IEEE Open Journal of the
Solid-State Circuits Society

Received 14 June 2023; revised 23 August 2023 and 15 October 2023; accepted 16 October 2023. Date of publication 25 October 2023; date of current version 21 December 2023.

Digital Object Identifier 10.1109/OJSSCS.2023.3327326

Physical-Layer Security for Energy-Constrained Integrated Systems: Challenges and Design Perspectives

ALPEREN YASAR (Graduate Student Member, IEEE), AND RABIA TUGCE YAZICIGIL (Senior Member, IEEE)

Electrical and Computer Engineering Department, Boston University, Boston, MA 02215, USA

CORRESPONDING AUTHOR: A. YASAR (e-mail: ayasar@bu.edu)

This work was supported in part by Analog Devices, Inc.

ABSTRACT The expanding scale and growing connectivity of Internet of Things (IoT) devices coincide with the emergence of next-generation communication technologies. These devices serve various purposes, including communication, manufacturing, biomedical, and environmental monitoring. However, the increasing number of connected devices raises concerns about data security and integrity. Previous research has highlighted the severe consequences of security inadequacies, shown by incidents involving biomedical devices [1], [2], [3] as an example. Nevertheless, due to resource constraints like power, hardware complexity, and latency, digital cryptography is not universally suitable for these devices [4], [5], [6]. An alternative is embedding physical-layer security (PLS) measures. Diverse countermeasures within the physical layer have been explored, including wireless network security [4], [5], [6], [7], [8], [9] and resistance against side-channel attacks (SCAs) [10], [11], [12]. This study reviews threat modeling for PLS, underlining its significance and emphasizing its similarities and distinctions from conventional security threat models. We then investigate two commonly employed adversarial techniques: 1) eavesdropping and 2) SCAs. This exploration involves an investigation of distinct security approaches, alongside an evaluation of their associated threat models and tradeoffs. While PLS techniques address the aforementioned resource and latency constraints, they do not universally apply to all devices. Ultralow-power or ultralow-latency devices might necessitate balancing security with performance. However, the absence of a standardized framework in the realm of PLS poses challenges for designers in comparing and selecting the most fitting approach. To conclude, this work provides suggestions for addressing current gaps and enhancing the field of PLS.

INDEX TERMS Eavesdropping, intelligent sensing systems, Internet of Things (IoT), physical-layer security (PLS), side-channel attacks (SCAs).

I. INTRODUCTION

As COMMUNICATION technology evolves into next-generation networks, massive Internet of Thing (IoT) networks involving millions to billions of devices is an emerging use case [1], [4], [5], [13]. These devices in such networks exchange information and take measurements for various applications, including but not limited to home and transportation automation, industrial, biomedical, mining, or environmental monitoring [3], [14], [15]. Some IoT devices such as sensing modules are often designed to be ultralow power, that can rely on a small battery, or even energy harvesting in some cases to sustain autonomous operation for a longer duration while reducing costs [16], [17]. Each device transmitting potentially confidential data through such networks creates a security concern. These security concerns are exacerbated by the latency and energy requirements and other resource constraints of IoT networks.

Currently, devices in IoT networks are not co-designed with their security solutions. Security is traditionally added as an afterthought through well-established digital cryptography methods. These encryption schemes leverage a computationally hard-to-reverse function [18], [19].

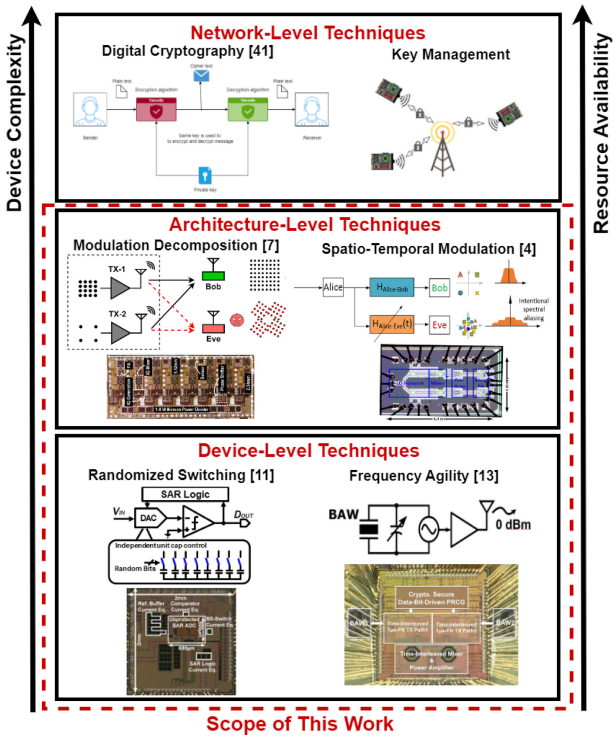


FIGURE 1. System-level security approach leveraging cross-layer optimization and different resource utilization levels.

However, those functions typically require significant computational power to perform their calculations over multiple iterations, which adds to the memory requirement and energy consumption. Moreover, not all encryption algorithms are suitable for ultralow-latency and low-power wireless communications [4] since executing multiple rounds of computation increases the latency, starting to become the bottleneck of the data transfer.

Physical-layer security (PLS) focuses on leveraging the unique physical properties of devices or their communication channels to secure the information exchange [6], [8], [20]. Security solutions can be implemented in different layers, including network, architecture, and device level techniques as shown in Fig. 1. For the scope of this work, architecture and device-level techniques will be investigated. Recently, there have been several PLS research works securing against threat models such as the information leak in the radio-frequency (RF) communication [4], [7], [9]. However, new threat models are introduced with PLS, where attackers same wise can leverage the physical properties to crack the devices or communication, such as side-channel attacks (SCAs) [10], [11], [12], [21], or spoofing. Here, we review the literature around PLS, analyzing the tradeoffs with each solution, and investigating them according to their threat models, device compatibility, and security capabilities to understand improvements awaiting for the PLS in the future.

This article is organized as follows. In Section II, we provide an introduction to PLS threat models, their importance, and their difference from conventional security models. Eavesdropping is investigated in Section III, going over different security techniques and their comparison. SCAs are investigated in Section IV in the same manner. In Section V, we provide our insights on possible future research directions for PLS for energy-constrained integrated systems.

II. PHYSICAL-LAYER SECURITY THREAT MODELS

Threat modeling is an essential part of any security work where the attack model, attacker capabilities, and scenario of the attack are defined. Even though some assumptions can be made depending on the application of the proposed security model, the threat model should be as realistic as possible to make the work applicable in real-world cases. However, there should naturally be some limitations for the attacker, as an attacker with unlimited computational power and unlimited time would be able to crack any security model. In conventional security methods using cryptography, this limitation is the time it would take for a modern computer to break the code, and its power consumption to do that. A scheme can be called practically secure if the power consumption and the time requirement are infeasibly high. In the case of elliptic-curve cryptography (ECC), the amount of power required to break the cipher is equivalent to the power needed to boil all the water on Earth, making the scheme practically secure [22].

As PLS gives the capability to utilize the physical properties of devices, materials, waves, etc., to the defender, these capabilities should be given to the attacker as well. This will create a new attacker model, that is aware of the PLS model and has new tools such as laboratory equipment to break the security. For instance, the attacker will usually have access to the EM probe station (∼$50 000) in an electromagnetic (EM) SCA model, or to an RF spectrum analyzer (∼$100 000) for wireless communication attacks. This new attacker model creates a challenge to previously defined threat models in the case of cryptography. Additional physical observations made by the attacker can drastically reduce the power and time required for the attack, lowering them within the feasible region and breaking the security scheme [21], [23]. This introduces new metrics in a threat model other than power and time, such as the financial budget of the attacker, or the number of adversary devices as will be detailed in Section III. These metrics are necessary to determine whether a PLS solution is applicable to the device we are seeking to secure.

With the introduction of new metrics, a PLS threat model must be well defined with realistic assumptions. The threat model should clearly define its attacker model, such as eavesdropping or SCA, and its range of target devices to be secured. Considering ultralow-power or ultralow-latency devices, some PLS solutions would require high energy consumption that could be the bottleneck in the system. The threat model should clearly include the capabilities of the attacker, the equipment they have, their knowledge about the PLS scheme, and sometimes their financial budget.

These metrics can define the feasible limits for the proposed security scheme. The PLS solution will naturally have a tradeoff between its security level and resource consumption that can be tuned according to the adversarial environment and performance requirements of the system. For example, in the case of a sensor within a network that does not transmit highly confidential data on its own, security using a very complicated PLS technique that targets a high-budget, highly capable threat model would be an over-engineered solution. Instead, a low-cost solution can be utilized that would require infeasible resources from the attacker concerning the importance of the information obtained from it. This requires the threat model to specify which group of secured devices are targeted, considering performance metrics, such as their power consumption and latency requirements.

In this work, threat models will be categorized under two groups: 1) passive and 2) active attacks. Passive attacks consider an adversary that does not alter the data, or cause the victim device to dysfunction. The sole reason behind a passive attack is to retrieve confidential information from the system without being detected by anyone. An eavesdropper may perform a passive attack by listening to the channel without getting into any interaction with other nonadversary nodes within the network. Whereas an active attacker would interact with other victim nodes in the network to make them leak information, dysfunction, or accept fault-injected data from the adversary impersonating a valid node. Active attacks can also include SCAs where the adversary can give specific inputs to a system to measure its response, and, in return, try to obtain some information, e.g., secret key, or make it dysfunctional such as skipping security protocols [21], [23].

This work will investigate different PLS techniques from the literature, comparing their threat models and countermeasures to highlight their security versus performance tradeoffs.

III. EAVESDROPPING

An eavesdropping attack can be defined as an adversary *sniffing* over the communication channel to capture confidential information. An adversary can decide to stay passive or use the obtained information for an active attack, such as jamming, injecting false data, or spoofing. In both cases, the adversary should remain incognito, and the attack is considered to be unsuccessful if that's not the case. For that reason, throughout this section, it is assumed that eavesdroppers position themselves at side lobes of the beam pattern, as they can be detected if they reside in the main lobe [4]. For the ease of threat model description, names *Alice* for the message source, *Bob* for the intended receiver and *Eve* for the adversary will be used throughout this article. Cryptography is a well-developed and powerful way to obfuscate the data systematically before transmission to secure it against eavesdroppers. The message can be encrypted using a secret key, that is only recoverable by the intended receiver, Bob, who knows the corresponding key to decrypt. This key can either be the same or a different one depending on whether the system is symmetric or asymmetric. However, cryptographic engines often require multiple rounds of calculation-intensive operations, making them power-hungry. For resource-constrained systems using digital cryptographic engines may become the power consumption bottleneck. Conventional cryptography also makes it challenging to meet the ultralow-latency requirements of 5G and 6G [4]. From the security perspective, significant research efforts in digital hardware and algorithms [24] have been cast. However, the PLS of wireless systems under a tight power and latency budget remains a critical need [13], [25], [26]. PLS must be addressed at the forefront of the design process and intrinsically leverage the physical properties of the device, signal, or wireless channel to obfuscate the confidential data against adversaries.

A wire-tap channel introduced by Wyner [27] can be defined as a communication channel where the eavesdropper, Eve, can listen but has a worse channel condition than the main channel. This scheme provides secrecy by creating a signal-to-noise ratio (SNR) difference between the intended receiver, Bob, and the adversary, Eve. Following the wire-tap channel model, phased-array antenna systems performing beamforming to direct a higher amount of power to the intended receiver and less to the side lobes have been demonstrated to achieve secrecy against a side-lobe Eve by degrading the SNR of the Eve. However, a highly sensitive receiver can still recover the original message under low SNR channel conditions. This requires Alice to perform additional processes on the transmitter end to scramble the signal even further, aggravating the channel condition for Eve while keeping it the same for Bob.

A. SPATIAL DOMAIN SOLUTIONS

In a radio system utilizing a digital modulation such as commonly used FSK, APSK, QAM, etc., the receiver would map the received signals to a constellation map, each point (symbol) representing a binary number based on the modulation. The error rate in recovering those symbols can be quantified with error vector magnitude (EVM), which is a measure of how close the received symbol is to the ideal symbol location. For error-free communication, parties would try to minimize EVM at the receiver side. However, similar to wire-tap channels, a PLS scheme can target to achieve a higher EVM for Eve, reducing their symbol recovery rate by scrambling their received constellation. Emerging from the original idea of using phased-array antennas for secrecy, spatial domain solutions can scramble the constellation by utilizing the phase difference between the signals received by Bob and Eve.

One of the earlier works in this area by Babakhani [20] targets achieving secrecy by using a near-field antenna modulation technique. This work modulates the signal after the antenna, as opposed to the more conventional way of doing it before, introducing different scrambling at each receiver angle. Using an antenna array of two antennas, $N_a = 2$, one antenna is chosen to be the main radiator,

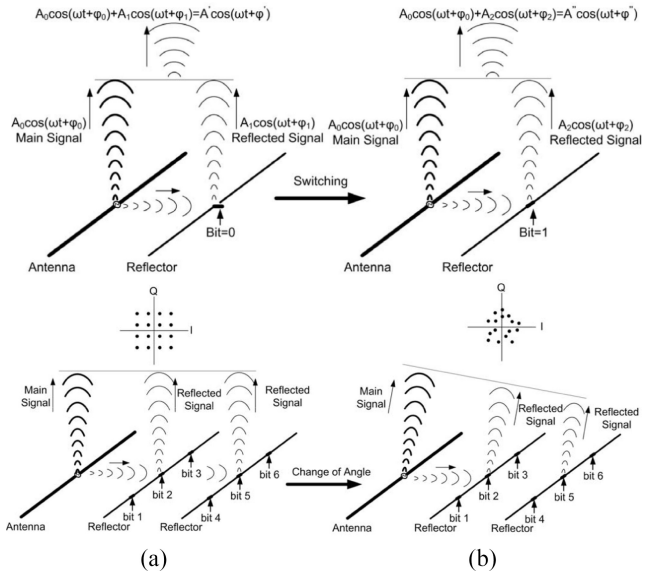


FIGURE 2. Reflector antenna switching-based constellation scrambling and received constellations by the (a) intended receiver and (b) eavesdropper [20].

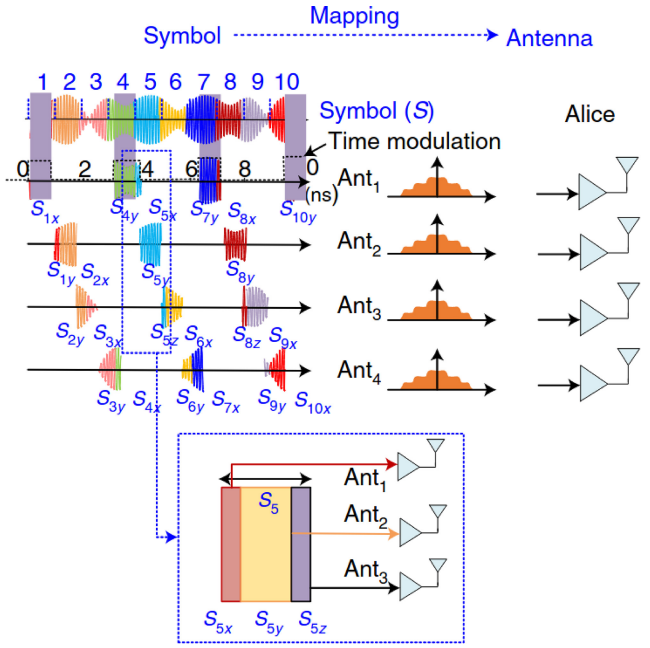


FIGURE 3. Symbol to antenna mapping and time modulation [4].

and the other is set as the reflector, as shown in Fig. 2. The reflected signal will interfere with the original signal from the main radiator, forming different signal patterns for each angle. If a switch is positioned on the reflector antenna, the length of the antenna can be changed digitally. By doing so, the phase and amplitude of the reflected signal would change since the reflection is determined by the boundary conditions of the reflector antenna. Higher order modulations can be achieved by increasing the number of reflector antennas and configurability of each antenna by adding more switches. This, in return, will also increase the number of possible ways the waves can interfere, scrambling the phase and amplitude further for the eavesdropper. It should be noted that this higher order modulation does not require any additional power consumption from the power amplifier (PA) or the phase shifter (PS) as the modulation happens in space through wave interference. Even though this scheme achieves constellation scrambling, transmitting the information at the desired angle by Alice is calculation intensive [7]. Furthermore, it does not involve any spatial aliasing, thus Eve can find classification boundaries on the constellation map to recover the original message [4].

To obtain a higher security level, spatial aliasing can be introduced which causes the spectrum at the side lobes to be aliased depending on Bob and Eve's spatial position, making it harder for the eavesdropper to recover the symbols. As proposed by Venkatesh et al. [4], [9], spatiotemporal modulation allows aliasing the symbols in space by routing each symbol to one or more antennas within the array, having a single element active at a given time as shown in Fig. 3. Due to the phase shift between each antenna, the symbols will align perfectly at the main lobe (Bob) but will alias each other in time over side lobes. This aliasing is dependent on the receiver angle and time, thus forming the *spatiotemporal modulation*. As the eavesdropper is forced to listen from a side lobe, each symbol will take a path with variant distances, arriving earlier or later than it should, and overlapping with the consecutive symbol.

Symbols are mapped dynamically to the antenna array such that each antenna will only transfer a portion of the symbol. Waveforms from the antenna array will realign in space for the main lobe, making it possible for Bob to recover the original message. However, for the side lobes spectral aliasing is observed, substantially degrading the recovery rate for the adversary. This spectral aliasing is caused by the time modulation happening with the dynamic symbol to antenna mapping. Each antenna element transmits a portion of the symbol that is modulated in time with frequency f_{mod}, which is lower than the signal bandwidth BW causing aliasing in the frequency domain. This effect is canceled out by the realignment of the waveforms in the main channel, but sustained in the side lobes, forming a wire-tap channel for Eve. Now, the Alice-to-Eve channel is not only worse because of its lower SNR level and modulation scrambling as in the previous case, but the spectral aliasing obfuscates the message itself against any constellation classification.

To assess the security strength of the proposed scheme Venkatesh et al. [4] also considered a distributed eavesdropping attack. Instead of listening through a single receiver, Eve can deploy multiple receivers across space, not residing in the main lobe. If synchronized, these devices can gather enough spatial and orthogonal information from the channel to perform a channel inversion attack. If Bob's position is known by Eve, and it is assumed to be known as Eve stays out of the main lobe, Eve can use the channel inversion to calculate what is received by Bob. For a system where Alice has a phased array of N_a many elements, and Eve has M_E

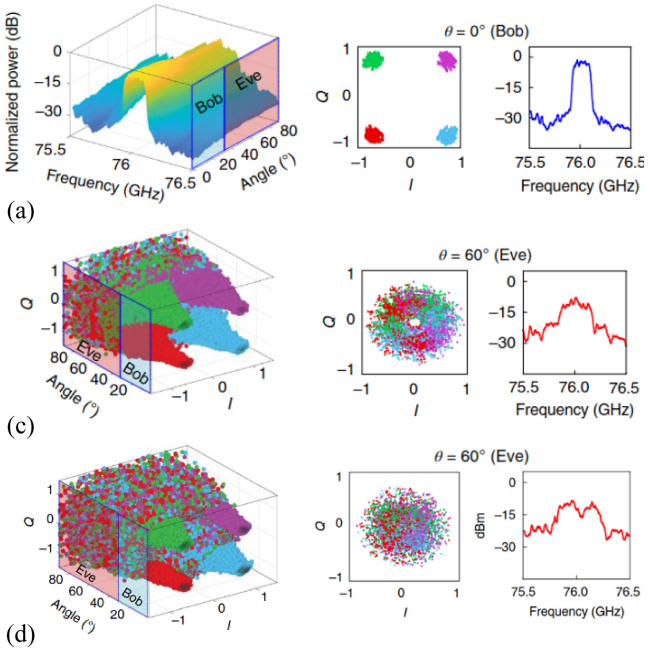


FIGURE 4. Received constellation and frequency spectrum for (a) conventional phased array antenna, (b) Spatiotemporal modulation sampled at fixed rate, (c) Spatiotemporal modulation dynamically sampled with sync function [4].

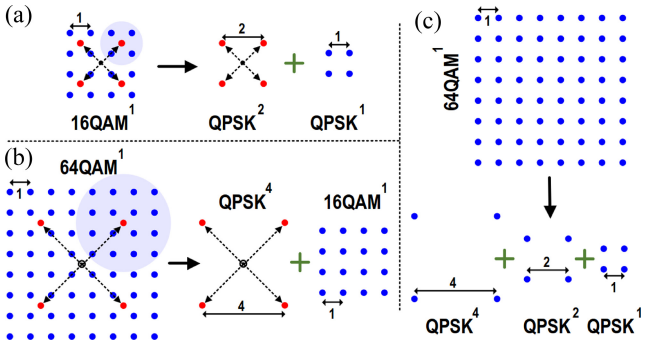


FIGURE 5. Constellation decomposition for (a) 16QAM into 2, (b) 64QAM into 2, (c) 64QAM into 3 subconstellations [7].

many distributed eavesdroppers, $M_E >= N_a$ shall be satisfied for Eve to obtain enough information to calculate H_{A-E}, channel matrix for the Alice-to-Eve channel. Practically, this requires at least N_a many eavesdropper devices to be in a precise wireless synchronization while placed away from each other at a considerable distance. In practice, precise synchronization for that many devices will be a challenge for Eve, making the attack practically infeasible. Although it seems impractical, the system is theoretically still vulnerable to a distributed eavesdropping attack. A channel inversion with such an attack is possible because a fixed modulation frequency, e.g., $f_{\text{mod}} = 0.25\text{BW}$, will only cause finite different ways of constellation scrambling. If the modulation frequency is set to an irrational fraction of the bandwidth, e.g., $f_{\text{mod}} = (1/\pi)\text{BW}$, the number of different scramblings will approach infinity, making the channel inversion process much more challenging. Similarly, a nonperiodically changing modulation frequency can be used such as a chirp signal. It is important to note that to retain the spectral aliasing, the maximum frequency of the chirp signal should be kept under the Nyquist rate, i.e., $\max|f_{\text{mod}}| < 2\text{BW}$. As shown in Fig. 4, the system achieves a constellation scrambling outside the main lobe, forming a secure zone within the main lobe even though the signal level in side lobes is still close to a conventional phased array antenna. Outside of this secure zone bit error rate (BER), which can be used as another quantification of PLS, approaches 50%, essentially meaning that *the best guess of the original bit is a random guess*.

Spatiotemporal modulation suffers challenges due to its at least per-symbol rate steering requirement, putting latency stress on the hardware. Furthermore, it only utilizes a single antenna at a time, significantly reducing the transmitted power and array gain [7]. Addressing these issues, an alternative spatial solution, constellation decomposition array (CDA) is proposed by Mannem et al. [7]. Instead of doing a symbol-to-antenna mapping, each antenna transmits a decomposed fraction of the original constellation. This arises from the fact that a higher order modulation can be decomposed to and recovered from lower order ones, as shown in Fig. 5. For instance, a 64QAM modulation can be decomposed to QPSK^4, QPSK^2, and QPSK^1, where n in QPSK^n shows the Euclidean distance between symbols. If each decomposed constellation is transmitted through a separate antenna or group of antennas, the original higher order constellation can be formed in the direction of Bob, while Eve will receive a scrambled constellation from a different angle.

While this scrambles the constellation for Eve, it is only dependent on the angle and an intelligent receiver can recover the original symbol as in the case of spatiotemporal modulation with a fixed modulation rate. To enable a large number of possible scrambled constellation patterns over time, techniques, such as antenna swapping or changing the decomposition can be used. Antenna swapping will change which decomposed modulation is mapped to which antenna over time, increasing the possible number of outcomes, as shown in Fig. 6. Additionally, how the higher order modulation is decomposed to lower ones can be changed over time to create an additional challenge for the eavesdropper. As in the case for 64QAM in Fig. 5, it can be decomposed to three QPSK modulations, or a QPSK^4 and a 16QAM^1. In both techniques, the constellation will align in the direction of Bob, ideally not affecting his correct recovery rate. Although it utilizes constellation scrambling without spectral aliasing and does not include distributed eavesdropper attack in its threat model, CDA is a more hardware-friendly solution with respect to spatiotemporal modulation. CDA does not require per symbol rate steering, which reduces the tight latency performance requirement on the hardware and utilizes all antennas simultaneously, hence decreasing the load on a single PA and utilizing the entire multiantenna array gain.

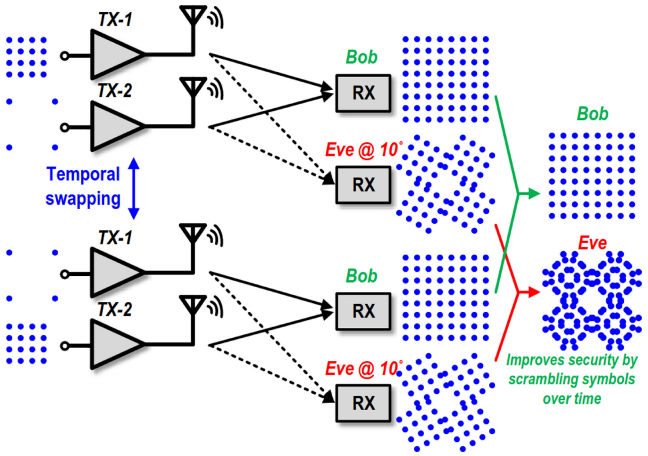


FIGURE 6. Constellation scrambling by temporal swapping [7].

B. NOISE INJECTION SOLUTIONS

Another subset of PLS solutions against eavesdropping attacks focuses on forming a wire-tap channel by introducing additional noise to the side lobes, degrading their SNR level more than what is naturally achievable with phased array antennas [5], [6], [8]. Although they are not specifically designed for scrambling the received constellation by Eve, this additional artificial noise (AN) will distort the signal significantly, which is much more than natural noise sources can. This, in return, will scramble the constellation, therefore reducing the SNR level and increasing the EVM on adversary devices, while ideally keeping the channel artificial-noise-free for Bob.

Injecting AN on side lobes without distorting the main lobe, where Bob receives information from, requires additional beamforming specifically for the AN. This beamforming should overlap with the side lobes as much as possible, as otherwise there would be noise-free eavesdropping locations, and not distort the main beam. However, this would require additional RF chains within the system that are usually the most power-consuming blocks in a millimeter wave communication circuit [6]. As proposed by Zhang et al. [8], each RF chain drives a subset of antennas from the phased array to transmit either noise or information. A power allocation ratio can be assigned to the system that will determine how much of the maximum power shall be used for transferring the information, and for transmitting the noise to side lobes. The secrecy capacity between the main channel and the wire-tap channel is enhanced as the power allocated to noise generation increases, degrading the symbol recovery rate by the adversary. However, the SNR level of Bob will also degrade as this would decrease the power utilization by the RF chain transmitting the information. Thus, for a given power capacity, a tradeoff between the secrecy level and the main-channel user SNR exists.

In order to see how this solution works and what are the possible attacks against it, let $y(\theta_t, \phi_t, t)$ be the signal received by Eve, where t is the time, and θ_t and ϕ_t are spatial angles at time t. Then, for a system with one RF chain for the information and K-1 chains for the noise

$$y(\theta_t, \phi_t, t) = \sqrt{P}h(\theta_t, \phi_t)\Bigg[\sqrt{\alpha}w_s x_s(t) + \sum_{i=1}^{K-1}\sqrt{\alpha_n^i}w_n^i x_n^i(t)\Bigg] + n(t) \quad (1)$$

where P is total transmit power, $h(\theta_t, \phi_t)$ is the channel condition matrix, α is power allocation ratio, and $\mathbf{w}_s$ and $\mathbf{w}_n$ are beamforming vectors for information and AN, respectively, x_s and x_n signals for the information and AN, and $n(t)$ is the additive white Gaussian noise modeling the channel noise. Thus, Eve receives the information signal mixed with the AN sources, not being able to extract the information $x_s(t)$ without knowing the contribution from the noise sources. The challenge for Eve is now to estimate the noise beamforming vector w_n^i to calculate the second half of the equation, leaving only the signal coming from the information source.

To provide security against more challenging attacks, a distributed eavesdropper attack can be once again defined as the threat model. Additionally, we can assume that Eve knows the location of Bob, and is capable of deriving $\mathbf{w}_s$ from that information. For ease of demonstration, we assume that the system consists of two RF chains, one for the information and the other for AN, simplifying (1) as

$$y(\theta_t, \phi_t, t) = \sqrt{P}h(\theta_t, \phi_t)\Big[\sqrt{\alpha}w_s x_s(t) + \sqrt{1-\alpha}w_n x_n(t)\Big] + n(t). \quad (2)$$

If Eve positions herself within a null space of the information signal $\mathbf{w}_s$, which we assumed that she already knows, the contribution of the information chain in the received signal will be zero, leaving the received signal equation as

$$y(\theta_t, \phi_t, t) = \sqrt{P}h(\theta_t, \phi_t)\Big[\sqrt{1-\alpha}w_n x_n(t)\Big] + n(t). \quad (3)$$

Eve can travel between N_a many null spaces, taking measurements to derive the noise beamforming vector $\mathbf{w}_n$. Since $\mathbf{w}_n$ is time invariant, it is enough to use a single eavesdropper for this task. Once $\mathbf{w}_n$ is calculated, Eve can now deploy a device to an information null position to receive and extract the noise signal, $x_n(t)$, being able to calculate the contribution purely from the noise source. Now, using the synchronized multiple devices attack, Eve can position a second device to a mixed signal point combining information with AN, and extract $x_s(t)$ as everything else is now known, hence achieving a successful eavesdropping attack.

If Alice utilizes multiple RF chains for noise, i.e., $K > 2$, additional noise sources will make the attack more complicated as Eve will now have to identify pure-noise locations for each noise chain. This task is more challenging since Eve only knows about $\mathbf{w}_s$ and its null spaces, but now has to

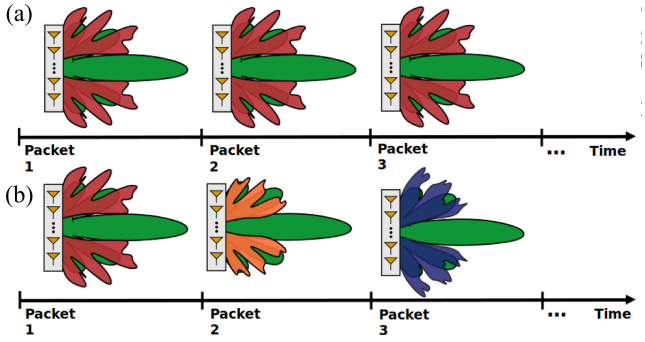


FIGURE 7. AN in side lobes. (a) AN with fixed noise beam vector. Fixed noise beam vector over time is shown in red while the main signal is shown in green. (b) ANH scheme with packet-rate hopping of noise beam vectors. Different noise beam vectors over time are shown in red, orange, and blue while the main signal is shown in green.

differentiate between noise sources as well and find points where only one of them is effective. This will get harder as K increases, making this system practically secure even though it is theoretically susceptible to eavesdropping with two eavesdroppers. An additional tradeoff emerges between the security level and power consumption as the number of RF chains in the system increases.

AN hopping (ANH), as proposed by Ju et al. [6], targets to solve this vulnerability against multiple eavesdroppers by introducing time dependency on the noise beam vector $\mathbf{w}_n$. Instead of having multiple RF chains for the noise signal and increasing the power consumption in return, this system involves strictly two RF chains, but randomizing $\mathbf{w}_n$ over time with per-packet rate as shown in Fig. 7, forming the *noise hopping*. Starting with a single eavesdropper, the signal received by Eve as a mixture of the noise and information can be modeled as

$$y(\theta_t, \phi_t, t) = \sqrt{P}h(\theta_t, \phi_t)\Big[\sqrt{\alpha}w_s x_s(t) + \sqrt{1-\alpha}w_n(t)x_n(t)\Big] + n(t) \quad (4)$$

that is very similar to the previous case where $K = 2$ in (2), but with a time-dependent noise beam vector $\mathbf{w}_n(t)$. Similarly, Eve requires multiple eavesdroppers to be working under precise synchronization. Once again knowing $\mathbf{w}_s$, Eve can determine null spaces to measure the noise and try to derive $\mathbf{w}_n$. However, as Eve starts to take multiple measurements from different null spaces to derive $\mathbf{w}_n$, it will change over time and make Eve's previous measurements useless. Now, Eve should move very fast to derive $\mathbf{w}_n$ before it hops to the next pattern. If $\mathbf{w}_n$ changes every 1 ms, Eve will have to move at least five times faster than an airplane [6], making it physically infeasible. Instead, Eve can decide to deploy N_a many synchronized eavesdroppers at different null spaces to make those measurements in parallel all at once. In that case, Eve is able to derive $\mathbf{w}_n$ at each hop and can recover $x_s(t)$ if an additional eavesdropper is placed in a mixed location as it was in the previous case. However this attack requires N_a+1 synchronized eavesdroppers instead of two as earlier, and it is practically very challenging to synchronize separately placed $N_a + 1$ many wireless devices with high precision. When compared with [8], this work reduces the number of RF chains to two, significantly reducing the power consumption and improving the security level by requiring $N_a + 1$ synchronized eavesdroppers for a successful attack instead of two.

C. EVOLVING INTO ACTIVE ATTACK: JAMMING

In case of a successful eavesdropping attack, the adversary can choose between staying passive and listening to the communication or taking an additional action to evolve the attack into an active one. An active attack can include changing the message, spoofing the message source, or blocking the communication. Jamming can be used as a tool to block communication by creating high-power interference within the channel, lowering the SNR, and increasing the error rate at the receiver. However, similar to the eavesdropping threat model, most of the time the attacker has to remain undetected. A wideband jamming attack covering the entire channel with interference is effective, but prone to be detected by other parties. Instead, the adversary could prefer performing a selective jamming, that only targets a smaller subchannel within the full bandwidth of the used protocol.

Bluetooth low energy (BLE) is a short-distance communication protocol used frequently for IoT devices due to its low-power design. Similar to WiFi and Bluetooth, BLE communicates over 2400 MHz, spanning an 83.5-MHz bandwidth up to 2483.5 MHz. It is divided into 40 channels and 37 of them are used for data exchange. Performing adaptive frequency hopping, BLE reduces the probability of collisions where a different set of devices, not necessarily using BLE, try to communicate over the same bandwidth. This frequency-hopping mechanism can also be used as a technique to mitigate the jamming attacks. Not desiring to be exposed, an advanced adversary can apply selective jamming that first detects the channel of the communication, and then jams the signal only within that bandwidth. With each hop, the adversary should repeat scanning the bandwidth, detecting the signal, and jamming that specific channel. Additionally, once the channel is discovered, the adversary can interfere with individual bits, leveraging the knowledge of the modulation scheme. As the time between each hop reduces, it makes it challenging for the attacker to perform this chain of attacks within a very limited amount of time.

A conventional transmitter design for BLE uses packet-level, 612-μs frequency hopping, whereas the attacker only needs around 1 μs to detect the channel and then can jam the rest [13]. The security can be achieved if the hopping period is reduced to 1 μs, which is equivalent to bit-level hopping, at which the attacker will have just enough time to detect the channel. By the time the channel is detected and the attacker starts to jam, the next bit will be sent from another jam-safe channel. On the other hand, the authorized receiver will generate the same pseudorandom number sequence of

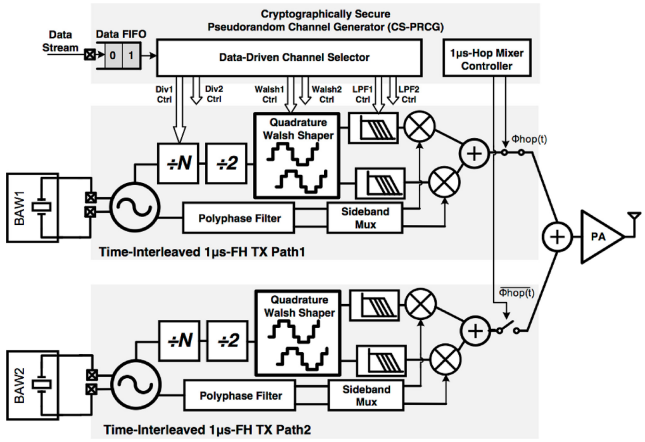


FIGURE 8. Hardware architecture of BAW resonator-based frequency hopping chain with time interleaving [13].

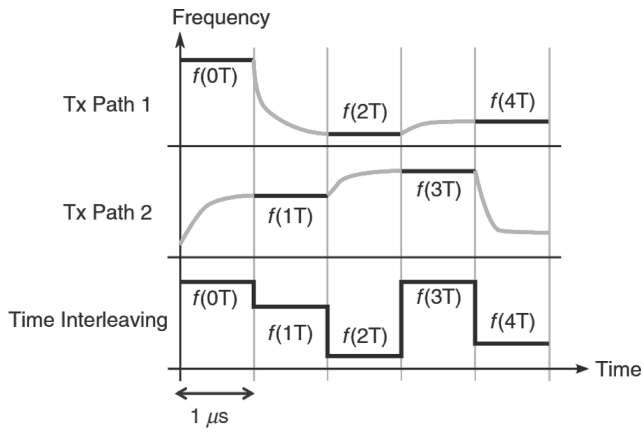


FIGURE 9. Time interleaving of two transmitter paths to avoid dead zones [13].

channel transitions to know the next channel and expect the new bit from that. However, significantly reducing the hopping period is not trivial as it puts stress on the hardware design. As proposed in [13], rather than implementing phase-locked-loops (PLLs) using crystal oscillators, bulk acoustic wave (BAW) resonators can be used for a fast-hopping scheme, leveraging their frequency agility property. However, BAW resonators are limited by their tuning bandwidth range, usually requiring integrating multiple of them to cover a larger bandwidth. Instead, covering a wider range with a single resonator is achieved by mixing the BAW resonator frequency with a programmable integer divider output. Additionally, dead zones caused by the settling time of the hardware chain are avoided by utilizing two hardware channels and time interleaving the output. Corresponding hardware design is shown in Fig. 8, and the effect of time interleaving is demonstrated in Fig. 9. While the active transmitter path holds its steady state, the other path settles to the next state before the switching occurs and, thus, eliminates any dead zone due to settling time. This allows the system to operate at the target 1 μs hopping period while halving the stress on each chain and successfully prevents the communication from being selectively jammed, or altered by the adversary.

IV. SIDE-CHANNEL ATTACKS

The second group of attacks to be investigated in this article, SCAs, deals with an adversary gathering additional side information about the system to break or bypass for gathering confidential data or reverse-engineering its functionality. Side-channel information can be of various types dependent on the application, such as time, EM waves, or data characteristics. Some of the commonly used threat models are shown in Fig. 10. SCA applies to many different concepts and, thus, has different solutions belonging to different layers of security, including algorithm [28], coding [29], hardware architecture [30], and PLS [13], [31].

SCA can be explained with a simple example of a Caesar cipher, where each character in the alphabet is mapped to another character by a linear rotation of a fixed secret number K. The system becomes vulnerable if side-channel information is known such as the language being used. An easy way to break the cipher other than brute-forcing all possible K values is to count the most frequent character in a sufficiently long text and map it to the most frequently used letter in that specific language. Once a mapping is known, the secret value K can be calculated to break the system, which concludes the attack. Although it is a simple case of breaking one of the earliest ciphers, even modern encryption schemes can be vulnerable to such attacks. As most of the security schemes depend on the infeasibility of time and resources required to break the system, this additional information can be used to lower the effort needed to a feasible range. It is previously shown that the secret key K can be retrieved from a cryptographic core using EM or power analysis SCA if precautions against such an attack are not taken [21], [23]. The system can be secured against such an eavesdropper by using algorithm-level techniques such as equalizing the number of 0's and 1's at the output to have an equal probability for each bit or architecture-level techniques such as implementing the algorithm in a way that it is not traceable through the power lines [21], [32]. However, the SCA requires the whole chain to be secure, as the eavesdropper can shift their focus on the weakest link to break the chain. This section will focus on analog-to-digital converters (ADCs), how they can leak information as a result of EM or power SCA, and how to secure them against these SCAs using architecture- and device-level techniques.

ADC is an essential component in any communication or sensing system that requires digital evaluation or post-processing. In a system where the analog and/or digital signal conveys confidential information, this domain transition can be the weakest point in terms of security [10], [11], [12]. Successive approximation register (SAR) ADC is one of the frequently used ADC types that performs a binary search over the range to find the closest possible point to the input analog signal. Utilizing a chain of parallel capacitors with switches as a digital-to-analog converter (DAC), SAR

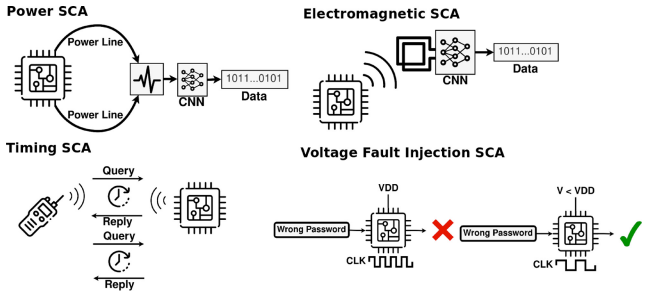


FIGURE 10. Commonly used SCA techniques.

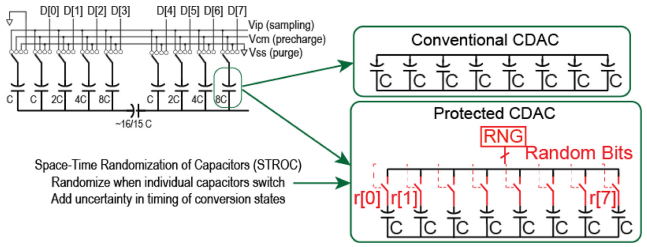
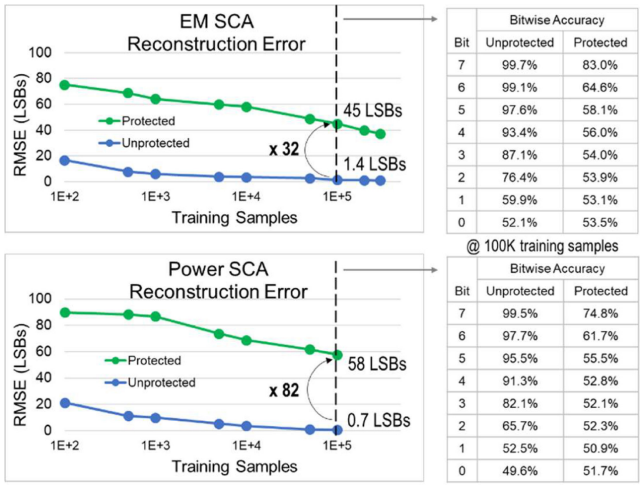


FIGURE 11. DAC capacitor array with space-time randomization of capacitors [11].



	Bitwise Accuracy	
Bit	Unprotected	Protected
7	99.7%	83.0%
6	99.1%	64.6%
5	97.6%	58.1%
4	93.4%	56.0%
3	87.1%	54.0%
2	76.4%	53.9%
1	59.9%	53.1%
0	52.1%	53.5%

@ 100K training samples

	Bitwise Accuracy	
Bit	Unprotected	Protected
7	99.5%	74.8%
6	97.7%	61.7%
5	95.5%	55.5%
4	91.3%	52.8%
3	82.1%	52.1%
2	65.7%	52.3%
1	52.5%	50.9%
0	49.6%	51.7%

FIGURE 12. Resilience of randomized switching SAR ADC against EM and power SCA [11].

ADC can search the best possible binary sequence (switch positions) that generates the closest possible voltage to the input through the DAC. However, the systematical way of sequencing the guesses can leak information through the power channel, each guesses requiring a slightly different power consumption and EM radiation within the DAC. An adversary having necessary laboratory equipment can capture this side-channel information and feed it into a statistical model such as neural networks to identify the results of the ADC without tampering with the chip. To make the information less traceable, an additional factor of randomization can be embedded into the system as a PLS solution.

Randomized switching SAR ADC, as proposed by Ashok et al. [11], replaces the most significant bit (MSB) single capacitors with parallel smaller capacitances that form the same net capacitance, as shown in Fig. 11. Each smaller capacitance has its switch and is controlled through a random number generator (RNG). Due to the random switching, the time required for each bit to flip to its correct value will be variable, making it challenging for the adversary to determine when each bit is decided during the conversion. Once a random switch sets the capacitor to its correct value, it will be retained as in the conventional SAR ADC, equalizing the total charge transfer while resulting in different current profiles. Furthermore, in a differential SAR model with two DAC modules with their own RNGs, randomization over space can be achieved. This model achieves a reconstruction error 32 times higher than the unprotected SAR ADC against EM SCA, and 82 times higher against power SCA, as shown in Fig. 12, with a 15.5% increase in power as the overhead of the security scheme.

Random-mapping SAR ADC (RaM-SAR), as proposed by Chen et al., tackles the same problem by targeting better energy efficiency compared to prior work [12]. Based on a least-significant-bit (LSB)-first SAR ADC [33], this work randomizes the search pattern by changing the first guess at each conversion process. The LSB-first SAR has a different but deterministic switching sequence based on the initial guess, which is equivalent to the result of the previous conversion cycle. By randomizing the first guess at each conversion, RaM-SAR randomizes the conversion sequence, weakening the correlation between side-channel information and the digital output. Additionally, two half-sized comparators are used to provide two thresholds, reducing the number of cycles in the worst case from 25 (LSB-first SAR) to 15.

The conversion consists of four phases: 1) the random start phase (P1); 2) the overshooting phase (P2); 3) the ternary search phase (P3); and 4) the binary search phase (P4). In the first phase, a random guess is made for the voltage. If the guess is higher than both thresholds, the search direction (DIR) is set as 0 to lower both thresholds. Otherwise, DIR is set as 1 to increase them. In phase 2, bits are flipped according to the direction until an overshoot happens, i.e., one of the comparator outputs flips, finalizing the conversion process for MSBs. A ternary search begins in phase 3 which takes two clock cycles. In phase 4, conversion continues with a binary search toward LSB, combining the two DACs and finalizing the result. The conversion process is shown in Fig. 13. The next conversion cycle will start from an independent random point, randomizing the searching pattern and, thus, making EM/power tracing challenging. A comparison of RaM-SAR and RS-SAR in terms of their security and performance metrics is provided in Fig. 14. RaM-SAR provides a higher RMS error for the attacker which indicates a higher level of security against SCA. This additional security is achieved while maintaining a lower figure-of-merit (FoM) than RS-SAR, that is a lower energy consumption per conversion as targeted.

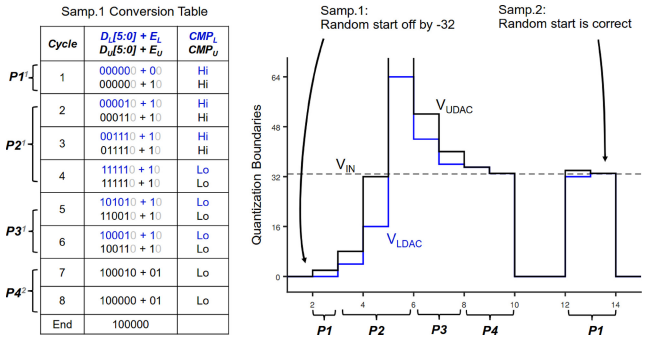


FIGURE 13. Random-mapping SAR ADC conversion table and operation diagram [12].

	Work	RaM-SAR	RS-SAR
Security	Protected Blocks	All	All
	Threat Model	EM + Power	EM + Power
	Attack Method	CNN	CNN
	V_{DD}-PSCA RMSE*	0.40	0.23
	EM SCA RMSE	0.45	0.18
Performance	Sample Rate [MS/s]	25	2
	Area [mm^2]	0.072	0.073
	ENOB** [b]	10.9	7.7
	FoM***	11.3	120.7

* Power SCA Root-mean-square error
** Effective number of bits
*** Figure-of-merit (fJ/conv.-step.)

FIGURE 14. Security and performance comparison of RaM-SAR and RS-SAR.

Besides the works reviewed, there are various other SCA methods with different aims, such as a fault injection, or a security bypass. The devices processing confidential information need to be secured against an SCA, as the conventional way of encrypting the information before transmitting is now not sufficient by itself. It is crucial to define a realistic but strong threat model against an SCA. The financial budget of the attacker can be considered as a factor since most SCA techniques require high-end technologies that can be costly. The confidentiality of the information and its importance will determine how strong the threat model should be, i.e., how high their budget will be. An increased budget means higher quality equipment, meaning higher precision attacks. For instance, a fault injection attack where the adversary targets a memory to flip the stored bits can be modeled by having the capability to do a bit-flip (high precision), byte-flip, or a word-flip (low precision), to a specific location (high precision) or a random location (low precision) [34]. As securing against a stronger threat model usually comes with a tradeoff in power and area, it may not be possible to secure every device against it. The threat model should answer "How much effort and budget would an adversary spend to obtain the information that is hidden, and how to secure the system against such an adversary?"

V. WHAT IS NEXT FOR PHYSICAL-LAYER SECURITY?

The need for PLS is increasing as the number of low-resource devices in our networks, such as sensors, is expected to vastly increase. The conventional way of securing those devices may become the bottleneck of the system, forcing the designers to make the mistake of totally neglecting security. Furthermore, it is reviewed that with a threat model capable of physical-layer attacks, such as SCA, even high-power systems utilizing strong, well-proven cryptographic cores can fail [21]. Consequences of neglecting security were shown previously in various areas such as the biomedical devices [1], [2], [3], [35] where an attack can cause leakage of patients' information or may involve an action that could be fatal.

There is a need to develop a holistic security approach to mitigate attacks against resource-constrained devices. This includes exploiting a system-level approach with cross-layer optimization extending from the networking layer through encryption and authentication down to the physical layer. Recent works address some physical-layer threat models and have demonstrated countermeasures in integrated hardware for energy-constrained wireless systems [4], [5], [6], [8], [9], [20], [36], [37], [38], [39], [40]. However, it is difficult to compare those works and determine which one to use based on an application since there is no single security metric to be used. Most of the PLS security metrics are dependent on experimental results and use different measures, such as EVM, SNR, symbol recovery rate, or number of eavesdroppers to break. Those measures also differ based on the system itself, test setup, and the threat model hardening the evaluation process. Instead, as is the case with cryptography, developing a systematical way of evaluating those works based on a mathematical framework should be addressed.

Once such a framework and evaluation metrics are defined, a library of PLS techniques, mapped with their target threat model, security level, and tradeoffs can be formed. Leveraging that secure design protocol, instead of embedding the security as an afterthought, the device can be co-designed with its security technique, sharing hardware and resources as needed. By determining the power and area budget of the device, and the threat model they want to secure against, designers will be able to choose the best option among many solutions.

VI. CONCLUSION

PLS is an alternative solution for securing resource-constrained devices where conventional cryptography methods are not feasible. It also provides additional security to the hardware implementation of well-known cryptographic methods, making them more robust against adversaries. This work reviewed two of many attack types, namely, eavesdropping and SCAs, investigating different solutions and comparing their security and performance metrics.

REFERENCES

[1] V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, "Threat modeling and risk analysis for miniaturized wireless biomedical devices," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13338–13352, Aug. 2022.

[2] A. Yasar, Q. Liu, M. Mao, D. Starobinski, and R. T. Yazicigil, "Live demonstration: Cyber attack against an ingestible medical device," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS)*, 2022, p. 250.

[3] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. e-Health Netw., Appl. Services*, 2011, pp. 150–156.

[4] S. Venkatesh, X. Lu, B. Tang, and K. Sengupta, "Secure space–time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks," *Nat. Electron.*, vol. 4, no. 11, pp. 827–836, 2021.

[5] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure Millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[6] Y. Ju, Y. Zhu, H.-M. Wang, Q. Pei, and H. Zheng, "Artificial noise hopping: A practical secure transmission technique with experimental analysis for millimeter wave systems," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5121–5132, Dec. 2020.

[7] N. S. Mannem, T.-Y. Huang, E. Erfani, S. Li, and H. Wang, "A mm-Wave transmitter MIMO with constellation decomposition array (CDA) for keyless physically secured high-throughput links," in *Proc. IEEE Radio Freq. Integr. Circuits Symp. (RFIC)*, 2021, pp. 199–202.

[8] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[9] S. Venkatesh, X. Lu, K. Sengupta, and B. Tang, "Spatio-temporal modulated Millimeter-wave antenna arrays for secure wireless links," in *Proc. IEEE Int. Symp. Antennas Propag. North Amer. Radio Sci. Meeting*, 2020, pp. 1565–1566.

[10] T. Jeong, A. P. Chandrakasan, and H.-S. Lee, "S2ADC: A 12-bit, 1.25MS/s secure SAR ADC with power side-channel attack resistance," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2020, pp. 1–4.

[11] M. Ashok, E. V. Levine, and A. P. Chandrakasan, "Randomized switching SAR (RS-SAR) ADC protections for power and electromagnetic side channel security," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2022, pp. 1–2.

[12] R. Chen, H. Wang, A. Chandrakasan, and H.-S. Lee, "RaM-SAR: A low energy and area overhead, 11.3fJ/conv.-step 12b 25MS/s secure random-mapping SAR ADC with power and EM side-channel attack resilience," in *Proc. IEEE Symp. VLSI Technol. Circuits*, 2022, pp. 94–95.

[13] R. T. Yazicigil et al., "Beyond crypto: Physical-layer security for Internet of Things devices," *IEEE Solid-State Circuits Mag.*, vol. 12, no. 4, pp. 66–78, Nov. 2020.

[14] D. Ying and D. A. Hall, "Current sensing front-ends: A review and design guidance," *IEEE Sensors J.*, vol. 21, no. 20, pp. 22329–22346, Oct. 2021.

[15] M. Zhang, A. Raghunathan, and N. K. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.

[16] Q. Liu et al., "Zero-crossing-based bio-engineered sensor," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2021, pp. 1–2.

[17] T. Sanislav, G. D. Mois, S. Zeadally, and S. C. Folea, "Energy harvesting techniques for Internet of Things (IoT)," *IEEE Access*, vol. 9, pp. 39530–39549, 2021.

[18] D. Gordon, *Discrete Logarithm Problem*. Boston, MA, USA: Springer, 2011, pp. 352–353. [Online]. Available: https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_445

[19] P. Paillier, "Trapdooring discrete logarithms on elliptic curves over rings," in *Proc. Adv. Cryptol. (ASIACRYPT)*, 2000, pp. 573–584.

[20] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "A near-field modulation technique using antenna reflector switching," in *IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers*, 2008, pp. 188–605.

[21] D. Das and S. Sen, "Electromagnetic and power side-channel analysis: Advanced attacks and low-overhead generic countermeasures through white-box approach," *Cryptography*, vol. 4, no. 4, p. 30, 2020.

[22] A. K. Lenstra, T. Kleinjung, and E. Thomé, "Universal security; from bits and mips to pools, lakes—And beyond," IACR, Bellevue, WA, USA, Rep. 2013/635, 2013, [Online]. Available: https://eprint.iacr.org/2013/635

[23] L. Zussa, J.-M. Dutertre, J. Clediere, and B. Robisson, "Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter," in *Proc. IEEE Int. Symp. Hardware-Oriented Security Trust (HOST)*, 2014, pp. 130–135.

[24] M. Alioto, "Trends in hardware security: From basics to ASICs," *IEEE Solid-State Circuits Mag.*, vol. 11, no. 3, pp. 56–74, Aug. 2019.

[25] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci.*, vol. 114, no. 1, pp. 19–26, 2017. [Online]. Available: https://www.pnas.org/content/114/1/19

[26] J. Ma et al., "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018. [Online]. Available: https://doi.org/10.1038/s41586-018-0609-x

[27] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[28] F. Zhang et al., "Design and evaluation of fluctuating power logic to mitigate power analysis at the cell level," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 6, pp. 1063–1076, Jun. 2021.

[29] S. Mesnager, C. Tang, and Y. Qi, "Complementary dual algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2390–2397, Apr. 2018.

[30] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-STELLAR: An EM/power SCA-resilient AES-256 with synthesis-friendly signature attenuation," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, Jan. 2022.

[31] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming channels: When electromagnetic side channels meet radio transceivers," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2018, pp. 163–177. [Online]. Available: https://doi.org/10.1145/3243734.3243802

[32] R. Kumar et al., "A SCA-resistant AES engine in 14nm CMOS with time/frequency-domain leakage suppression using non-linear digital LDO cascaded with arithmetic countermeasures," in *Proc. IEEE Symp. VLSI Circuits*, 2020, pp. 1–2.

[33] F. M. Yaul and A. P. Chandrakasan, "A 10 bit SAR ADC with data-dependent energy reduction using LSB-first successive approximation," *IEEE J. Solid-State Circuits*, vol. 49, no. 12, pp. 2825–2834, Dec. 2014.

[34] S. Lim, J. Han, and D.-G. Han, "Single-byte error-based practical differential fault attack on bit-sliced lightweight block cipher PIPO," *IEEE Access*, vol. 10, pp. 67802–67813, 2022.

[35] D. K. Gurazada. "What is an insulin pump and what are the different types?" 2020. [Online]. Available: https://www.drkalyan.com/what-is-insulin-pump

[36] J. Chen et al., "A digitally modulated mm-Wave cartesian beamforming transmitter with quadrature spatial combining," in *IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers*, 2013, pp. 232–233.

[37] R. T. Yazicigil, P. Nadeau, D. Richman, C. Juvekar, K. Vaidya, and A. P. Chandrakasan, "Ultra-fast bit-level frequency-hopping transmitter for securing low-power wireless devices," in *Proc. IEEE Radio Freq. Integr. Circuits Symp. (RFIC)*, Jun. 2018, pp. 176–179.

[38] N. Ebrahimi, B. Yektakhah, K. Sarabandi, H. S. Kim, D. Wentzloff, and D. Blaauw, "A novel physical layer security technique using master-slave full duplex communication," in *IEEE MTT-S Int. Microw. Symp. Dig. Paper*, 2019, pp. 1096–1099.

[39] X. Lu, S. Venkatesh, B. Tang, and K. Sengupta, "4.6 space-time modulated 71-to-76GHz mm-Wave transmitter array for physically secure directional wireless links," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2020, pp. 86–88.

[40] M. I. W. Khan et al., "A 0.31THz CMOS uniform circular antenna array enabling generation/detection of waves with orbital-angular momentum," in *Proc. IEEE Radio Freq. Integr. Circuits Symp. (RFIC)*, 2021, pp. 203–206.

[41] N. S. Noor, D. A. Hammood, A. Al-Naji, and J. Chahl, "A fast text-to-image encryption-decryption algorithm for secure network communication," *Computers*, vol. 11, no. 3, p. 39, 2022. [Online]. Available: https://www.mdpi.com/2073-431X/11/3/39

ALPEREN YASAR (Graduate Student Member, IEEE) received the B.Sc. degree in electronics engineering from Sabanci University, Istanbul, Turkey, in 2021. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Boston University, Boston, MA, USA.

Since the Fall of 2021, he has been a member of the Wireless Integrated Systems and Extreme Circuits Laboratory, Boston University. His research interests focus on ultralow-power analog design for biomedical applications and analog/RF solutions for physical-layer security.

RABIA TUGCE YAZICIGIL (Senior Member, IEEE) received the Ph.D. degree from Columbia University, New York, NY, USA, in 2016.

She was a Visiting Scholar from 2019 to 2023, and a Postdoctoral Associate with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, from 2016 to 2018. She is an Assistant Professor with the Department of Electrical and Computer Engineering, Boston University, Boston, MA, USA, a Visiting Scholar with MIT, and a Network Faculty Member with Sabanci University, Istanbul, Turkey. Her research interests lie at the interface of custom integrated circuits, signal processing, security, biosensing, and wireless communications to innovate system-level solutions for future energy-constrained applications.

Dr. Yazicigil has received numerous awards, including the Catalyst Foundation Award in 2021, the Boston University ENG Dean Catalyst Award in 2021, the Electrical Engineering Collaborative Research Award for her Ph.D. research in 2016, the Second Place at the Bell Labs Future X Days Student Research Competition in 2015, and the 2014 Millman Teaching Assistant Award of Columbia University. She served as the Vice Chair for the Rising Stars 2020 Workshop at the IEEE International Solid-State Circuits Conference (ISSCC) and is a member of the 2015 MIT EECS Rising Stars Cohort. From 2021 to 2022, she served as a Guest Associate Editor for the IEEE JOURNAL OF SOLID-STATE CIRCUITS for the European Solid-State Circuits Conference (ESSCIRC) Special Issue. She recently presented a lecture at the IEEE ISSCC 2023 Circuit Insights event and delivered a tutorial on physical-layer security for latency- and energy-constrained integrated systems at the IEEE ISSCC 2023. She serves as an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I: REGULAR PAPERS and on the IEEE Council for RFID Advisory Committee as a Solid-State Circuits Society (SSCS) representative. She has been an active member of the SSCS Women-in-Circuits Committee since 2016. She has been a Technical Program Committee Member of the IEEE ISSCC since 2019, ESSCIRC since 2019, International Electron Devices Meeting since 2021, and Radio-Frequency Integrated Circuits Symposium since 2023.