Journal of Engineering and Applied Sciences 13 (3): 790-794, 2018
ISSN: 1816-949X

Smart Grid Security using PUF

Pentyala Sumanth and A.S. Remya Ajai
Department of Electronics and Communication Engineering, Amrita School of Engineering,
Amrita University, Amrita Vishwa Vidyapeetham, Amritapuri, India

Abstract: In this study, we employ the Ring Oscillator (RO) based security for the smart grid. Smart grid is the integration of advanced computing and communication technology with the existing power systems. Smart grid can transfer information and data in a bidirectional way. The information exchange provides better management. As the smart grid is much dependent on network it became vulnerable to potential threats. Advanced Metering Infrastructure (AMI) is the part of the smart grid that establishes connections either way. In the present technologies of smart grid, the AMI authentication is done by using the non-volatile memory to store the security keys and using a digital signature or encryption schemes. These methods are costly in terms of area and consume more power. Moreover, memory based authentications are vulnerable to spoofing attacks. In this research, a secure technique independent of non-volatile memory is proposed. This research uses Ring Oscillator Physically Unclonable Functions (ROPUF) on Field Programmable Gate Arrays (FPGA). Instead of storing keys; the circuit derives keys using physical characteristics of FPGA or IC. In this study different levels of security is implemented using ROPUF on FPGA. The keys are modelled from minor feature differences that are occurred at the manufacturing time. So, these keys cannot be modelled, since, irregularities occurred during fabrication process are highly random. In current research, authentication key of programmable sizes is implemented.

Key words: Smart grid, Advanced Metering Infrastructure (AMI), Ring Oscillator (RO), Ring Oscillator Physically Unclonable Function (ROPUF), Field Programmable Gate Array (FPGA), network

INTRODUCTION

Smart grid is the integration of advanced computing and communication technology with the existing power systems (Wang and Lu, 2013). The smart grid can transfer information and data in a bidirectional way. The advantage of the smart grid is improved demand response feature. The main objective of the smart grid is better utilization of available resources. Smart grid integrates the generation, transmission and distribution networks of the electrical grid with communication network. Using the communication network, the operations performed can be controlled. Smart grid has the demand response feature (NIST, 2010) that is enabling active participation of consumer for improved utilization of resources. Real-time information exchange with the consumers is the key for the demand response feature management system. Seamless, secured communication needs to be provided between service provider (utility company) and the consumer. The pricing information will be available for the consumers at the same time sensing the consumption of consumers and measuring it is important. Smart meters are used at the user end to measure the consumption of user.

Depending on the pricing information and the consumer usage, consumer may like to take certain actions he uses the communication network to communicate with the utility company. So, smart grid is depending on the communication system which might cause security issues. Security is a concern about information exchange in the smart grid. Advanced Metering Infrastructure (AMI) (Khurana *et al*., 2010) is the part of the smart grid which establishes a connection between the smart meter at user side and utility company. Security comes in place as the data available in the smart meter should be available to the utility company. And the data should not be modified without authorized access. So that, secure communication is needed to prevent unauthorized access and modification of data. The security schemes that are using digital signature are prone to spoofing attacks. Certain countermeasures can be used to prevent the attacks against spoofing attacks but the circuits used for that are costly.

So, for the security between the consumer and the utility company a security scheme is propose which uses the implementation of ROPUF on FPGA. ROPUF is ring oscillator based PUF. PUF (Physically Unclonable

Corresponding Author: A.S. Remya Ajai, Department of Electronics and Communication Engineering,
Amrita School of Engineering, Amrita University, Amrita Vishwa Vidyapeetham, Amritapuri, India

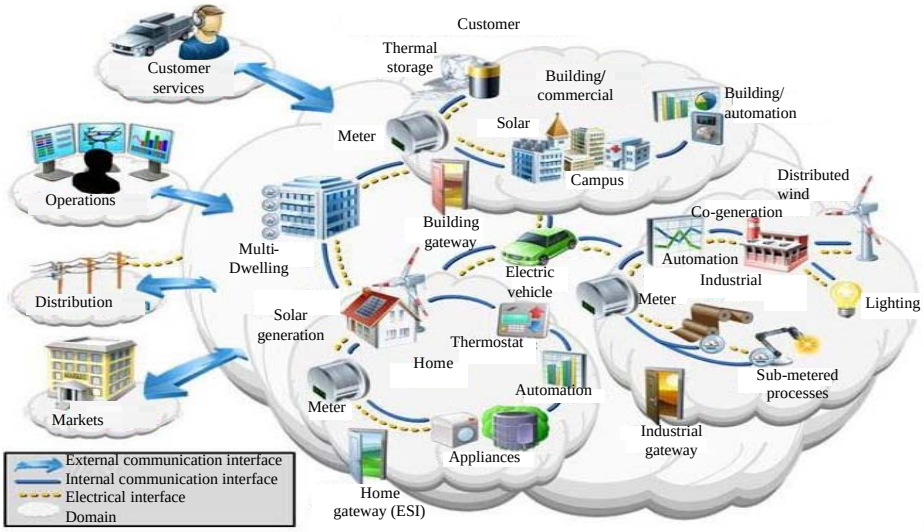

Fig. 1: Smart grid

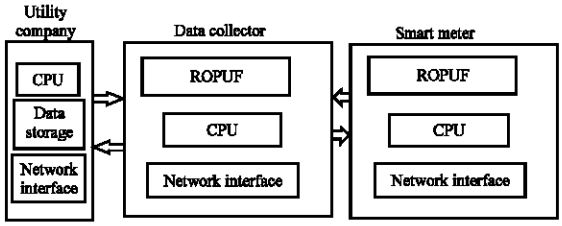

Fig. 2: Advanced metering infrastructure

Function) (Herder *et al*., 2014) is a concept of hardware security. In PUF the minor feature differences that are occurred during the manufacturing time of a chip are exploited. At the tie of manufacturing, although, the mask and process are same there will be certain factors that are uncontrollable leads to minor feature differences. These random variations are unique because these are caused by random changes occurred at the time of manufacturing. So, these keys generated by the ROPUF are unique form chip to chip and modelling these codes is impossible since these are caused by random changes.

The main blocks of the AMI are service provider, data collectors and smart meter. The data collectors are used to collect the data over smart meters and service providers takes data from data collectors.

When a customer needs service, the service provider performs required operations to meet the requirement of the consumer. Figure 1 shows the smart grid in that AMI is the network between the consumer and the service provider/customer care. The block diagram for the AMI is shown in Fig. 2. In literature survey, several security schemes are proposed they can be classified into two types. One is with existing resources and the other is employing hardware security. Security schemes that are using available resources are a scheme that employs message authentication (Suh and Devadas, 2007) where this method causes overhead issues.

In another research a remote password scheme is used is used. All the methods that are using password scheme as well as the message authentication schemes will depend on non-volatile memory. But non-volatile memory can be easily attacked.

Secondly, in the scheme that using the hardware security, schemes are used those are mainly using the volatile keys generated by PUF. Some schemes employed the SRAM-PUF scheme (Huth *et al*., 2015). In SRAM-PUF scheme; the key will be generated by the data acquired by the SRAM when it is turned on. In another research authentication scheme proposed using ROPUF where there are fixed number of levels of security. There are five levels of security in that earlier proposed scheme. The current work is based on hardware security concept. Where ROPUF (Mustapa *et al*., 2013) implemented on FPGA is used to generate security keys. The number of levels of security is not fixed. The proposed scheme can be implemented on FPGA and also can be made as an IC.

MATERIALS AND METHODS

Proposed scheme: The proposed scheme deals with the security between the smart meter and the service provider. In the customer side, a smart meter will be there and a data collector collects data from different smart meters and sends it to the service provider. The parts of the smart

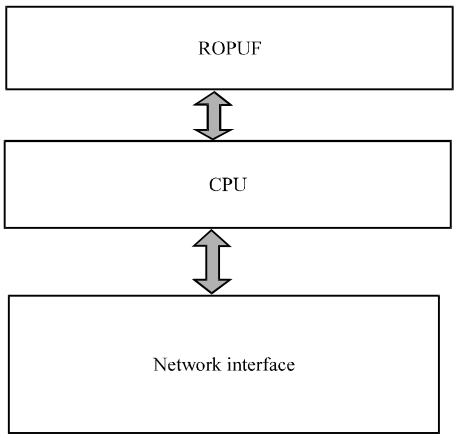

Fig. 3: Smart meter

meter are it consists an ROPUF for the generation (Mustapa and Niamat, 2014; Seferian *et al*., 2014) of the ecurity keys and a CPU and a network interface to connect to the network connecting all the smart meter, data collector, service provider or utility company. The block diagram of the smart meter is as shown in Fig. 3 show the smart meter is different from the normal current reading meter on the user side is smart meter can communicate with the service provider (ANSI, 2017). And smart meter can generate the security key using the ROPUF. This smart meter scheme is like enhancing the current electric grid.

The service provider connects the smart meter to the network. At the service provider side, data storage will be there to store the challenge response pairs of all smart meters connected to the network. The input to the ROPUF is called as challenge and the output generated by ROPUF is called as response. So, when a smart meter is getting connected to the network, the service provider stores all the possible Challenge Response Pairs (CRP) of particular ROPUF inside the smart meter.

ROPUF introduction: PUF is Physically Unclonable Function means that it cannot be cloned or modelled. In the case of ROPUF it is the Ring Oscillator based PUF, ring oscillators are used to exploit the inherent physical characteristics of the chip. ROPUF exploits the inherent delay characteristics of integrated circuits. During the fabrication of the integrated circuits, even though all the processing steps are same there are certain factors that will occur randomly. Because of those random changes all chips manufactured do not have same internal delay characteristics. But all chips meet their primary requirement (Maiti *et al*., 2010) that is all the outputs of

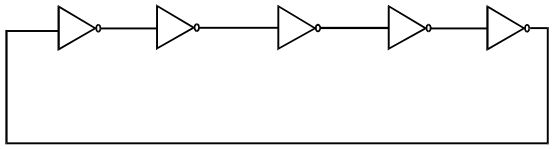

Fig. 4: Ring oscillator

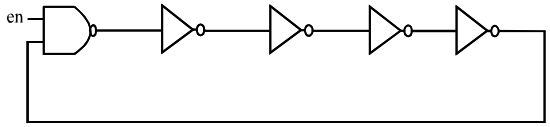

Fig. 5: Ring oscillator with enable

chips of same kind will be same, although, the internal delays have minute differences. Here we are using ROPUF to exploit those minute delays. So, we cannot model the ROPUF behaviour into another ROPUF, since, we cannot create same random changes at the time of manufacturing.

The ring oscillator is a connection of inverters such that output of the final stage is fed back to the input. A 5 stage ring oscillator is shown in Fig. 4. In current research, a block of ring oscillators are used. In this case, an enable is needed for each ring oscillator (Yu *et al*., 2009) circuit in order to control it. So, to control it a NAND gate is used in front. Figure 5 shows the modified design of the ring oscillator.

Two ROPUFs produces different responses for same challenge, although, they are of the same kind and implemented on same type of FPGA. So, no two ROPUFs produce the same response for same challenge means all responses are unique.

ROPUF design: A programmable ring oscillator based physically unclonable function (Mustapa *et al*., 2016) is implemented. The design consists of programmable ring oscillator block where we can program the number of ring oscillators as per requirement. The number of ring oscillators is more if the security key length is more in terms of bits. Each bit is generated from the comparison of two ring oscillator frequencies. The ring oscillators are connected to the muxes, so that, when a challenge is given, the challenge acts as a selection line to the mux and selects a ring oscillator from all the ROs connected. All the ring oscillators are connected to both the muxes. But the selection line that is a challenge will be different. The outputs of muxes are connected to the counters as shown in Fig. 6. Effectively it is like two ROs connected to two counters and then the two counters count the oscillating frequencies of the ring oscillators. After the specified amount of time, the counter values will be compared and

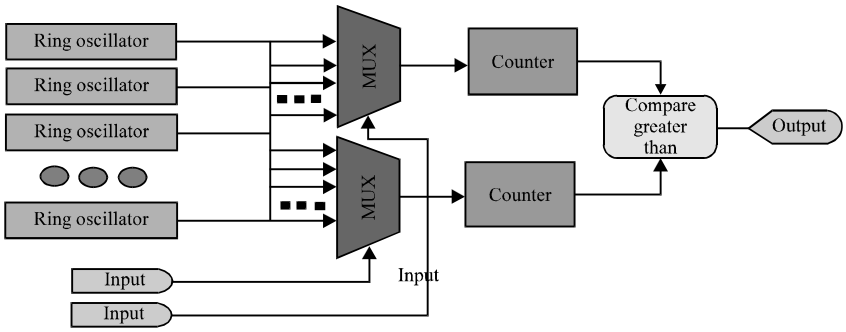

Fig. 6: Ring oscillator PUF

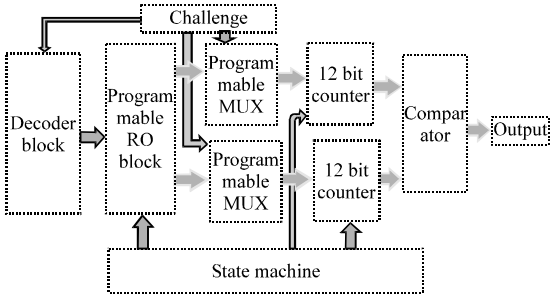

Fig. 7: ROPUF block diagram

depending on the comparator logic for comparison the output will be sent. The time after which the counter values have to be compared is decided by the control circuitry.

The control circuitry used in here is a state machine. The block diagram for the implemented design is as shown in Fig. 7. The state machine is having an internal counter where a value can be set in it. When the required value of the counter inside the state machine is reached then the two counter values of counters counting the Ro oscillations will be counted.

When one comparison is over the state machine is needed to reset all the counter values for the next comparison. From Fig. 2 when a smart meter needs to communicate with the UC (Utility Company/service provider) it needs to be authenticated. In the process of authentication, the UC sends a challenge to the smart meter where the ROPUF inside smart meter has to generate a response using that challenge and send it back to the UC. As UC is assumed to have secured data storage; data storage contains the challenge response of that particular ROPUF. On UC side the result from the smart meter and the result stored at the time of connection of smart meter to the network are compared. If both are not same then the data requested by the smart meter will not be sent.

When the smart meter receives a challenge, the state machine clears all the counters and decoders enables the respective ROs and challenge is also selection lines to the muxes, so, it selects the respective ROs connected from the input. Counting is carried out and results compared. When the counter value inside state machine is reached, the two counter values will be compared and the result is obtained. And state machine clears all counters.

RESULTS AND DISCUSSION

The ROPUF is designed in VHDL and implemented in FPGA. The total design between the smart meter and the service provider is implemented using PCs. That is a PC is used as a utility company and the FPGA is used as a smart meter. The inputs are given to the ROPUF and the outputs are stored in PC to make it act as a UC. FPGA used is Spartan 3E. Now different challenges are passed from PC to FPGA and results are checked. The challenge bits should be provided by the manufacturer. The challenge bits decided based on the level of security used. The level of security is a number of bits for the secure key. In this research, a programmable ROPUF is designed, so, any number of response bits can be taken from ROPUF by providing the challenge bits.

But at the time of connecting the smart meter to the network, all the challenge response pairs must be stored in the UC. So, if the number of ring oscillators used for the security key is 64 and smart meter needs to authenticate to UC in each 10 min then in a year it needs to authenticate 52,560 times and if we consider a 20 years span it is 1,051, 200 times. And the number of challenge-response pairs available is 8.81e+121.The challenge-response pairs are abundant enough. So that, no need of using the same key twice. The security improves as the keys are unused each time. The number of ring oscillators increased then comparison pairs will be more. And if the security level increased that is if the

Table 1: Number of comparison pairs for given ring oscillators

Ring oscillators	Comparison pairs	CRPs (64 bit)
64	2016	8.81e+121
128	8128	1.065e+161
256	32640	8.578e+246

number of response bits is increased then CRPs will also increase. So, challenge-response pairs are abundant for any level of security.

To increase the level of security, bits of response should be increased for that ring oscillators need to be increased. Table 1 shows the number of ring oscillators and the comparison pairs they can generate. From each comparison pair, a bit of response can be generated.

CONCLUSION

In this research, a novel scheme that will derive keys for authentication is proposed. Instead of storing the keys using non-volatile memory, keys are derived using ROPUF. The proposed scheme is implemented in VHDL. This scheme provides high security at lower cost. It is a programmable key generation, so, the level of security can be changed. This scheme is using the physically unclonable functions, so, there is no chance of spoofing, since, no two challenges will produce the same output. It is done on FPGA, so, re-configurable feature allows the circuit evolvable and no need for additional circuitry.

ACKNOWLEDEGMENTS

We would like to thank to Jyothi S.N., Principal, Amrita School of Engineering for providing necessary facilities and an ideal environment to carry out this research. We avail this opportunity to express our sincere gratitude to our teachers for their guidance, advance and encouragement in every step of this endeavour.

REFERENCES

ANSI., 2017. ANSI C12 smart grid meter package. American National Standards Institute, Washington, D.C., USA. http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.+Smart+Grid+Meter+Package

Herder, C., M.D. Yu, F. Koushanfar and S. Devadas, 2014. Physical unclonable functions and applications: A tutorial. Proc. IEEE., 102: 1126-1141.

Huth, C., J. Zibuschka, P. Duplys and T. Guneysu, 2015. Securing systems on the Internet of things via physical properties of devices and communications. Proceedings of the 9th Annual IEEE International Conference on Systems (SysCon), April 13-16, 2015, IEEE, Vancouver, British Columbia, Canada, ISBN:978-1-4799-5928-0, pp: 8-13.

Khurana, H., R. Bobba, T. Yardley, P. Agarwal and E. Heine, 2010. Design principles for power grid cyber-infrastructure authentication protocols. Proceedings of the Hawaii International Conference on System Sciences, January 5-8, 2010, Honolulu, HI., pp: 1-10.

Maiti, A., J. Casarona, L. McHale and P. Schaumont, 2010. A large scale characterization of RO-PUF. Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), June 13-14, 2010, IEEE, Anaheim, California, USA., ISBN:978-1-4244-7811-8, pp: 94-99.

Mustapa, M. and M. Niamat, 2014. Relationship between number of stages in ROPUF and CRP generation on FPGA. Proceedings of the 2014 International Conference on Security and Management, July 21-24, 2014, Janis Research Company, Las Vegas, Nevada, pp: 1-6.

Mustapa, M., M. Niamat, A.P.D. Nath and M. Alam, 2016. Hardware-oriented authentication for advanced metering infrastructure. IEEE. Trans. Smart Grid, 1:1-1.

Mustapa, M., M. Niamat, M. Alam and T. Killian, 2013. Frequency uniqueness in ring oscillator Physical Unclonable Functions on FPGAs. Proceedings of the 2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS'13), August 4-7, 2013, IEEE, Columbus, Ohio, ISBN:978-1-4799-0065-7, pp: 465-468.

NIST., 2010. NIST framework and roadmap for smart grid interoperability standards. National Institute of Standards and Technology, Gaithersburg, Maryland. https://www.nist.gov/sites/default/files/documents/public_affairs/releases/smartgrid_interoperability_final.pdf.

Seferian, V., R. Kanj, A. Chehab and A. Kayssi, 2014. PUF and ID-based key distribution security framework for advanced metering infrastructures. Proceedings of the 2014 IEEE International Conference on Smart grid Communications (SmartGridComm'14), November 3-6, 2014, IEEE, Venice, Italy, ISBN:978-1-4799-4933-5, pp: 933-938.

Suh, G.E. and S. Devadas, 2007. Physical unclonable functions for device authentication and secret key generation. Proceedings of the 44th annual Design Automation Conference, June 4-8, 2007, San Diego, CA., pp: 9-14.

Wang, W. and Z. Lu, 2013. Cyber security in the smart grid: Survey and challenges. Comput. Networks, 57: 1344-1371.

Yu, H., P.H.W. Leong, H. Hinkelmann, L. Moller and M. Glesner *et al*., 2009. Towards a unique FPGA-based identification circuit using process variations. Proceedings of the 2009 International Conference on Field Programmable Logic and Applications (FPL'09), August 31-September 2, 2009, IEEE, Prague, Czech Republic, ISBN:978-1-4244-3892-1, pp: 397-402.