# Security of Cloud Services with Low-Performance Devices in Critical Infrastructures

Michael Molle[1], Ulrich Raithel[1], Dirk Kraemer[2], Norbert Graß[3], Matthias Söllner[4] and Andreas Aßmuth[4]

[1]SIPOS Aktorik GmbH, Altdorf, Germany, Email: {michael.molle | ulrich.raithel}@sipos.de
[2]AUMA Riester GmbH & Co. KG, Müllheim, Germany, Email: dirk.kraemer@auma.com
[3]Grass Power Electronics GmbH, Nuremberg, Germany, Email: norbert.grass@grass-pe.com
[4]Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany,
Email: {m.soellner | a.assmuth}@oth-aw.de

***Abstract*—As part of the Internet of Things (IoT) and Industry 4.0 Cloud services are increasingly interacting with low-performance devices that are used in automation. This results in security issues that will be presented in this paper. Particular attention is paid to so-called critical infrastructures. The authors intend to work on the addressed security challenges as part of a funded research project, using electrical actuators and battery storages as specific applications. The core ideas of this research project are also presented in this paper.**

***Keywords–Low-performance devices; Cloud; automation.***

## I. INTRODUCTION

The increasing integration of the Internet of Things into industrial production has lead to the next industrial revolution called "Industry 4.0". [1] Increasing digitisation and automation leads to a greater number of systems being connected to the Cloud. This also means that in addition to traditional IT systems a growing number of Operational Technology (OT) systems is also connected to Cloud services. Nowadays, even Supervisory Control And Data Acquisition (SCADA) systems without a suitable built-in Industry 4.0 implementation will be hard to find. All of this leads to the so-called "Industrial Internet of Things" (IIoT) as a part of the IoT.

However, besides the big SCADA systems there is a great variety of embedded systems on devices like sensors, storage systems and actors running in physical processes. A power plant, for example, has only one process control system, but a couple of thousands of actuators to control the actual processes of energy generation. In recent years, many of these devices have been connected to Cloud services for advanced analytics that cannot be computed on the devices themselves because of their limited resources concerning computing power or memory. These embedded devices very often consist of a low-cost micro controller with low clock rate (usually in double-digit MHz range), using proprietary protocols on proprietary operating systems, while maintaining the real-time capability as topmost objective. This quite significant number of embedded devices incorporates a steadily growing part of the processes and infrastructure of whole branches of industrial production. It also means that industry and economy of whole countries more and more rely on such components.

The government of each individual country defines for itself which processes and infrastructures are especially important and which sectors of infrastructure have to be considered critical. In Germany, for instance, these critical infrastructures are devided into nine sectors, namely energy supply, information technology and communication, transportation and traffic, health, water supply and wastewater disposal, food provisions, finance and insurance industry, government and administration, and, finally, media and culture. [3] In the United States of America, a similar definition comprises even sixteen critical sectors. [4] Because of the high security requirements for

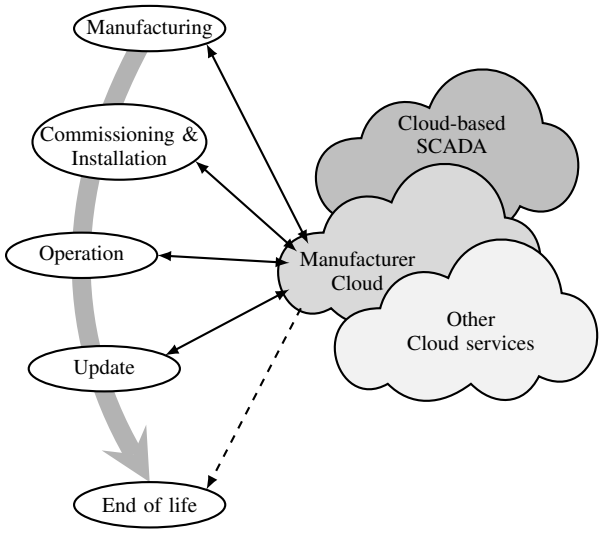


Figure 1. Lifecycle of a low-performance device and its connection to Cloud services. [2]

critical infrastructures, not only the operation of such a low-performance device must be taken into account, but all cross-relationships to Cloud services that occur during the life cycle of the device must be considered, too (cf. Figure 1). The manufacturer of the low-performance device stores specifications or maybe even initial versions of the device's firmware in their Cloud. When the device is installed in an industrial plant, it needs to be commissioned in order to communicate with the manufacturer's Cloud service. During operation, the device communicates with the Cloud service. It sends, for example, sensor data that is analysed maybe not only by the manufacturer, but also by one of the already mentioned Cloud-based SCADA systems. Therefore, an interface or gateway is needed to interconnect the manufacturer's Cloud service and the Cloud-based SCADA system. It can not be ruled out that the data is shared with other Cloud services, too. Because of known security issues or in case of new additional features, there might be updates for the software of the device. At the end of the lifecycle, e.g., when the device is broken or it no longer meets the requirements and therefore needs to be

 ISBN: 978-1-61208-703-0 

replaced, the manufacturer may wish to swipe all data and zeroise the device.

The paper is structured as follows: in Section II, we discuss threats and security challenges for Cloud-based SCADA systems as well as connected operational technology devices. In Section III, we review related work and present our own approach in Section IV. This approach is the subject of a current grant proposal by the authors, the different project partners are named in Section V. We conclude in Section VI with an outlook on future work.

## II. Threats and security challenges

Most countries consider energy and water supply as critical sectors deserving special protection – and the increasing number of cyberattacks [5] confirm this assessment to be correct. In recent years, there have been numerous attacks, like the Ukrainian blackout in 2015, when 225,000 people were suffering for a number of hours from a power outage. [6] During this attack, not only Industrial Control System (ICS) but also the firmware of serial-to-Ethernet adapters was damaged in order to disconnect servers from their Uninterruptible Power Supply (UPS) to maximise the length of the blackout. In December 2016, there was another attack on the Ukrainian energy supply which again resulted in a blackout for 100,000 to 200,000 people over a period of several hours. [7] Such targeted attacks are no longer carried out by single attackers but by full groups with considerably different motivations. It is likely that groups of organised crime or intelligence services might be involved.

The lifecycle of such an embedded device used in critical infrastructures, as described above and depicted in Figure 1, can be used to identify many attack vectors. If the adversary has access to the manufacturer's Cloud service, he could attempt to install backdoors in the initial firmware while the device is being manufactured. In addition to that, the specifications stored in the Cloud would surely be interesting for competitors and also be helpful to the attacker to detect vulnerabilities that can be exploited later. During the on-site installation, an attacker could, in principle, redirect the connection to the manufacturer's cloud service via a computer controlled by him as a starting point for a man in the middle attack. Security issues during operation are discussed explicitly in the following sections. Based on the last two phases, "update" and "end of life", requirements for the protection of the manufacturer's intellectual property can be exemplified. For instance, suppose another manufacturer reproduces the embedded devices in order to sell them at a lower price. This competitor would certainly like to benefit from new features or security updates that the original device manufacturer rolls out. It must therefore be ensured that a manufacturer can distinguish their original devices from clones in order not to supply those with new firmware. Likewise, it must be ensured that at the end of an original device's lifecycle its identity cannot be copied or reused so that a cloned device can pretend to be an original one.

Due to these threats some operating companies start to prevent their devices from any kind of communication to outside their own network. But most of the manufacturers, however, do not want or cannot afford to dismiss the advantages of interconnectedness, e.g., for systems like energy storages in a Smart Grid. Because this development was discernible through recent years, developments ranging from classic SCADA up to Cloud-based SCADA solutions incorporate a growing number of security-critical functions. Additionally, the corresponding norms as well as legislation were pushed along, resulting, for example, in standards like IEC 62443. Legislation in Germany also has acknowledged the problem and demands – in accordance with requirements for Cloud operators stated by the Federal Office of Information Security [8] and along with a "CE-conformity label for IT security" for manufacturers of products for critical infrastructure applying similar rules. [9]

### A. Security challenges for Cloud-based SCADA systems

In recent years, numerous Cloud-based ICS or SCADA systems have been developed and are now readily available. These systems interconnect on-site low-performance operational technology devices with Cloud services that run data acquisition and data analytics algorithms. The aggregation and analysis of these huge amounts of data is then used to optimise operation of the on-premise low-performance OT devices. This means that such Cloud-based SCADA systems are vulnerable against attacks targeting their Internet connection. A Distributed Denial of Service (DDoS) attack that prevents the above mentioned data acquisition and data analytics algorithms from being available for the on-premises devices certainly affects production in a non-beneficial way. In addition, data provided to these Cloud services might cause difficulties as well because of the loop back. If a sensor is hijacked and thus its data acquisition compromised, a control system today hardly has any chance at all to determine whether the data has been manipulated or not. At best, important data is provided redundantly which usually is true in plants only if the data emitting sensors are rated as safety critical. Manipulating a seemingly unimportant measurement often bears the potential of considerably interfering with a production plant's processes. Even worse are attacks on actors controlling these processes. If, for example, one of the couple of thousands actuators in a power plant can be compromised in a way that physically perturbs the process, the shutdown of the power plant – and so disconnecting it from the grid in order to reach a safe condition – is one of the more harmless scenarios imaginable.

Since OT networks benefit from having all data communication at precisely deterministic and thus predictable time slots, anomaly detection can be a means of locating interference caused by an attacker. However, direct manipulation of measurement within a sensor would not alter the sensor transmitting valid data using the proper protocol to its superior control system and anomaly detection would in most cases not recognise the data being counterfeit.

### B. Security challenges for OT devices

For the development of low-performance devices which are deployed in critical infrastructures, security-related topics are usually the last on the list of requirements – if present at all. In most cases their importance is overruled by economic concerns, since they are neither really relevant for manufacturing issues nor (at least up till now) for the customers' purchasing decisions. In addition, the following fact is also in many cases unattended: a security level for low-performance systems that is comparable to traditional IT systems can only be achieved with great effort – if at all possible. For economic reasons these systems' soft- and hardware is usually designed to have exactly the performance to fulfil their main purpose – and nothing beyond. The deployment of higher performance or more complex security procedures, with respect to small profit

 ISBN: 978-1-61208-703-0 

margins and multiply optimized supply chains, quickly leads to unprofitable and uneconomic products.

Apart from such economic reasons several other factors may cause even partially secured systems to fail:

- insufficient communication security,
- lacking authentication of communication end points,
- faulty implementation of algorithms,
- faults at the protocol level,
- compatibility problems with applied protocols or
- problems with the initial key deployment.

All this increases the probability of security breaches which are either patched only infrequently or lead to a complete replacement of these devices. [9] While IT systems usually provide options to implement and install patches easily, big installations, like power plants, allow only precisely defined time slots for revisions during which systems may be patched without financial losses or penalties.

## III. Related work

On a global scale, numerous institutions and companies are developing Cloud-based services for all kinds of devices, where they all have to consider security requirements.

As an example, the GE Predix service platform connects industrial assets (such as turbines, sensors, etc.) with a Cloud in order to collect and analyse operational and historical data to allow and improve predictive maintenance. [10] An additional application security service comprises two main features: a user account and authentication service using industry standards for identity management via whitelisting (amongst others), and an access control service using policy-driven authorisation for access restriction to resources programmed in a special policy language.

The AUMA Cloud is a free and secure Cloud-based solution for cost-effective asset management and predictive maintenance of AUMA actuators, promoting high plant availability. [11] It provides an easy-to-use interactive platform to collect and assess detailed device information on all the AUMA actuators in a plant. It allows plant operators to detect excessive loads or potential maintenance requirements at an early stage and take remedial action in time to prevent unexpected failures.

MindSphere is an open cloud platform developed by Siemens for applications in the context of the Internet of Things. [12] It stores operational data from all kinds of devices and makes it accessible through digital applications in order to allow industrial customers to make decisions based on factual information. Assets can be securely connected to MindSphere with auxiliary products (e.g., MindConnect IoT2040 or MindConnect Nano) that collect and transfer relevant machine and plant data.

## IV. The iSEC approach

The authors have submitted a funding proposal entitled "Intelligent Security for Electric Actuators and Converters in Critical Infrastructures (iSEC)" in order to solve some of the security challenges mentioned above.

The technology, which is in the scope of the authors of this paper, like actuators from SIPOS and battery storage combined with electric vehicle chargers from GPE, belongs to such critical infrastructure due to the widely distributed type of the installation and remote operation of such systems. The idea behind the funding proposal is to develop an integrated data communication which facilitates both, a high internal computing performance for the processing of real-time control algorithms and secured communication.

Primarily, the untampered local operation of the equipment needs to be ensured at any time and therefore the local firmware needs to be secured from any unauthorised access. Additionally, the local equipment's data communication containing real-time signals to system wide controllers or Cloud services is essential for proper and stable plant or grid operation. For service purposes, local equipment needs to be accessible by service staff to integrate new features into the system. The confidentiality of data and signals needs to be considered and ensured.

As stated before, microcontroller-based systems usually provide only very limited computing power and memory. Because of that, the computation of state of the art cryptographic algorithms or key negotiation algorithms may take several minutes. Almost all of these systems are run in environments where real-time requirements demand response times in the range of milliseconds or even microseconds, e.g., frequency converters in energy smart grids. Thus, system performance represents a significant limitation to the effectiveness of cryptographic operations. A further limitation is restricted amount of system memory – cryptographic algorithms have to be tailored to fit into the available RAM and ROM. As an approach to solve this problem the research of "lightweight cryptography" for low-performance embedded systems is just at its beginnings. [14]

Energy storage systems in larger quantities are essential to integrate higher contents of renewable energy sources into public distribution grids. Fluctuating power generation of photovoltaic or wind power systems requires short term storage to match the exact value of power consumption at any time of the day. Stationary energy storage systems and electric vehicle chargers become more common and are currently being installed into industrial buildings which are connected to public distribution grids. With increasing numbers, storage devices contribute to grid stability and therefore, they become critical infrastructure for grid operation and grid reliability. Data security becomes an important issue, as these systems are equipped with fully digital control systems, which are connected to remote systems for control and service access functionality. Furthermore, firmware updates can be installed via remote access, which is a very useful and system-critical feature likewise. Therefore, such critical systems need to be able to verify the data they receive and to authenticate the sender of the data before starting any actions based on the data received. Additionally, the data requires confidentiality to protect the systems from competitors and invaders.

Figure 2 depicts the data communication architecture. The power converters, controlled by digital signal processors (Level 1) are connected via a local CAN network to a Linux-based system and communication controller (Level 2). The system controller has a TCP/IP interface which facilitates data communication to local or via Internet connected Level 3 devices for operation and service functionalities. While CAN communication is restricted to the local system, TCP/IP is critical as it can be accessed from outside the local system.

It is planned to perform a detailed investigation of how internal and external interfaces can be constructed in a verifiable secure design, and how in-situ tests can prove their efficacy in terms of security and usability.

Cloud services shall be used for mechanisms of identifi-

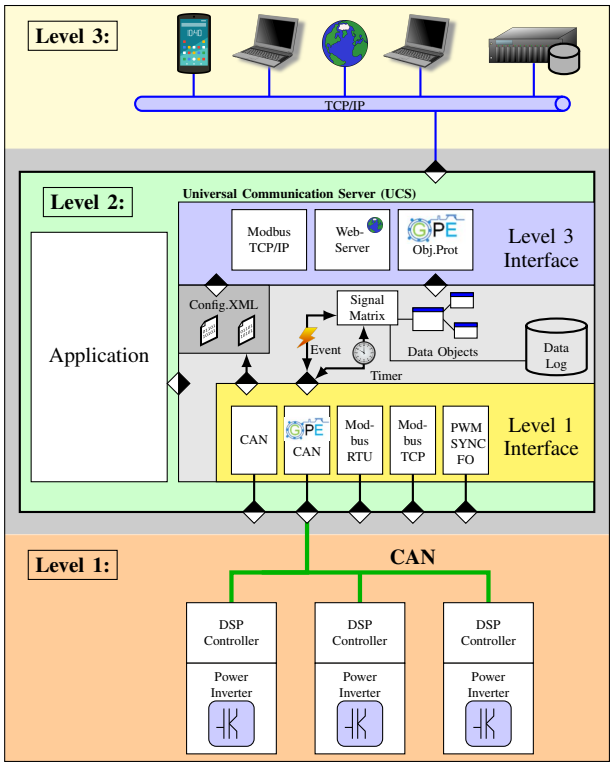


Figure 2. Data communication architecture. [13]

cation and authentication, for easing the task of performing necessary software patches and thus improving facilities' outage times and service intervals.

In addition, it is planned to investigate how Physical Unclonable Functions (PUF) can be used to secure communication between a Cloud server and (low-performance) sensor clients and to clearly identify a sensor client with a digital fingerprint. Hardware intrinsic deviations caused by the manufacturing process of semiconductors can be used to identify chips [15] and generate random encryption keys. The drawbacks of using non-volatile storage-mechanisms for storing encryption keys, can be overcome by using this relatively new approach. PUFs are a current subject of research, different approaches have yet been investigated. [16] [17] For example, with arbiter PUFs a race condition can be generated between two different digital paths on the same semiconductor. An arbiter circuit is used to measure which of the paths won the race. With different challenges the path can be configured and for every challenge, the winner is determined. Because of the manufacturing deviations every chip will give a different response, despite having the same hardware configuration and therefore, a digital fingerprint can be read out. As the response cannot be read out or predicted by an attacker it is called unclonable. Also, PUFs based on digital bistable storage elements, like SRAM cells, latches or flip flops, have been demonstrated. They are based on the principle of bringing them in, in an unstable state, and letting them settle in one of their stable states. Due to statistical variations during the manufacturing process, different chips cause different results despite the same hardware configuration. Many other solutions using deviations of the manufacturing process for identifying a chip are conceivable. [18] In this context, new protocols have also been investigated to secure lightweight communication based on PUFs. [19] [20] [21] Which lightweight PUF based protocols can be used for encryption of sensor data connected to a cloud-server is another topic of our studies. Just recently, first semiconductor devices with PUF-functionality are now readily available in order to identify hardware and implement a digital fingerprint, for example. [22] [23] [24] It has to be investigated whether these semiconductor devices can be used in order to help solving some of the security challenges mentioned before.

## V. The Consortium

SIPOS Aktorik GmbH emanated in 1999 from the former actuator division of Siemens AG in Nuremberg, since 2008 situated at Altdorf. Main proprietor of SIPOS Aktorik GmbH is the AUMA Riester GmbH & Co KG, Muellheim, which as a holding also provides commercial services. Today, SIPOS Aktorik GmbH employs a staff of 85 people in the departments assembly, R&D, customer service and administration. During the last 20 years SIPOS Aktorik GmbH succeeded in positioning itself on the global market for electric actuators with an export quota of 80 %. Main customers are international plant engineering and construction companies, valve manufacturers, and operating companies of conventional and nuclear power plants in Europe and Asia.

Grass Power Electronics GmbH, Nuremberg, is working on grid conected stationary battery storage systems in the range of some hundreds of kilowatts. Core technology components are digital computer modules for real time power converter control and for system control, including TCP based data communication.

The security research group at the Technical University of Applied Sciences OTH Amberg-Weiden has already worked on funded research projects using lightweight cryptographic algorithms. They have also experience in developing security protocols using PUFs for authentication and device identification. [25]

## VI. Conclusion and Future Work

In this paper, we showed that when it comes to combining low-performance embedded devices with Cloud services, all components must be secured to harden these systems against cyberattacks. Otherwise, compromised sensors can falsify computations and analytics performed in the cloud. And attacks against the Cloud services, e.g., a DDoS attack, has a direct impact on an ICS when it relies on a permanent connection to the cloud, too.

To master the challenges of IIoT and Industry 4.0, it is imperative to consider possible vulnerabilities and attack vectors when designing such systems ("security by design").

The authors hope that their submitted grant proposal iSEC will be approved to work on these security challenges.

## References

[1] M. Hermann, T. Pentek and B. Otto, "Design Principles for Industrie 4.0 Scenarios," in Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), January 5–8, 2016, Koloa, USA. IEEE, Jan. 2016, pp. 3928–3937, T. X. Bui and R. H. Sprague, Jr., Eds., ISBN: 978-0-7695-5670-3, ISSN: 1530-1605, URL: https://doi.org/10.1109/HICSS.2016.488 [accessed: 2019.04.12]

[2] G.-J. Schrijen, G. Selimis, J.-J. Treurniet, "Secure Device Management for the Internet of Things" in Proceedings of the 2019 embeddedworld Exhibition & Conference, February 26–28, 2019, Nuremberg, Germany. To be published.

[3] Federal Ministry of the Interior, Building and Community, Ed., "Nationale Strategie zum Schutz Kritischer Infrastrukturen" (National Strategy for the Protection of Critical Infrastructures), 2009.

 ISBN: 978-1-61208-703-0 

[4] Department of Homeland Security, Ed., “Critical Infrastructure Sectors”, URL: https://www.dhs.gov/cisa/critical-infrastructure-sectors [accessed: 2019.04.12]

[5] Federal Office for Information Security, Ed., “Die Lage der IT-Sicherheit in Deutschland 2017” (The State of IT Security in Germany in 2017), No. BSI-LB17/506, August 2017.

[6] E-ISAC, Ed., “Analysis of the Cyber Attack on the Ukrainian Power Grid”, Technical Report, March 18th, 2016, URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [accessed: 2019.04.12]

[7] M. Strathmann, “Malware führte zum Blackout” (Malware led to Blackout), Zeit-Online, January 5th, 2016, URL: https://www.zeit.de/digital/internet/2016-01/stromausfall-hacker-ukraine-blackenergy [accessed: 2019.04.12]

[8] Federal Office for Information Security, Ed., “Anforderungskatalog Cloud Computing (C5)” (Cloud Computing Compliance Controls Catalogue), September 2017.

[9] UP KRITIS, Ed., “Empfehlungen zu Entwicklung und Einsatz von in Kritischen Infrastrukturen eingesetzten Produkten” (Recommendations for the Development and Deployment of Products used in Critical Infrastructures), Version 1.00, November 29th, 2018.

[10] General Electric Company, Ed., “Predix Architecture and Services”, Technical Whitepaper, November 28th, 2016, URL: https://d154rjc49kgakj.cloudfront.net/GE_Predix_Architecture_and_Services.pdf [accessed: 2019.04.12]

[11] AUMA Riester GmbH & Co. KG, Ed., “The AUMA Cloud”, 2019, URL: https://www.auma.com/en/service-support/digital-services/the-auma-cloud/ [accessed: 2019.04.12]

[12] S. Naujoks, “MindSphere – Siemens cloud for industry: What is it all about?”, May 9th, 2016, URL: https://www.pac-online.com/mindsphere-siemens-cloud-industry-what-it-all-about [accessed: 2019.04.12]

[13] N. Grass, F. Ferner and F. Nickl, “Modular and Intelligent Battery Control System for Electric Vehicles and Stationary Storage Systems” in Proceedings of the 2016 IEEE International Telecommunications Energy Conference (INTELEC), October 23–27, 2016, Austin, USA. IEEE, Nov. 2016, pp. 1–7, ISBN: 978-1-5090-1877-2.

[14] “NIST Issues First Call for ’Lightweight Cryptography’ to Protect Small Electronics”, 2018, URL: https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics [accessed: 2019.04.12]

[15] S. Choi, D. Zage, Y. R. Choe and B. Wasilow, “Physically Unclonable Digital ID”, in Proceedings of the 2015 IEEE International Conference on Mobile Services, June 2015, pp. 105–111.

[16] R. Maes and I. Verbauwhede, Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. Springer, Berlin; Heidelberg, 2010, chapter 1, pp. 3–37, in A.-R. Sadeghi, D. Naccache, Eds., Towards Hardware-Intrinsic Security, ISBN: 978-3-642-26578-5.

[17] H. Handschuh, G. J. Schrijen and P. Tuyls, Hardware Intrinsic Security from Physically Unclonable Functions. Springer, Berlin; Heidelberg, 2010, chapter 2, pp. 39–53, in A.-R. Sadeghi, D. Naccache, Eds., Towards Hardware-Intrinsic Security, ISBN: 978-3-642-26578-5.

[18] S. Katzenbeisser, Ü. Kocabaş, A.-R. Sadeghi, I. Verbauwhede and C. Wachsmann, PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon. Springer, Berlin; Heidelberg, 2012, pp. 283–301, in E. Prouff and P. Schaumont, Eds., Cryptographic Hardware and Embedded Systems – CHES 2012, ISBN: 978-3-642-33027-8.

[19] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach and S. Devadas, “Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching” in Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops, May 24–25, 2012, San Francisco, USA. IEEE, Jul. 2012, pp. 33–44, ISBN: 978-1-4673-2157-0.

[20] T. Idriss and M. Bayoumi, “Lightweight highly secure PUF protocol for mutual authentication and secret message exchange” in Proceedings of the 2017 IEEE International Conference on RFID Technology Application (RFID-TA), September 20–22, 2017, Warsaw, Poland. IEEE, Nov. 2017, pp. 214–219, ISBN: 978-1-5386-1833-2.

[21] M. Delavar, S. Mirzakuchaki, M. H. Ameri and J. Mohajeri, “Puf-Based Solutions For Secure Communications In Advanced Metering Infrastructure (AMI)”, IACR Cryptology ePrint Archive, Report 2016/009, https://eprint.iacr.org/2016/009, [accessed: 2019.04.12]

[22] Maxim Integrated, “ChipDNA”, https://www.maximintegrated.com/en/design/partners-and-technology/design-technology/chipdna-puf-technology.html [accessed: 2019.04.12]

[23] INTRINSIC ID, “QuiddiKey”, https://www.intrinsic-id.com/products/quiddikey/ [accessed: 2019.04.12]

[24] NXP, “Secure microcontroller family SmartMX2”, https://www.nxp.com/docs/en/brochure/75017516.pdf [accessed: 2019.04.12]

[25] A. Aßmuth et al., “Improving Resilience by Deploying Permuted Code onto Physically Unclonable Unique Processors”, in Proceedings of the 2016 Cybersecurity and Cyberforensics Conference (CCC), August 2–4, 2016, Amman, Jordan. IEEE, Oct. 2016, pp. 144–150, ISBN: 978-1-5090-2657-9.

 ISBN: 978-1-61208-703-0 