Experimental Investigation on Wireless Key Generation for Low Power Wide Area Networks

Henri Ruotsalainen, *Member IEEE,* Junqing Zhang, and Stepan Grebeniuk

***Abstract*—The wireless key generation is a potential way to implement information theoretically secure key refreshment for IoT devices. The state-of-the-art work on key generation mainly utilizes the wireless local area network technologies. However, they have not sufficiently considered the typical characteristics of low power wide area network (LPWAN) such as lengthy payloads, duty cycled transmission and reception, or limitations for channel utilization. In this paper, we carried out a comprehensive experimental investigation on key generation applied with LPWAN, taking LoRa/LoRaWAN as case studies. A key generation protocol optimized for typical LPWAN applications is proposed. According to the extensive evaluations with deep in-building and long distance (up to 7 km) outdoor LoRaWAN links, extraction of keys with high randomness becomes feasible. Moreover, we study the achievable AES128 key refreshment periods for different eavesdropper key disagreement rates. As indicated by our measurement based evaluations, the AES128 key can be renewed every three hours with the proposed key generation protocol and with the maximum LoRaWAN spreading factor setting (longest range). A further interesting evaluation result demonstrates that a secure key refreshment is still possible even when the eavesdropper key disagreement rate is very close to the rate of the legitimate users.**

***Index Terms*—Internet of Things, low power wide area networks, physical layer security, key generation, LoRa/LoRaWAN**

I. Introduction

Low power wide area network (LPWAN) optimizes long range communication and low energy consumption and has become a key enabler of many transformative internet of things (IoT) applications in the areas of healthcare, smart cities, manufacturing, and agriculture, etc. A number of LPWAN techniques have been proposed within the past few years, such as LoRaWAN, narrowband IoT (NB-IoT), Weighless N/P and Sigfox [1]. These techniques operate typically with relatively narrow signal bandwidths and give support for infrequent uplink signaling. They are well suited for simple applications where small amounts of data transfer is sufficient. Furthermore, the high communication ranges facilitate the mobility and flexible employment of end devices.

The communication security between the LPWAN end devices and the back-end systems is typically handled by the symmetric encryption, e.g., by Advanced Encryption Standard (AES). However, it is challenging to provide lightweight, robust, cost efficient and secure key exchange for symmetric encryption in IoT applications. Asymmetric cryptography is used to distribute keys in conventional communication and computer networks, which requires extensive computation and is not suitable to the resource limited IoT devices. Key pre-distribution, e.g., programming keys into to IoT devices manually, is nowadays a popular option and utilized, e.g. in LoRaWAN. However, such a method is inefficient and potentially insecure. Firstly, key material stored in plain-text could easily be compromised from a firmware dump [2]. Secondly, key refreshment by programming becomes a burden in large-scale networks (100-1000 nodes). On the other hand, as elaborated in [2] the compromised LoRaWAN secure keys enable replay attacks and malicious end-devices, which are classified as critical according to the risk assessment. By mounting such attacks to IoT devices connected to a critical infrastructure might lead to large scale data leakages or even disasters [3].

Key generation from wireless channel is a promising technique to fulfill the aforementioned challenges [4], [5], where two legitimate users extract key bits from their common wireless channel via bi-directional channel measurements. This technique is shown to be information theoretically secure as it exploits the unpredictable channel fading. Many theoretical works of the subject, have concentrated, e.g. on the achievable secret key capacity [6], on the artificial randomness injection [7] or reconfigurable antennas [8]. In addition, key generation is lightweight and energy efficient, which is very suitable for low cost IoT devices [9]. Because of the above beneficial features, key generation has attracted many research efforts in terms of principles validation [10], protocol design [8], [11]–[13], and prototyping [14], [15].

The research focus also lies on key generation applications with wireless technologies. The existing applications are mainly designed with WiFi [10], [11] or ZigBee [9], [12], [14]–[16]; both are limited in communications ranges, i.e., less than 100 meters. However, there are very few studies on investigating full key generation implementations. Particularly, key generation in LPWAN has not been comprehensively investigated yet and the following challenges arise.

Manuscript received xxx; revised xxx; accepted xxx. Date of publication xxx; date of current version xxx. The work was supported by the grant nr 10774964 of the Austrian Research Promotion Agency. This paper was presented in part at the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, August, 2018. The associate editor coordinating the review of this paper and approving it for publication was xxx xxx.

H. Ruotsalainen is with Institute of IT Security Research at St. Pölten University of Applied Sciences, Austria. (email: Henri.Ruotsalainen@fhstp.ac.at)

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk)

S. Grebeniuk is with BDO IT&Risk Advisory Austria. (email: stepan.grebeniuk@bdo.at)

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier xxx

- *Channel reciprocity*. LPWAN usually operates in long range in the order of km, where the signal-to-noise ratio (SNR) is quite low. There will be usually long receive delay between uplink and downlink in LPWAN. The low SNR and large sampling delay will impact correlation of channel measurements [6], [17].
- *Key refreshment*. LPWAN runs at industrial, scientific and medical (ISM) band and does not use channel detection and sensing, thus it has to comply with duty cycle regulations. This will limit the channel usage and thereof increase the time required to generate a full set of keys.
- *Static environment*. Many IoT devices, e.g., smart meters, are stationary and the channel is thus static or quasi static, where the randomness is quite limited.

Although there are preliminary explorations utilizing LoRa signaling for key generation [18], [19], the above issues have not been fully studied yet. Xu *et al.* carried out extensive experiments of secret key generation with LoRa signaling for various wireless scenarios [18]. Zhang *et al.* presented a differential value-based quantization algorithm to capture the large variation of the received power [19], which is well suited to extract keys from typical LoRa channel conditions. However, neither of them considered the effects brought by the LoRaWAN protocol.

Inspired by the above observation, this paper investigated LPWAN-based key generation by using both LoRa and LoRaWAN signaling as case studies. Our contributions are listed as follows.

- We carry out an experimental study on the key generation with large turn-around time latency (seconds) during the channel probing stage. With LoRa-based measurement setup, the key disagreement rate tends towards 50% for a conventional key agreement as the turn-around time grows due to the LoRa communication overhead. In the sequel, an revised wireless secret key agreement protocol is proposed, which overcomes challenges related to the channel probing latency and the static channel conditions.
- The first LPWAN based key generation demonstration is presented. Based on the commercial off-the-shelf (COTS) LoRaWAN end devices and gateway, it is feasible to generate keys securely under the LoRaWAN protocol, application scenarios such as deep in-building penetration and static long range outdoor communications (up to 7 km), and EU ISM band regional regulations (e.g., duty cycle limitations).
- We quantify the key generation performance from the application point of view. Specifically, we evaluate the key generation rate, key disagreement rate and expected AES128 key refreshment periods for various eavesdropper statistics. According to our evaluations, periodic updates of the cryptographic keys for AES128 are feasible, even by considering strong eavesdropping attackers, wide communication ranges and low communication rates.

Part of this paper was presented in [20], which investigated LoRa-based key generation by studying the effects of LoRa configurations. This paper significantly extends our previous work by an enhanced key generation protocol and novel experimental measurements and evaluations.

The rest of the paper is organized as follows: The Section II introduces preliminary knowledges of LoRa/LoRaWAN protocol, system model of wireless key agreement and reconfigurable antenna. Section III presents our novel key generation protocol. Section IV and Section V give our design and results of the LoRa-based and LoRaWAN-based key generation, respectively. Section VI concludes the paper with potential directions for further research.

II. Preliminary

This section introduces the preliminary knowledge, including the LoRa physical layer and LoRaWAN media access control (MAC) layer, network structure and security, system model of wireless key agreement, reconfigurable antenna concept, and the challenges related to the wireless secret key generation in LoRaWAN networks.

Strictly speaking, LoRa refers to the physical layer modulation patented by the Semtech. LoRaWAN defines the higher layers of the protocol stack, proposed by the LoRa Alliance. It is worth noting that Symphony Link also operates above LoRa physical layer [21] but LoRaWAN is the most popular protocol with LoRa.

A. LoRa Physical Layer

LoRa physical layer is based on the chirp spread spectrum (CSS) modulation, where phase shifted constant envelope chirp signals convey the data symbols. CSS enables an energy efficient long-range wireless communications. The commercially available LoRa modems, the Semtech SX127x family, allow seven discrete selections for the so called spreading factor and three bandwidth among 125 kHz, 250 kHz and 500 kHz. The symbol duration is given as [22]

$$T_{sym} = \frac{2^{\mathrm{SF}}}{\mathrm{BW}}, \tag{1}$$

where SF and BW denote the spreading factor and bandwidth, respectively. The air-time of the entire LoRa packet will be proportional to the symbol duration. These parameters become relevant from the key generation perspective since they have a large impact on the duration of a single channel probing event. Depending on the configuration of spreading factor and bandwidth, the air-time of a LoRa packet varies from a few milliseconds to a few seconds.

The popular SX127x LoRa transceivers offer two types of channel and signal quality measures, namely RSSI and SNR. The Semtech SX127x model provides direct RSSI sampling and averaged RSSI per packet [23], which are denoted in this paper as RSSI_r and RSSI_p, respectively.

The LoRaWAN gateways implement typically half-duplex multi-channel and multi-spreading factor reception to support uplink communication from multiple LoRaWAN end devices. The multi-channel transceivers include typically the SX1257 RF front-end and the SX1301 baseband processor. The different transceiver hardware architectures might turn out unfavourable for the secret key generation due to different analog RF components on the transmitter/receiver, which cause asymmetry in the RSSI recordings.

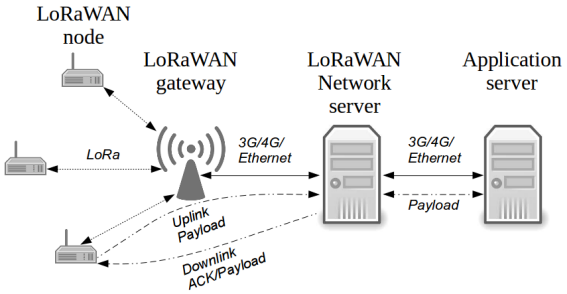


Fig. 1. LoRaWAN network components and their interconnections.

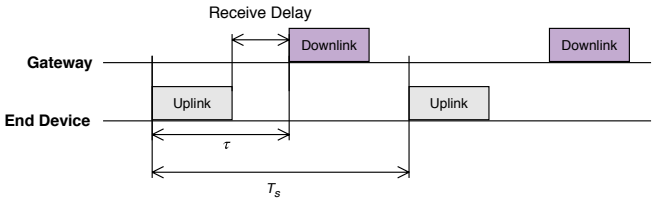


Fig. 2. Timing between uplink and downlink transmissions in LoRaWAN.

B. LoRaWAN MAC Layer and Communication Security

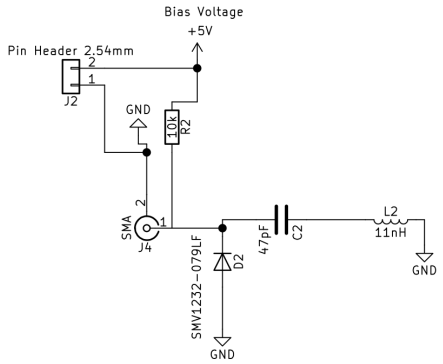
As illustrated in Fig. 1, the LoRaWAN network consists of end devices, gateways and servers [24]. A packet forwarder software at the gateway encapsulates LoRaWAN data together with metadata (RSSI, SNR, timestamp) to an UDP/TCP datagram [25]. The datagram is forwarded to LoRaWAN network server over 3G/4G or Ethernet link. The network server is also responsible for the scheduling of the downlink packets, i.e. acknowledgements or MAC command packets towards the end devices via the gateway with the best connectivity.

LoRaWAN specification defines mandatory device Class A and two optional device Classes B and C, based on their different medium access methods.

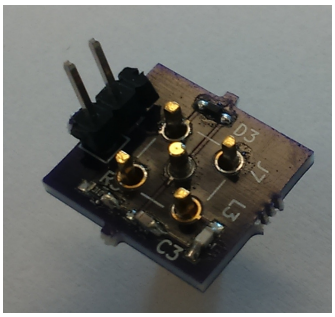
- The Class A only allows the gateway to send downlink to the end device when the gateway receives an uplink, as shown in Fig. 2. After transmitting an uplink, the end device will open the receive window after a Receive Delay, which is 1s or 2s, to receive a downlink from the gateway. Class A is best suited for low-power operation.
- The Class B introduces more reception time slots based on synchronization beacon sent by the gateway, which can support higher downlink data rates.
- The Class C applies no restriction for reception, which is helpful for low latency communication.

The delayed reception windows in Class A and B increase the channel probing latency, which may exceed the coherence time of the channel and thereof increase key bit errors due to asymmetric RSSI measurements.

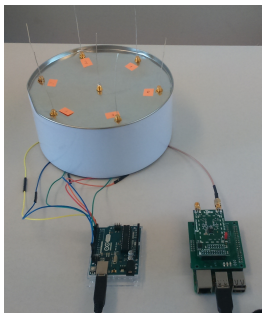
Because LoRaWAN uses ALOHA as the MAC mechanism without channel detection and sensing, regional ISM band regulations may apply, which restrict the maximum LoRaWAN air-time per device. For example, European Telecommunications Standards Institute (ETSI) restricts a 1% duty cycle for the LoRaWAN frequency in Europe, namely 868 MHz [26].



(a)



(b)



(c)

Fig. 3. (a) The schematic of the tunable reactive element. (b) A manufactured reactive element. (c) A six-element ESPAR antenna controlled by an Arduino platform.

As per the end device, it has to satisfy

$$\frac{T_{pkt}}{T_s} < 1\%, \tag{2}$$

where T_{pkt} is the packet duration and T_s is the transmission interval.

Communication security in LoRaWAN is established by the symmetric AES cipher to provide payload confidentiality and by CMAC-AES to implement message integrity checks. The involved session keys can be programmed permanently onto the nodes (activation by personalization (ABP)) or derived while the node joins the network (over-the-air activation (OTAA)). LoRaWAN specification 1.0 and 1.1 defines one and two root keys, respectively. However, the specification does not recommend any key distribution algorithms but leaves the implementation to the user's discretion. Passive key distribution might lead to vulnerabilities like device impersonation or replay attacks, as elaborated in [27]. A secure key distribution protocol for LoRaWAN is thus extremely desirable.

C. System Model of Wireless Key Agreement

Two legitimate users, namely Alice and Bob, generate shared secret key out of their correlated channel measurements. A passive eavesdropper, Eve, attempts to obtain measurements correlated to those with Alice and/or Bob. Given the channel observation X, Y and Z for Alice, Bob and Eve, respectively, a theoretical upper bound for achievable key generation rate is equal to the secret key capacity, given as

$$C_k = \min[I(X;Y), I(X;Y|Z)], \tag{3}$$

where $I(\cdot)$ denotes mutual information of two variables. Hence, secret key generation becomes feasible given that $C_k > 0$, which refers to situation where Eve's information on channel measurements does not exceed that of the legitimate users. By applying wireless channel fading model, e.g., Rayleigh model, closed-form solutions to (3) can be obtained. For detailed formulations and derivations of such solutions we refer the reader to [6] and [28]. The important aspect, delivered by the theoretical analysis, is that C_k becomes dependent on the channel probing delay τ, channel probing rate T, channel coherence time T_c and SNR at the legitimate users.

D. Challenges Related to Wireless Secret Key Generation in LoRaWAN Networks

The fundamental differences between LoRaWAN and short-range wireless networks (e.g. 802.11) in terms of physical layer, MAC layer and use cases imply some additional hurdles in terms of secret key agreement. Below we identify and elaborate the three most important challenges.

1) Static Channel Conditions: Typical use cases of LoRaWAN involve remote sensing applications, where gateways and sensor nodes locate on fixed positions [29]. Hence, the rapid channel variations due to the user movement, which is the typical source of randomness in wireless key agreement, are less likely in LoRaWAN scenarios. For many LoRaWAN use cases, the coherence time T_c becomes large, which drives C_k close to zero.

2) Lengthy Payloads and Delayed Receive Windows: As described above, the LoRaWAN applies narrow-band CSS signaling, which results in RF payload lengths of up to a few seconds. Furthermore, as depicted in Fig. 1, the network server is responsible for the scheduling of the downlink ACK packets, additional communication and computation latency is thus generated. In LoRaWAN Class-A standard this (unknown) latency is solved by the delayed reception windows. These design considerations place, however, hurdles on the channel probing part of the wireless key generation. Ideally, the node and the gateway would exchange short wireless packets within T_c to ensure that the sensed channel properties are nearly identical. However, as τ grows, the correlation between the measurements decreases. Consequently, the lower the correlation between X and Y, the lower C_k becomes.

3) Limited Channel Utilization: Because LoRaWAN operates at the ISM band and uses ALOHA protocol to access the channel, it has to comply with the channel regulation. For example, ETSI regulates the 1% duty cycle for the 868 MHz band in Europe [26]. Hence, the constrains on T directly affect the rate at which secret keys can be generated in LoRaWAN networks.

The above mentioned challenges motivate us firstly to study ways to improve the randomness of the channel conditions. Furthermore, it is of our interest to investigate key generation methods which take account of fading scenarios, where $\tau \gg T_c$.

E. Reconfigurable Antenna as Randomness Source

Electrically steerable parasitic array of radiators (ESPAR) type antenna is first included in the wireless secret key generation and experimentally validated for 802.15.4 communication in [30], [31]. Such an antenna design allows for tuning antenna radiation pattern by a fixed number of reactive elements, which ultimately leads to increased variance in measured RSSI traces. A theoretical analysis of reconfigurable antenna arrays in wireless secret key agreement schemes is given in [8]. The central piece of the work is the evaluation of the "secret key bits" metric, given as

$$I_{\mathrm{SK}} = I(X, Y|Z), \tag{4}$$

which represents the number of generated key bits per measurement secure from the eavesdropper. Via numerical simulations and experimental measurements, the authors were able to show that $I_{\mathrm{SK}} > 0$ is achievable even despite the presence of multiple eavesdroppers. Moreover it was shown that I_{SK} can be maximized by switching the reactive elements between two impedance configurations.

Inspired by the presented results, a six-element ESPAR antenna construction was built for 868 MHz. This construction supports for switching between 5V and 0V bias voltage to control the impedance of the reactive elements. The schematic, the manufactured reactive elements and the ESPAR antenna connected to the control unit (Arduino) and the LoRaWAN modem are shown in Fig. 3 (a), (b) and (c), respectively. In case of LoRaWAN network, the reconfigurable antenna can be installed to the gateway and/or end devices in order to improve key generation performance.

III. Secret Key Generation Algorithm

This section presents the steps to establish an effective secret key generation, the attack model and figures of metrics (FoM).

A. Protocol

The complete key generation chain can be broken down into elementary steps: 1) channel probing, 2) measurement pre-selection, 3) measurement match, 4) pre-correction, 5) quantization, 6) information reconciliation, and 7) privacy amplification, which are elaborated below. A more comprehensive and detailed explanation of the algorithms and measurement techniques can be found in [4].

1) Channel Probing: An end device communicates in a bi-directional manner with the gateway. For each received uplink and downlink packet the communication parties record RSSI, SNR and the packet counters. As shown in Fig. 2, the sampling delay between the uplink and downlink is

$$\tau = T_{pkt} + \text{Receive Delay}. \tag{5}$$

As specified in LoRaWAN Class A requirements, the downlink can only occur 1s or 2s later after an uplink reception. On the other hand, LoRa signaling does not have to delay the message transmission so the downlink can be sent immediately after an uplink packet, namely, $\tau = T_{pkt}$. After a packet is successfully received, the end device or the gateway reconfigures the ESPAR antenna parameters randomly.

2) Measurement Pre-Selection: The gateway analyzes the collected measurements and selects only those measurements for which the perturbations in RSSI/SNR values stems mostly from ESPAR antenna reconfigurations.

Firstly, the measurement set is divided into smaller subsets, each with N_s samples. The empirical distribution function of the i^{th} subset can be calculated as $F_{i,N_s}(x)$. The two-sample Kolmogorov-Smirnov (KS) test is able to test the equality of two probability distributions, which is performed for each neighboring subset as

$$D_{N_s} = \sup_x |F_{i,N_s}(x) - F_{i+1,N_s}(x)|, \tag{6}$$

where $\sup(\cdot)$ is the supremum function. When the D_{N_s} is above a selected threshold, these two sets can be deemed to follow the same distribution and will be selected for further processing.

3) Measurement Match: The CSS modulation utilized in LoRaWAN leads to long packet durations and ultimately to packet collisions as only a limited number of ISM bands are available for the end user [32]. Therefore it shall be expected that a continuous channel probing for each uplink/downlink packet is not possible and a measurement match between the end device and the gateway has to be accomplished before the key extraction, which can be completed as follows.

- The gateway sends the first and last uplink packet number of the pre-selected measurements to the end device.
- The end device examines the corresponding downlink packet numbers and determines subsets of continuous measurements, i.e. set of measurements without packet drops, which are communicated back to the gateway.

Now both the end device and gateway are informed about the pre-selection and the available measurements.

4) Pre-Correction: The synchronized measurements are corrected by discrete cosine transform (DCT), which is performed block-wise for the measured values as

$$X(k) = \sum_{n=0}^{N-1} x(n) \cos\big(\frac{\pi}{N}(n+0.5)k\big), \tag{7}$$

where N denotes the block size, $x(n)$ denotes the measured value and the $X(k)$ denotes the transformed measured values. Subsequently, as a precorrection step, those frequency components of DCT, which cause significant error to key bit quantization can be removed as presented in [16]. This step is helpful to overcome bit-errors due to low SNR LoRaWAN signal conditions.

5) Quantization: The obtained measurements are converted into key bits $k(n)$ by

$$k(n) = \begin{cases} 0 & x(n) > gb \\ drop & -gb < x(n) < gb \\ 1 & x(n) < -gb \end{cases}, \tag{8}$$

where $x(n)$ denotes a single entity of a normalized set of measured values, and the gb is the guard-band value. Hence, the measured value between negative and positive guard-band tolerance values will not be involved during the further steps. The packet numbers of the dropped measurements are communicated from the end device towards the gateway to ensure the synchronicity of the quantized key bits.

6) Reconciliation: Due to imperfect measurements, the quantized key bits contain bit errors even after pre-correction. The remaining key errors have to be corrected bitwise with traditional information reconciliation protocols. The secure sketch algorithm with BCH encoding was chosen as it is suitable for low resource LoRaWAN devices. Specifically, the BCH (127, 22) were chosen, which can correct up to 23 bits out of 127 key bits.

7) Privacy Amplification: According to the passive attacker model, the eavesdropper can follow the reconciliation communication between Alice and Bob, and hence utilize the information to correct her key sequence as well. Since this might in the worst case lead to exposure of the secret key, the final step in the key generation protocol is privacy amplification. The goal of this step is to remove the potentially leaked information during the reconciliation step. This paper applies the SHA256 hash function to implement the privacy amplification, which ultimately produces the final secret key.

B. Attacker Model

Following the lines of the many state-of-the-art work [4], this paper utilizes a passive eavesdropper model to verify the security of the secret key generation model. The attacker possesses clones of the LoRa transceivers, the end-device firmware and the current session keys of the LoRaWAN traffic. Hence, from the point of view of attackers, all the necessary communication, e.g., reconciliation, is considered to be communicated in plain-text.

C. Figures of Merit

A selection of performance metrics shall be utilized in order to investigate the key generation effects. Such FoM deliver ultimately relevant information on reliability and practicality of the proposed key generation scheme.

The cross correlation coefficient provides a way to assess the symmetry of the wireless channel, which is defined as

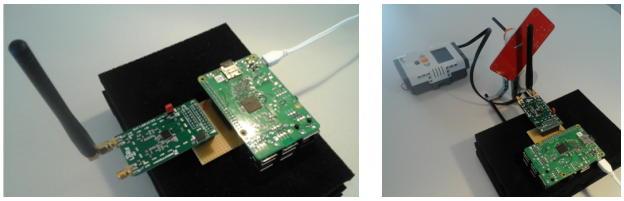
$$\rho = \frac{\mathrm{E}[(X-\mu_x)(Y-\mu_y)]}{\sigma_x \sigma_y}, \tag{9}$$

where $\mathrm{E}[\cdot]$ denotes the expectation function, μ_x and σ_x represent mean of a random variable X and standard deviation of X, respectively. A $\rho \sim 1$ means that the bi-directional wireless channel conditions are nearly independent on the direction of the communication, i.e. they are reciprocal. Otherwise for $\rho \ll 1$ indicates channel asymmetry, which might stem from channel dynamics or from different transceiver hardware on the gateway and end devices.

From applications point of view, an important factor is the rate that secret key bits can be produced. The number of key bits per measurement (KPM) is adopted, which is defined as

$$\mathrm{KPM} = \frac{N_{\mathrm{RSSI}}}{N_{\mathrm{KEY}}}, \tag{10}$$

where N_{RSSI} and N_{KEY} denote the number of RSSI measurements and the number of quantized key bits, respectively.



(a) (b)

Fig. 4. (a) LoRa equipment. (b) Measurement setup for LoRa Signaling in Scenario II

The key disagreement rate (KDR) quantifies rate of different bits at the keying parties, given as

$$\mathrm{KDR} = \frac{N_{\mathrm{ERR}}}{N_{\mathrm{KEY}}}, \tag{11}$$

where N_{ERR} denotes the number of erroneous key bits within the quantized key bit stream. It determines the success of the key generation, the required key correction capacity during reconciliation and the rate of the leaked key bits.

Finally, to prevent key guessing attacks the quantized key material shall have properties close to a key stream produced by a true random number generator (TRNG). For this purpose a popular tool-set is the National Institute of Standards and Technology (NIST) test suite [33], which includes several statistical randomness tests for binary sets. The outcomes of each test are reported by a P-Value which denotes the level of confidence, where a value above 1% indicates a strong evidence that the quantized keys stem from a TRNG.

As discussed in [34], the NIST tests should be applied to the key sequence before privacy amplification. This is because the output of the hash function is usually random, which may pass the tests. However, when the input is not random, it will result in a dictionary attack. Therefore, in order to produce a secure and random key, we need to guarantee the quantized key, before the privacy amplification, should be random.

IV. LoRa-Based Key Generation

This section will present key generation with LoRa signaling, without the restriction of the delay between uplink and downlink. This includes a comprehensive characterization of the LoRa physical layer in the light of key generation. Aspects such as available channel quality indicators and effects of LoRa modulation to the channel measurements will be covered.

A. Measurement Setup

Fig. 4 depicts the hardware components, which consist of two units, a Raspberry Pi 3B+ and a SX1276RF1JAS LoRa evaluation board. The LoRa parameters of the experimental setup apply as given in Table I, unless otherwise specified.

On the software side, the Libelium LoRaWAN Stack was modified to create bi-directional LoRa links [35]. The primary modification to the original software implementation include:

- Optimization of the turn-around time between RX and TX;
- Storage of the packet counters and measured values;
- Direct sampling of instantaneous RSSI values during the reception.

TABLE I
Parameters for LoRa Scenarios

Parameter	Value
Center frequency	865.2 MHz
Payload size	4 bytes
Bandwidth	125 kHz
Spreading factor	7
Coding rate	$4/5$
Transmission power	20 dBm

The packet counter values were later utilized to determine the package drops so that the secret key bits could be calculated from correctly aligned measurements. Finally, the $\mathrm{RSSI_r}$ values were calculated by taking an average of 100 instantaneous RSSI values collected from the preamble part of the LoRa signal; the $\mathrm{RSSI_p}$ is read directly from the packet RSSI register.

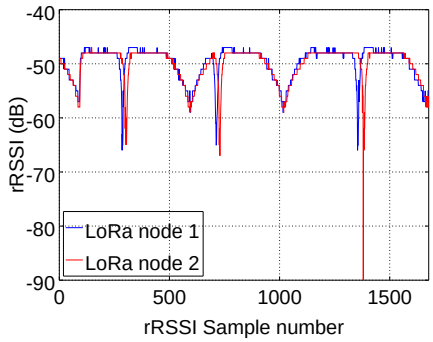
This section adopted only part of the steps in Section III, namely steps: 1), 3) and 5), because the goal at this point is to quantify the LoRa physical layer effects on the quantized raw key material.

B. Results

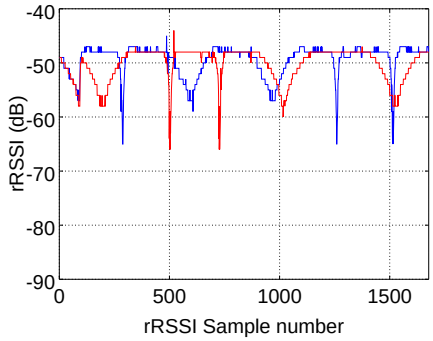
1) Scenario I: Symmetry of LoRa Payloads: The CSS modulation leads to wireless waveforms with a constant envelope when the payload is the same. Hence, it shall be expected that the instantaneous RSSI values are nearly constant for packets with identical payload. However, as illustrated in Fig. 5, those values show a clear pattern of LoRa modulation, which is likely a result of filtering in analog and/or in digital domain inside the SX127x modem. Identical payloads leads to a very consistent RSSI but random payload results in asymmetric RSSI recordings. Thus, the computation of the $\mathrm{RSSI_r}$ shall be performed over instantaneous RSSI values collected from the symmetrical part of the LoRa packets such as the preamble. The encrypted payload part will vary from packet to packet, which subsequently causes asymmetric $\mathrm{RSSI_r}$ measurements.

2) Scenario II: LoRa Parameters: The selection of the spreading factor and bandwidth has a large impact to the turn-around time, which potentially increases the asymmetry in RSSI measurements. The order of the impact of the different LoRa parameters was studied by de-tuning one of the end-device antennas in a controllable manner. As shown in Fig. 4(b), a two-sided printed circuit board was mounted on a stepper motor, placed a few centimeters from the antenna. The antenna and thereof wireless channel characteristics can be controlled, which allows for reproducible measurements. With this setup the following parameter combinations were considered: $\mathrm{SF} = \{7, 8, 9, 10, 11, 12\}$, $\mathrm{BW} = \{125, 250, 500\}$ kHz, and transmission power $P_t = \{20, 0\}$ dBm. The stepper motor was configured to produce approximately 30 revolutions per minute.

The effects of the constantly changing channel conditions on the key generation performance can be seen in the Fig. 6. As shown in Figs. 6 (a), (d), and (b), (e), the attained correlation



(a)



(b)

Fig. 5. $\mathrm{RSSI_r}$ values from a single LoRa packet with (a) identical payloads and (b) random payloads.

coefficients and KDRs are directly proportional to the LoRa packet duration. Since the channel varies with a constant rate, when $\mathrm{SF} \geq 10$ the duration of the channel probing exceeds the channel coherence time, which ultimately leads to asymmetric measurements and higher KDR. Secondly, $\mathrm{RSSI_r}$ measurements show better KPM and KDR over $\mathrm{RSSI_p}$ for several considered parameter combinations. As depicted in Fig. 6 (e), $\mathrm{RSSI_r}$ shows superior performance also for low transmission signal power. Due to the direct sampling of a small part of the LoRa packet and averaging, the measurement noise can be suppressed, which leads to a lower KDR.

V. LoRaWAN-Based Key Generation

This section delivers the performance evaluations on secret key generation optimized for long distance LoRaWAN links. The considered wireless measurements are conducted for typical use cases of LoRaWAN Class A and the evaluation results thus illustrate real world key generation performance for duty cycled ultra-low power operation.

A. Measurement Setup

A LoRaWAN gateway was established with a Raspberry Pi 3+ and an iC880a multi-channel LoRa modem, which is based on Semtech SX1257 RF front-end and SX1301 baseband processor. The packet forwarder software carries out redirection of the uplink and downlink between LoRaWAN end devices and the network and application servers [25]. The packet forwarder was modified to extract the RSSI and the SNR values of the uplink packets. The LoRaWAN end devices are the same hardware components as the LoRa end devices presented in Section IV-A. The LMIC 1.6 stack was adopted [36] and the firmware was modified in order to implement simple confirmed Class A LoRaWAN communication and measure $\mathrm{RSSI_r}$ during the two downlink RX windows. In order to optimize key generation for LoRaWAN, the complete key generation chain including steps 1)-7) presented in Section III was adopted.

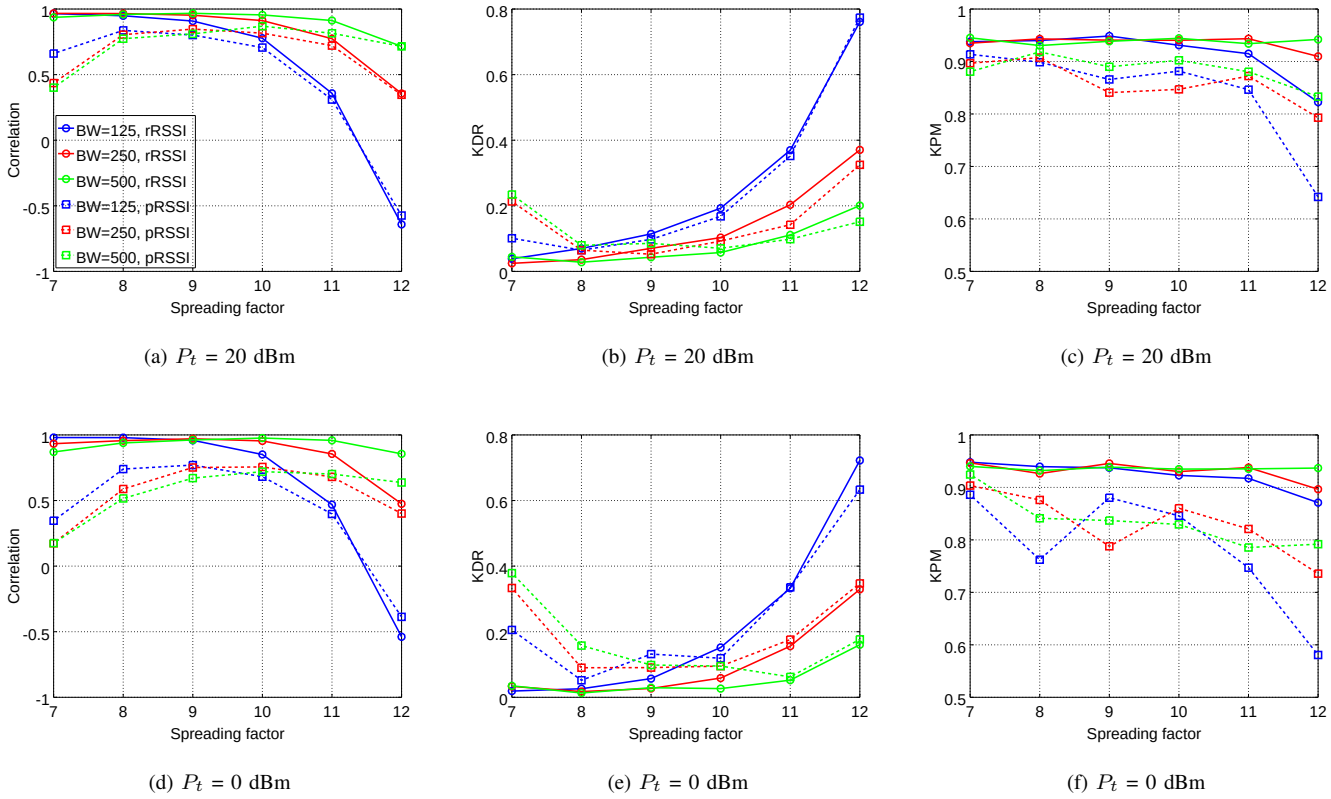
B. Results

1) Scenario III: Deep In-Building Penetration: The first set of measurements were obtained from a non-line-of-sight wireless link, where the end device and the gateway were located on the 2nd and 5th floor inside an office building, respectively. During 12 hours period 6750 measurements were collected with $\mathrm{SF} = 12$, $\mathrm{BW} = 125$ kHz and the uplink center frequency of 868.1 MHz. The reconfigurable ESPAR antenna was mounted on the gateway side to improve the nearly static communication scenario. The packet forwarder software was modified to update the antenna parameters after each transmitted downlink packet.

During the first step the pre-selection of the RSSI values was accomplished by the KS test method, where $N_s = 450$ and the threshold value was set to 0.5. As shown in Fig. 7, the measured trace contains sub-sets of RSSI values (highlighted by red) for which the statistical distributions are nearly equal. On the other hand the sub-sets for which KL test tends towards zero (depicted by blue) indicate random perturbations to RSSI for which the statistical properties change over time and hence, those sub-sets contain randomness from the ESPAR antennas and the dynamics of the wireless channel.

The evaluation results for KDR, KPM and NIST randomness tests are listed for four distinct key generation settings in Table II. Firstly, by comparing key generation performance for RSSI values without and with KS test preselection, it can be observed that KDR decreases from 29% down to 18%, respectively. An additional improvement to the key agreement performance is provided by the DCT processing of the RSSI values before the quantization. As it turns out, randomized selection of the ESPAR antenna configurations might produce repetitive bit patterns, which makes subsequent 1-bit quantization based key generation more vulnerable to dictionary attacks. This property is visible from the NIST test results in Table II, where four out of eight tests fail for the case without DCT. Therefore, the transformation by the DCT acts here as a whitening operation, which reduces the bit pattern repetitions and enables key generation close to TRNG.

2) Scenario IV: Long Distance Outdoor Communication: A line-of-sight LoRaWAN link in suburban environment over a distance of approximately 7 km was considered, which is depicted in Fig. 8. The gateway monopole antenna is mounted on the balcony of a five store office building and the end device with the ESPAR antenna is placed on a roof of a car, which remained stationary over the measurement period of



(a) P_t = 20 dBm (b) P_t = 20 dBm (c) P_t = 20 dBm

(d) P_t = 0 dBm (e) P_t = 0 dBm (f) P_t = 0 dBm

Fig. 6. LoRa signaling based measurement results of Scenario II, where (a)-(c) and (d)-(f) show correlation, KDR and KPM for high & low signal levels, respectively.

TABLE II
LoRaWAN Key Generation Performance with Different Scenarios and Setups

	Scenario III				Scenario IV	
Environment	Indoor	Indoor	Indoor	Indoor	Outdoor	Outdoor
Setup	Guard-band 0.125, w/ KS, w/ DCT	Guard-band 0.125, w/ KS, w/o DCT	Guard-band 0.125, w/o KS, w/ DCT	Guard-band 0.125, w/o KS, w/o DCT	Guard-band 0.25, w/o KS, w/ DCT	Guard-band 0.25, w/o KS, w/o DCT
KDR	0.16	0.18	0.29	0.18	0.15	0.21
KPM	0.91	0.91	0.85	0.94	0.7	0.74
Monobit	0.81	0	0.53	0	0.96	0
Block frequency	0.65	0	0.98	0	0.8	0
Runs	0.66	0	0.77	0	0.84	0.28
Longest Runs	0.21	0.3	0.85	0.05	0.25	0.27
Frequency	0.42	0.44	0.6	0	0.33	0.5
Serial	0.68	0	0.4	0	0.26	0
Approximate entropy	0.93	0	0.53	0	0.53	0
Cumulative Sums	0.84	0	0.76	0	0.96	0

3 hours. The same LoRaWAN parameters were selected as in Scenario III. Due to the RF signal attenuation along the given range in combination with the ESPAR antenna detuning, approximately 50% of the SNR measurements were negative. Hence, the SNR was chosen over RSSI as the randomness source in this scenario.

For the obtained measurements the KS tests were above the tolerance value of 0.5, and thus the entire measurement set was selected for the key generation. Similarly to the Scenario III, the positive effect of the DCT to reduce the predictability of the generated keys is visible in Table II. Finally the obtained performance metrics are close to the scenario III which confirms the efficiency of the proposed methods for secret key generation over very long distances.

3) Scenario V: Passive Eavesdropping: This scenario evaluated the attacker statistics on the leaked raw key material (before and after error correction). This scenario is extended from Scenario IV with an attacker end device, which was equipped with a 868 MHz monopole antenna placed approximately 5 cm from the legitimate node equipped with an ESPAR antenna, which is much smaller than the wavelength ($\lambda = \frac{c}{f_c} = \frac{3*10^8}{868*10^6} = 34.6$ cm.) The attacker was configured for the continuous reception of the downlink transmission and afterwards the attacker and the legitimate measurements were

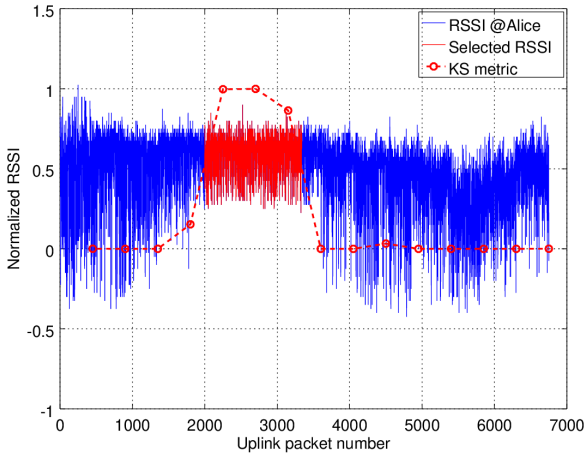


Fig. 7. Illustration of RSSI values selected by the KS pre-selection method.

synchronized based on the packet counter values.

As it turns out, the KDR for eavesdropper's raw key material becomes near 50%, which indicates the increased security provided by the ESPAR antenna. The large KDR despite of a close distance and equal LoRaWAN transceiver hardware can be explained by the variations in the antenna characteristics.

C. Key Refreshment in LoRaWAN Class A Device

The ultimate goal of the secret key agreement in LoRaWAN networks is to produce 128 key bits in order to enable key refreshment for the AES encryption/decryption. This is accomplished by the privacy amplification step, where a longer key bit stream is converted to a shorter one via hash function. The number of measurements required to generate secure key bits between Alice and Bob is dependent firstly on the selected quantization algorithm and secondly on the eavesdropper statistics. Logically, the more key bits the eavesdropper can determine by her measurements, the more measurement (bits) Alice and Bob have to collect (extract), in order to arrive at an amount of bits out of which at least 128 are unknown to eavesdroppers. Assuming that exact statistics are available, the minimum number of quantized key bits to be extracted become

$$n_{keys} = \frac{128}{\mathrm{KDR_{eve}} - \mathrm{KDR_{ab}}}, \tag{12}$$

where $\mathrm{KDR_{ab}}$ denotes the KDR between Alice and Bob. Additionally $\mathrm{KDR_{eve}} > \mathrm{KDR_{ab}}$ shall hold. Hence, the total amount of measurements required is

$$n_{meas} = \frac{n_{keys}}{\mathrm{KPM}}. \tag{13}$$

At next, the time required per AES128 key can by estimated as

$$T_{\mathrm{AES}} = n_{meas} T_s. \tag{14}$$

Finally, the frequency for the key refreshment, given as AES128 per time unit (hours/days), becomes

$$f_{\mathrm{AES}} = \frac{\delta_t}{T_{\mathrm{AES}}}, \tag{15}$$

TABLE III
COMPARISON WITH THE STATE-OF-THE-ART WORK

	Xu *et al.* [18]	**Zhang *et al.* [19]**	**This work**
Deep In-building Penetration	No	Yes	Yes
Outdoor range	4 km	500 m	7 km
Spreading Factor	7	7	12
Bandwidth	500	125	125
Transceivers	2xSX1276	2xSX1276	SX1276 and SX1301 & SX1257)
Antennas	Monopole	Monopole	ESPAR and Monopole
Signaling	LoRa	LoRa	LoRaWAN
Communication scenarios	Dynamic and Static	Dynamic	Static
Quantization algorithm	Multi-bit	Single-bit	Single-bit

where δ_t denotes a unit of time.

An example T_{AES} estimations for various spreading factor are illustrated in Fig. 9(a) with ETSI duty cycle limitations (1%) and in Fig. 9(b) without duty cycle limitations. The following parameters hold: LoRaWAN payload size is 32 bytes, SF = 12, KPM = 70%, $\mathrm{KDR_{ab}} = 17\%$, $20\% < \mathrm{KDR_{eve}} < 50\%$. The T_s was calculated based on the LoRaWAN airtime calculator [37]. The most important observation from the Figs. 9(a) and 9(b) is that a regular AES128 key refreshment is feasible by the presented key generation method. In the case of the longest air-time (SF = 12), $\mathrm{KDR_{eve}} = 33\%$ and no duty cycle restriction, a new key can be generated approximately every three hours (ca. eight keys per day). With 1% duty cycle limitation the key refreshment period becomes approximately three days (ca. 10 keys per month). The robustness against eavesdropping attacks can be improved by assuming more conservative expectation for $\mathrm{KDR_{eve}}$.

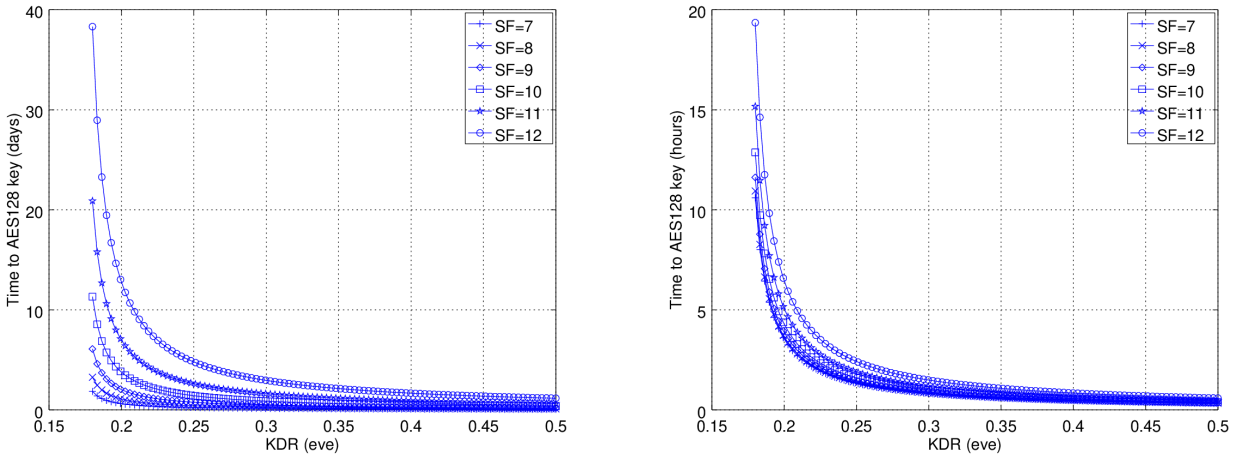
D. Implications on LoRaWAN Security and Communication

In terms of application security in LoRaWAN, the importance of key refreshment is especially relevant for the ABP network join procedure, where pre-programmed AppKey and NwkKey are applied directly for AES128 encryption. On the other hand, OTAA join procedure utilizes those keys for deriving session keys. However, as soon as an attacker possesses the DevNonce, JoinNonce and AppKey, she will be able to calculate session keys, and thus reveal the entire captured uplink and downlink data. By increasing the AppKey (and NwkKey) refreshment periods, the forward security will be improved as the compromise of a single key does not result in leakage of the entire communicated data.

By comparing the state-of-the-art works on LPWAN based key generation given in Table III, it becomes clear that our work provides the best compatibility for the existing LoRaWAN networks. Specifically, by supporting high SF settings and typical LoRaWAN Gateway hardware (SX1301 multichannel transceiver) opens up new possibilities to implement secret key agreement in large scale networks. From the practical implementation point of view, the proposed secret key agreement protocol can be embedded next to the re-join procedure, to reset both the master keys and the session keys.

(a) (b) (c)

Fig. 8. Outdoor LoRaWAN scenario. (a) Line-of-sight wireless link. (b) Antenna of Alice mounted on the balcony of a 5th floor of an office building. (c) ESPAR antenna of Bob mounted on the roof of a car.



(a) (b)

Fig. 9. Estimated time required to produce an AES128 key vs. Eve's KDR given the different spreading factor settings. (a) the EU868 band duty cycle limitations for LoRaWAN communication. (b) without duty cycle limitations

Similar to forward security, the physical layer key agreement also provides protection against quantum computer attacks. Without information on the RSSI measurements (and with sufficient key lengths), the brute-force attacks shall remain infeasible. According to NIST recommendations [38] the cryptoperiod, i.e., the period of time over which the cryptographic key is in utilization, for a symmetric master key shall be one year. Hence it can be assumed that the key agreement even with asynchronous non-frequent LoRaWAN uplink communication can support for this recommendation.

As mentioned in Section III, the key agreement utilizes the existing transmissions to arrive at the required RSSI measurements. Hence, the channel probing part of the protocol does not introduce additional communication overhead. On the other hand, the parts "Measurement Match" and "Reconciliation" necessitate exchange of LoRaWAN packets to synchronize the measurements and to perform error correction. Depending on the amount of dropped uplink/downlink packets and n_{meas}, a slight increase to the communication overhead shall be expected. As an example: In the scenario given in previous subsection, the generation of a single AES128 key demands ca. 130-150 bytes to be exchanged between the end-device and the gateway. Hence, a communication overhead of ca. five (32 byte) LoRaWAN packets shall be added. Nevertheless, this overhead is marginal when compared with the entire LoRaWAN packet exchange during the normal end-device operation.

VI. Conclusions

This paper presented a wireless key generation method tailored for LoRa and LoRaWAN Class A devices. We have carried out extensive experiments to evaluate key generation performance with different LoRa physical layer configurations (spreading factor and bandwidth). We have also performed experiments for LoRaWAN-based key generation with scenarios of deep in-building penetration and line-of-sight outdoor communication up to 7 km. An ESPAR antenna was designed to tackle the static channel conditions, which is common in many IoT scenarios. The results demonstrated that a regular refreshment of the AES128 key can be achieved even for challenging SNR conditions ($\mathrm{SNR} < 0$) or for long channel probing signals. The presented key generation chain shall be applicable for other long range communication protocols as well. The future work will be targeted at system level performance evaluations for large-scale LoRaWAN networks and on ultra-low power implementations of the presented algorithms.

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their constructive comments and suggestions.

REFERENCES

[1] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2017.

[2] N. Butun, I. Pereira and M. Gidlund, "Security risk analysis of lorawan and future directions," *Future Internet*, 2019.

[3] E. Ronen, A. Shamir, A. O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *Proc. IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 195–212.

[4] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[5] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the internet of things: Authentication and key generation," *IEEE Wireless Commun.*, 2019.

[6] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, 2017.

[7] G. Li, A. Hu, J. Zhang, and B. Xiao, "Security analysis of a novel artificial randomness approach for fast key generation," in *Proc. IEEE GLOBECOM*, Singapore, 2017, pp. 1–6.

[8] J. W. W. R. Mehmood and M. A. Jensen, "Key establishment employing reconfigurable antennas: Impact of antenna complexity," *IEEE Transactions on Wireless Communications*, vol. 13, no. 11, 2014.

[9] C. T. Zenger, M. Pietersz, J. Zimmer, J.-F. Posielek, T. Lenze, and C. Paar, "Authenticated key establishment for low-resource devices exploiting correlated random channels," *Computer Networks*, vol. 109, pp. 105–123, 2016.

[10] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, Aug. 2016.

[11] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Computing and Networking*, San Francisco, California, USA, 2008, pp. 128–139.

[12] 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. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[13] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[14] C. T. Zenger, M. J. Chur, J. F. Posielek, C. Paar, and G. Wunder, "A novel key generating architecture for wireless low-resource devices," in *Proc. International Workshop on Secure Internet of Things*, Sept 2014, pp. 26–34.

[15] K.-F. Krentz and G. Wunder, "6doku: Towards secure over-the-air preloading of 6LoWPAN nodes using PHY key generation," in *Proc. European Conf. on Smart Objects, Systems and Technologies*, Aachen, Germany, Jun. 2015, pp. 1–11.

[16] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, "Physical layer secret-key generation with discreet cosine transform for the Internet of Things," in *Proc. IEEE Int. Conf. Communications (ICC)*, May 2017, pp. 1–6.

[17] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *Proc. 17th IEEE Int. Workshop Signal Process. Advances in Wireless Commun. (SPAWC)*, Edinburgh, UK, July 2016, pp. 1–5.

[18] W. Xu, S. Jha, and W. Hu, "LoRa-Key: Secure key generation system for LoRa-based network," *IEEE Internet Things J.*, 2018.

[19] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12 462–12 466, 2018.

[20] H. Ruotsalainen and S. Grebeniuk, "Towards wireless secret key agreement with LoRa physical layer," in *Proc. Int. Conf. Availability, Reliability and Security*, Hamburg, Germany, Aug. 2018, p. 23.

[21] Symphony Link™. Accessed on 8 June, 2019. [Online]. Available: https://www.link-labs.com/symphony

[22] "SX1272/3/6/7/8: LoRa Modem, Designer's Guide," Semtech, Tech. Rep. AN1200.13, accessed on 8 June, 2019. [Online]. Available: https://www.semtech.com/uploads/documents/LoraDesignGuide_STD.pdf

[23] *SX127x, Low Power Long Range Transceiver*, Semtech Std., accessed on 12 April, 2019. [Online]. Available: https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1276

[24] *LoRaWAN™ 1.1 Specification*, LoRa Alliance Std., accessed on 9 May, 2019. [Online]. Available: https://lora-alliance.org/resource-hub/lorawantm-specification-v11

[25] *LoRaWAN packet forwarder software*, Semtech Std., accessed 19 January, 2019. [Online]. Available: https://github.com/Lora-net/packet_forwarder

[26] Duty Cycle for LoRaWAN Devices. Accessed on 5 June, 2019. [Online]. Available: https://www.thethingsnetwork.org/docs/lorawan/duty-cycle.html

[27] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of LoRa," in *Proc. 3rd IEEE Int. Conf. Cybernetics (CYBCONF)*, June 2017, pp. 1–6.

[28] X. W. . al., "Physical layer secret key capacity using correlated wireless channel samples," in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016.

[29] B. I. O. Khutsoane and A. M. Abu-Mahfouz, "Iot devices and applications based on lora/lorawan," in *43rd Annual Conference of the IEEE Industrial Electronics Society*, 2017.

[30] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, 2005.

[31] T. Ohira, "Secret key generation exploiting antenna beam steering and wave propagation reciprocity," in *Proc. European Microwave Conf.*, vol. 1, 2005, pp. 1–4.

[32] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 34–40, 2017.

[33] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, Tech. Rep. Special Publication 800-22 Revision 1a, Apr. 2010.

[34] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, 2018.

[35] *Libelium LoRa library*, Libelium Std., 2017, accessed on 20 June, 2019. [Online]. Available: https://github.com/CongducPham/LowCostLoRaGw

[36] *LMIC 1.6 communication stack*, IBM Std., 2017, accessed on 20 June, 2019. [Online]. Available: https://github.com/wklenk/lmic-rpi-lora-gps-hat

[37] LoRa air time calculator. Accessed on 18 June, 2019. [Online]. Available: https://www.loratools.nl

[38] *Recommendation for Key Management Part 1*, National Institute of Standards and Technology, 1 2016.