Special Section: Physical Unclonable Function

A Secure Hardware-Assisted AMI Authentication Scheme for Smart Cities

Fathi Amsaad
Eastern Michigan University

Selc¸uk Kose
University of Rochester

Abstract—In this article, an area-efficient dynamic ring oscillator-based physical unclonable function design utilizing field-programmable gate arrays technology is proposed. An enormous amount of secret keys are generated to securely authenticate advanced metering infrastructure (AMI) nodes throughout their useful lifetime meting National Institute of Science and Technology (NIST) real-time authentication key and security standards. A secure key exchange scheme between a smart meter and utility center is implemented within an AMI network while preserving the privacy and identity of the meter using lightweight encryption. The proposed framework is demonstrated for six different security levels (L0 to L5), which have authentication keys with different length and robustness according to the NIST standards. Experimental results show that our AMI scheme meets the NIST real-time requirements (efficiency) with security levels, L1 and L2, taking, respectively, 6.45 ms and 12.9 ms, which is considerably smaller than the existing techniques.

& SMART CITIES INCORPORATE different components including smart transportation, smart building, smart infrastructure, smart power grid and energy, smart and connected e-health care, and smart IoT regimes. These components make the smart cities faster, greener, safer, friendlier, and more reliable and efficient. [1,2] In the context of a smart city, the advanced metering infrastructure (AMI) is one of the state-of-the-art

Digital Object Identifier 10.1109/MCE.2020.3040717
Date of publication 25 November 2020; date of current version 10 June 2021.

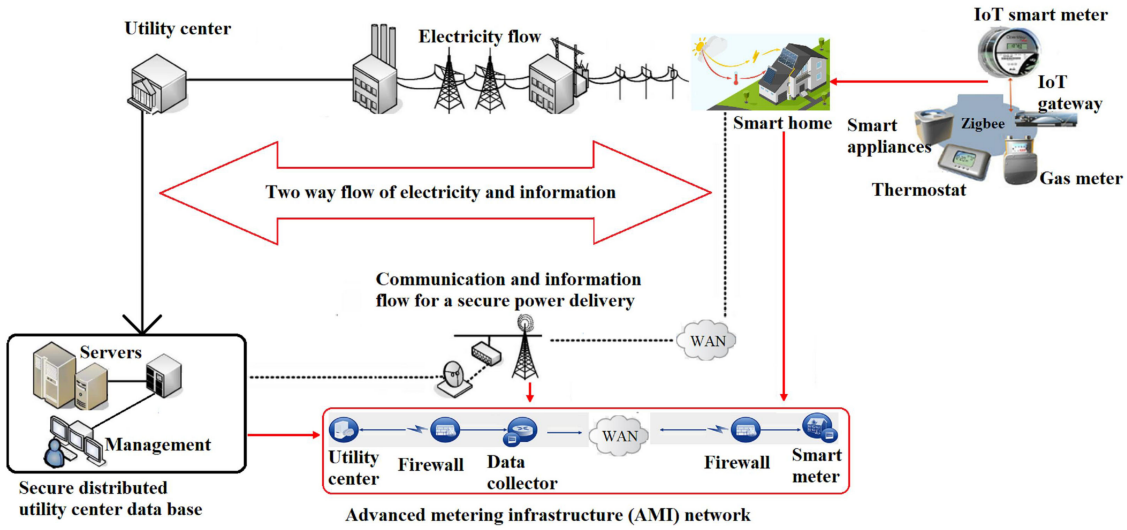

Figure 1. Illustration of an AMI network in a smart power grid. [3]

research topics in the area of next generation smart power grid that houses a sophisticated system of meters, relays, connectors, loads, and generators. [2,3]

Figure 1 shows a smart power grid with two-way communication as a mechanism to exchange electricity and information flow between a smart home and utility center (UC). This communication, however, can potentially lead to important security challenges while protecting some of the smart grid infrastructure nodes from emerging cyber and physical attacks. [4] One of the primary challenges in an AMI network is, therefore, the design of a compulsively trusted and highly secure AMI framework that achieves real-time authentication among smart meters (SMs) and UCs.

This article proposes a hardware-assisted framework for the AMI network to achieve end-to-end key management and enable trusted and secure authentication in AMI systems. This framework generates chip-specific identifiers (i.e., chip-fingerprint IDs) at real-time by exploiting the unique characteristics of manufacturing process variations, extracted from the fabrication imperfections of integrated circuits (ICs). [5] This framework utilizes low-cost and efficient physical unclonable functions (PUFs) with improved challenge–response pair characteristics, namely, dynamic ring oscillator-based PUF (d-ROPUF) to obtain a large amount of authentication keys. [5]

An lightweight encryption technique [6] is also realized on hardware using field-programmable gate arrays (FPGA) technology, contained within SMs, to encrypt PUF-based authentication keys generated within an FPGA, before the keys are transmitted over the AMI network. Such encryption is important to ensure the integrity of the exchanged secret keys and to protect the private information, i.e., identity, of the authenticated meter devices. The National Institute of Science and Technology (NIST) has recommended using multiple levels of secret keys for real time and robust authentication. The results of the proposed AMI framework are promising and offer significant security enhancements such as fast authentication capability and small storage overhead, as compared to the state-of-the-art techniques. According to our results, for a 50-year lifespan, the total time spent to authenticate each SM for all of the security levels (L1 to L5) is approximately 5 h. The results also demonstrate that for each AMI network with 200 SMs, only 3.98-GB space is needed to store all encrypted PUF-based key information for a period of 50-year SM lifespan, satisfying the NIST real-time security requirements.

RELATED WORK

Different AMI authentication schemes can be categorized into two main groups, network communication-based and hardware-assisted schemes.

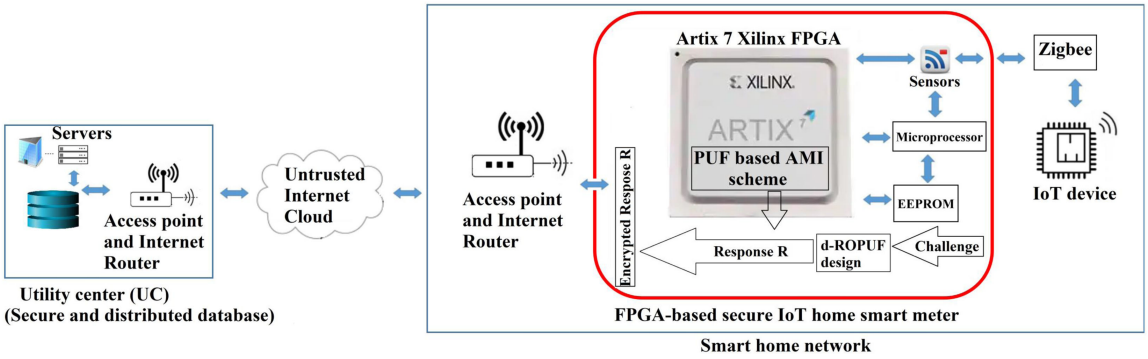

Figure 2. High level overview of the proposed AMI authentication framework. Each SM houses a PUF implemented within an FPGA and lightweight encryption.

Network-Based AMI Authentication Schemes

These AMI schemes mainly focus on the usage of network protocols with new cryptographic techniques for message encryption and authentication. A lightweight authentication scheme that uses a shared key protocol for message exchange and connects distributed hierarchical networks based on the Diffie–Hellman is proposed by Fouda et al. [7] The main drawback of this scheme is its usage of public-key cryptography, which leads to greater key certification and management overhead. To overcome this issue, a secure AMI scheme using the Merkle hash-tree technique with a small computational overhead is introduced by Li et al.[8] An authentication scheme between the SMs and a server that reduces the required amount of both communication steps for a secure remote password exchange and network packets exchange is presented by Nicanfar et al.[9] In this scheme, the authors also propose an enhanced public-key-based cryptography approach. A novel AMI framework that uses a key graph approach for multicast, broadcast, and unicast key management modes is introduced. [10] This framework is, however, vulnerable to both invasive physical and spoofing attacks since it relies on nonvolatile memory technique for storing the secret keys.

Hardware-Based AMI Authentication Schemes

The second category of the AMI authentication scheme is based on the emerging hardware-assisted security techniques. An intrinsic PUF is proposed for IP protection of SRAM memory cells of FPGA hardware designs by Guajardo et al. [11] A novel approach that utilizes both PUF and physical key generation (PKG) techniques to ensure secure wireless communication between smart appliances and OEM servers is proposed by Huth et al.[12] The proposed technique is proven to have lower overhead as compared to the existing public-key schemes, such as PKG and RSA. However, there is no discussion about the real-time requirements for secure communication and the computation time overhead of the scheme subsystems. Another ID-based scheme that incorporates PUF and symmetric-key cryptography is introduced by Seferian et al.[13] This scheme is primarily proposed to mitigate cyber-attacks, i.e., denial of service, and improve network latency by a factor of 14 times.

SYSTEM AND NETWORK MODELS

Figure 2 illustrates our AMI system model that consists of two main AMI components: The utility company and the smart building environment that house SMs with a capability to communicate with smart devices via home Wi-Fi connections. As illustrated in Figure 3, the framework's network model consists of three main components: the authenticator, the utility company, and the SMs. First, challenge inputs are applied to the implemented PUF design for generating secret keys by an SM. A lightweight cryptography is then employed to encrypt the generated SM keys.

After the keys are received, a search is accomplished over encrypted key information at the UC to authenticate the SM. This search is a critical component to protect the integrity and confidentiality of the exchanged authentication keys against external attackers who may try to

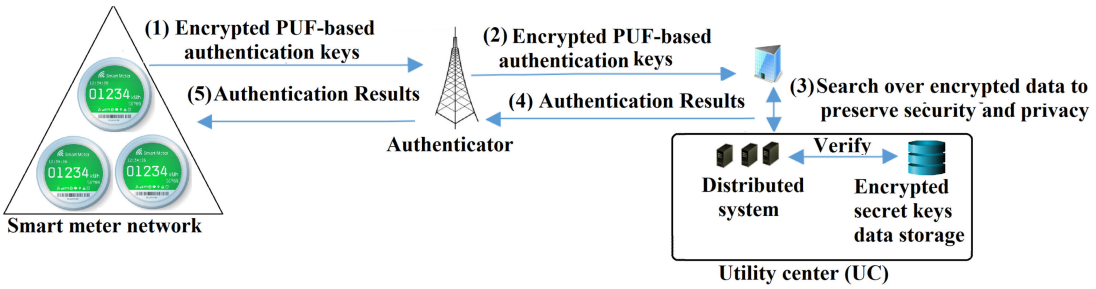

Figure 3. Network model and message exchanges.

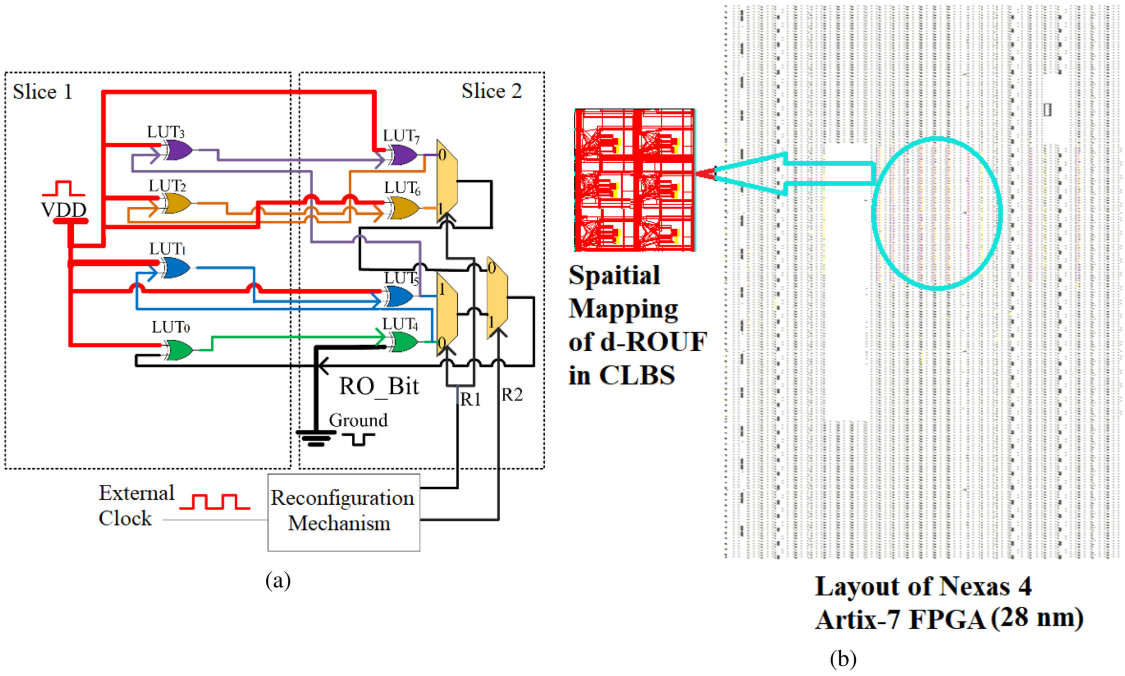

Figure 4. (a) High-level illustration of d-ROPUF design. (b) d-ROPUF design is split mapped on Artix-7 FPGAs.

impersonate an SM to retrieve the hardware-based fingerprints. Additionally, a malicious eavesdropping attack may aim to learn the secret SM keys, which is prevented by the encrypted keys, i.e., using the lightweight encryption in this case.

PROPOSED AMI AUTHENTICATION SCHEME

Figure 4(a) illustrates the proposed PUF design for the authentication scheme. The proposed scheme uses a d-ROPUF that is capable of reconfiguring itself into four different RO stages structures for generating highly unclonable and, thus, strong secret keys that are less susceptible to cloning, modeling, and machine learning attacks. Two signals, R1 and R2, are generated by the reconfiguration mechanism and connected to internal multiplexers (i.e., F5 and F6) to configure to a new PUF structure. Figure 4(a) also shows four RO stage structures (i.e., 1, 3, 5, and 7 stages) with different colors that are, respectively, green, blue, gold, and purple. The design is area efficient and is implemented onto a small FPGA area (single CLB). The high signals (red lines) are connected to configure LUTs as inverters, as shown in Figure 4(a).

The PUF design is realized on Artix-7 family of FPGAs, which is demonstrated in Figure 4(b). The RO structures are identically instantiated, with fixed CLB routing, using a hard-macro procedure that eliminates the dynamic delay

Table 1. Authentication Time for the Different Authentication Levels Determined by the NIST Framework and Security Standards.

Authentication levels and secret keys		Authentication time			
Name	Length of generated encrypted secret keys (bits)	Transfer time (milliseconds)	Authentication time for one year (seconds)	Authentication time for 10 years (minutes)	Authentication time for 50 years (hours)
L1	64	6.5	226.01	30.78	2.57
L2	128	12.9	113.01	18.83	1.57
L3	256	25.8	28.25	4.71	0.40
L4	512	51.6	18.83	3.14	0.26
L5	1024	100.32	12.56	2.01	0.18
Total	–	199.95	398.65	59.47	4.98

component imposed by dynamic FPGA routing. [5] Using a hard-macro design, the dynamic structures of ROPUF can be spatially mapped on adjacent CLBs within an FPGA. A large amount of PUF-based secret keys, from multiple FPGA chips are obtained for the authentication of large-scale SMs, improving their lifespan. The security of our scheme in terms of integrity and confidentiality is preserved by sending the authentication keys as encrypted text and perform the search over encrypted information.

EXPERIMENTAL RESULTS

The security of the proposed scheme is evaluated based on the NIST authentication time and storage requirements. [4]

NIST Security Requirements

As a proof of concept, this article focuses on hardware-based AMI authentication process using PUF-based key generation that satisfies different levels of NIST security requirements. Five different lengths of encrypted authentication keys are used for these levels (L1–L5), with 64, 128, 256, 512, and 1024 b, respectively. [4] Impersonating the UC is quite infeasible for an attacker since the secret keys are encrypted and even the UC will not have the key to decrypt the message and obtain the information (authentication key). A search over encrypted information is required to perform the authentication. Based on the aforementioned requirements, a lightweight cryptography is used to encrypt the authentication keys to preserve the integrity of the scheme and prevent impersonation and man in the middle attacks. Being hardware oriented, the proposed scheme uses inherently unique hardware-based authentication keys to verify the identity of the SM against spoofing attacks.

Timing and Latency Analysis

The authentication times for different standard authentication determined by an NIST framework are listed in Table 1. For the first security level L1 that has 64 b, the total authentication time is 64 0.10073 = 6.45 ms for every 15 min. The needed authentication time, in seconds (s), for the other levels (L2–L5) are, respectively, 0.0129 s (each hour), 0.0258 s (each 4.8 h), and 0.0516 s (each 24 h), and 0.1032 s (each 72 h). In a single year, the authentication process for L1 is accomplished 35 040 times (4 24 365 days) and require 35 040 0.007 = 226.01 s. Similarly, the yearly timing requirement for each level (L2–L5) are, respectively, 113.01 s (24 365 0.01), 28.3 s (3 365 0.03), 18.8 s (1 365 0.05), and 12.6 s (0.10 365/3).

The time required by our proposed scheme is compared with the authentication computation times of 10 other authentication protocols proposed by earlier researchers. As reported by Mohammadali et al.[14] the total authentication time for these protocols ranges from 0.8 to 45.4 s with an average time of 14.5 s. The authentication speed of the proposed scheme meets the NIST real-time application requirements (efficiency) with level L1 and L2, the most frequently used authentication levels, with only 6.5 ms and 12.9 ms, respectively, which are orders of magnitude lower than the aforementioned schemes. Some of these authentication schemes take 11

Table 2. Storage Requirements of the Proposed AMI Scheme for Different NIST Security Levels.

Authentication levels	An SM for 50 years (Megabytes)	200 meters for 50 years (Gigabytes)
L1	10.80	2.16
L2	5.40	1.08
L3	1.75	0.35
L4	1.17	0.24
L5	0.78	0.16
Total	19.91	3.98

steps to complete; however, our proposed scheme needs only five steps, as depicted in Figure 3. As per the authentication time requirements, for 10- and 50-years lifespan, the scheme will require less than an hour and less than 5 h, respectively, for all the AMI authentication levels (L1–L5).

Storage Requirements

As discussed in the previous section, according to the five different security levels proposed by NIST, L5 is the most secure level and requires 1024 b (1 K). [4] A key management scheme framework of an AMI system has been proposed with a maximum storage cost of 1.088 kB for each SM in the work by Liu et al.[10] A smart grid topology of 200 SMs with a long simulation time of 800 s and significant increase in memory usage of SMs over the simulation time, 6-GB RAM is used for emulating the SMs. [7] For a 50-year lifetime, the storage requirement of these existing authentication schemes for AMI of smart grid based on a simple ROPUF and configurable ROPUF, respectively, require an external storage of 96.1 GB for secret keys of a network of 200 SMs.[15]

Table 2 lists storage requirements for the proposed AMI authentication levels according to NIST standards. As compared to the existing schemes, for a 50-year lifetime, a total of 2.16 + 1.08 + 0.35 + 0.24 + 0.156 = 3.98 GB storage is required by an AMI network with 200 m using the proposed authentication scheme. There is significant savings in the amount of storage due to the fact that the SM also implements lightweight encryption that sends encrypted response to the UC. By doing this, only the encrypted response bits will need to be stored at the UC side for SM authentication, whereas the UC will perform a search over encrypted data to match the encrypted response received from an SM. Alternatively, there is no need to store the input challenges and parity bits unlike earlier techniques. In addition to the savings in storage, searching over encrypted data also protects the integrity and preserves the privacy of the SMs.

CONCLUSION

A novel authentication framework for AMI technology is proposed in this article. This framework utilized d-ROPUFs to realize a dynamic hardware-based authentication scheme. The design details of the proposed framework and implementation details on FPGAs are discussed. Additionally, the authentication protocol between SM, authenticator, and utility company is explained. To ensure high confidentiality and data integrity, the PUF-based keys are encrypted with the help of lightweight encryption. Experimental results demonstrate that the proposed AMI scheme is significantly faster and requires smaller storage capacity than the existing state-of-the-art techniques.

ACKNOWLEDGMENTS

This work was supported in part by the NSF Award under Grant CNS-1929774 and in part by SRC under Contract 2019-ST-2890.

& REFERENCES

1. S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," IEEE Consum. Electron. Mag., vol. 5, no. 3, pp. 60–70, Jul. 2016.
2. C. Konstantinou and S. P. Mohanty, "Cybersecurity for the smart grid," Computer, vol. 53, pp. 10–12, May 2020,
3. The Smart Grid Interoperability Panel—Cyber Security Working Group, "Guidelines for Smart grid cyber security," Gaithersburg, MD, USA, NISTIR 7628, 2010, pp. 1–597
4. 2010. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

5. F. Amsaad, N. Pundir, and M. Niamat, “A dynamic area-efficient technique to enhance ROPUFs security against modeling attacks,” in Computer and Network Security Essentials. Berlin, Germany: Springer, 2018, pp. 407–425.
6. B. J. Mohd and T. Hayajneh, “Lightweight block ciphers for IoT: Energy optimization and survivability techniques,” IEEE Access, vol. 6, pp. 35966–35978, 2018.
7. M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, “A lightweight message authentication scheme for smart grid communications,” IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 675–685, Dec. 2011.
8. H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, ”An efficient Merkle-tree based authentication scheme for smart grid,” IEEE Syst. J., vol. 8, no. 2, pp. 655–663, Jun. 2014
9. H. Nicanfar, P. Jokar, and V. C. M. Leung, “Smart grid authentication and key management for unicast and multicast communications,” in Proc. IEEE PES Innovative Smart Grid Technol., 2011, pp. 1–8.
10. N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, “A key management scheme for secure communications of advanced metering infrastructure in smart grid,” IEEE Trans. Ind. Electron., vol. 60, no. 10, pp. 4746–4756, Oct. 2013.
11. J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, “FPGA intrinsic PUFs and their use for IP protection,” in Proc.Int. Workshop Cryptographic Hardware Embedded Syst., 2007, pp. 63–80.
12. C. Huth, J. Zibuschka, P. Duplys, and T. Güneysu, “Securing systems on the Internet of Things via physical properties of devices and communications,” in Proc. Annu. IEEE Syst. Conf., 2015, pp. 8–13.
13. V. Seferian, R. Kanj, A. Chehab, and A. Kayssi, “PUF and ID-based key distribution security framework for advanced metering infrastructures,” IEEE Int. Conf. Smart grid Commun., 2014, pp. 933–938.
14. A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, “A novel identity-based key establishment method for advanced metering infrastructure in smart grid,” IEEE Trans. Smart Grid, vol. 9, no. 4, pp. 2834–2842, Jul. 2018.
15. A. P. D. Nath, F. Amsaad, M. Choudhury, and M. Niamat, “Hardware-based novel authentication scheme for advanced metering infrastructure,” in Proc. IEEE Ohio Innov. Summit, Jul. 2016, pp. 364–371.

Fathi Amsaad is currently an Assistant Professor with the School of Information Security and Applied Computing, Eastern Michigan University, Ypsilanti, MI, USA. He is the corresponding author of this article. Contact him at fathi.amsaad@emich.edu.

Selçuk Köse is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Rochester, Rochester, NY, USA. Contact him at selcuk.kose@rochester.edu.