), pp 160–164. doi:10.1109/SFCS.1982.38, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4568388
112. Goldreich O, Micali S, Wigderson A (1987) How to play any mental game. In: ACM symposium on theory of computing, STOC '87, pp 218–229. ACM. doi:10.1145/28395.28420
113. Rivest RL, Adleman L, Dertouzos ML (1978) On data banks and privacy homomorphisms. In: Foundations of secure computation, pp 169–179
114. Gentry C (2009) A fully homomorphic encryption scheme. Ph.D. thesis. doi:10.1145/1536414.1536440, url:http://cs.au.dk/stm/local-cache/gentry-thesis.pdf
115. Paillier P, Pointcheval D (1999) Efficient public-key cryptosystems provably secure against active adversaries. In: ASIACRYPT'99, vol 99, pp 1–13. doi:10.1007/978-3-540-48000-6_14, url:http://link.springer.com/chapter/10.1007/978-3-540-48000-6_14

116. Paillier P, Stern PJ, Eurocrypt C (1999) Public-key cryptosystems based on composite degree residuosity classes. Advances in cryptology EUROCRYPT 99, vol 1592, pp 223–238. doi:10.1007/3-540-48910-X_16
117. Boneh D, Goh E, Nissim K (2005) Evaluating 2-DNF formulas on ciphertexts. Theory of cryptography, pp 325–341. doi:10.1007/978-3-540-30576-7_18
118. Erkin Z, Tsudik G (2012) Private computation of Spatial and temporal power consumption with smart meters. In: Applied cryptography and network security. Lecture notes in computer science, vol 7341, pp 561–577, url:http://link.springer.com/chapter/10.1007/978-3-642-31284-7_33
119. Garcia FF, Jacobs B (2011) Privacy-friendly energy-metering via homomorphic encryption. Secur Trust Manage 6710:226–238, url:http://link.springer.com/chapter/10.1007/978-3-642-22444-7_15
120. Kirschbaum M, Plos T, Schmidt JM (2013) On secure multi-party computation in bandwidth-limited smart-meter systems. In: 2013 international conference on availability, reliability and security, pp 230–235. IEEE. doi:10.1109/ARES.2013.137, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6657245
121. Lu R, Liang X, Li X, Lin X, Shen X (2012) EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans Parallel Distrib Syst 23:1621–1632. doi:10.1109/TPDS.2012.86
122. Rottondi C, Verticale G, Krauss C (2013) Distributed privacy-preserving aggregation of metering data in smart grids. IEEE JSAC 31(7):1342–1354. doi:10.1109/JSAC.2013.130716
123. Cramer R, Shoup V (1998) A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: EUROCRYPT ‘98: advances in cryptology, pp 13–25. doi:10.1007/BFb0055715, url:http://www.springerlink.com/content/bejnetn8v8n5vkc3/
124. Baharlouei Z, Hashemi M (2014) Efficiency-fairness trade-off in privacy-preserving autonomous demand side management. IEEE Trans Smart Grid 5(2):799–808. doi:10.1109/TSG.2013.2296714, url http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6740907
125. Clifton C, Kantarcioglu M, Vaidya J, Lin X, Zhu MY (2002) Tools for privacy preserving distributed data mining. SIGKDD Explor Newsl 4(2):28–34. doi:10.1145/772862.772867
126. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613. doi:http://doi.acm.org/10.1145/359168.359176, url:http://doi.acm.org/10.1145/359168.359176
127. Chim TW, Yiu SM, Hui LCK, Li VOK (2011) PASS: privacy-preserving authentication scheme for smart grid network. In: 2011 IEEE international conference on smart grid communications, SmartGridComm 2011, pp 196–201. IEEE. doi:10.1109/SmartGridComm.2011.6102316, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6102316
128. Liu H, Ning H, Zhang Y, Xiong Q, Yang LT (2014) Role-dependent privacy preservation for secure V2G networks in the smart grid. IEEE Trans Inf Forensics Secur 9(2):208–220. doi:10.1109/TIFS.2013.2295032
129. Goldreich O, Micali S, Wigderson A (1991) Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. J ACM 38(3):690–728. doi:10.1145/116825.116852, url:http://dl.acm.org/citation.cfm?id=116825.116852
130. Rial A, Danezis G (2011) Privacy-preserving smart metering. In: Proceedings of the 10th annual ACM workshop on privacy in the electronic society—WPES ‘11. ACM Press, New York, p 49. doi:10.1145/2046556.2046564, url:http://dl.acm.org.proxy2.library.illinois.edu/citation.cfm?id=2046556.2046564
131. Bellare M, Goldreich O (1993) Advances in cryptology CRYPTO 92. In: Brickell EF (ed) Advances in cryptology CRYPTO 92. Lecture notes in computer science, vol 740. Springer, Berlin, pp 390–420. doi:10.1007/3-540-48071-4, url:http://www.springerlink.com/index/10.1007/3-540-48071-4
132. Chaum D (1983) Blind signatures for untraceable payments. In: Chaum D, Rivest RL, Sherman AT (eds) Advances in cryptology 1983. Springer, Boston, pp 199–203. doi:10.1007/978-1-4757-0602-4, url:http://link.springer.com/10.1007/978-1-4757-0602-4

133. Stadler M, Piveteau JMJJM, Camenisch J (1995) Fair blind signatures. In: Advances in Cryptology Eurocrypt 95, pp 209–219. doi:10.1007/3-540-49264-X_17, url:http://link.springer.com/chapter/10.1007/3-540-49264-X_17
134. Rabin MO (1981) How to exchange secrets by oblivious transfer
135. Aiello B, Ishai Y, Reingold O (2001) Priced oblivious transfer: how to sell digital goods. In: Advances in cryptology EUROCRYPT 2001. Lecture notes in computer science, vol 2045. Springer, Berlin, pp 119–135. doi:10.1007/3-540-44987-6_8, url:http://www.springerlink.com/index/557e8bykh3vbf0kc.pdf
136. Fan CI, Huang SY, Artan W (2013) Design and implementation of privacy preserving billing protocol for smart grid. J Supercomput 66(2):841–862. doi:10.1007/s11227-013-0905-z, url:http://dx.doi.org/10.1007/s11227-013-0905-z
137. Cárdenas A, Amin S, Schwartz G (2012) Privacy-aware sampling for residential demand response programs. In: Proceedings of 1st international ACM, url:http://www.eecs.berkeley.edu/schwartz/HiCons2012ASG.pdf
138. Yan Y, Qian Y, Sharif H (2011) A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. In: IEEE WCNC, pp 909–914. doi:10.1109/WCNC.2011.5779257
139. Chrestenson HE (1955) A class of generalized Walsh functions. Pac J Math 5(1):17–31, url:http://projecteuclid.org/euclid.pjm/1103044605
140. Wallis JS (1975) On Hadamard matrices. J Comb Theory Ser A 18(2):149–164. doi:10.1016/0097-3165(75)90003-5, url:http://www.sciencedirect.com/science/article/pii/0097316575900035
141. Berrar DD, Dubitzky W (2013) Information gain (KullbackLeibler divergence). In: Dubitzky W, Wolkenhauer O, Cho KH, Yokota H (eds) Encyclopedia of systems biology 2013. Springer, New York, pp 1022–1023. doi:10.1007/978-1-4419-9863-7, url:http://link.springer.com/10.1007/978-1-4419-9863-7
142. Gunduz D, Gomez-Vilardebo J, Poor HV, Tan O (2013) Information theoretic privacy for smart meters. In: 2013 information theory and applications workshop (ITA), pp 1–7. IEEE. doi:10.1109/ITA.2013.6503006, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6503006
143. Sankar L, Rajagopalan SR, Mohajer S, Poor HV (2013) Smart meter privacy: a theoretical framework. IEEE Trans Smart Grid 4(2):837–846. doi:10.1109/TSG.2012.2211046
144. Kim Y, Ngai ECH, Srivastava MB (2011) Cooperative state estimation for preserving privacy of user behaviors in smart grid. In: 2011 IEEE international conference on smart grid communications, SmartGridComm 2011, pp 178–183. doi:10.1109/SmartGridComm.2011.6102313
145. Huang YF, Werner S, Huang J, Kashyap N, Gupta V (2012) State estimation in electric power grids: meeting new challenges presented by the requirements of the future grid. IEEE Signal Process Mag 29(5):33–43. doi:10.1109/MSP.2012.2187037, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6279588
146. Jia W, Zhu H, Cao Z, Dong X, Xiao C, Member S (2014) Human-factor-aware privacy-preserving aggregation in smart grid. Syst J IEEE 8(2):598–607. doi:10.1109/JSYST.2013.2260937
147. Bohli JM, Sorge C, Ugus O (2010) A privacy model for smart metering. In: IEEE ICC, pp 1–5. doi:10.1109/ICCW.2010.5503916
148. Lin HY, Tzeng WG, Shen ST, Lin BSP (2012) A practical smart metering system supporting privacy preserving billing and load monitoring. In: Feng B, Samarati P, and Zhou J (ed) Applied cryptography and network security. Springer, Berlin, pp 544–560, url:http://link.springer.com/chapter/10.1007%2F978-3-642-31284-7_32#
149. Ren X, Yang X, Lin J, Yang Q, Yu W (2013) On scaling perturbation based privacy-preserving schemes in smart metering systems. In: 2013 22nd international conference on computer communication and networks (ICCCN), pp 1–7. IEEE. doi:10.1109/ICCCN.2013.6614162, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6614162

150. Zhang H, Yu N, Wen Y, Zhang W (2014) Toward optimal noise distribution for privacy preserving in data aggregation. Comput Secur. doi:http://dx.doi.org/10.1016/j.cose.2014.05.009, url:http://linkinghub.elsevier.com/retrieve/pii/S016740481400090X, http://www.sciencedirect.com/science/article/pii/S016740481400090X

151. Acs G, Castelluccia C, Gergely Acs G (2011) I have a DREAM! (DiffeRentially privatE smArt Metering). In Filler T, Pevný T, Craver S, Ker A (eds) Information hiding. Lecture notes in computer science, vol 6958. Springer, Berlin, pp. 118–132. doi:10.1007/978-3-642-24178-9, url:http://www.springerlink.com/index/10.1007/978-3-642-24178-9, http://link.springer.com/10.1007/978-3-642-24178-9, http://link.springer.com/chapter/10.1007/978-3-642-24178-9_9

152. Ghosh A, Roughgarden T, Sundararajan M (2009) Universally utility-maximizing privacy mechanisms. In: Proceedings of the 41st annual ACM symposium on theory of computing—STOC '09. ACM Press, New York, p 351. doi:10.1145/1536414.1536464, url:http://dl.acm.org/citation.cfm?id=1536414.1536464

153. Dwork C (2008) Differential privacy: a survey of results. Theory Appl Models Comput 4978:1–19. doi:10.1007/978-3-540-79228-4_1, url:http://www.springerlink.com/index/u963k75981004046.pdf

154. Dwork C, Kenthapadi K, McSherry F, Mironov I, Naor M (2006) Our data, ourselves: privacy via distributed noise generation. Lecture notes in computer science (including subseries Lecture notes in artificial intelligence and Lecture notes in bioinformatics), vol 4004. LNCS, pp 486–503. doi:10.1007/11761679_29

155. Dan G, Lui KSKS, Tabassum R, Zhu Q, Nahrstedt K (2013) SELINDA: a secure, scalable and light-weight data collection protocol for smart grids. In: 2013 IEEE international conference on smart grid communications (SmartGridComm), pp 480–485. IEEE. doi:10.1109/SmartGridComm.2013.6688004, url:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6688004

156. Cho S, Li H, Choi BJ (2014) PALDA: efficient privacy-preserving authentication for lossless data aggregation in smart grids. In: 2014 IEEE international conference on smart grid communications (SmartGridComm). Venice, Italy

157. Feng T, Wang C, Zhang W, Ruan L (2008) Confidentiality protection for distributed sensor data aggregation. In: IEEE INFOCOM. doi:10.1109/INFOCOM.2008.20

158. Groat MM, He W, Forrest S (2011) KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks. In: IEEE INFOCOM, pp 2024–2032. doi:10.1109/INFCOM.2011.5935010

159. He W, Liu X, Nguyen H, Nahrstedt K, Abdelzaher T (2007) PDA: privacy-preserving data aggregation in wireless sensor networks. In: IEEE INFOCOM 2007, pp 2045–2053). doi:10.1109/INFCOM.2007.237

160. He W, Nguyen H, Liu X, Nahrstedt K, Abdelzaher T (2008) iPDA: an integrity-protecting private data aggregation scheme for wireless sensor networks. In: IEEE MILCOM 2008, pp 1–7. doi:10.1109/MILCOM.2008.4753645

161. Kursawe K, Danezis G, Kohlweiss M (2011) Privacy-friendly aggregation for the smart-grid. Privacy enhancing technologies, vol 6794. Springer, pp 175–191. doi:10.1007/978-3-642-22263-4_10

162. Nicanfar H, Alasaad A, Talebifard P, Leung VCM (2013) Network coding based encryption system for advanced metering infrastructure. In: IEEE ICCCN, pp 1–7. doi:10.1109/ICCCN.2013.6614158

163. Jin H, Uludag S, Lui KS, Nahrstedt K (2014) Secure data collection in constrained tree-based smart grid environments. In: 2014 IEEE international conference on smart grid communications (SmartGridComm): communications and networks to enable the smart grid (IEEE SmartGridComm'14 symposium—communications and networks). Venice, Italy (2014)

164. Uludag S, Lui KS, Ren W, Nahrstedt K (2014) Practical and secure machine-to-machine data collection protocol in smart grid. In: Workshop on security and privacy in machine-to-machine communications (M2MSec'14) in conjunction with IEEE conference on communications and network security (CNS). San Francisco, USA

165. Badra M, Zeadally S (2013) An improved Privacy Solution for the Smart Grid. Int J Netw Secur 17(1):225–232
166. Cloud Security Alliance (CSA), B.D.W.G. (2013) Expanded top ten big data security and privacy challenges. White Paper
167. Castelluccia C, Druschel P, Hübner SF, Gorniak S, Ikonomou D, Pasic A, Preneel B, Tschofenig H, Tirtea R (2011) Privacy, accountability and trust challenges and opportunities (The European Network and Information Security Agency (ENISA)). White Paper, url: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study
168. Rottondi C, Barbato A, Verticale G (2014) A privacy-friendly game-theoretic distributed scheduling system for domestic appliances. In: 2014 IEEE international conference on smart grid communications (SmartGridComm). Venice, Italy
169. Egarter D, Prokop C, Elmenreich W (2014) Load hiding of household's power demand. In: 2014 IEEE international conference on smart grid Communications (SmartGridComm): communications and networks to enable the smart grid (IEEE SmartGridComm'14 symposium—communications and networks). Venice, Italy
170. Mashima D, Roy A (2014) Privacy preserving disclosure of authenticated energy usage data. In: 2014 IEEE international conference on smart grid communications (SmartGridComm). Venice, Italy (2014)
171. Paverd A, Martin A, Brown I (2014) Privacy-enhanced bi-directional communication in the smart grid using trusted computing. In: 2014 IEEE international conference on smart grid communications (SmartGridComm). Venice, Italy
172. Yang L, Xue H, Li F (2014) Privacy-preserving data sharing in smart grid systems. In: 2014 IEEE international conference on smart grid communications (SmartGridComm). Venice, Italy