Exploiting the Physical Environment for Securing the Internet of Things

Christian T. Zenger, Jan Zimmer, Mario Pietersz, Jan-Felix Posielek, and Christof Paar
Horst Görtz Institute for IT-Security (HGI)
Ruhr-University Bochum, Germany
{christian.zenger, jan.zimmer, mario.pietersz, jan-felix.posielek, christof.paar}@rub.de

ABSTRACT

Using the randomness provided by the physical environment to build security solutions has received much attention recently. In particular, the shared entropy provided by measuring ambient audio, luminosity modalities or electromagnetic emanations has been used to build location-based, proximity-based, or context-based security mechanisms. The majority of those protocols is based on a standard model consisting channel probing, quantization, information reconciliation, privacy amplification, and key verification. The main problem for almost all approaches is the limited understanding of the security that is provided. For example, security analyses often only address single components and not the entire system or are based on broad abstractions of the physical source of randomness. Further, a big open question is the feasibility of such systems for low-resource platforms. Our first contribution is a detailed, optimized realization of a key establishment system. We demonstrate the feasibility of deriving a shared secret from correlated quantities on resource-constrained devices with tight power budget. Our system was realized on the popular ARM Cortex-M3 processor that reports detailed resource requirements. The second major contribution is a summary and abstraction of previous works together with a rigorous security analysis. We substantiate our investigation by presenting practical attack results.

CCS Concepts

•**Security and privacy** → **Key management; Mobile and wireless security;** *Security requirements; Formal security models; Embedded systems security;* Usability in security and privacy; •**Software and its engineering** → *Software prototyping;*

Keywords

Key establishment from correlated observations, physical layer security, security analysis, implementation, IoT

NSPW '15, September 08-11, 2015, Twente, Netherlands

DOI: http://dx.doi.org/10.1145/2841113.2841117

1. INTRODUCTION

One feature of many IoT devices is the ability to measure and quantify their physical environment. Such systems range from smart phones to wearable computers all the way down to industrial sensors. At the same time, security for IoT systems has developed from a "nice to have" to a "must have" due to numerous attacks, e.g., against networked cars or medical devices [18, 51]. Virtually all traditional security solutions are based on cryptographic primitives. Even though they are very mature, they have drawbacks in IoT settings. First, public-key algorithms are computationally expensive, especially on small embedded nodes. Second, the issue of key management is often non-trivial. To overcome those hurdles, exploiting the physical environment has been drawing increased attention in recent years. The idea of using measured physical quantities such as sensor readings or wireless channel profiles for security purposes is not new. Security solutions for (group) key establishment, (mutual) authentication, device pairing, and access control that are based on correlated physical observations have been proposed. In particular, due to the constantly increasing number of sensors in combination with the variation inherent in many of the measurable quantities, novel security approaches — treating those readings as *common random number generators* (CRNG) — has been brought into spotlight recently. Work based on shared sensor readings as entropy source include:

- ambient audio contexts (e.g.,[24, 37]),
- luminosity modalities (e.g.,[37]),
- wireless channel measurements (e.g.,[63]), and
- electromagnetic environmental fingerprints (e.g.,[55]).

We believe that due to the evolution towards the IoT, a paradigm shift from trusted third-party verified randomness (e.g., PKI or Kerberos) to CRNG-based security approaches will become highly attractive. Potentially, there are many more physical processes that could be measured by sensors and utilized for security, such as:

- fluctuation of the electromagnetic grid,
- temperature,
- barometric pressure,
- solar radiation, and
- location dependent radioactivity.

Most recently, work on practical realizations in this area has addressed high-end personal devices, such as modern

smart phones and smart watches. However, we believe that physical layer key establishment is particularly interesting for even smaller IoT nodes, on which public-key operations and key management are very difficult. Hence, we will focus on the required algorithm complexity and resource requirements for low-resource IoT devices. Moreover, the security of recent approaches is either based on broad abstractions of the random source or on experimental evaluations, which are not fully substantiated as we will demonstrate later. In this work, we analyse the security and IoT suitability of mutual information extraction from correlated observations in general and investigate the associated real-world challenges. Our main contributions are the following:

Security analysis: We present a rigorous security analysis of key agreement protocols from correlated observations. Additionally, we perform an experimental security analysis of a real-world implementation. We analyse the three-phase standard approaches in detail. Further, we perform extensive measurements in realistic environments for various use-cases. We provide a summary of potential weaknesses against passive attacks and vulnerabilities against active manipulation attacks.

Implementation and comparison: We describe two comprehensive implementations of key agreement protocols based on the recycling of Received Signal Strength Indicators (RSSI): (a) The first one represents a Wi-Fi Protected Access 2 (WPA2) driver extension and a real-time capable prototypical demonstration system based on three credit card-sized computers. (b) The second implementation was performed on an ARM Cortex-M3 processor. This provides exact resource requirements such as code size, the number of clock cycles, and power consumption. By comparing these approaches with well known Elliptic Curve Diffie-Hellman (ECDH) implementations, we show that physical layer approaches can be a promising alternative for existing and upcoming IoT systems.

The remainder of the paper is structured as follows: In Section 2 we present the background, the problem definition, and related work. The system architecture, as well as the implementation details of the exemplary real-world realization, are provided in Section 3. A extensive analysis of the security properties of the general approach based on attack-trees is presented in Section 4. In Section 5 we perform an extensive experimental analysis of the implemented architecture. Afterwards, Section 6 provides a brief discussion on the attack trees and their vectors. Section 7 summarizes thoughts about a new authentication scheme and motives future work. We conclude the paper in Section 8.

2. BACKGROUND

Wyner [60] introduced secret communication with assurance information theoretical for the wiretap channel. A key observation is that there is a trade-off between the transmission rate of the legitimate system and the equivocation at a potential wire-tapper. From these two quantities, he derived the capacity region, which is a measure of the theoretical possibility of a perfectly secret communication. However, in many broadcast media, e.g., in a wireless environment, there is no guarantee that the eavesdropper's observation will be worse than the observations of the legitimate system, and the secret capacity may be zero. Therefore, the degraded wiretap channel model may not hold [9].

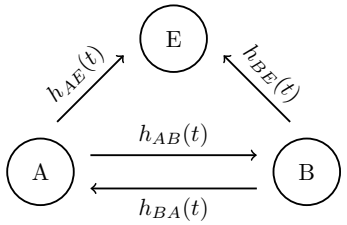


Figure 1: System model: Legitimate nodes A and B measure reciprocal properties of the physical channel, denoted by $h_{BA}(t)$ and $h_{AB}(t)$. A passive attacker E's observations $h_{AE}(t)$ and $h_{BE}(t)$ depend on her relative position and are usually less correlated with $h_{BA}(t)$ and $h_{AB}(t)$ than $h_{BA}(t)$ with $h_{AB}(t)$.

Based on Wyner's wiretap channel model, Maurer [35] considered the problem of how to generate secret keys from dependent random variables. His cryptographic system is provably secure against enemies with unlimited computing power under realistic assumptions about the partial independence of the noise on the involved communication channels.

Hershey et al. [25] introduced an alternative paradigm for generating shared secret keys, called Physical Layer Security (PHYSEC). The approach is based on a common estimation of the wireless channel by the sender and receiver, whereby secret symmetric keys are derived from the common channel parameters. Without taking noise, interferences and non-linear components into account, the joint randomness of the symmetric key relies on the principles of *antenna reciprocity* [50] and *channel reciprocity* [57]. In other words, the radio channel from Alice to Bob is similar to the channel from Bob to Alice. For most practical channels, this reciprocity property holds and the entropy of spatial, temporal, and spectral characteristics is sufficiently high due to unpredictable dynamics in the environment.

The classical system model for channel-based symmetric key extraction schemes is based on the following scenario. Two *keying nodes*, Alice A and Bob B, agree on extracting a symmetric key for secure communication while an eavesdropper, Eve E, capable of observing information tries to recover the secret key (cf. Figure 1). Observable information of Eve are, for example, error-correcting information and channel measurements (or other common quantities) between herself and the legitimate communicating nodes. We assume that A and B do not share any mutual information (e.g., shared keys) a priori.

Besides the commonness of randomness due to *channel reciprocity*, the scheme should also be inherently secure against passive attacks. Mathur et al. [34] claimed that, if a potential attacker is located more than half the wavelength of the carrier frequency away from a legitimate node, the eavesdropper will observe uncorrelated channel characteristics. For instance, for 2.4 GHz WiFi this translates to the relatively short distance of 6.25 cm. This phenomenon is called *spatial decorrelation* or *channel diversity* and is explained by Jake's Doppler spectrum [57, 20].

The requirement of spatial proximity is the basis for making eavesdropping impossible for most practical systems. As

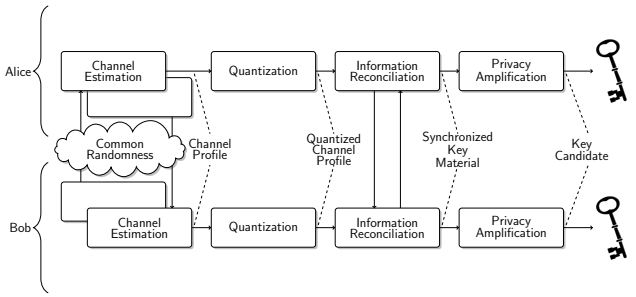


Figure 2: Overview of the core components involved in the security architecture for key agreement systems from correlated observations.

an example, for classical eavesdropping a directional antenna can be used from a greater distance. However, with PHYSEC it is ensured that no meaningful information can be obtained from such a location. As described above, for WiFi an attacker is forced to place an antenna within a few centimetres of either Alice or Bob during the key establishment phase.

The first practice-oriented protocol for unconditionally secure extraction of a symmetric key over public wireless fading channels was introduced by Tope et al. [54] in 2001. Based on this method many protocols for key extraction have been proposed. One family of contributions is based on received signal strength indicators (RSSI) [2, 3, 34, 28, 41, 33, 1, 63]. RSSI-based PHYSEC systems are very attractive because virtually every wireless communication interface provides RSSI on a per packet base, so that PHYSEC can easily be integrated in existing systems. Another family exploits the channel impulse response (CIR) more generally [23, 34, 61, 64]. Other variants are based on channel phase randomness [56] or frequency hopping [58]. Mathur et al. [34] and Jana et al. [28] included brief thoughts on potential attacks in their proposals. Simple countermeasures against spoofing attacks by active adversaries were introduced by Mathur et al. [34] and Ye et al. [61].

The generic security architecture for generating secret symmetric keys from correlated random variables is shown in Figure 2. Note that the variables might originate from physical quantities, such as sensor readings, channel measurements or other shared sources of physical randomness. These readings are quantized into vector bits to obtain an initial preliminary key. The non perfect reciprocity in measurement and noise leads to errors in the vector bits of the preliminary key. These errors are detected and corrected in the information reconciliation stage by using error correcting techniques. Since information for error correction is exchanged over the channel during the information reconciliation stage that leads to loss of entropy, the left-over entropy gets extracted in the step of privacy amplification. At the end a key verification protocol is executed.

However, above-discussed approaches for key agreement between two devices without any prior trust (also known as *pairing*) typically only protect against passive attackers. As a remedy, some authentication procedure can be employed. For example, an out-of-band communication via a second, location-limited channel (such as visual or audio) is involved for comparison of authentication credentials which defeats man-in-the-middle attacks targeting the initial key establishment. Therefore, pairing mechanisms utilizing context fingerprints, e.g., correlated observations of physical events of the direct environment, are highly interesting. First approaches of authentication mechanisms which do not require prior trust due to the utilization of common randomness are [24, 7, 47, 45, 37]. The distance-bounding protocols for mobile nodes [24, 7] are based on ultra-wideband pulse measurements. Heart-to-Heart (H2H) [45] implements a pairing scheme between a medical instrument and pacemakers by utilizing the commonly sensed characteristic of heartbeats as a secret. The work of Schürmann et al. [47] establishes a secure communication channel among devices based on similar audio patterns. The approach of Miettinen et al. [37] utilizes ambient context information gathered through commonly available sensor modalities like ambient noise and luminosity.

Since a wireless communication interface is virtually always implemented in sensor nodes, beside the key extraction approach, also an authentication mechanism based on channel measurements is a highly attractive approach and has been brought into the spotlight recently. In [55], dynamic characteristics of a common trustworthy radio environment are used as proof of physical proximity. The approach in [29] analyses variations in RSSI values to determine whether the pairing devices are in physical proximity to each other. The scheme is based on the propagation characteristic of the wireless channel and exploits multiple antennas [6]. In [52, 53, 48, 49], the wireless channel measurements are used for device authentication and a fast secret key extraction scheme. Based on the assumption that a network of mobile nodes is given, in which each node has a line-of-sight to at least one other trusted node, the authentication scheme can distinguish between on- and off-body channels.

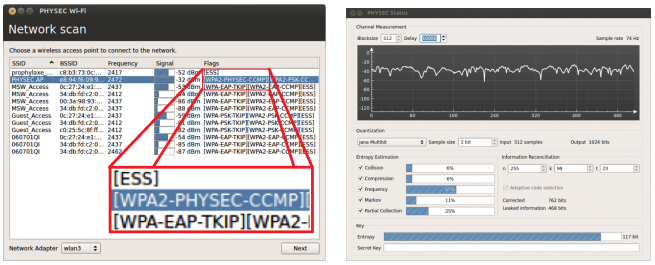
Additionally, various access control mechanisms and systems have been proposed using context sensing. GPS-based, Bluetooth-based or WiFi-based *Contexts-of-Interests (CoIs)* are used in [38, 39] for profiling and classification of the environment to make access control decisions based on sensing the environment and finding context-familiarities. Furthermore, the authors claim that light, temperature, etc. sensor readings are interesting variables for context-aware access control as well.

3. EXPERIENCE WITH REAL-WORLD REALIZATIONS OF A PHYSEC SYSTEM

In this section, we present the first (to the best of the author's knowledge) real-time capable prototypical demonstration system of PHYSEC as well as the first embedded implementation (on an ARM Cortex-M3 processor).

3.1 Fully real-time capable integration of PHYSEC into WPA protocol

We implemented an extended version of the PHYSEC architecture, illustrated in Figure 2, to generate a mutual key using channel variations. The extension involves a bit-wise on-line entropy estimation based on SP-draft [4] by NIST. The security level is verified by considering the estimated bit-entropy and the entropy loss due to public communication. (Details are given in Section 5.6.) The quantization is performed using the multi-bit scheme by Jana et al. [28]. For information reconciliation, we use secure sketches as defined by Dodis et al. [13] which are based on Bose-Chaudhuri-



(a) (b)

Figure 3: Screenshot of (a) the network scan interface and (b) the PHYSEC connection interface that provides additional information about the progress.

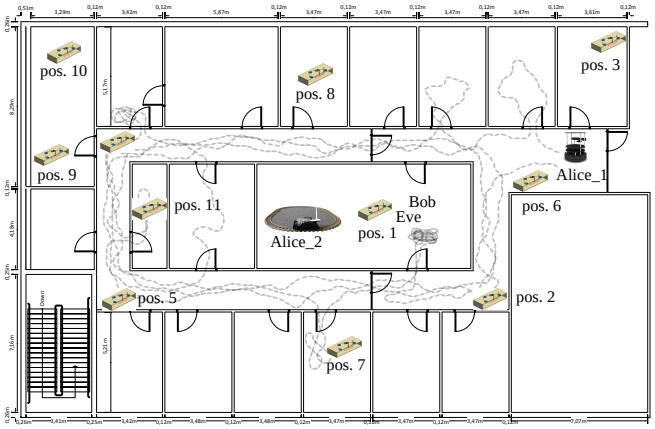


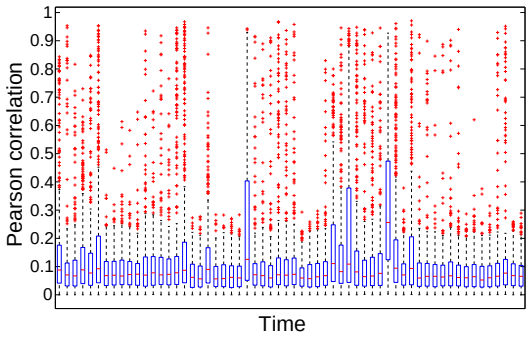
Figure 4: The spatial representation of the testbed includes several experimental setups for performance evaluation (marked with Alice$_1$, Bob, and Eve) as well as for security analysis (marked with Alice$_2$ and pos.i).

Hocquenghem (BCH) codes [44]. Because of low loss of conditional entropy (compared to other approaches), Edman et al. [17] proposed the scheme for channel-based key establishment systems.

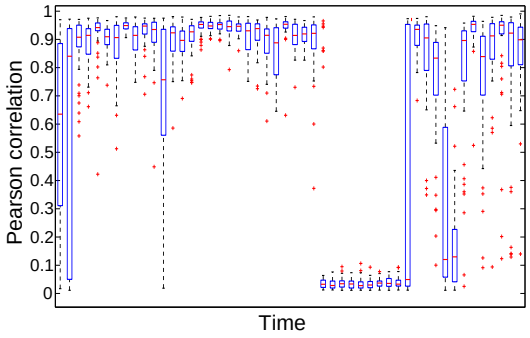
One field of application is WiFi networks in which this key can be used as an input for the WiFi Protected Access (WPA) encryption. WPA is the most popular security protocol to secure wireless networks. We added the ability to connect a new device to a WiFi network using the push-button method known as WiFi Protected Setup (WPS). The button resets the association of a device. The user then initiates the imprinting by pressing the button on the Access Point (AP). This starts the channel measurement between the AP and the client that uses this data to establish a unique network encryption key. During key establishment, the environment is assumed to be secure with no active attackers present.

3.1.1 Implementation

Our implementation has been written for Linux-based operating systems with wireless network interface cards (NIC) that support a virtual monitor mode and raw packet injection. This is necessary to communicate on the physical layer without being associated to a network. The protocol implementation is based on a master/slave role allocation. The



(a) static scenario



(b) mobile scenario

Figure 5: The box-plot illustrate the blockwise correlation behaviour between the channel measurements of Alice an Bob over time. A blocksize of 1024 RSSI values and 60 blocks per box is applied.

client acts as the master who initiates the channel measurement. The AP acts as the slave who relies on the master to control the process. It listens for frames from the client and will answer measurement requests, reconciliation requests, and verification challenges.

Since we utilize the NIC in monitor mode, we receive IEEE 802.11 packets in userspace with a radiotap header. This header supplies additional information such as the RSSI, which is used for our key generation protocol.

Figure 3 (a) shows the client interface that lets the user select a network. We added a new authentication method, PHYSEC, which is indicated by the flag *WPA2-PHYSEC-CCMP*. If the user decides to use PHYSEC to establish a network key, a detailed window can be opened to provide additional information on the progress. Figure 3 (b) shows the information that is visualized for the user. The progress of the key entropy is shown on the bottom with the key in plain text for demonstration purpose. Once a key is generated, the network connection is established. For achieving perfect forward secrecy (PFS), the key is refreshed when another 128 bit of entropy has been generated.

3.1.2 Testbed and results

The continuously changing environment plays a major role in the extraction of joint entropy. Therefore, we analysed two realistic scenarios. In the first one, two nodes are statically positioned at several locations. Here the entropy stems from motion in the environment, e.g., people moving or door opening. The second scenario represents IoT wearables, such

Table 1: Real-world based evaluation results of key extraction for two scenarios.

Scenario	# of measurements	EER [bit/s]
static	256,882	0.06
motion	5,396	2.13

as smart watches or medical sensors. Here a turtle-bot[1] is carrying such a device and moving around randomly with a regular speed of 0.5 m/s. The testbeds are illustrated in Figure 4.

The correlation of the mutual observation strongly depends on the motion in the environment and of the devices themselves. This is due to the nature of an automatic gain controller of a radio frequency (RF) receiver. If no *strong* signal variation due to motion occurs the only signal variations are based on noise and, therefore, lead to low correlation. The results of both measurement campaigns are illustrated in Figure 5 and summarized in Table 1. The entropy extraction rate (EER) represents our measurement unit for generated left-over conditional entropy per second. Only the mobile scenario results in consistently high correlated measurements and consequently in a performant system.

3.2 ECC vs. PHYSEC on ARM Cortex-M3

In the majority of cases, IoT-platforms are small embedded devices without continuous power supply. The selection of algorithms, therefore, is more restricted compared to fully grown platforms. In particular, resource requirements such as code size, the number of clock cycles, and power consumption are the crucial factors.

In state-of-the-art IoT-systems, (lightweight) public key cryptography (PKC) has been implemented to establish dynamic key management for resource-constrained devices. In particular, elliptic curve cryptography (ECC) is the most efficient algorithm among the established PKC algorithms. The efficient implementation on embedded systems has been well investigated, e.g., [32]. However, the known results do not include the energy consumption of transmitting, listening for and receiving data (see [19, 21, 10] for a detailed discussion).

Table 2: Approximate resource overhead of each of the PKC blocks of reference implementation on a 32-bit ARM Cortex-M3 GG990F1024. The source code of the used ECDH implementation can be found on github[1].

Block name	Size (Kb)	# of cycles	Power (μJ)
secp128r1	5.796	4,379,000	15,803
secp192r1	5.656	7,458,000	21,606
secp256r1	**5.918**	**19,387,000**	**50,480**
secp384r1	5.752	51,706,000	115,693

To study the performance of PHYSEC algorithm systematically, we introduce the first embedded prototype implementation of five PHYSEC schemes in an 32-bit ARM Cortex-M3 processor (EFM32GG-STK3700). The used development board Giant Gecko provides an attractive power- consumption profile and convenient evaluation tools. This platform is also used in pacemakers and provides efficient energy management [45].

Table 3: Approximate resource overhead of each of the component blocks (ASBG/ASBG-MB quantizers, secure sketch with BCH$[n,k,d]$, AES in Hirose's construction for privacy amplification) of reference implementation on a 32-bit ARM Cortex-M3 GG990F1024.

Block name	Size (Kb)	# of cycles	Power (μJ)
Quantization	0.896/0.61	$209K/43K$	94/6
Reconciliation	0.876	254,065	290
Privacy amp.	0.960	5,214	6

For the key establishment, we implemented the Diffie-Hellman key exchange with elliptic curves (ECDH) protocol. The results of the ECDH reference implementation[2] are summarized in Table 2. As highlighted in the table, our goal is to achieve a 128-bit security level. The approximate resource overhead of the computation of each component of the PHYSEC scheme is given in Table 3. The results of our implementations are based on input vectors of 128 RSSI values for the quantizations schemes and 256 bit input for information reconciliation and privacy amplification.

As mentioned above, we implemented both, the single bit and the multi-bit variation of the adaptive secret bit generation (ASBG), quantization schemes by Jana et al. [28] and the fuzzy extractor with BCH$[n,k,d]$ codes introduced by Dodis et al. [13] for information reconciliation. For privacy amplification, we applied the Hirose's construction [26] in combination with the hardware accelerated AES implementation. For comparison, we also implemented the quantization schemes by Aono et al. [2], Azimi-Sadjadi et al. [3], and Mathur et al. [34].

We calculate the energy costs for data communication by considering transmission and receiving results [10], which are based on the widespread sensor node TelosB [42]. Note that our calculations are based on the (experimentally verified) assumption that the common channel measurements are provided due to application layer communication. We call this *recycling*-based channel measurement. Figure 6 summarizes the computational and communicational energy costs of the PHYSEC schemes as well as for the ECDH implementations using channel measurements of the mobile scenario. The energy consumption of Mathur et al.'s scheme requires approximately 140 mJ per key due to the extremely low EER. The on-line evaluated security level of the PHYSEC scheme is based on the SP-draft [4] by NIST for on-line entropy estimation.

While in the best case (mobile scenario applying single-bit ASBG) the key extraction via the wireless channel requires 61.3 times less energy than for ECDH, the duration time of 1 minute is relatively high, and there are questions whether this enables the technology to exercise the requisite level of usability.

[1] http://www.turtlebot.com/

[2] https://github.com/kmackay/micro-ecc

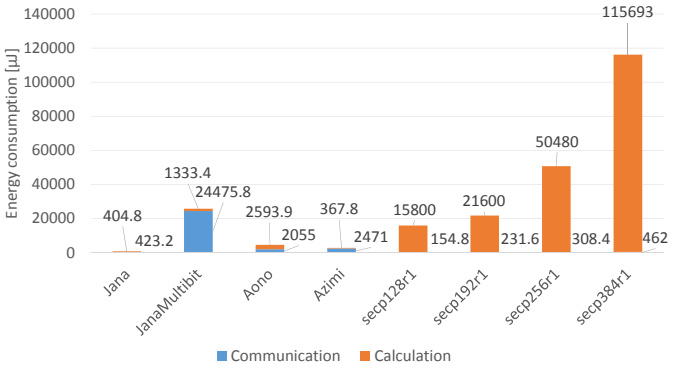


Figure 6: Performance evaluation: energy consumption of four different PHYSEC schemes (128-bit security level) and ECDH ($64-192$-bit security level).

4. THREATS AGAINST ENVIRONMENT-DEPENDENT SECURITY

To systematically address potential threats against PHYSEC, we use attack trees that describe and analyse potential attack scenarios. For completeness, we summarize their properties below. An attack tree is a unidirectional graph representing the attack vectors for a specific adversarial goal. They show how an asset might be attacked [31] by representing attacks against a system in a tree structure with the goal as the root node and different ways of achieving that goal as leaf nodes [31, 46]. Attack trees are constructed from the point of view of the adversary [27].

The root node of the tree is the global goal of an adversary, e.g., a specific asset to be captured or a specific cryptographic goal to be defeated. The children of the root node are requirements that must be met in order for the adversary to achieve this goal, i.e., to launch a successful attack. The leaf nodes of the attack tree represent attacks that can no longer be refined.

Once the attack tree is completed, different values can be assigned to the individual nodes. Typically, such values include the level of adversarial expertise as well as the attack cost for each individual node. Based on the assigned values, calculations can be made for all possible paths from the root node to the leaf nodes to determine the cheapest attack with the highest probability of success, the cheapest low-risk attack, most likely non-intrusive attack, best low-skill attack, and so on [46].

However, we present a generic attack tree applicable for CRNG-based security mechanisms without calculating system specific path attributes or efforts. For the attacks on the physical layer key agreement, it is assumed for the attacker to know everything about the sender- and receiver-architecture and corresponding parameters as well as the protocols. She can operate at the packet, bit, or signal levels. The first path separation divides the tree into the 'Learn the secret key'-path (passive attacks only) and the 'Influence the secret key generation'-path (active attacks). We hope our work represents a good cornerstone for CRNG security analyses.

4.1 Learn the secret key

Figure 7 illustrates the attack tree of the attacker's aim 'Learn the secret key'. It presents several path separations:

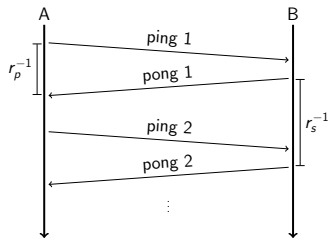


Figure 8: Important timing parameter of the channel measurement process. A high probing rate r_p lead to highly correlated measurements between Alice and Bob. A low sampling rate r_s leads to low memory-afflicted random variables (in time).

We deal with potential statistical defects that are essential to make brute force attacks feasible. We address passive attackers measuring a correlated version of the observation by Alice and Bob as well as passive attackers eavesdropping the data of public discussions. Further, potential side-channel attacks are considered.

4.1.1 *Learn parts of the key from statistical defects*

The elimination of most key candidates due to statistical defects makes exhaustive search attacks more feasible. Statistical defects may occur in the random source or due to post-processing.

The shared entropy extraction of any physical quantity allows the establishment of a common secret between two parties that can be used as an encryption key. To do so, the quantity needs to be measured on both sides. Two important parameters for the common measurements are given: The probing time $t_p = r_p^{-1}$ represents the duration in what both parties commonly measured the quantity, e.g., within 10 milliseconds. The second parameter is the (maximum) sampling rate r_s; it sets the number of common measurements per second. Please refer to Figure 8 for illustration. A communications engineering rule of thumb, applied in previous works of PHYSEC [54, 2, 3, 34, 28, 23, 41, 1], states that the common channel measurement needs to be done within the coherence time in which the channel can be assumed to be fixed [20]. Unfortunately, the coherence time is a physical parameter changing over time and space. Further, if the probing rate r_p of the channel coefficients is high compared to the inverse of the coherence time T_c^{-1}, the channel coefficients of the reciprocal channel estimations (Alice to Bob and vice versa) may be correlated in time [63]. Therefore, artificially generated scenarios, potentially arranged by an adversary, could lead to a low entropy source.

Further, post-processing techniques, e.g., for making the system robust against noise and interference, may lead to statistical defects and potentially represent an attack vector. By considering any sensor readings as a (C)RNG for cryptography, the physical source of randomness must be thoroughly evaluated with respect to:

- bias,
- correlation,
- agility, and
- manipulability.

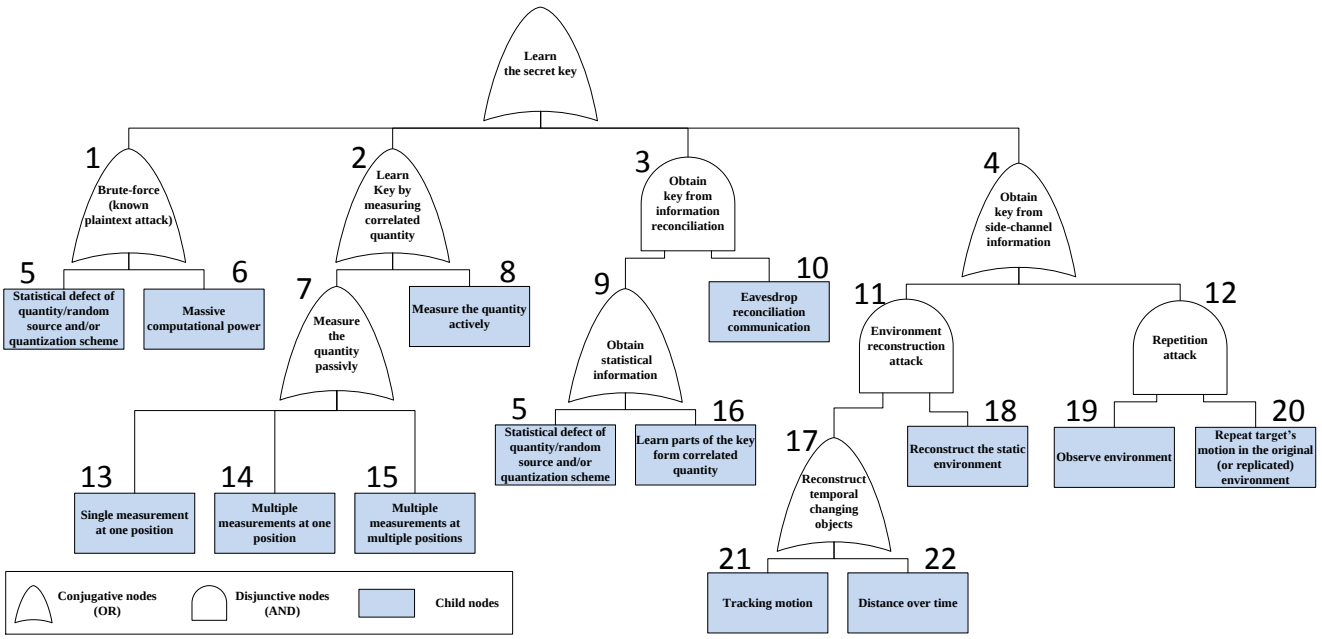


Figure 7: High-level overview of potential attack scenarios to learn the secret key.

4.1.2 *Learn key from eavesdropped quantity measurements*

This sub-tree represents the passive attacks, where the attacker receives packets from Alice (or Bob) and measures correlated observations - which implies a location-dependent eavesdropper. Classically, an eavesdropper (Eve) does not estimate the channel by actively sending and receiving packets. Eve's position is unequal to both legitimate users (Alice and Bob). Eve is equipped with the same hardware (or better) as Alice's and Bob's.

Eve can measure the random source to generate (strongly) correlated observations between Alice and Bob. The usual assumption claims that the closer the attacker gets to the victim the higher its observation gets correlated to the one of the legitimate parties. There are several different possibilities to get potentially correlated sensor readings. Single or multiple measurement devices could be used. The sampling rate could be increased for minimizing noise influences. A setup with higher quantity or spatial resolution could be applied. If the mechanism requires a pilot signal for measuring a physical quantity (such as a wireless channel) an active measurement setup might be required.

Practical measurements done by Döttling et al. [15] have shown that also the antenna reflections could be an important issue in the context of key agreement approaches based on physical layer security. This observation might be relevant in general for sensor readings.

4.1.3 *Obtain key from eavesdropping on data communication*

Key agreement protocols built on the physical environment are based on the assumption of correlated quantities between the legitimate communicating parties Alice and Bob. In practice, however, the measured quantity is not perfectly symmetric due to various environmental effects. For instance, an interfering signal whose source is located in the proximity of one of the communicating parties might affect the channel reciprocity.

Because of the imperfect symmetry, the values of the observations, e.g., RSSI values, sampled by Alice will be slightly different from those sampled by Bob. In the subsequent step Alice and Bob map the values of the measured property to a bit string based on the quantization scheme they agreed upon in advance. The bit strings therefore represent the data from which the shared secret key is derived. Because of the differences in the measured channel property values, mismatches in the bit strings will be present after the initial phase of a physical layer key agreement protocol.

To correct the mismatching bits, the communicating parties execute so called *information reconciliation*. Information reconciliation is a form of error correction/detection carried out between two communicating parties in order to align the bit strings generated in the initial key agreement phase, i.e., to make both bit strings identical. An example of a reconciliation scheme is the well-known Cascade protocol introduced by Brassard and Salvail [5]. Originally, Cascade protocol was designed for use in the Quantum Key Distribution (QKD), but it was later adopted to physical layer key agreement protocols over wireless fading channels [36, 28, 43]. Lately, various error correction codes were proposed for use in information reconciliation (e.g., [14, 12, 30, 64, 11, 17]). Fuzzy extractors (e.g., [14, 11]) are cryptographic approaches and have been proposed as a solution to securely generate keys from noisy data.

Regardless of the protocol and the error correction code, information reconciliation is always conducted over a public channel and an adversary can eavesdrop on the data exchanged between Alice and Bob. To allow correcting erroneous bits, this data contains information, e.g., parity bits, about their bit strings. Consequently, an adversary might be able to exploit this information to determine the complete secret key shared between Alice and Bob or, at least,

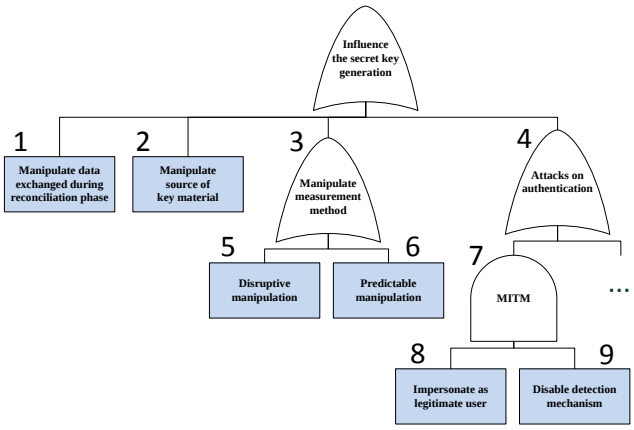


Figure 9: High-level overview of potential attack scenarios to manipulate the secret key.

to reduce the number of potential key candidates such that a brute force attack becomes feasible.

If entropy loss occurs, which was not considered in the process of choosing secure parameters of the information reconciliation protocol, the revealed information during the public discussion between Alice and Bob may lead to promising attack vectors. Further possible reasons for loss of entropy are:

- statistical defects on random source,
- statistical defects due to post-processing,
- public communication, and
- correlated measurements by an attacker.

4.1.4 *Obtain key from CRNG side-channels*

Side-channel information of the physical characteristics, which underlies the CRNG, gained from physical observation of the random source might lead to several attack vectors. The attack might use each kind of source, e.g., visual, audio, EM, etc.. One possible realization of such a side-channel attack (SCA) is a *repetition attack*. These attacks are not targeting the actual establishment between Alice and Bob but are run after the fact. An attacker's goal is to recreate the measurement setup between Alice and Bob as close as possible. The attacker Eve may take the position of Alice for example and trigger one or several key establishments with Bob. Eve may not learn every detail about the channel between Alice and Bob at the time of their run, but she may learn certain characteristics about the random source.

Eve having full knowledge of the steps taken by Alice and Bob with their measurements and even having observed them as well, may now try to use all of this information to gain an advantage against Alice and Bob. Eve can be considered successful if her observations allow her to predict better the measurement between Alice and Bob. Given her knowledge of the measurement and the observed characteristics of the random source, she may be able to learn a (major) part of the key material of Alice and Bob.

Döttling et al. [15] briefly introduced an *environment reconstruction attack*. Under too simple environment conditions, an eavesdropper can reconstruct the environment and, therefore, extract the common secret key established between the two legitimate parties.

4.2 Influence the secret key generation

The path of the attack tree for active attacks is illustrated in Figure 9. In this Section, several manipulation possibilities on the random source, measurement engine, and public communication are introduced.

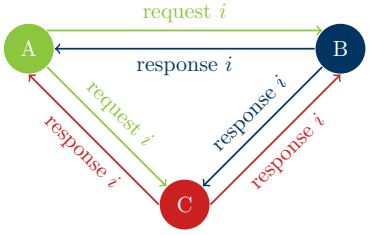


Figure 10: The 3-party channel measurement protocol.

4.2.1 *Manipulate data exchanged during reconciliation phase*

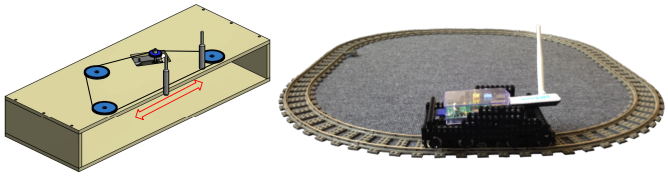
As discussed in Section 4.1.3, a physical layer key agreement protocol usually involves the so-called information reconciliation phase where the communicating parties can correct/detect the mismatching bits in their respective bit strings. In case of a passive attack, an adversary can eavesdrop on the error correction information exchanged between the legitimate communicating parties Alice and Bob and, subsequently, try to infer the secret shared between them using that information.

An active adversary, on the other hand, might be able to manipulate the error correction information forcing Alice and Bob to correct their respective bit strings in an adversary-favourable way. This would allow the adversary to manipulate how Alice and Bob decode their respective bit strings and, in turn, to influence the shared secret key that Alice and Bob agree upon.

This particular attack vector can become a critical vulnerability of a sensor reading based key agreement mechanism since the manipulation of the error correction data does not require the adversary to measure or tamper the physical properties of the random source during the key agreement phase. Instead, the manipulation of the public channel - which is insecure by definition - is sufficient. Moreover, depending on the type of the public channel, the range at which the attack can be applied might increase compared to passive measurement attacks where the adversary must be located in relative proximity of the legitimate communicating parties. Theoretically, as long as the adversary has access to the public channel used by Alice and Bob to exchange the reconciliation information, the attack can be applied even remotely.

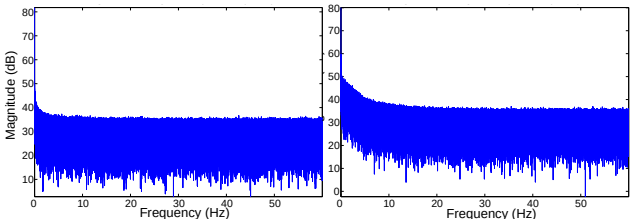
4.2.2 *Manipulate source of key material*

An attacker of this class controls (i.e., manipulate) the measurement between Alice and Bob by manipulating the random physical source during the measurement phase. Eve has to be considered successful if she can influence at least a single measurement point between Alice and Bob in such a way that she can predict the outcome of that particular measurement [59, 8].



(a) (b)

Figure 11: Illustration of the test environment and layout of sensor nodes: (a) automated antenna positioning setup, (b) cyclic moving robotic measurement platform.



(a) static scenario (b) motion scenario

Figure 12: Spectral representation of the RSSI values showing statistical defect.

In [28] a so-called *predictable channel attack* is briefly introduced. Here an adversary can cause desired changes in the channel between Alice and Bob by controlling the movements of some intermediate object or of the actual hardware platform.

4.2.3 Manipulate measurement method

Manipulating the measurement process and, therefore, the result of the measurement process without physical control of the random source represents a strong active attack.

Zafer et al. [62] proposed a jamming attacks against physical layer security to disrupt the channel probing process. The attack can be used to reduce the key generation efficiency rapidly with adversarial signal power and signal interference.

An active *key recovery attack* on physical-layer key generation schemes was introduced by Eberz et al. [16]. The attack is based on an active channel-influencing through packet injection and, therefore, manipulating the RSSI sensor reading.

4.2.4 Attacks on authentication

The key generation via radio between two parties using any of the methods described in this paper takes place fully unauthenticated. The radio channel is public; any party identifiers can be spoofed, and the system functionality is always assumed to be fully understood by an attacker. Hence, any protocol to establish a key between two identifiable parties has to include an additional authentication layer or consider some pre-shared, trusted information. Any attacks where Eve tries to impersonate another party, relay or manipulate other party's messages as her own or as parties different from the original sender's are authentication attacks.

5. EXPERIMENTAL SECURITY ANALYSIS

In this section, we provide an experimentally-supported security analysis of the PHYSEC system. Therefore, we analysed the child nodes of the attack tree. Child nodes are conditions that must be satisfied to make the direct parent node true. Recent security analyses of systems from correlated observations are based on broad channel abstractions or claims based on elusively experimental evaluations and thus are not fully substantiated as we will see later.

5.1 Testbed implementation

The protocol ensures that all three common measurements are done within the probing duration of $r_p^{-1} \leq 5\,\text{ms}$. The sampling rate is $r_s \approx (10\,\text{ms})^{-1}$. Figure 10 illustrates the procedure for synchronized measurements between Alice, Bob, and a potential passive attacker. The common channel measurement process is implemented on the hardware platform Raspberry Pi. This credit card sized computer is universally deployable with a Linux-based operating system and flexible expansion options. We equipped the computer with a TP-Link TL-WN722N wireless USB adapter as well as with a battery for mobility. Alice is mounted on a cyclic moving robotic measurement platform.

Motion is required because otherwise no channel reciprocity is given due to a low reciprocity-to-noise ratio. Additionally, in realistic scenarios no unpredictable motion leads to no new entropy. Bob and Eve are mounted on an automated antenna positioning setup. Please refer to Figure 11 for illustration. With this setup, we evaluate the correlation possibilities of a potential measurement attack for different distances between Bob and Eve. The minimum distance between Bob and Eve is 1 mm and the maximum is 300 mm. Due to a servo motor 1000 (angular) position in this 300 mm range of Eve are programmable.

5.2 Statistical defect of raw readings

Statistical defects of the random source, as introduced in Section 4.1.1, is the very first attack vector we utilize. Our analysis showed that for measurements within $\approx 300\,\text{ms}$ still exhibit temporal correlation. Several further approaches for analysing the statistical defect could be applied. For instance, temporal correlations or the mutual information $I(X;Y)$ between the observation X of a legitimized node and the observation Y of an eavesdropper represents further potential statistical defects.

For simplicity, we analysed the statistical defect of the raw sensor readings by applying a spectrum analysis. The magnitude spectrum of both setups is illustrated in Figure 12. Clearly, the frequencies are not entirely uniformly distributed; a bias towards low frequencies is given. After quantization, the defect will lead to symbol frequencies that dramatically reduce the space of the preliminary key material. For this reason, on-line statistical testing is urgently required. Further, we address in Section 5.6 how such a defect can effect the security even more drastically.

5.3 Statistical defects of quantizers

To analyse potential statistical defects of quantization schemes, the following metric is introduced. The *bit disagreement rate* (BDR) indicates the percentage of bits that are in disagreement between the initial key material of two parties. With decreasing BDR, the effort needed to detect and correct errors decreases as well. BDR is evaluated after quantization by the relation: $\text{BDR} = \frac{b_e}{b}$ where, b_e is the number of bits in

the sequence that disagree and b is the length of the initial key. A defect is given if the quantizers output leads to a BDR lower than 0.5 for low correlated observations.

To evaluate quantization schemes, we first applied the Monte-Carlo simulation environment presented in [22]. Two independent random sequences of length $1,000,000$ are modelled as temporally correlated Rayleigh distributed random variables. The maximum Doppler shift specifies the assumed Jake's Doppler spectrum. To achieve a quantitative measure for the grade of reciprocity, we define $\rho_{\alpha\beta} \in [0;1]$ as the correlation coefficient between the channel measurements of two nodes.

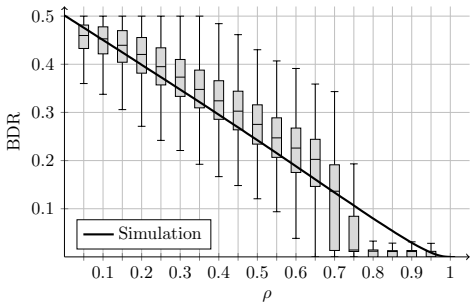
Further, based on all data of the extensive measurement campaign, we evaluated the BDR versus the correlation coefficient ρ. Therefore, we calculated the block-wise correlation as well as the corresponding block-wise BDR and sorted those by correlation value. Further, we sorted those by correlation strength and calculated the BDR distribution for the following subgroups: $[0 : 0.05, 0.05 : 0.1, ..., 0.95 : 1]$. Figure 13 shows the distribution of the block-wise BDR of the preliminary key material as well as the simulation results of both quantization schemes of Jana et al. [28].

The BDR distribution of the real-world measurements is very similar to the pattern of the simulation. Our results show that the *single-bit* scheme of Jana et al. [23] has an approximately linearly increasing BDR for decreasing correlation. Thereby the BDR for correlations higher than $\rho = 0.75$ is smaller than $\rho = 0.03$ and BDR values larger than BDR$= 0.4$ are reached if the correlation is smaller than 0.2. This indicates that passive attackers with low correlated observations can reconstruct a large amount of the preliminary key material. The BDR function of the *multi-bit* scheme shows a stable correlation coefficient behaviour of over 0.4 between 0 and 0.7, which strongly decreases towards higher correlations. The BDR for high correlations is not as low as for the single-bit version, which leads to stronger error correction capabilities, but the behaviour for low correlations fulfils the security requirement, as we will present in Section 5.4.

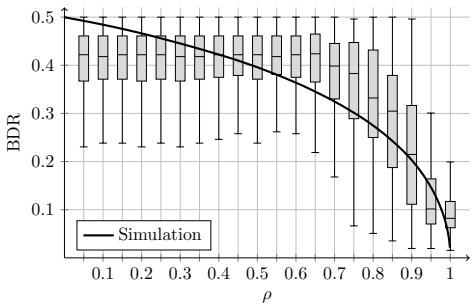
Further, for statistical analysis we evaluated the preliminary key material off-line by applying a subset of the NIST suite of statistical tests [40]. As some of these tests require a large number of bits, we constrain the evaluated tests to those who can evaluate blocks of 128 bit. The success (or acceptance) rates of the NIST statistical tests for each quantizer are listed in Table 4. The single-bit quantizer's output passes the tests with high rates, whereas the blocks produced by the multi-bit quantizer by Jana et al. [28] do not have high pass rates. The results of the sub-test fast Fourier transform (FFT) implicate the same result as our frequency analysis of the raw measurement sequence. With the knowledge of the statistical defect, a subset of the preliminary key space can be easily constructed, but it is not performed in this work.

5.4 Measurement attack

The attacker measures corresponding quantities of the random source between legitimate parties and itself. We assume that a (partial) access to the random source depends on the physical position of the attacker. To evaluate the correlation between Bob's and Eve's channel measurements over distance, we measured the channel $100,000$ times per millimeter. Then the absolute value of the Pearson correlation coefficient was calculated for blocks of 1000 measured values. The distributions of the correlation coefficients for different experiments are exemplary illustrated in Figure 14. The three illustrations represent a good example of the diversity of the correlation function.



(a) ASBG single bit



(b) ASBG multi-bit

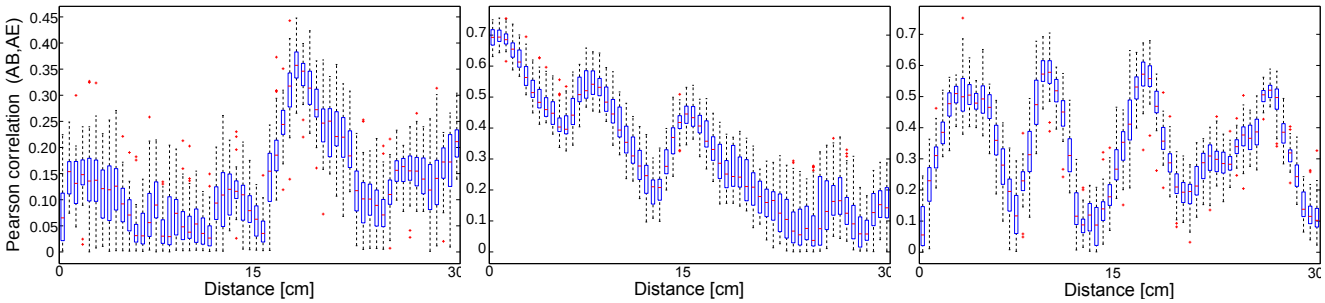
Figure 13: Evaluation results based on simulation and real-world measurements for both quantization scheme of Jana et al. [28]. The bit disagreement rate versus correlation coefficient ρ is presented.

Several positions for the automated antenna position setup were applied. The positions of each experiment are marked in Figure 4. The correlation over distance function strongly depends on the positioning of the setup. As the results show, the usual assumption which claims, that the closer Eve gets to Bob the higher its observation correlates to that of the legitimate parties, is only true for certain positions of the setup, e.g., position 10 as illustrated in Figure 14(b). The reason for this may be that the positions of the (multipath-creating) scatterers are not uniformly distributed as required.

5.5 Repetition attack

We evaluated the repetition attack using the cyclic moving robotic platform. We measured $10,000$ runs of the robotic platform passing the entire elliptic course. The robotic platform was moving with a speed of 0.6 m/s along a trail of length 3 m. One run is represented by approximately 700 RSSI values. The results of the correlation between one observation and the resulting repetitions are illustrated in Figure 15. The results show that reproduction of correlated channel measurements is possible.

The success rate of the attack depends strongly on the applied quantizations scheme. E.g., the bad BDR behaviour for low correlations of the single-bit scheme leads to very similar pre-liminary key material. Repetitions of the attack



(a) Position 5 (b) Position 10 (c) Position 12

Figure 14: Three exemplary correlation results of attacker's observation versus his distance are given. Unequal to general claims - total decorrelation after half of carrier wavelength (6.25 cm) - no uniform behaviour can be recognized.

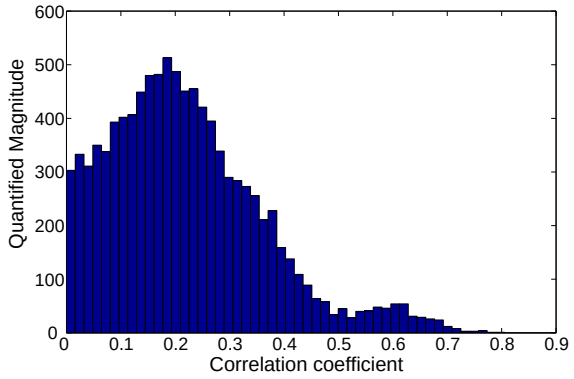


Figure 15: The distribution of the results of 10,000 repetition attacks are given. Several attacks lead to correlations larger than 0.7.

lead to a $\approx 96\%$ reproduction of the key material after quantization and 100% after information reconciliation.

Table 4: Pass rates of several NIST statistical tests for preliminary key material of the quantization schemes by Jana et al. [28]. A block size of 128 bit was applied.

Statistical tests	ASBG	ASBG-MB
Frequency	0.9637	0.2184
Block Frequency	0.9637	0.2184
Cum. Sums (fwd)	0.9517	0.2356
Cum. Sums (rev)	0.9508	0.2370
Runs	0.8480	0.4859
Longest Run	0.9463	0.5545
FFT	0	0

5.6 Eavesdropping reconciliation data

Information of the key material might be revealed due to the publicly transmitted error correction information. The passive eavesdropper Eve is able to listen to communication in the network. The distance of our attacker eavesdropping the communication on the channel was 100 m. With special equipment, e.g., directed antennas, the attack works even outside the connection range of network specifications.

For example, transmitted parity check bits always reveal information of the encoded information. Further, considering an attacker knowing statistical defects in the preliminary key material or even measuring correlated observations, the attack might be more effective. We summarize this potential knowledge of an attacker in the variable Y. The left-over secret information per bit between Alice and Bob is called conditional min-entropy $H_\infty(\mathbf{r}|Y)$, where $\mathbf{r}$ is the mutual information between Alice and Bob.

Consider a *state-of-the-art* information reconciliation approach, e.g., the one by Dodis et al. [13], where no parity check bits are transmitted and instead syndrome decoding is used. The observed quantity is interpreted as a received codeword $\mathbf{r}$. The transmitted syndrome usually only reveals information about the error $\mathbf{e}$ of a received codeword $\mathbf{r} = \mathbf{c} + \mathbf{e}$ and not about the codeword $\mathbf{c}$ itself. Therefore, the amount of information that an attacker can infer from eavesdropping $\mathtt{syn}(\mathbf{r})$ corresponds to the number of transmitted bits: $p = n - k$, where n is the codeword length and k the number information bits.

However, the assumption, that k bit entropy for each codeword is retained, is not true if the conditional min-entropy $H_\infty(\mathbf{c}|Y)$ or even the min-entropy $H_\infty(\mathbf{r})$ is low. Here, we do not perform the attack, but introduce concrete security boundaries for secure parametrization of the secure sketch information reconciliation scheme [13] based on estimated entropy, e.g., by using on-line entropy estimation. Addressing the worst-case (WC) where the potential knowledge of statistical defects of an attacker and the revealed syndrome information are independent, the following condition needs to be fulfilled to secure the system against passive eavesdropping:

$$0 < H_\infty^{\mathrm{WC}}(\mathbf{r}|Y, \mathtt{syn}(\mathbf{r})) = \frac{(H_\infty(\mathbf{r}|Y) \cdot n) - (n-k)}{n} = H_\infty(\mathbf{r}|Y) - \frac{n-k}{n}. \quad (1)$$

5.7 Manipulating channel

The attacker might be capable of manipulating the environment or forcing one or both legitimate parties into an artificial environment, e.g., using a Faraday cage to artificially build a static scenario. The aim of the attacker is to determine the symmetric key material by exploiting statistical defects. For simple physical setups, manipulation attacks on RSSI-based key extraction schemes are presented in [28]. Here, the attacker intermittently blocks the line of

sight path causing a predictable drop in the RSS values.

An active key recovery attack on physical layer key generation schemes was introduced by Eberz et al. [16]. The attack is based on an active channel-influencing attack through packet injection. The attack's performance was verified for the quantization scheme by Mathur et al. [34] which is a robust bit extraction scheme utilizing a guard interval and, therefore, leads to a recovery rate of 47 %.

We implemented the attack on a fourth Raspberry Pi with attached TL-WN722N WiFi USB stick. We applied the setup for different positions and with several antennas, gains, and channels. First results of the proposed key recovery attack lead to a recovery rate of 0 % (also for the quantization scheme by Mathur et al.). The reason for this could be the different RF front end (Eberz et al. applied MicaZ hardware). More advanced manipulation techniques are conceivable and are also part of the scope of our future work.

6. DISCUSSION

The provided attack tree offers much information on how potential adversaries undermine the security assumptions of devices in the large field the IoT. However, the tree is by no means complete as it is a tough problem finding all attack vectors. Further work is strictly required to increase the usefulness.

We think some of the points made need to be discussed more precise. It should be tested if specific changes to the environment enable adversaries to introduces statistical defects. Even more effort can be expended to check if the measurements of an attacker correlate when she uses a combination of methods to enhance correlation. Choosing parameters for the information reconciliation step affects the entropy strongly and needs to be investigated further by future work. Active attackers who can influence channel measurements or messages exchanged can be big issues depending on the chosen algorithms. There are still many open questions on this topic since the big variety of algorithms makes it difficult to generalize and make recommendations.

Even though many attack vectors exist, our experience shows that the goal of, for example, learning the secret key is not easy to achieve; and if an attack works successfully, e.g., a repetition attack, the attack does not scale to other devices. We believe that the impossibility of scaling successful attacks plus the lightweight dynamic key management are the most powerful advantages of CRNG-based approaches.

Another point is the measured energy consumption that can be set in relation to particular use-cases to provide even more realistic evaluations. Due to the estimated entropy, the required security level strongly depends on the variance of the channel that also influences the mean key extraction time. If the devices get even more constrained it should be a good idea to think about adjusting the protocol to this new environment.

7. AUTHENTIC KEY DISTRIBUTION

In this section, we shortly discuss possibilities for a novel authenticated key agreement mechanism based on proximity. The idea is, given three nodes Alice, Bob and Charlie—where Alice already trusts Charlie—to *authentically* establish a key between Alice and Bob.

The approach is based on channel profiles varying in time, space and frequency. If two nodes (Bob, Charlie) are sufficiently close to each other (a few centimetres) the profiles of the channels between them and a third device (Alice) will show similar physical characteristics. Establishing an authentic key between Alice and Bob works as follows:

1. Charlie moves close to Bob and makes sure there are no other nodes in direct proximity.

2. Alice exchanges data packets with Charlie and Bob on a channel and continually measures the two channel profiles. The communication to Bob and Charlie can be done using time-division duplex, frequency-division duplex or code-division duplex.

3. Bob continuously measures his channel profile.

4. After a while, Alice and Bob have both collected enough entropy which can be used as secret key.

5. Alice evaluates the cross-correlation between the two channels profiles she has measured to determine proximity between Charlie and Bob.

Since Alice has trust in Charlie's identity, she can use the profile of the channel shared between them as a reference. Therefore, if the correlation of the two measurement series is above a pre-defined threshold, Alice can be confident she now has established a key with Bob.

What to chose as threshold and how reliable this approach works in practice remains to be explored in future work.

8. CONCLUSION

A continuously increasing interest in unconditionally secure cryptographic approaches for a variety of security systems and mechanisms is clearly visible in literature. For instance, prior work, which is summarized in this work, had utilized context-dependent random variables coming from sensor readings and has documented that it could help address some of the important challenges that architects face when designing security solutions for advanced mobile platforms and environments without a trusted third-party or prior security association.

However, the majority of those works is based on a 3-phase standard model (please refer to [63]) which has neither been challenged by a rigorous security analysis nor has focused on the energy budget of real-world devices or the integration into commercial off-the-shelf hardware.

We implemented and tested five key extraction schemes based on correlated random channel measurements to verify the applicability for resource-constrained platforms. We provide justification of real-world applicability regarding the algorithm's complexity and resource requirements on an ARM Cortex-M3 processor. These results suggest that, for example, tiny sensor systems that do not have the energy capabilities to perform any conventional dynamic key agreement, might be upgraded with physical environment-dependent security.

In our main analysis, we found that the 3-phase standard model provides a wide variation of potential attack vectors. These findings extend previous security analysis of physical-layer key extraction [17, 16, 28] confirming that there is limited evidence for the security of these protocols. Also, we demonstrate the practical feasibility of several passive and

active attacks by applying a realistic testbed with an extensive measurement campaign. Our results provide compelling evidence for the necessity of improvement of protocols and may help future architects to develop countermeasures.

Finally, we have roughly sketched an approach for the authentic distribution of keys which may turn out to be crucial in bringing environment-dependent security schemes into real-world applications.

9. ACKNOWLEDGEMENTS

This work was supported in part by BMBF within the projects PROPHYLAXE (Grant 16KIS0010) and the project UNIKOPS (Grant 16KIS0003). Many thanks to Jürgen Förster for creating and editing figures; the members of the EMSEC Group, and the PROPHYLAXE team, especially Paul Duplys, for feedback on drafts.

10. REFERENCES

[1] A. Ambekar, M. Hassan, and H. D. Schotten. Improving channel reciprocity for effective key management systems. In *Signals, Systems, and Electronics (ISSSE), 2012 International Symposium on*, pages 1–4. IEEE, 2012.

[2] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *Antennas and Propagation, IEEE Transactions on*, 53(11):3776–3784, 2005.

[3] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 401–410. ACM, 2007.

[4] E. Barker and J. Kelsey. NIST DRAFT Special Publication 800-90b recommendation for the entropy sources used for random bit generation, 2012.

[5] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 410–423. Springer, 1993.

[6] L. Cai, K. Zeng, H. Chen, and P. Mohapatra. Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011*. The Internet Society, 2011.

[7] S. Capkun, M. Cagalj, G. Karame, and N. O. Tippenhauer. Integrity regions: Authentication through presence in wireless networks. *IEEE Trans. Mob. Comput.*, 9(11):1608–1621, 2010.

[8] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor. Physical layer security in wireless networks with passive and active eavesdroppers. In *2012 IEEE Global Communications Conference, GLOBECOM 2012, Anaheim, CA, USA, December 3-7, 2012*, pages 4868–4873. IEEE, 2012.

[9] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[10] G. de Meulenaer, F. Gosset, F. Standaert, and O. Pereira. On the energy cost of communication and cryptography in wireless sensor networks. In *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2008, Avignon, France, 12-14 October 2008, Proceedings*, pages 580–585. IEEE, 2008.

[11] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, and A. Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. *IEEE Transactions on Information Theory*, 58(9):6207–6222, 2012.

[12] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Syndrome encoding and decoding of bch codes in sublinear time, 2006.

[13] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[14] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 523–540. Springer, 2004.

[15] N. Döttling, D. E. Lazich, J. Müller-Quade, and A. S. de Almeida. Vulnerabilities of wireless key exchange based on channel reciprocity. In Y. Chung and M. Yung, editors, *Information Security Applications - 11th International Workshop, WISA 2010, Jeju Island, Korea, August 24-26, 2010, Revised Selected Papers*, volume 6513 of *Lecture Notes in Computer Science*, pages 206–220. Springer, 2010.

[16] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic. A practical man-in-the-middle attack on signal-based key generation protocols. In S. Foresti, M. Yung, and F. Martinelli, editors, *Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*, volume 7459 of *Lecture Notes in Computer Science*, pages 235–252. Springer, 2012.

[17] M. Edman, A. Kiayias, Q. Tang, and B. Yener. On the security of key extraction from measuring physical quantities. *CoRR*, abs/1311.4591, 2013.

[18] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani. On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme. In *Advances in Cryptology–CRYPTO 2008*, pages 203–220. Springer, 2008.

[19] D. Galindo, R. Roman, and J. Lopez. On the energy cost of authenticated key agreement in wireless sensor networks. *Wireless Communications and Mobile Computing*, 12(1):133–143, 2012.

[20] A. Goldsmith. *Wireless communications*. Cambridge university press, 2005.

[21] J. Großschädl, A. Szekely, and S. Tillich. The energy cost of cryptographic key establishment in wireless sensor networks. In F. Bao and S. Miller, editors, *Proceedings of the 2007 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2007, Singapore, March 20-22, 2007*, pages 380–382. ACM, 2007.

[22] R. Guillaume, A. Mueller, C. T. Zenger, C. Paar, and A. Czylwik. Fair comparison and evaluation of quantization schemes for phy-based key generation. *OFDM 2014*, 2014.

[23] S. T. B. Hamida, J. Pierrot, and C. Castelluccia. An adaptive quantization algorithm for secret key generation using radio channel measurements. In K. A. Agha, M. Badra, and G. B. Newby, editors, *NTMS 2009, 3rd International Conference on New Technologies, Mobility and Security, 20-23 December 2009, Cairo, Egypt*, pages 1–5. IEEE, 2009.

[24] G. P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005, Athens, Greece, 5-9 September, 2005*, pages 67–73, 2005.

[25] J. E. Hershey, A. A. Hassan, and R. Yarlagadda. Unconventional cryptographic keying variable management. *IEEE Transactions on Communications*, 43(1):3–6, 1995.

[26] S. Hirose. Some plausible constructions of double-block-length hash functions. In M. J. B. Robshaw, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*, pages 210–225. Springer, 2006.

[27] T. Ingoldsby. Fundamentals of capabilities-based attack tree analysis. *Amenaza Technologies Limited*, pages 406–917, 2005.

[28] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In K. G. Shin, Y. Zhang, R. Bagrodia, and R. Govindan, editors, *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, MOBICOM 2009, Beijing, China, September 20-25, 2009*, pages 321–332. ACM, 2009.

[29] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca. Ensemble: cooperative proximity-based authentication. In S. Banerjee, S. Keshav, and A. Wolman, editors, *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services (MobiSys 2010), San Francisco, California, USA, June 15-18, 2010*, pages 331–344. ACM, 2010.

[30] B. Kanukurthi and L. Reyzin. Key agreement from close secrets over unsecured channels. In A. Joux, editor, *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*, pages 206–223. Springer, 2009.

[31] B. Kordy, S. Mauw, S. Radomirovic, and P. Schweitzer. Attack-defense trees. *J. Log. Comput.*, 24(1):55–87, 2014.

[32] A. Liu and P. Ning. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In *IPSN*, pages 245–256, 2008.

[33] H. Liu, J. Yang, Y. Wang, and Y. Chen. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In A. G. Greenberg and K. Sohraby, editors, *Proceedings of the IEEE INFOCOM 2012, Orlando, FL, USA, March 25-30, 2012*, pages 927–935. IEEE, 2012.

[34] S. Mathur, W. Trappe, N. B. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In J. J. Garcia-Luna-Aceves, R. Sivakumar, and P. Steenkiste, editors, *Proceedings of the 14th Annual International Conference on Mobile Computing and Networking, MOBICOM 2008, San Francisco, California, USA, September 14-19, 2008*, pages 128–139. ACM, 2008.

[35] U. M. Maurer. Protocols for secret key agreement by public discussion based on common information. In E. F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 461–470. Springer, 1992.

[36] U. M. Maurer and S. Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In B. Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 351–368. Springer, 2000.

[37] M. Miettinen, N. Asokan, T. D. Nguyen, A. Sadeghi, and M. Sobhani. Context-based zero-interaction pairing and key evolution for advanced personal devices. In G. Ahn, M. Yung, and N. Li, editors, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*, pages 880–891. ACM, 2014.

[38] M. Miettinen, S. Heuser, W. Kronz, A. Sadeghi, and N. Asokan. Conxsense - context sensing for adaptive usable access control. *CoRR*, abs/1308.2903, 2013.

[39] M. Miettinen, S. Heuser, W. Kronz, A. Sadeghi, and N. Asokan. Conxsense: automated context classification for context-aware access control. In S. Moriai, T. Jaeger, and K. Sakurai, editors, *9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '14, Kyoto, Japan - June 03 - 06, 2014*, pages 293–304. ACM, 2014.

[40] S. NIST. 800-22. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, 2000.

[41] N. Patwari, J. Croft, S. Jana, and S. K. Kasera. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Trans. Mob. Comput.*, 9(1):17–30, 2010.

[42] J. Polastre, R. Szewczyk, and D. E. Culler. Telos: enabling ultra-low power wireless research. In *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks, IPSN 2005, April 25-27, 2005, UCLA, Los Angeles, California, USA*, pages 364–369. IEEE, 2005.

[43] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. Secret key extraction from wireless signal strength in real environments. *IEEE Trans. Mob. Comput.*, 12(5):917–930, 2013.

[44] J. Proakis. Digital communications, new york: Mcgrawhill, 2001.

[45] M. Rostami, A. Juels, and F. Koushanfar. Heart-to-heart (H2H): authentication for implanted medical devices. In A. Sadeghi, V. D. Gligor, and M. Yung, editors, *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, pages 1099–1112. ACM, 2013.

[46] B. Schneier. Attack trees. *j-DDJ*, 24(12):21–22, 24, 26, 28–29, Dec. 1999.

[47] D. Schürmann and S. Sigg. Secure communication based on ambient audio. *IEEE Trans. Mob. Comput.*, 12(2):358–370, 2013.

[48] L. Shi, M. Li, S. Yu, and J. Yuan. BANA: body area network authentication exploiting channel characteristics. In M. Krunz, L. Lazos, R. D. Pietro, and W. Trappe, editors, *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC 2012, Tucson, AZ, USA, April 16-18, 2012*, pages 27–38. ACM, 2012.

[49] L. Shi, J. Yuan, S. Yu, and M. Li. ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks. In L. Buttyán, A. Sadeghi, and M. Gruteser, editors, *Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC'13, Budapest, Hungary, April 17-19, 2013*, pages 155–166. ACM, 2013.

[50] G. S. Smith. A direct derivation of a single-antenna reciprocity relation for the time domain. *Antennas and Propagation, IEEE Transactions on*, 52(6):1568–1577, 2004.

[51] D. Strobel, B. Driessen, T. Kasper, G. Leander, D. Oswald, F. Schellenberg, and C. Paar. Fuming acid and cryptanalysis: Handy tools for overcoming a digital locking and access control system - full version. *IACR Cryptology ePrint Archive*, 2013:598, 2013.

[52] C. C. Tan, H. Wang, S. Zhong, and Q. Li. Body sensor network security: an identity-based cryptography approach. In V. D. Gligor, J. Hubaux, and R. Poovendran, editors, *Proceedings of the First ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, VA, USA, March 31 - April 02, 2008*, pages 148–153. ACM, 2008.

[53] C. C. Tan, H. Wang, S. Zhong, and Q. Li. Ibe-lite: A lightweight identity-based cryptography for body sensor networks. *IEEE Transactions on Information Technology in Biomedicine*, 13(6):926–932, 2009.

[54] M. A. Tope and J. C. McEachen. Unconditionally secure communications over fading channels. In *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE*, volume 1, pages 54–58. IEEE, 2001.

[55] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara. Amigo: Proximity-based authentication of mobile devices. In J. Krumm, G. D. Abowd, A. Seneviratne, and T. Strang, editors, *UbiComp 2007: Ubiquitous Computing, 9th International Conference, UbiComp 2007, Innsbruck, Austria, September 16-19, 2007, Proceedings*, volume 4717 of *Lecture Notes in Computer Science*, pages 253–270. Springer, 2007.

[56] Q. Wang, H. Su, K. Ren, and K. Kim. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *INFOCOM 2011. 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 10-15 April 2011, Shanghai, China*, pages 1422–1430. IEEE, 2011.

[57] J. WC Jr. Microwave mobile communications, 1974.

[58] M. Wilhelm, I. Martinovic, and J. B. Schmitt. Secret keys from entangled sensor motes: implementation and analysis. In S. Wetzel, C. Nita-Rotaru, and F. Stajano, editors, *Proceedings of the Third ACM Conference on Wireless Network Security, WISEC 2010, Hoboken, New Jersey, USA, March 22-24, 2010*, pages 139–144. ACM, 2010.

[59] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders. Short paper: reactive jamming in wireless networks: how realistic is the threat? In D. Gollmann, D. Westhoff, G. Tsudik, and N. Asokan, editors, *Proceedings of the Fourth ACM Conference on Wireless Network Security, WISEC 2011, Hamburg, Germany, June 14-17, 2011*, pages 47–52. ACM, 2011.

[60] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal, The*, 54(8):1355–1387, 1975.

[61] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam. Information-theoretically secret key generation for fading wireless channels. *IEEE Transactions on Information Forensics and Security*, 5(2):240–254, 2010.

[62] M. Zafer, D. Agrawal, and M. Srivatsa. Limitations of generating a secret key using wireless fading under active adversary. *IEEE/ACM Trans. Netw.*, 20(5):1440–1451, 2012.

[63] C. T. Zenger, M.-J. Chur, J.-F. Posielek, G. Wunder, and C. Paar. A novel key generating architecture for wireless low-resource devices. In *International Workshop on Secure Internet of Things (SIoT)*, volume 3, pages 74–89, 2014.

[64] J. Zhang, S. K. Kasera, and N. Patwari. Mobility assisted secret key generation using wireless link signatures. In *INFOCOM 2010. 29th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 15-19 March 2010, San Diego, CA, USA*, pages 261–265. IEEE, 2010.