Physical Layer Security: About Humans, Machines and the Transmission Channel

Christoph Lipps[1] and Hans Dieter Schotten[1,2]
[1]German Research Center for Artificial Intelligence, Intelligent Network Research Department, Kaiserslautern, Germany
[2]University of Kaiserslautern, Division of Wireless Communication and Radio Positioning, Kaiserslautern, Germany
Christoph.Lipps@dfki.de
Hans_Dieter.Schotten@dfki.de

Abstract: In an increasingly interconnected and globalized world in which the volume but also the confidentiality of transmitted content is becoming ever more important, trust, confidence and trustworthiness are of fundamental importance. Particularly in human societies, this trust is established, sustained and strengthened by personal relationships and experiences. But, in a globally connected world with Cyber-Physical Production Systems (CPPS), Industrial Internet of Things (IIoT) and Digital Twins (DTs), these personal relationships do not longer exist. (Remote) access to systems is possible from anywhere on the globe. However, this implies that there have to be technical solutions to detect, identify and acknowledge entities -people and machines- in the networks and thus to establish an initial level of trust. Especially since the proliferation of appropriate use-cases, Physical Layer Security (PhySec) is becoming increasingly popular in the scientific community. Using systems' intrinsic information for security applications provides a lightweight but secure alternative to traditional computationally intensive and complex cryptography. PhySec is therefore not only suitable for the IIoT and the multitude of resource-limited devices and sensors, it also opens up alternatives in terms of scalability and efficiency. Moreover, it provides security aspects regarding the entropy H and Perfect Forward Secrecy (PFS). Therefore, this work provides insight into three major branches of PhySec: i) *Human* - Physically Unclonable Functions (PUFs) ii) *silicon/electrical - PUFs*, and iii) *Channel-PUFs*. Based on the PUF operating principle, the silicon derivatives consider the electrical properties of semiconductors. Individual and uninfluenceable deviations during the manufacturing process result in component-specific behavior, which is described in particular for Static- and Dynamic Random Access Memory (S-/DRAM). Following this PUF principle, human characteristics -biological, physiological and behavioral features-, are used to recognize and authenticate them. With respect to the wireless channel, the characteristic properties of electromagnetic wave propagation and the influences on the wireless channel -diffraction, reflection, refraction and scattering-, are used to achieve symmetric encryption of the channel. In addition to the "conventional" wireless PhySec, especially the development of the Sixth Generation (6G) Wireless Systems, opens up a wide range of possibilities in terms of PhySec, for example in relation to Visible Light Communication (VLC), Reconfigurable Intelligent Surfaces (RIS) and in general the application of frequencies in the (sub)THz range. Thus, the work provides an overview of PhySec fields of application in all areas of the IIoT: in terms of humans, machines, and the transmission channel.

Keywords: physical layer security, physically unclonable functions, Human-PUFs, Channel-PUFs, (cyber)security, trust

1. The (Industrial) Internet of Things and the matter of security

Trust is not only a fundamental requirement for social coexistence, without trustworthy and confidential relationships, economic cooperation is inconceivable. Furthermore, without trust and without doubtless identification and authentication of contacts -humans and machines-, further security goals such as confidentiality, integrity and availability (Schäfer & Rossberg, 2016) are not achievable. But, it is becoming increasingly challenging to meet the requirements: Whereas previous relationships were characterized by personal contacts, these are disappearing in a progressively interconnected and globalized communication environment. Access to systems is available via remote maintenance from anywhere around the world, a technician does not necessarily have to be physically present on the machine at the factory, she may not even have to enter the company premises, or even be in the same country.

In addition, the growing number of connected devices is increasing as well: The International Telecommunication Union (ITU) predicts that the number of Mobile Broadband (MBB) subscribers worldwide will reach more than 17 billion by 2030 and the amount of Machine-to-Machine (M2M) terminals will exceed 100 billion (this is 14 times more than in 2020) by the same timescale (International Telecommunication Union, 2015). This is accompanied by demands on the performance of the interconnected devices. Many of them are limited in their features, computing power, as well as battery lifetime and -capacity. Especially in relation of the Fifth Generation (5G) New Radio (NR) technology a new term arises: reduced capability (RedCap) devices. The

4GPP Release-17 describes this group of devices as “Mid-Speed Smart IoT application” (Valerio, 2021) addressing the Sector of smart Internet of Things (IoT).

But, especially in terms of the terminology of the IoT there are many different aspects and applications in this area. So to provide a certain structure, a distinction is made between the terms used, as illustrated in **Figure 1**: i) The **Internet of Things** encompasses the cyber networking of physical objects, including everyday (household) items such as smart light bulbs, door keys, and wearables. *Kevin Ashton* “coined” that term back in 1999 during a presentation at Procter & Gamble where he introduced the Radio-Frequency Identification (RFID) chip into the company's value chain, but also pointed out the interdependencies between computer technology and humans (Kramp, van Kranenburg & Lang, 2013); ii) **Industrial Internet of Things (IIoT),** in turn, is shifting the scope from home applications to industrial manufacturing, transportation and critical infrastructure. With the purpose of saving costs and resources, and generally minimizing risks, the IIoT primarily includes “smart sensors and actuators to enhance manufacturing and industrial processes” (Posey, et al., 2022). These ”connected sensors and actuators enable companies to pick up in inefficiencies and problems sooner and save time and money” (Posey, Rosencrance & Shea, 2022); iii) Another specialization is the term **Industry 4.0 (I4.0),** which was introduced by *Wolfgang Wahlster, Henning Kagermann* and *Wolf-Dieter Lukas* in 2011 as a marketing term in “INDUSTRIE 4.0: The 4th Industrial Revolution and the Internet of Things” as part of the Hannover Fair (DFKI, 2021). I4.0 is focused on the process within production facilities with smart interconnection of devices and scenarios such as M2M and Machine-to-Service (M2S) communication.

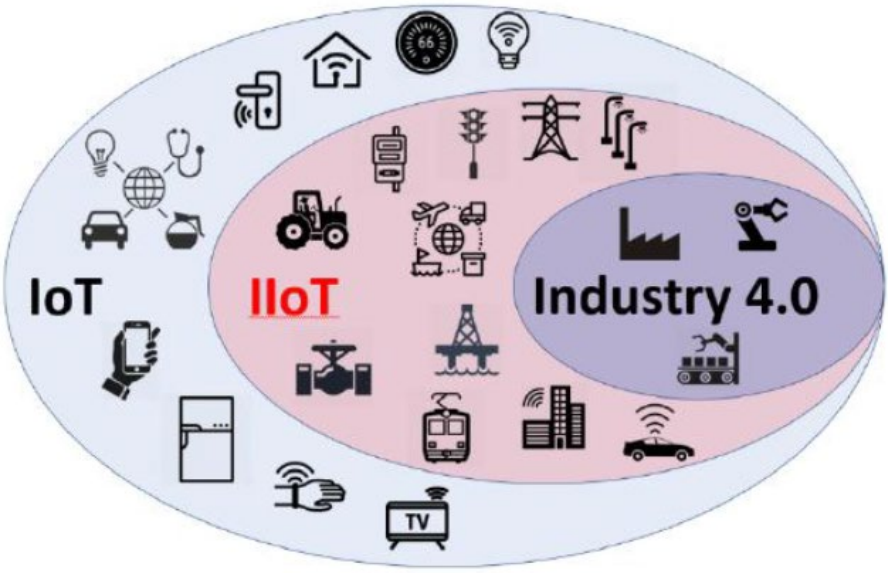


Figure 1: Linking the terms Internet of Things, Industrial Internet of Things and Industry 4.0. While the IoT primarily describes the interconnection of everyday objects, the IIoT also includes applications of critical infrastructures, means of transport (Hoffman, 2019)

The various concepts are accompanied by different threat scenarios and attack vectors, from which individual security requirements can be deduced. For instance, a smart light bulb in a home environment - switching lights on and off - does not require the same level of security as, say, controlling a robotic arm in an industrial environment - uncontrollable movements could injure/kill people. In addition to the requirements, the capabilities of the devices used are crucial. As already mentioned, they differ significantly in terms of memory, energy and computing power. A comprehensive overview of the constraints in the IIoT context is given by (Hoffman, 2019), for instance, whereas *Zou et al.* discuss security aspects in the area of radio communication (Zou, et al., 2016). *Schneier* (2015) gives a detailed insight into the field of cryptography in which he explains, for example, the differences between symmetric and asymmetric cryptography, together with the different requirements for their implementation. Especially with RedCap devices, asymmetric crypto and key exchange (Diffie & Hellman, 1976) has drawbacks that could be overcome by "modern" approaches.

A promising approach to meet these requirements is provided by Physical Layer Security (PhySec) methods, on which this work focuses. Therefore, in Section 2, a definition of the term is provided and the different aspects of the methods such as hardware related PhySec, solutions considering the wireless propagation channel and

approaches which put the human body in the spotlight, are discussed. Since the authors of this work are involved in the development of the Sixth Generation (6G) Wireless Systems and consider its development as a major opportunity to incorporate PhySec methods into the corresponding standardization, Section 3 gives an insight into key enabling technologies that could lead to the breakthrough of PhySec algorithms. Section 4 discusses the approaches described and provides a classification in the security context. Finally, Section 5 concludes the work and gives an outlook for future work.

2. Physical Layer Security

In the conventional perspective on the subject of Physical Layer Security, derived from the bottommost layer of the Open System Interconnection (OSI) model, which refers to seven layers (Application-, Presentation-, Session-, Transport-, Network, Data Link-, and Physical Layer) (ITU, 1994), it describes a set of applications targeted specifically at the wireless communications channel. These applications are relevant because no security mechanisms are addressed in the OSI model, but are only added in the X.800 standard (ITU, 1991).

However, the basic principle, the utilization of inherently available information, does not only apply to the wireless channel, but can be transferred to other applications such as semiconductors or even the human body as well. That is why the authors have extended this term, as explained in Section 2.1.

2.1 Definition and classification

The topic Physical Layer Security is not a new one, but due to the proliferation of use-cases it is stepping towards the focus of researchers worldwide. Due to the “already available” characteristic and intrinsic features it offers benefits with respect to secure the environments indicated in the previous Section. As the purpose of the work, on which this paper is based, is the comprehensive approach in securing various entities –humans and machines- and in addition the transmission channel, a definition is required comprising all of the different approaches.

Based on the hardware related *silicon/electrical* Physically Unclonable Functions (PUFs), addressed in the Section below, *Halak* is defining them as a “physical entity whose behaviour is a function of its structure and the intrinsic variation of its manufacturing process” (Halak, 2018). In combination with the wireless PhySec perspective from *Hamamreh, Furqan and Arslan* to “exploit the characteristics of the wireless channel and its impairments” (Hamamreh, Furqan & Arslan, 2018) the deviation and proposed definition is that:

> *Physical Layer Security comprises various methods of how to utilize inherently present characteristics of media (hardware, wireless channel and human body) to derive secrets applicable as cryptographic primitives.*

2.2 The human factor

Although an increasing number of (I)IoT, I4.0 and Industrial Automation and Control Systems (IACS) procedures are automated - with M2S and M2M applications -, there is still a human factor involved. Starting with workers within the manufacturing sites to on-site service technicians to remote maintainers, different people are integrated into the processes and have to be identified, authenticated and authorized accordingly.

Even though biometric authentication is the simplest and oldest form of identification - even animals are able to recognize each other by smell, behaviour and voice (Schneier, 2014) -, the conditions in the (I)IoT/I4.0 context place special requirements on biometrics. On the one hand, many of the traditional authentication mechanisms such as fingerprints, iris- and facial recognition, or speech are not possible due to industrial safety equipment (helmet, goggles, gloves), and on the other hand, the general operating conditions have changed. Globalization has increased the distances for identification, although the verification is no longer carried out by humans alone; in short, the type of authentication has certainly changed.

In general, authentication is differentiated into the three areas *Knowledge*, *Possession* and *Inherence* factors, whereby biometrics (Jain, Ross & Prabhakar, 2004) are assigned to the *Inherence* factors. As indicated in **Figure 2,** these are in turn divided into *biological, physiological* and *behavioral* factors. In addition to the traditional methods mentioned above (fingerprinting, etc.), there are some interesting "modern" approaches, such as the Mechanomyogrm (MMG), whose mode of operation, the use of signals by muscle fibers movement is described, for instance, by *Pal, Gautam* and *Singh* (2015). *Bidgoly et al.* Examine the use of bio-electrical signals of the brain

by recording Electroencephalogram (EEG) (Bidgoly, Bisgoly & Arezoumand, 2020), whereas *Sarkar, Abbott and Doerzaph* (2016) use the volumetric changes of blood in the peripheral areas via Photoplethymography (PPG).

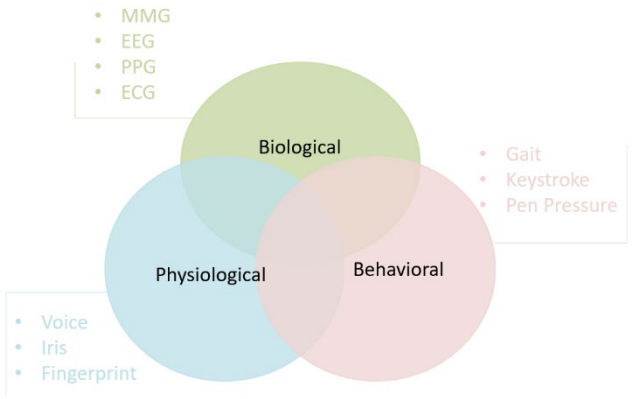


Figure 2*:* The three main categories of biometric authentication: biological, physiological and behavioral factors

Following the argumentation regarding PhySec from the previous Section, the working principle can be extended to the human body. The intrinsic, individual (bio-)physical characteristics can be used for authentication and for further cryptographic primitives. However, it is essential to consider that the human body is a living organism and is therefore continuously in a process of change: Cells are dying and new cells are being formed. Especially with regard to cryptographic applications, however, this entails certain requirements, since in such procedures a key needs to be identical every time it is required. This is where the capabilities of Artificial Intelligence (AI) in particular can contribute decisively and support the training of systems. The authors' work exemplifies the added value of such approaches and also the appropriateness of modern biometric methods.

Lipps, Herbst and *Schotten* (2021c), for instance, have developed a pressure-sensitive capable of distinguishing between people. Using an 18x6 sensor matrix, a footprint of 77 points is generated based on the form factor, which takes into account features such as pressure distribution within the foot, weight and step length. With a detection rate of about 60% after the first step, the initial setup already provides solid results, which will be further improved by i) the use of stitched conductive threads (instead of horizontal and vertical arrangement of conductive material) and ii) machine learning algorithms to train the system.

In another approach to using biometrics, *Lipps, Bergkemper* and *Schotten* (2021b) use Electrocardiogram (ECG) signals to derive conclusions about the individual. Therefore, data are derived by a 3-lead ECG, pre-processed due to noise via butterworth filtering and segmented according to the PQRST-waves. A comparison between the ML algorithms k-nearest Neighbor, Support Vector Machines (SVMs), and Gaussian Naive Bayes (GNB) indicates that the methods differ in their suitability for differentiation. For example, with a group of 20 people, SVMs can distinguish them with an accuracy of around 90%, whereas with KNN classifier only an accuracy of below 40% was achieved.

Since the individual methods already show good results with regard to the use of biometrics, it will be interesting to examine how the results are when combined and additional features are integrated. For this purpose, the authors are currently working on the use of EEG signals and the evaluation of behavior-based features.

2.3 Hardware-based Physically Unclonable Functions

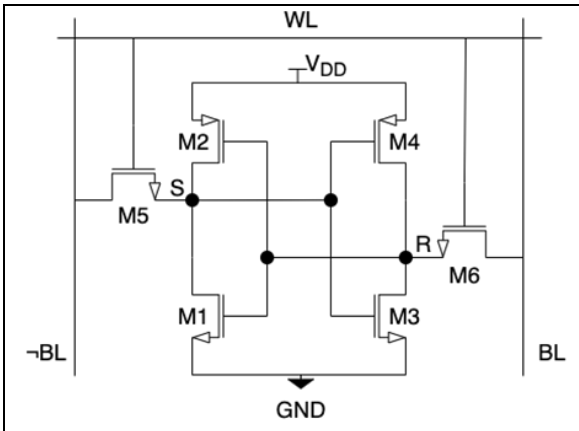
In addition to humans, it is primarily the machines that are particularly relevant in the (I)IoT/I4.0 scenarios. However, the requirements for sensors, actuators and controls are different from those for human authentication, simply because machines themselves have different individual characteristics, but also have different validation mechanisms. Besides, already back in 2012, *Bonneau et al.* emphasized the importance to abolish and replace (traditional) passwords (Bonneau, et al., 2012).

This is another area where PhySec, and in particular the field of Physically Unclonable Functions (PUFs), provides a suitable solution which offers benefits compared to conventional hardware security mechanisms such as Trusted Platform Modules (TPMs) (Höller & Toegl, 2018), certificates (McLuskie & Belleken, 2018) or asymmetric cryptography (Schneier, 2015). In particular, due to the inherent availability and thus low acquisition cost - for

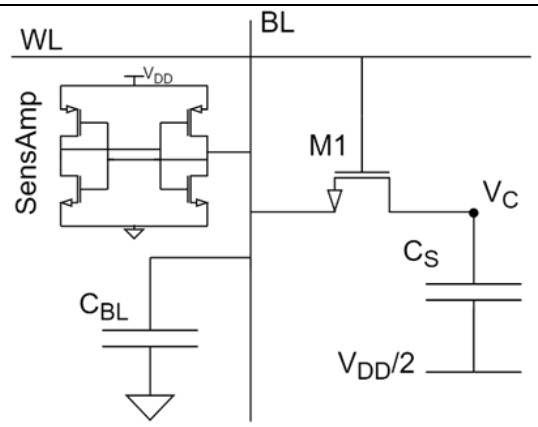
example, Random Access Memory (RAM) is already built into almost all electronic devices -, and time until the primitives are available - a few nanoseconds -, PUFs are more than just an alternative to be considered.

Nevertheless, the overall idea is not completely new, as since the general description of the principle by *Gassend et al.* in 2002 (Gassend, et al., 2002), there are many different approaches how PUF derivatives can be used. According to *Ahr, Noushinfar* and *Lipps* (2021), a fundamental distinction of the approaches is possible into Memory-based and Timing-based PUFs. Memory-based include among others, Flip-Flop (Khan, et al., 2020), Butterfly (Kumar, et al., 2008) and SRAM-PUFs (Halak, 2018), whereas Arbiter- (Machida, et al., 2014), Ring-Oscillator- (Gao, et al., 2014) and Self-Timing PUFs are attributed to the Timing-based PUFs (Halak, 2018).

The authors' work focuses on memory-based PUFs, although here in the two different RAM types, static (see **Figure 3 a)**) and dynamic (see **Figure 3b)**). For instance, *Lipps et al.* provide an evaluation of the various external and internal influences to the SRAM-behaviour. Besides others, they examined the influences of the environmental temperature in a range between -10°C and 60°C to the Start-Up behaviour of SRAM cells. They observed fluctuations in the entropy of the stat-up values between an average of 0.87 (at -10°C) and an average of 0.96 (at +60°C). In contrast, the runtime before the restart, fluctuations in the supply voltage and the values stored in the non-volatile memory (NVM) before the restart had only little influence in their studies (Lipps, et al., 2018). In the studies of *Ahr, Lipps and Schotten* (2021), the stability of the cells could also be evaluated - in cryptographic applications, it is important that primitive cells are reproducible. In the examinations, 30 SRAMs were respectively read out 500 times and compared with regard to the stability of the start-up patterns. The results indicated that the cells are well suited for cryptographic applications with a stability of over 99.5%. In *Ahr, Noushinfar and Lipps* (2021) they highlight the differences between SRAMs and DRAMs and compare them, among others, in terms of availability, challenge-response pairs, reliability, and uniformity.



(a) Typical structure of a 6T SRAM cell. The transistors form two cross-coupled inverters, storing the a stable state, one or zero.



(b) Structure of a DRAM cell. BL build a capacity C_{BL} much bigger then C_S. The amplifier SensAmp

Figure 3: The structural design of SRAM and DRAM cells differs, among others, in the number of transistors used and their wiring

2.4 Wireless Secret Key Generation

The transmission channel does not only represent the connection between the addressed entities, the original definition of PhySec, respectively the Secret key Generation (SKG) (Ambekar & Schotten, 2014) and Channel-Reciprocity based Key Generation (CRKG) (Zenger, et al., 2015), mainly refers to wireless communication. Based on influences on the wireless channel - such as diffraction, refraction, reflection and scattering - values such as Received Signal Strength Indicator (RSSI), Reference Signal Received Power (RSRP) and Channel State Information (CSI) are measured on both sides of a channel according to the principle of channel reciprocity and used for cryptographic processes. Accordingly, this is a well-researched field, at least for the IEEE802.11 WLAN sector. For instance, *Zhang et al.,* developed a Wireless open-Access Research Plattform (WARP) based testbed to examine SKG on Wireless Local Area Network (WLAN) (Zhang, et al., 2016). Different channel types such as Multi-Antenna Channels, Multiple Access and Interference channels as well as broadcast channels are considered by (Mukherjee, et al., 2014). *Weinand, Karrenbauer and Schotten* (2018) propose a security

architecture for Ultra-Reliable Low-Lattency Communication (URLLC) and a plug & trust protocol, based on PhySec algorithms.

The underlying SKG working principle, as depicted in **Figure 4**, is based on the five building blocks: Channel Measurement, Reciprocity Enhancement, Quantization, Information Reconciliation and Privacy Amplification; which are described in details for instance by (Lipps, et al., 2020). But as this is based on the propagation of electromagnetic waves, and therefore radio standard-independent, there is work transferring the "idea" to cellular systems, for instance. Here, *Lipps et al*. apply the approach in Cellular Systems as well. They were able to decrease the Bit Error Rate (BER) significantly by applying Machine Learning (ML) algorithms for the channel prediction. Considering various use-cases (static and mobile application) they evaluated the metrics RSSI and RSRP with respect to the BDR and were abel to reduce this from about 40% (RSSI static and mobile) to about 5% (RSSI Static mobile). Merely with the mobile RSSP the BDR could be reduced only to about 10% (the reasons for this are different, lie e.g. with interferences of the environment during the measurements) (Lipps, et al., 2020).

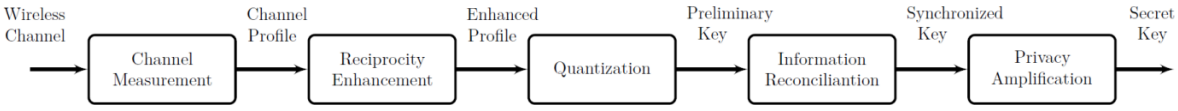


Figure 4: The Secret Key Generation building blocks

In addition to the existing radio standards, the application of PhySec will particularly be relevant during the development and subsequent standardization of the Sixth Generation Wireless Systems. As these are also wireless systems, they are discussed separately in Section 3.

3. Physical Layer Security and the Sixth Generation Wireless Systems

Despite the indicated suitability of Physical Layer Security methods and their wide potential for application, the methods have not yet become properly established as security mechanisms and unfortunately still lead a niche existence. However, the development of the Sixth Generation Wireless Systems and the (even) greater involvement of RedCab devices raises the opportunity to integrate PhySec algorithms into the standardization process. Moreover, many of 6G's claimed key enabling technologies correlate directly with PhySec methods: Reconfigurable Intelligent Surfaces (RISs), intended as passive "repeaters", open up the possibility of actively influencing the transmission channel; Wireless Optical Communication (WOC) has different properties than Radio Frequencies (RF), but still offers PhySec starting points, as known from fiber optics, for example; or the use of higher frequency bands up to the (sub)terahertz range, increases the entropy within the radio channel and thus increases the quality of the SKG key material.

3.1 Reconfigurable Intelligent Surfaces

Reconfigurable Intelligent Surfaces, Intelligent Reflecting Surfaces (IRS) or metasurfaces -depending on the scientific point of view- are "planar surfaces" (Pan, et al., 2021) composed of individually controllable passive reflecting elements. Through phase shifts or active beamforming/splitting they enable to actively influence the characteristic properties of the radio channel and thus to increase the entropy of the channel and at the same time to improve and strengthen the SKG generated keys (Lipps, et al., 2021).

3.2 Wireless Optical Communication

The visible light spectrum, in the range between 400-800 THz and wavelength range between 375-780nm, is used by the Visible Light Communication (VLC) as a subset of the WOC. One of the main advantages is the robustness against electromagnetic interference such as occurs in Radio Frequency (RF) communication. Unlike RF, however, light is hindered in its propagation by simple walls, for example, and offers advantages in terms of protection against eavesdropping. In particular, the combination with RIS offers additional opportunities to open up new use cases (Uysal, et al., 2016).

3.3 (sub)Terahertz Frequencies

Another possible way to meet the requirements of 6G is to push the communication into higher frequency ranges. The technological capabilities of (sub)terahertz communication allow signal bandwidths of more than 1GHz and data rates in the range of terabits per second. This is accompanied by advantages in terms of accurate

positioning and sensing, which includes benefits in targeted communication (beamforming). Especially with regard to the entropy of the channel, on which the quality of the SKG is based, the higher frequency brings advantages up to a certain level, since the reflections further increase the entropy.

4. Discussion

Safeguarding systems, networks and end devices is becoming more and more important in an increasingly interactive world. However, with increasing complexity and heterogeneity, the requirements for the appropriate security mechanisms are growing as well. For this purpose, three different types of lightweight and inherently available and thus easy-to-implement and cost-effective security mechanisms have been described in this work. All of them with different strengths and weaknesses, even in comparison with conventional solutions. But one thing is always important to keep in mind in conjunction with the PhySec methods discussed herein: The methods can never be as strong as dedicated individual security mechanisms, but should always be considered as a complement and additional security feature.

In terms of modern biometrics, the proposed solutions such as gait-based recognition or ECG authentication offer a very simple but secure way to be used as an additional security feature, for instance, as additional contextual information. Otherwise, they are more uniquely linked to a particular person than passwords or tokens are. Passwords can be shared, tokens and mechanical keys can be stolen, which makes it easy to impersonate a fake person and gain unauthorized access. Shoes might be stolen as well, but it is almost impossible to imitate the gait profile of a person. There will always be deviations in stride length, weight and pressure distribution. Similar applies to ECG values, behavior-based features or EEG signals. In addition, biometric features (from fingerprints to gait profiles) contain more derivable information than, for example, a 128-bit password (and what user remembers a 128-bit password?).

A major advantage of the aforementioned methods is the inherent existence of the information. This applies in particular to the Physically Unclonable Functions. RAM is contained in almost all electronic devices. Certainly, there are powerful and technically sophisticated hardware modules and Trusted Platform Modules, but they all have to be introduced into an existing system from the outside. In addition, these are cost-intensive thus not economically feasible for (I)IoT/I4.0 applications that involve a large number of devices. So for "simple" security applications, PUF implementation are way more attractive. Similarly, certificates can contain sophisticated security chains, but they need to be i) inserted into a system from the outside and ii) require a non-volatile memory in the system on which they can be stored, which in turn is vulnerable to attacks. Like any of these systems, PUF security mechanisms require a validation system consisting of challenge-response pairs, for example. The prerequisite is the secure and uncompromisable storage of these pairs on the validator side (on device side the information can be generated on demand and does not have to be stored).

The advancing wireless networking and especially the just started development of the Sixth Generation Wireless Systems open up possibilities for attack vectors but also for perspectives for proposed solutions. The mentioned SKG methods provide approaches for lightweight cryptography based on inherently available information. In addition, there are advantages with regard to Perfect Forward Secrecy (PFS), as keys can be recalculated at definable intervals. However, it is also obvious that the methods require a minimum of entropy within the systems. Channel-based encryption is not possible in static and low-reflection channels that are completely free of interference and noise. However, this is where 6G technologies such as Reconfigurable Intelligent Surfaces could provide a suitable contribution.

Trustworthiness and security of the systems are becoming increasingly relevant, and the mechanisms mentioned can make a contribution to this, but they are not the solution for everything. In their respective application areas, they provide good to great results and are more than worthy of consideration as an alternative in the (I)IoT/I4.0 environments. The further development, especially of 6G, will demonstrate to what extent the methods will manage to find their way into standardization and become correspondingly applicable in everyday practice.

5. Conclusion and future work

The ongoing globalization and interconnection of all types of sensors and devices to form an (industrial) Internet of Things with Industry 4.0, Industrial Automation and Control Systems and Cyber-Physical Production Systems implies an increasing demand for secure and trustworthy communication. But, these heterogeneous landscape

with its vast amount of entities -machines and humans- renders it a crucial task to identify a “one-size fits all” solution for security applications. Therefore, the respective requirements are simply too specific.

However, the methods of Physical Layer Security open up a variety of solutions, each with specific advantages tailored for the respective application: Physically Unclonable Functions as hardware-based approaches provide semiconductor-level device authentication, biometrical PhySec represent modern approaches for identifying and authenticating human entities and the Secret Key Generation, based on the propagation characteristics of electromagnetic waves, enables a symmetric encrypted communication independent of the radio standard. Nevertheless, the authors of this work are aware that the PhySec algorithms are not the answer to all problems, but they do provide a more than worthwhile and considerable complement to existing security mechanisms. They are inherently available, resource-saving and yet efficient and secure.

Here, the work provided insight into three different field of application for PhySec methods and discussed their benefits and drawbacks. The corresponding implementations, experimental results and evaluations are available in the referenced papers of the authors and demonstrate the operability and suitability of the described techniques.

Furthermore, the development of the Sixth Generation Wireless Systems with its promised key enabling technologies offers a substantial opportunity to bring PhySec out of its niche existence and to integrate them into the upcoming security standards.

Acknowledgements

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16KISK003K, Open6GHub). The authors alone are responsible for the content of the paper.

References

Ahr, P., Lipps, C. and Schotten, H.D., "The PUF Commitment: Evaluating the Stability of SRAM-Cells", *European Conference on Cyber Warfare and Security,* Chester, United Kingdom, 2021.

Ahr, P., Noushinfar, M. and Lipps, C., 2021. "RAM-based PUFs: Comparing Static- and Dynamic Random Access Memory", *Workshop on Next Generation Networks and Applications*, Kaiserslautern, Germany, 2021.

Ambekar, A. & Schotten, H.D., "Enhancing Channel Reciprocity for Effective Key Management in Wireless Ad-Hoc Networks", *IEEE 79th Vehicular Technology Conference (VTC Spring).* Seoul, South Korea, DOI: 10.1109/VTCSpring.2012.7022913, 2014.

Bidgoly, A.J., Bisgoly, H.J. and Arezoumand, Z., "A survey on methods and challenges in EEG based authentication", *Computers & Security,* Band 93, DOI: 10.1016/j.cose.2020.101788, 2020.

Bonneau, J., Herley, C., van Oorschot, P. and Stajano, F., "The Quest to Replace Passwords: A Famework for Comparative Evaluation of Web Authentication Schemes", *IEEE Symposium on Security and Privacy*, DOI: 10.1109/SP.2012.44, 2012.

Diffie, W. and Hellman, M., "New directions in cryptography", *IEEE Transactions on Information Theory*, 22(6), 1976.

Djordjevic, I. B., "Physical-Layer Security and Quantum Key Distribution*”.* 1st ed., Tucson, AZ, USA, Springer, ISBN: 978-3-030-27565-5, 2019.

Gao, M., Lai, K. and Qu, G., "A Highly Flexible Ring-Oscillator PUF", *Proceedings of the 51st Annual Automation Conference (DAC),* DOI: 10.1145/2593069.2593072, 2014.

Gassend, B., Clarke, D., can Dijk, M. and Devadas, S., "Silicon Physical random Functions", *Proceedings of the 9th ACM Conference on Computer and Communication Security*, pp. 148 -- 160, DOI:10.1145/586110.586132, 2002.

German Research Center for Artificial Intelligence, "Ten Years of Industrie 4.0 - Germany Driving Industrial AI as the means to Future Value Creation", [online] https://www.dfki.de/en/web/news/ten-years-of-industrie-4-0-interview-wolfgang-wahlster-cea-dfki, News 2021.

Halak, B., "Physically Unclonable Functions - From Basic Designn Principle to Advanced Haradware Security Apllications", 1st Edition Hrsg. Southampton: Springer, ISBN: 978-3-319-76804-5, 2018.

Hamamreh, J.M., Furqan, H.M. and Arslan, H., "Classifications and Applications of Physical Layer Security for Confidentiality: A Comprehensive Survey", *IEEE Couumnications Surveys & Tutorial,* DOI: 10.1109/COMST.2018.2878035, *2018.*

Hoffman, F., "Industrial Internet of Things Vulnerabilities and Threats: What Stakeholders Need to Consider", *Issues in Information Systems,* 20(1), pp. 119--133, 2019

Höller, A. and Toegl, R., "Trusted Platform Modules in Cyber-Physical Systems: On the Interference Between Security and Dependability", *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, DOI: 10.1109/EuroSPW.2018.00026, 2018.

International Telecommunication Union (ITU), "ITU-T X.200 - Data Networks and Open System Communications - Open Systems Interconnection, Model and Notation"*,* International Telecommunication Union (ITU), 1994.

___, "X.800: Security Architecture for Open System Interconnection for CCITT Applications*", 1991.*

___, "IMT Traffic estimates for the years 2020 to 2030"*, M Series Mobile, radiodetermination, amateur and related satelliteservices Report ITU-R M.2370-0*, 1994b.

Jain, A., Ross, A. and Prabhakar, S., "An introduction to biometric recognition" *IEEE Transactions on Circuits and Systems for Video Technology,* 14(1), pp. 4 -- 20, DOI: 10.1109/TCSVT.2003.818349, 2004.

Khan, S., Shah, A.P., Chouhan, S.S., Gupta, N., Pandes, J.G. and Vishvakarma, S.K., "A Symmetric D Flip-Flop based PUF with improved Uniqueness", *Micoelectronic Reliability*, DOI: 10.1016/j.microel.2020.113595, 2020.

Kramp, T., van Kranenburg, R. and Lange, S., "Introduction to the Internet of Things", In: A. Bassi, et al. Hrsg. *Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model.* Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1--10., 2013.

Kumar, S.S., Guajardo, J., Maes, R. Schrijen, G.-J. and Tuyls, P., "The Butterfly PUF Protecting IP on every FGPA". Anaheim, CA, USA, *IEEE International Workshop on Hardware-Oriented Security and Trust*, DOI:10.1109/HST.2008.4559053, 2008.

Lipps, C., Baradie, S., Noushinfar, M., Herbst, J., Weinand, A. and Schotten, H.D., "Towards the Sixth Generation (6G) Wireless Systems: Thoughts on Physical Layer Security", *Mobile Communication - Technologies and Applications - 25. VDE/ITG Fachtagung Mobilkommunikation*, 2021.

Lipps, C., Bergkemper, L. and Schotten, H.D., "Distinguishing Hearts: How Machine Learning identifies People based on their Heartbeat"*, Sixth International Conference on Advances in Biomedical Engineering (ICABME),* Islamic University of Lebanon - Faculty of Engineering - Werdanyeh Campus, Lebanon, DOI:10.1109/ICABME53305.2021.9604855, 2021b.

Lipps, C., Herbst, J. and Schotten, H.D., "How to Dance Your Passwords: A Biometric MFA-Scheme for Identification and Authentication of Individuals in IIoT Environments", *16th International Conference on Cyber Warfare and Security (ICCWS)*, Cookeville, TN, USA, 2021c.

Lipps, C., Mallikarjun, S.B., Strufe, M., Heinz, C., Grimm, C., and Schotten, H.D., "Keep Private Networks Private: Secure Channel-PUFs, and Physical Layer Security by Linear Regression Enhanced Channel Profiles"*, International Conference on Data Intelligence and Security (ICDIS),* DOI:10.1109/ICDIS50059.2020.00019, *2020.*

Lipps, C., Weinand, A., Krummacker, D., Fischer, C., and Schotten, H.D., "Proof of Concept for IoT Device Authentication Based on SRAM PUFs Using ATMEGA 2560-MCU*" 1*st International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 2018.

Machida, T., Yamamoto, D., Iwamoto, M. and Sakiyama, K., "A new Mode of Operation for Arbiter PUF to Improce Uniqueness on FPGA"*, Federated Conference on Computer Science and Information Systems*, Warsaw, Poland, DOI:10.15439/2014F140, 2014.

McLuskie, D. and Belleken, X., "X509 Certificate Error Testing", *Proceedings of the 13th International Conference on Aailability, Reliability and Security,* DOI:10.1145/3230833.3232820, 2018.

Mukherjee, A., Fakoorian, A.A.A., Huang, J. and Swindlehurst, A.L., "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", *IEEE Communications Surveys & Tutorials*, 16(3), pp. 1550 -- 1573, DOI: 10.1109/SURV.2014.012314.00178, 2014.

Pal, A., Gautam, A.K. and Singh, Y.N., "Evaluation of Bioelectric Signals for Human Recognition", *Procedia Computer Science,* Band 48, pp. 746 --752, DOI:10.1016/j.procs.2015.04.211, 2015.

Pan, C., Ren, H., Wang, K., Kolb, J.F., Elkashlan, M., Chen, M., Di Renzo, M., Hao, Y., Wang, J., Swindlehurst, A.L., You, X. and Hanzo, L., "Reconfigurable Intelligent Surfaces for 6G Systems: Principles, Applications, and Research Directions" *IEEE Communications Magazine*, 59(6), DOI: 10.1109/MCOM.001.2001076, 2021.

Posey, B., Rosencrance, L. and Shea, S., "Industrial Internet of Things (IIoT)"*,* [Online] Available at: https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT [Zugriff am 23 01 2022].

Sarkar, A., Abbott, A. L. and Doerzaph, Z., "Biometric authentication using photoplethysmography signals" *IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS),* Niagrara Falls, NY, USA, DOI: 10.1109/BTAS.2016.7791193, 2016.

Schäfer, G. and Rossberg, M., "Security in Fixed and Wireless Networks"*,* 2nd Edition, Red Hat., ISBN: 978-1119040743, 2016.

Schneier, B., "Carry On: Sound Advice from Schneier on Security"*,* 1st Edition, Wiley, ISBN: 978-1118790816, 2014.

___, "Applied Cryptography: Protocols, Algorithms and Source Code in C"*,* 25th Anniversary Edition, John Wiley & Sons Inc, ISBN: 978-1119096726, 2015.

Uysal, M., Capsoni, C., Ghassemlooy, Z., Boucoucalas, and Udvary, E., "*Optical Wireless Communications: An Emerging Technology (Signals and Communication Technology)",* 1st ed., ISBN: 978-3319302003, 2016.

Valerio, P., "What is NR-REDCAP on 5G, and why is it important for IIoT?," [Online] Available at: https://iot.eetimes.com/what-is-nr-redcap-on-5g-and-why-is-it-important-for-iiot/ [Zugriff am 23 1 2022], 2021.

Weinand, A., Karrenbauer, M. and Schotten, H.D., "Security Solutions for Local Wireless Networks in Control Applications based on Physical Layer Security" *3rd IFAC Conference on Embedded Systems, Computational Intelligence and Telematics in Control CESCIT*, pp. 32 -- 39, 2018.

Zenger, C.T., Zimmer, J., Pietersz, M., Posielek, J.-F. and Paar, C., "Exploiting the Physical Environment for Securing the Internet of Things", *Proceedings of the 2015 New Security Paradigms Workshop*, pp. 44--58, DOI: 10.1145/284113.2841117, 2015.

Zhang, J., Woods, R., Duong, T.Q., Marshall, A., Ding, X., Huang, Y., Xu, Q., "Experimental Study on Key Generation for Physical Layer Security in Wireless Communications", *IEEE Access* , Issue 4, pp. 4464 -- 4477, DOI: 10.1109/ACCESS.2016.2604618, 2016

Zou, Y., Zhu, J., Wang, X. and Hanzo, L., "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", *Proceedings of the IEEE*, 104(9), pp. 1727 -- 1765, DOI: 10.1109/JPROC.2016.2558521, 2016.