International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 2, No. 1, 27-36

Security of Smart-Meters against Side-Channel-Attacks (SCA)

Iqra Mustafa[1], Adeel Anjum[1], and Zineddine Kouahla[2]

[1] Comsats University Islamabad, Pakistan
[2] LabSTIC, Department of Computer Science, 8 Mai 1945 University. P.O.Box 401, 24000 Guelma, Algeria

Abstract. The smart meters become an important node for managing information about electric power system so, smart-meter drags cyber security attention in this regard. In this paper, the protocol for smart meters named as privacy preserving billing is used which provides authentication, non-repudiation and integrity by digital signature scheme and zero-knowledge proof. This protocol ensures secrecy and reliability of end to end communication. However, vulnerability lies in integrated circuits of smart meters that can leak sensitive information and side channel attacks (SCA), derive this information from integrated circuits(IC) while it's operating. The most well-known SCA's against smart-meters are electromagnetic radiations, timing and power analysis attacks. Due to side channel attacks integrated circuits physical and electrical effects broadcast information related to secret key and have emerged as a major vulnerability to security applications. SCA does not temper IC security as their non-invasiveness observes device under normal conditions. Hence, our ultimate goal is to make circuit of smart-meter immune against side channel attacks, specifically differential power analysis (DPA) attack is main focus, as it is more aggressive than other SCAs. For this reason, we present basis for SCA resistance and concept of CMOS library. Secondly, the other concept, we introduces is CMOS-based digital isolation

that provides immunity to electrical noise and external fields compared to optocouplers for smart-meters.

Keywords: Smart-Meters· Integrated Circuits (IC's)· Side channel attacks (SCA)· Digital CMOS (complementary metal-oxide-semiconductor)· Advanced Metering Infrastructure (AMI)

1 Introduction

In recent decades, application of Information and Communication Technologies (ICT) have increased enormously in the Critical infrastructures i.e energy grids[4], drinking water system, communication and financial infrastructures. Through these systems we obtained unforeseen amount of opportunity. These infrastructures became highly effective interms of efficiency and flexibilty, which is beneficial for our society. More specifically in energy infrastructures, growing dependecy in ICT opens gates to new threats, which need to be met. These threats are a reality and any disruption in electricity grids will have a huge impact on our economy and society. These threats motivates us to invest in secure architecture for resilent infrastructures.

In smart meter technology, Advanced Metering Infrastructure (AMI) is a key component to help connect smart grid to link two-way flow of electricity with two way flow of information[3,4]. Here, privacy and security concerns rise from meter's fundamental functions, which includes real-time data record of electricity consumption, transmission of data to smart grid and reception of data from smart grid i.e energy prices etc. Hence, data transmitted is subjected to potential interception or theft. However, [1] allow user and service provider to transmit their computation ans tariff policy involved through polynomial commitment and zero-knowledge proof, respectively. Hence,[1] dealt with two main categories: privacy concerns and cyber security issues.

But every electronic device needs security. Many cryptographic algorithms and protocols developed till now, need implementation in embedded devices for which effective arithmetic and side-channel secure architectures and design methods are necessarily required[5]. These architectures should be capable of resisting undesired intrusions.Since, side channel attacks (SCA), derive information from integrated circuits(IC) while it's operating, therefore, they are major source of concern for IC security. The most well known SCA'a are electromagnetic radiations, timing and power analysis attacks. The keybits can be derived by monitoring, through time execution or power analysis of algorithm. In order to resist simple timing and power analysis of algorithms, algorithmic counter measures are applied. However, differential power analysis (DPA) and some other high order attacks are more aggressive.

Due to SCA, these Integrated circuit physical and electrical effects broadcast information related to secret key and have emerged as a major vulnerability to security applications. SCA does not temper IC security as their non-invasiveness observes device under normal conditions. In order to realize security of smart meter through hardware we need to develop digital CMOS infrastructure. The

rest of the paper is organized as follows. In section 2, we discus threats, attacks and vulnerabilities against smart meters. In section 3, we define integrated circuit framework, which describes the development of CMOS infrastructure that makes SCA resistive IC designs. In section 3, our contribution is proposed. In section 4, conclusion is presented.

2 Privacy Preserving Billing Protocol

In [1], privacy preserving billing protocol is introduced which considers multi party and multi meter communications with the proposal of ideal functionality. In this protocol [1,5] temper resistant meters are considered in which user application receives signed tariff policy from service provider and signed meter readings from multiple meters, at the end of billing period b_p. While, the user application only reveals the total bill to service provider. This signed transmission of data is necessary due to the latest developments of threats in this field[6]. However, this protocol is still not resistant against SCA's. Some of the SCA at-

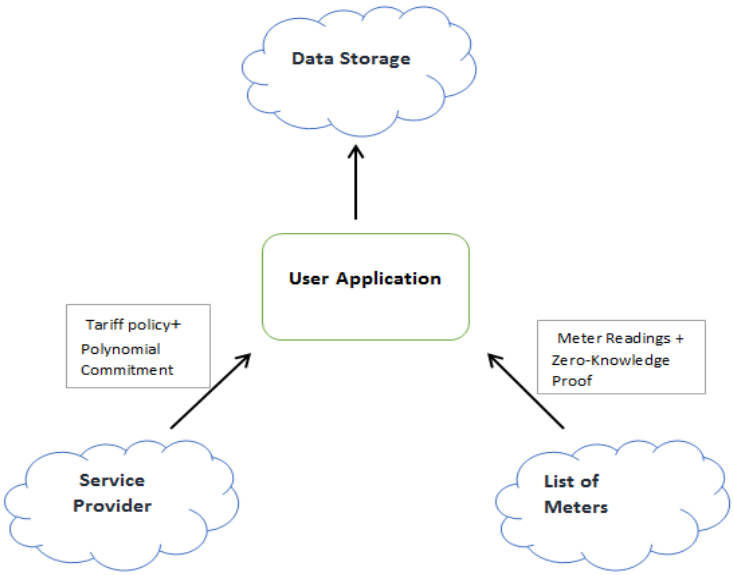

Fig. 1. Privacy Preserving Billing Protocol

tacks can be avoided by adding noise to the process however, DPA is the most aggressive of all which involves statistical analysis. Hence, our idea deals with CMOS at the hardware level, it deals with the power reduction of IC's to avoid SCA attack on Privacy Billing Protocol.

3 Attacks, threats and Vulnerabilities against Smart-Meters

Smart meters can be compromised by disrupting connectivity. Smart meters have physical access to the attacker. An attacker can try to tamper resources of smart meters. An attacker can also be a customer who wants to get utility without paying for it.

Smart meters connectivity can be a security hazard. Often smart meter shares, the internet connection from the home. If an attacker hack smart meter, then security of home internal network is also at risk, consequently attacker would be connected to your home network.

Smart meters, network gateway and connection between the various components are physically accessible by local attackers. An attacker can make attempts to reveal or modify resource that are kept in the smart meter or network gateway or while information is transferred between smart meters in MAN(Metro Politian area Network) and gateway. Local attackers are less ambition compared to WAN attackers as frightful attack of local attacker will solely affect one gateway.

A WAN attacker can attempt to compromise the integrity or/and confidentiality of the meter resources as well as configuration data transmitted by means of WAN. On the other hand the attacker can attempt to control a component of the infrastructure such as meter, gateway by means of WAN to do harm to the component itself or to the corresponding grid.

Smart meter stores a substantial amount of information. This includes smart meter own program, executed command, physical events, recorded user consumption among others. Attacker by tampering smart meter storage can completely control, smart meter behavior since all forms of smart meter behavior is controlled by the content of its storage.

We precisely discussed attacks against smart meter designed by Rial, Danezis and Kohlweiss. Although Rial, Danezis and Kohlweiss smart meter is secure against many attacks, but it is still vulnerable to side channel attacks. Following attacks can be launched against Rial, Denzis and Kohlwess smart meter. Latter we study adversary methods of cheating the electrical grid by manipulating smart meters[6,7].

3.1 Side channel Attacks

A side channel attack leak is a frequent threat found in smart meter. Electrical devices even a small electrical gadget, produce noticeable electric consumption signatures. Electricity consumption of a victim can be crumbed to distinguish the status of electrical appliances based on the signatures.

Power Analysis Attacks In Simple Power Analysis attacker graphically visualizes current used by smart meter over time. As the smart meter performs different operations, power consumption varies depending on the operation. DPA is a more advanced type of side channel attack in which attacker statistically

examines power consumption measurement. The attacker can try non-invasively get secret key of smart meter by analyzing power consumption.

Simple Power Analysis and Differential Power Analysis can be avoided by reducing the power consumption variation during chip or the system design phase. The Simple Power Analysis and Differential Power Analysis attacks cant get any useful information by flattering the power consumption flatten the power consumption, adding noise to power consumption such as by adding noise to power consumption measurements, scrambling different address lines and data bus during chip design can conceal the true power consumption. An attacker can get an insight of the cryptographic algorithm since cryptographic code have lots of bitwise arithmetic functions, examination of the code for a sequence of suggestion and constant can provide an attacker hint of type of cryptographic algorithm. Key Storage is the weakest link even if there is strong cryptography. Also, many smart meters store a number of copies of secret keys in different locations that an attacker might gain access to them.

SPA and DPA are non-invasive attack, hence can end up particulary threating as the owner of victim system might not pay attention that secret keys are hijacked and in this manner may not taken action sufficiently inappropriately used.

Differential Fault Analysis Attack In differential fault analysis attack, the attacker injects an error in the internal state of the circuit and then exploits weakness of the algorithm under bug. These faults can be anything from abnormal environment conditions such as increased heat, injection of data packets that clash with the legitimate packets and injection of laser beam at the appropriate frequency. The principal counter measure against fault analysis is fault detection. The scheme is to supervise if one has attempted to corrupt the computation and in such crisis to close down the processor and erase any important data as soon as could be expected under the circumstances.

3.2 Electromagnetic Radiation

The electromagnetic analysis attack is nearly like the power attack, the difference is this is launched against electromagnetic fields generated by the discharging gates as one of the side channel attack. The flow of the charges generates the electromagnetic fields. This slightly varies from the power attack as the power attack can only get into the global power consumption, can measure the limited area of the security Integrated chip. The power attack is easy and fast to launch against the off- the shelf devices. What an EMA cant do. As the electromagnetic fields are created by the electric charge flowing across power lines or the 2 differential output wires. So, the charge is equal in amount the only trick is to figure out in different events occurring which of the two-differential output was carrying the charge at that time. There is a common mechanism following in placing the differential output wires, by placing their placement and size can help covering up this attack vulnerability.

3.3 Timing attack

The timing attacks are the class of cryptanalysis that is done of the timing information. Such as when the cyphertext is to be arrived depends on the factors carrying this whole operation, here it depends on the secret key. But this doesnt mean that making the power consumption uniform ll reduce the threat of timing attack. Therefore, a design having always has a worst case running time is yet needed. This conventional design ll stop power measurements a great deal, there ll be the idle cycles which are being used to bluff the cryptanalyst for analyze the information about power consumption. The gates of the regular circuit wont be changed unless the state of the circuit is altered so it wont dissipate any power. But this is not feasible for the logic style as the state of the circuit must happens to change. This can be done in a secure flow. Like when desired insert the idle cycles. Then every gate ll have a switching event in every cycle with or without inserting the idle cycles.

3.4 Other Attacks

Extraction of Password In this attack, attacker motivation is to extract passwords. This is normally achieved through the optical port snooping. Optical port is used by field technicians to directly manage individual meter. Authentication credentials are necessary for interacting the meter optical port. An attacker can capture the password by placing a reader device on the optical port pins. Since the password is transmitted in clear, attacker can easily extract password.

Eavesdropping Since smart meters use wireless signals to communicate and thus is prone to eavesdropping by an adversary. The attacker can easily observe and asses sensitive information from a smart meter. Data encryption can be used to shield against this attack. However, intelligent adversary can still get information from message content. For example, if a household is untenanted, the electricity consumption will fall. If the smart meter is designed to interact with the data contractor unit when a specific limit of electricity consumption is crossed or if the data length transmitted to data contractor is directly proportional to electricity consumption, then a pattern of tenant activity can be constructed.

Jamming Attack The primary objective of this jamming attack is to block the smart meter communication with the utility provider, by jamming wireless communication with noise signals. There are two types of jamming attacks

- Proactive jamming attack where an attacker can transmit noise to totally block a wireless channel
- Reactive jamming where attacker first monitor on the radio channel and dispatch the attack just when signals are detected on the channel.

It is significant to understand between reactive jamming attack initiated by adversary and from routine communication jam.

4 Contribution

Even though the privacy-preserving billing protocol [1] provide authentication, integrity and non-repudiation but still our smart meters security have threat of side-channel attacks. The vulnerability lies in the multinational, distributed and multistep nature of integrated circuit of smart meters that can leak information. The sensitive information or secret key can be conjectured by observing the power fluctuation or variation, electromagnetic radiation and execution time of the integrated circuit. SCA's tools are less expensive ,that's why it's quiet easy to launch SCA's and they made intrusive monitoring possible at low cost.
So, side channel attacks are major concern for ICs. As SCAs derive information from ICs, while it is operational. The most common SCAs are discussed above. Since computation time depend on data values or key show, what they are doing. Visual information of circuit can be observed by simple timing or power analysis attacks such as; cryptographic algorithm is a best target in this regard. The branch relies on the key bit values. These key bits can be deduced by monitoring the computation time or electric power ingestion analysis of cryptographic algorithm. So, need to take algorithmic, counter measures that ensure that the key is not revealed by observation. Such as, an algorithm can be made immune against SCAs by ensuring that if then else is not a key.
After taking these safety measures, here we specifically concern about differential power analysis (DPA). Attack based on assumption that the circuit is designed by using CMOS technology in which electric-power features are dependent on information processing. It depends on error correction and statistical analysis used to retrieve information from electric-power ingestion measurements mutually related to secret key. Even if power fluctuation and dissipation is isolated from other processing components, DPA is still effective in that very situation. Hence, we introduces concept of digital CMOS library below to avoid DPA and other SCAs attacks.
For this reason, firstly need to realize the security perspective of smart meter through the hardware approach. Hence, it is essential to accomplish the design segment where the requirements of side channel attacks strengthened the digital CMOS logic cells [2].
Previously defining the design segment; in order to grasp the idea, take a look of Block diagram of E-smart meter in Figure 1. [3]
Moreover, for AMI environment to be deployed, it is important to describe light weight, low power cryptographic and transmission protocols. At development stage, it is considered that the creation of encryption chip mentioned in prior stage and then according to that the CMOS technology is designed that is sustainable by the use of the EUROPRACTICE amenities. The measurement and enactment of the SCA emanations of the designed chip is followed by the verification stage, that involves in the design and implementation stage of assessment method for verification of electrical and electronic functionality. In last stage it is essential to carry out testing of cryptographic protocol and functionality of data processing.
Since, there are two preliminary activities. Firstly, in order to design SCA resis-

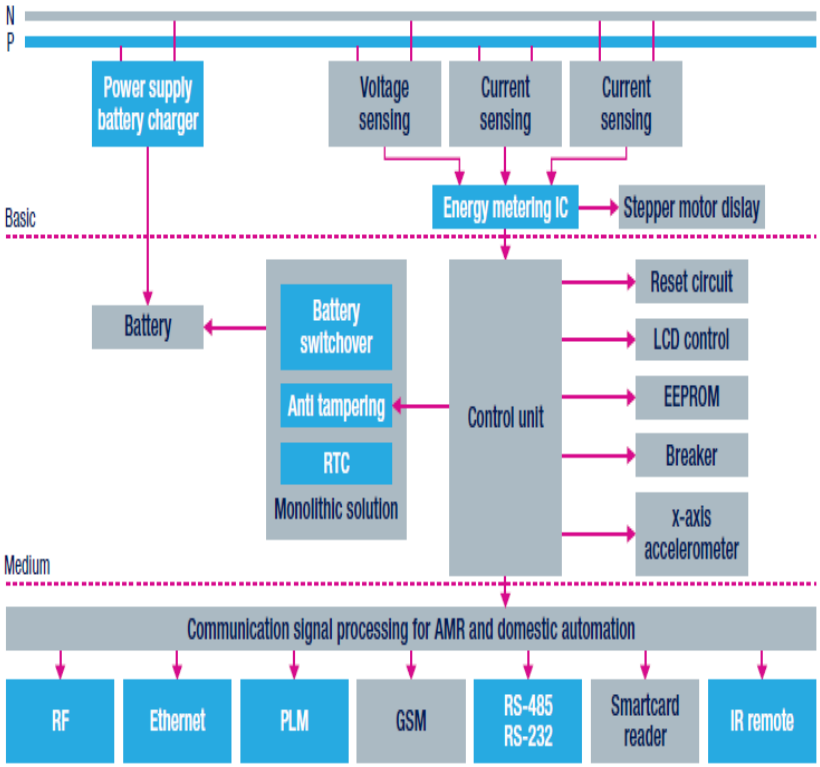

Fig. 2. Block Diagram of E-Smart Meter

tive integrated circuit, need to develop a digital CMOS infrastructure. Secondly, choose such security and transmission protocols that facilitate data protection in the transmission between the metering device and utility. Afterward, the outcomes of these activities congregate into a design of ICs layout.
However, in this case our main focus is on designing resistive integrated circuit by developing digital CMOS infrastructure , since we refer [1] as data protection protocol. Finally, all above mentioned approaches need to be verified by following two steps. In first step, need to verify the electrical and electronic functionality of the design. While in last step the resistance of the design against side channel attack will be assessed.
Hence, to make these activities successful, highly specialized tools and software is required. It is important to emphasize that neither any digital CMOS library exists to strengthen the cell against SCA nor many research laboratories have such expertise that allow integration of metering and cryptographic chip on single pellet that reduce cost and increase the performance.

– Thus, by the development of a library of digital CMOS cells, it is possible to increase the security of energy infrastructure which provides resistance

against SCAs. Moreover, it serves as a foundation for upcoming cryptographic chip versions that will ensure latest demands and challenges. Furthermore, through the deployment of secure transmission, contribute against the cyber security and launching secure protocols which will benefit the entire community.

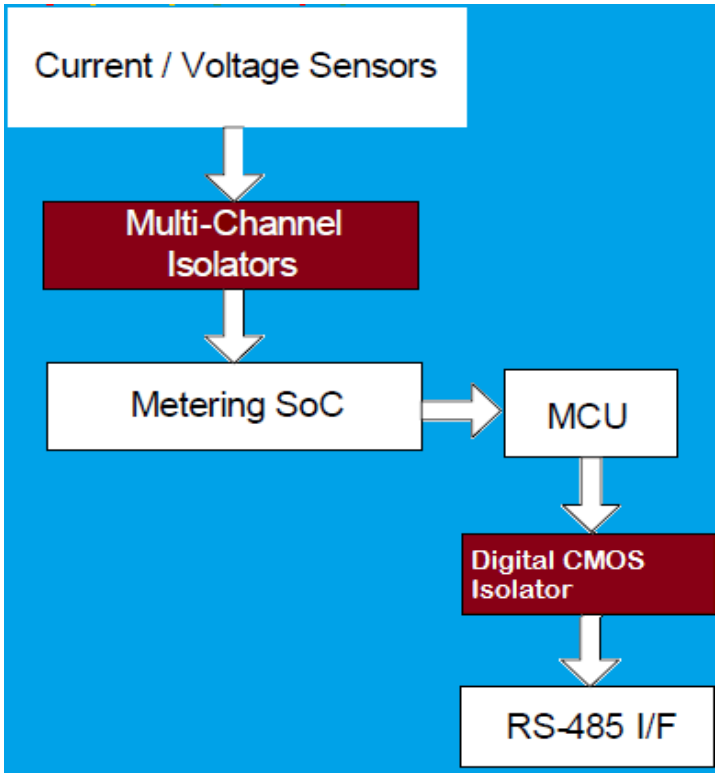

Fig. 3. Digital CMOS Isolator

– Secondly, the other concept, we are introducing is CMOS-based digital isolation that provides immunity to electrical noise and external fields for smart-meters. As, smart meters and build-out of smart grid becomes pervasive , therefore meter installers will become less discerning about the environment in which smart-meters are located. Due to this, the probability of data corruption is increases. Moreover, any component of smart-meter that is affected by electrical noise or electromagnetic fields considered to be a weak aspect of security as well as integrity. Since, these components can disrupt data to smart meter, and also a source of information leakage. Therefore, we move towards CMOS-based digital isolation that provides resistance to

electrical noise and external fields which could be a source of information for adversary. Furthermore, using CMOS isolators in smart meter ensures accurate, uncorrupted power measurement.

5 Conclusion

Attacks against smart meter does not influence the customer's alone, rather the service provider business also. There is plenty of threats against smart meter which may happen into attacks, in light of advantage they will give to adversary. In this paper, we discuss side channel attacks against smart meters. We introduced concept of CMOS library that provide resistance against SCA's. Moreover, in order to avoid external effects of environment use CMOS digital isolator that delivers significantly higher CMTI performance even though maintaining greater consistency and higher operating lifetimes. Finally, we should not overlook another important aspect: human factor. It is imperative that workers have enough training to avoid social attacks.

References

1. Rial, Alfredo, George Danezis, and Markulf Kohlweiss. Privacy-preserving smart metering revisited. International Journal of Information Security (2016): 1-31.
2. M. Stanojlovic and P. Petkovic, "Design and simulation of multiplexer cell resistant to side channel attacks". INDEL 2012.
3. Rakers, Patrick, et al. Secure contactless smartcard ASIC with DPA protection.IEEE Journal of Solid-State Circuits 36.3 (2001): 559-565.
4. Barthe, G., Danezis, G., Grgoire, B., Kunz, C., Zanella-Bguelin, S."Verified computational differential privacy with applications to smart metering". In: 2013 IEEE 26th Computer Security Foundations Symposium (CSF), pp. 287301.
5. Danezis, G., Fournet, C., Kohlweiss, M., Zanella-Bguelin, S."Smart meter aggregation via secret-sharing". In: Proceedings of the First ACM Workshop on Smart Energy Grid Security, pp. 7580
6. Barthe, G., Danezis, G., Grgoire, B., Kunz, C., Zanella-Bguelin, S."Verified computational differential privacy with applications to smart metering". In: 2013 IEEE 26th Computer Security Foundations Symposium (CSF), pp. 287301.
7. Ogden, K. "Privacy issues in electronic toll collection". Transp. Res. C: Emerg. Technol. 9(2), 123134.
8. Khattak A.M., Khanji S.I., Khan W.A. "Smart meter security: Vulnerabilities, threat impacts, and countermeasures Advances" in Intelligent Systems and Computing, Volume 935, 2019.