# Appendix 08
# RKD: Radio-Signal Key Distribution

## 1 Introduction

A systematic analysis of the state of research revealed a significant implementation gap between theoretical findings and practical market applications. Although RKD has been an established field of research for two decades and extensive scientific literature is available, only a single commercial product could be identified that enables RKD for the generation and distribution of cryptographic keys for end users. This single marketable RKD product is examined in more detail in this appendix.

The literature review (see section below) shows that the state of the art allows for many different approaches. Depending on the application environment, all of these approaches have advantages and disadvantages, which are often only partially apparent in the publications. Therefore, a comprehensive evaluation of the state of the art was conducted prior to the start of product development. This evaluation yielded two solution approaches, which were then implemented as a product. This chapter contains a comprehensive description of the two product variants. This is intended to provide the reader with a more detailed understanding of how RKD actually works.

Python 3 was chosen as the development platform to create an agile prototyping environment that enabled rapid iterations, flexible restructuring, and creative ideation. The project underwent continuous "restructuring" to ensure that as broad a range of approaches as possible could be thoroughly evaluated. Despite the dynamic development, the software development followed a consistent basic workflow that served as a stable foundation for all experiments. The development process was characterized by a constant switching between different algorithms and components. This methodical approach made it possible to identify the most effective approaches and develop them further in a targeted manner, while less successful concepts could be excluded and removed at an early stage.

**The following section focuses only on the components that were actually implemented.**

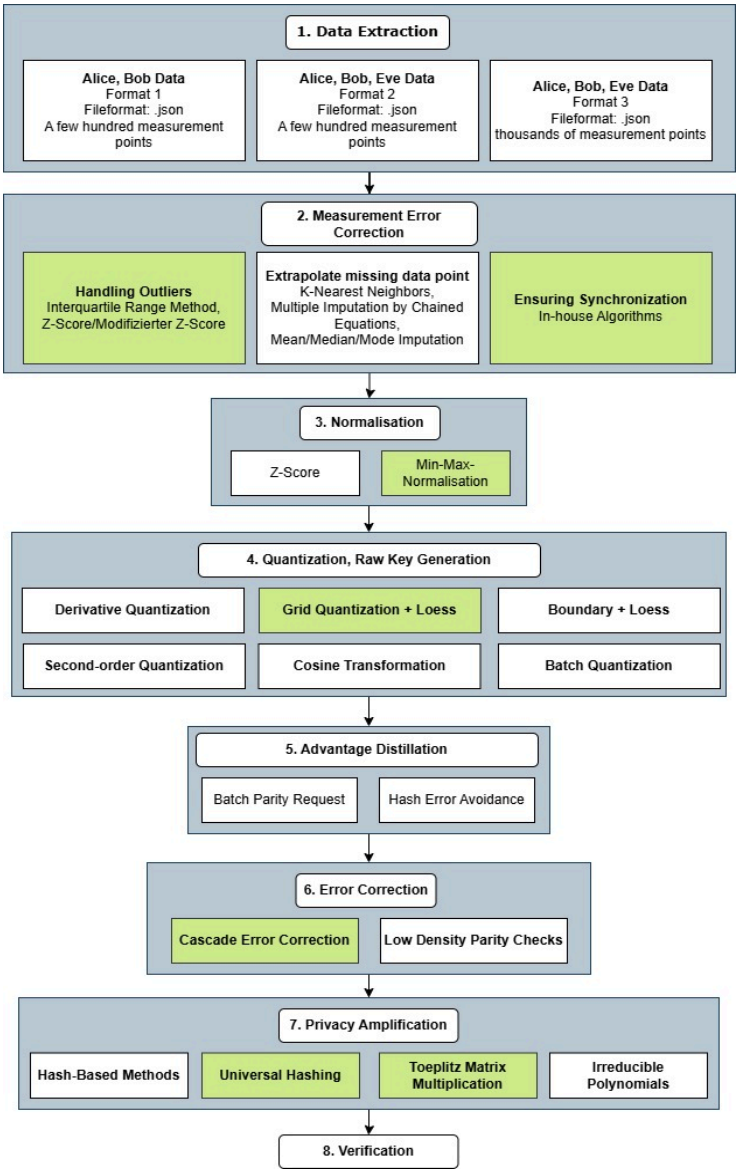



**Figure 1**: Overview of the process and tested methods

After all modules were tested, the best ones were identified. These are marked in green in the figure.

## 2 Measurement and error correction

Electronic errors repeatedly lead to unavoidable errors in the measurement data. This manifests itself in the absence of individual measurement blocks or severe outliers. These are corrected right at the start to prevent errors from occurring later in the data processing workflow.

## 3 Normalization

After evaluating a wide variety of measurement scenarios, it became clear that there is no significant difference between the preferred normalization methods. Due to its simpler and faster calculation, the Min-Max normalization was selected.

## 4 Grid Quantization + LOESS

After normalizing each measurement section, a LOESS (Locally Estimated Scatterplot Smoothing) transformation is applied. This statistical method is well-suited for RSSI measurements, as they are naturally subject to strong fluctuations and do not follow an exact line. LOESS uses local regression to generate a smoothed curve that reflects the underlying trend of the noisy RSSI data points while preserving the characteristic variations of the radio channel.

The resulting LOESS curve forms the basis for all further calculations.

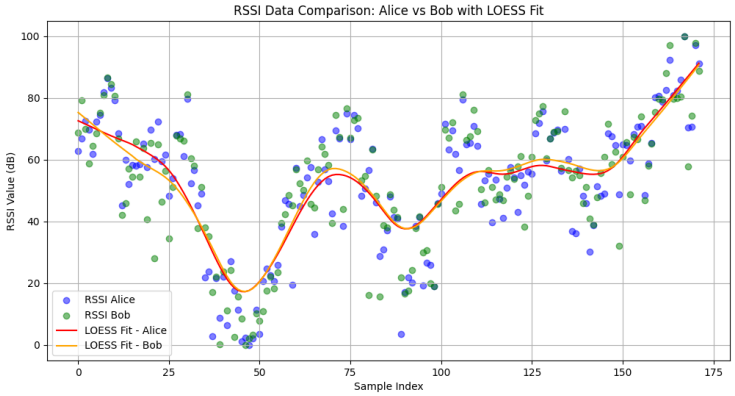



**Figure 3**: Representation of the LOESS curve

Depending on the desired accuracy, a grid with wide to fine mesh is now superimposed over the LOESS curve. Subsequently, based on the curve, the distance to the nearest points ( ) is calculated. The position of the nearest point on the Y-axis reflects the binary value of that part of the key. The process is repeated up to several thousand times, based on the desired total key length.

Depending on the desired resolution, a grid with points placed at varying densities is superimposed over the LOESS curve. The grid density serves as the primary control parameter:

- Coarse-mesh grid: Higher robustness against measurement noise, lower resolution
- Fine-mesh grid: Finer resolution, higher sensitivity to channel fluctuations

For each point in time during key generation, the Euclidean distance to all grid points is calculated based on the LOESS curve. The algorithm systematically identifies the grid point with the shortest distance to the selected curve position. The Y-coordinate of the nearest grid point is used to determine the binary value. This position is converted into a binary code according to the previously defined quantization logic, whereby the number of bits per measurement point determines the resolution of the Y-axis segmentation.

The described process is performed iteratively based on the desired total key length. For typical cryptographic keys, this iteration can occur up to several thousand times, with each iteration generating additional bits of the final key.

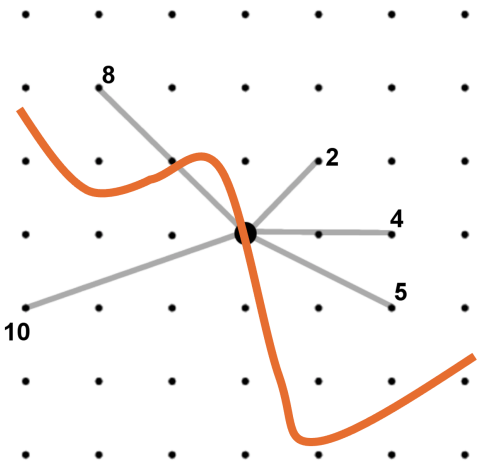



**Figure 4**: Visualization of the lattice

## 5 Discrete Cosine Transformation

An alternative approach to quantizing the raw key material is the Discrete Cosine Transform (DCT) for frequency analysis of the measurement data. In this method, the RSSI data is decomposed into its individual frequency components using DCT, and the key is generated from the individual frequency components. The analysis shows that both the lowest and highest frequency components of the spectrum exhibit only weak correlation between Alice and Bob ( ), which is likely due to system-induced noise and high-frequency interference. The mid-frequency range, on the other hand, exhibits a significantly higher correlation between the communication partners, while Eve shows significantly lower correlation data in this frequency range. This method makes it possible to use the frequency components for key generation that ensure both a high correlation between Alice and Bob and maximum decorrelation with respect to potential attackers.

## 6 Cascade Error Correction

Following an extensive analysis of Cascade Error Correction and Low Density Parity Check (LDPC), Cascade was selected. Cascade proved to be significantly easier to implement. While LDPC codes require a complex matrix structure and computationally intensive belief propagation algorithms, Cascade offers an intuitive, step-by-step approach to error correction. A key advantage of Cascade is its adaptive nature. The protocol can adapt to the actual error characteristics of the channel, whereas LDPC codes must be optimized for specific error rates.

For the moderate error rate of the present system (typically 10% to 12.5%), Cascade demonstrated lower computational complexity than LDPC. Cascade is particularly more efficient for smaller block sizes, such as those encountered in this application. Because Cascade is widely used in QKD (Quantum Key Distribution), it offers a solid, proven foundation with extensive literature and known optimization possibilities.

A comprehensive statistical evaluation of the Cascade implementation carried out in the project confirmed that the developed solution meets both the expected efficiency and the required security standards. The previously described paper “Error Reconciliation in Quantum Key Distribution Protocols” served as a reference standard, with its results and performance metrics used as a benchmark for the evaluation.

## 7 Secure Sketch

Secure Sketch is a potential alternative to the interactive cascade protocol that solves the error correction problem with a completely different approach. Instead of identifying errors step by step through multiple transmissions and corrections, this method uses a single, larger transmission for correction. The method is based on the idea that Alice can create a kind of "correction signature" of her key and transmit it publicly without revealing the key itself. This correction signature, also called a sketch, contains just enough information to help Bob correct his erroneous version without providing useful insights to an outsider.

Alice takes her correct key and combines it with a randomly generated sequence structured according to specific mathematical rules. This version is sent as a sketch over the public channel. Bob can automatically correct his errors using his corrupted key and the received sketch, provided the number of errors remains below a certain threshold. The correction process is fully automated without further interaction between the parties.

The method is secure because the sketch appears to an attacker as a completely random bit sequence. Without knowledge of a version of the original key, no usable information can be extracted from the sketch. Even if an attacker intercepts the entire sketch, they can draw hardly any conclusions about the original key material.

The biggest drawback is the lack of flexibility. The system must be calibrated in advance to a specific maximum error rate. If more errors occur than expected, the correction fails completely. If fewer errors are present, capacity is wasted. Additionally, the method requires that errors be evenly distributed across the key. If errors occur in larger clusters, this can lead to problems. Unlike Cascade, however, Secure Sketch requires only a single round of transmission and is thus significantly more efficient in terms of communication.

## 8 Privacy Amplification

After successful error correction via the Cascade protocol, Alice and Bob have identical bit sequences, which are, however, not completely secure. A potential attacker may have obtained information about parts of the key during public communication. To extract an information-theoretically secure key from this partially compromised material, Privacy Amplification is applied.

# 9 Measurement Data Collection

A thorough experimental evaluation was conducted to optimize the individual steps of the process. This systematic analysis required a large number of measurements under various environmental conditions and with different motion patterns in order to determine the optimal parameters for the respective algorithms and components.

All measurements were conducted under ideal attack conditions for third parties. An eavesdropper (Eve) was active during all experiments and always remained between 50 cm and 1 m away from Alice. Alice was stationary, as was Eve. This configuration enabled a precise analysis of the actual discrepancy between the signal measurements of the legitimate communication partners and the potential attacker. The chosen short distance of a maximum of 1 m represents an optimal case for an attacker, as maintaining such a close position undetected would be extremely difficult in real-world scenarios.

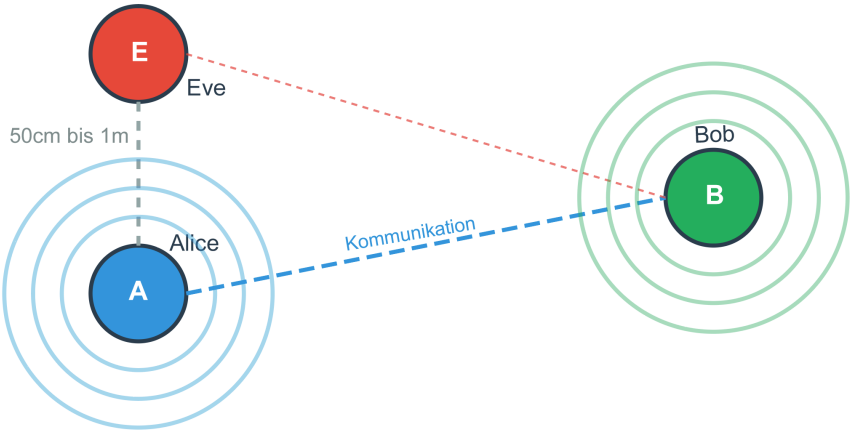



**Figure 5:** Measurement setup

By simulating these unrealistically favorable attack conditions, a conservative security assessment was achieved. If the system still functions securely under these ideal conditions for an attacker, security is all the more assured under realistic conditions—where an eavesdropper would be significantly farther away and less optimally positioned.

## *9.1 Measurement scenarios*

The following measurement scenarios were conducted:

**Static**

- Static systems without movement

**Movement within a building**

- Movement within the same room
- Movement across multiple rooms on the same floor
- Minimal movement in the adjacent room
- Fast/slow walking within the building across multiple floors

**Movement around the building**

- Movement around the building and at close range to the building

**Longer distances**

- Walking up to 1.2 km
- Running up to 800 m

**Vehicles up to 500 m**

- Driving away from the building
- Drive there and back
- Drive past

# 10 Evaluation of measurement data and methods

All previously performed measurements were tested using a wide variety of algorithm parameters, and the results were evaluated. This provided the project participants with information about the optimal operating parameters to be used in the final product.

### *10.1 Bits per measurement point, resolution*

A critical parameter is the number of bits to be generated per measurement point. This value reflects the resolution at which the Loess curve is viewed. A value that is too high causes even the slightest deviations between Alice and Bob to result in large differences in the raw key. This reduces the likelihood of being able to correct them all subsequently. A value that is too low significantly increases the resolution and allows attackers to guess the key.

- 2 bits per measurement point: Considered the lower limit, as the error rate remains tolerable here and the key is sufficiently secure
- 3–4 bits per measurement point: Represents the optimal operating range, in which a balanced ratio between key generation rate and error rate is achieved
- >4 bits per measurement point: Leads to an exponentially increasing error rate and is therefore usually unsuitable for practical applications

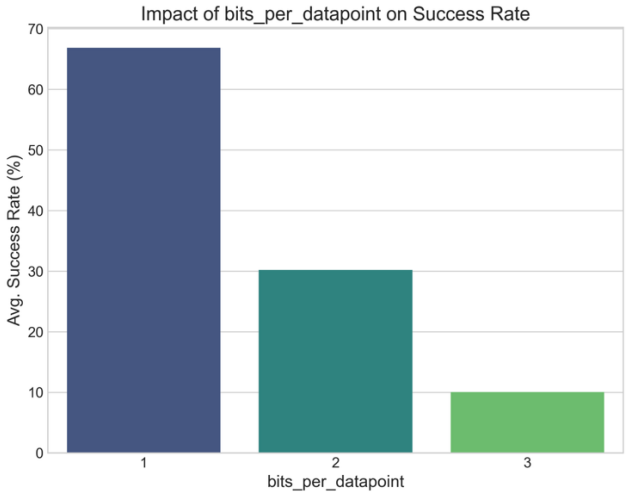



**Figure 6**: Bit resolution

## 11 Cascade Error Correction

The Cascade Error Correction algorithm is adaptive and automatically adjusts to the expected error rates of the raw key. At higher expected error rates, Cascade performs more iterations with finer block sizes. This increases the probability of identifying and correcting all discrepancies between Alice and Bob.

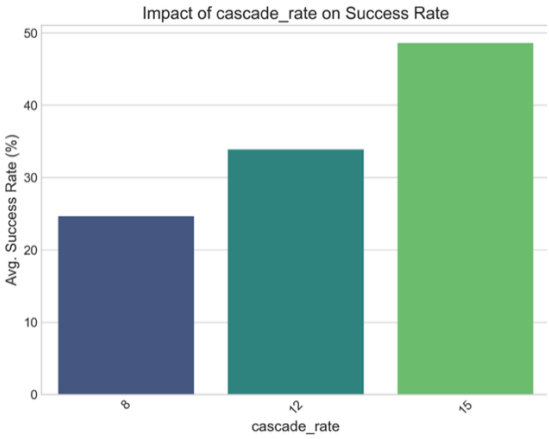



**Figure 7**: Cascade assumed error rate

However, this increased correction accuracy is not always optimal. Each additional iteration and each finer block division requires more parity information, which must be exchanged via the public channel between Alice and Bob. A passive attacker (Eve) eavesdropping on this communication can reconstruct parts of the raw key from these parity bits.

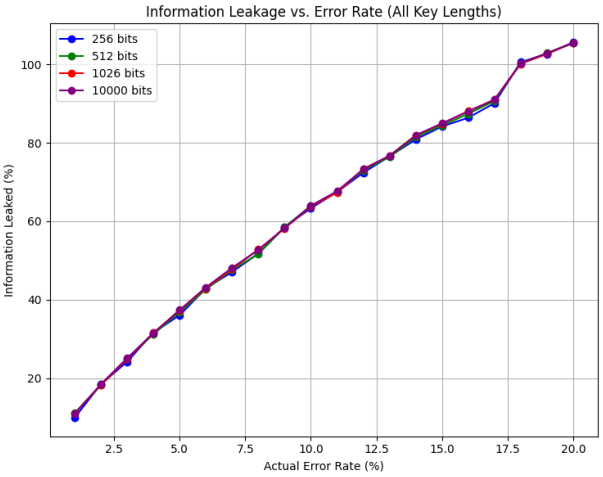



**Figure 8**: Information loss to third parties

The analysis showed that an expected error rate between 10% and 15% should be considered optimal for the system. These values offer the best compromise between correction efficiency and information leakage to third parties.

One initially counterintuitive aspect of the system is its tolerance for the large number of publicly disclosed bits. In fact, it does not pose a security problem if up to 80% of the original key material is publicly communicated during cascade correction. This robustness stems from the information-theoretical foundations of privacy amplification. The following example calculation illustrates this:

- Raw key: $n = 2000\ Bits$
- Publicly transmitted bits: $n \times 80\% = 1600\ Bits$
- Bits never transmitted: $v = n\ \times 20\% = 400\ Bits$
- Security margin: $s = 50\ Bits$

$$Sicherer\ Schlüssel = n - v - s = 2000 - 1600 - 50 = 350\ Bits$$

Even an attacker with knowledge of over 1600 bits of the original key material cannot draw any conclusions about the final 256-bit key. This property is based on the information-theoretical guarantees of the Leftover Hash Lemma and ensures that the remaining entropy is fully extracted into the secure key.

## 12 Key Generation Methods

Many of the initially implemented key generation methods failed in the early evaluation phases due to insufficient performance or practical limitations. The most promising methods that successfully passed the initial evaluation were subjected to a detailed performance analysis. This investigation revealed that the performance of the remaining candidates was nearly identical. The grid method showed a 5% higher probability of successful key generation. Therefore, it was ultimately selected.

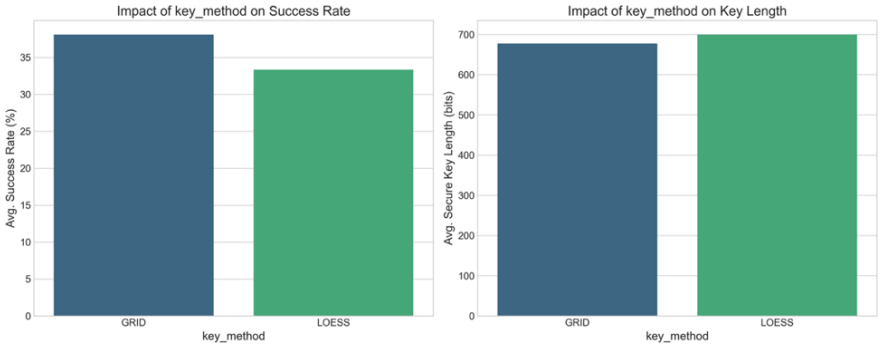



**Figure 9**: Comparison of Key Generation

## 13 Attacker (Eve) Analysis

For each measurement performed, Eve also generated a raw key based on her RSSI measurements. This was then compared with the keys from Alice and Bob to quantitatively assess the system's security. The analysis shows a statistically significant difference between the bit error rates of the legitimate communication partners and the attacker for both the 2-bit and 3-bit resolutions.

On average, Eve exhibits a bit error rate that is two to three times higher than that of Alice and Bob. This discrepancy confirms the theoretical expectations regarding the locality of the channel characteristics. Eve's increased error rate demonstrates that, despite optimal attack conditions (50 cm to 1 m distance, stationary position), the spatial decorrelation of the radio channel is sufficient to create an effective security barrier. The farther Eve is from Alice and Bob, the less her measurements correlate with the legitimate key material.

For the correct interpretation of the following graphs, note that a 50% bit error rate means that Eve's key is statistically indistinguishable from a randomly generated key. A 100% error rate would mean that Eve's key is perfectly anticorrelated. Eve could then invert all bits and obtain the correct key. This would be just as dangerous as a 0% error rate.

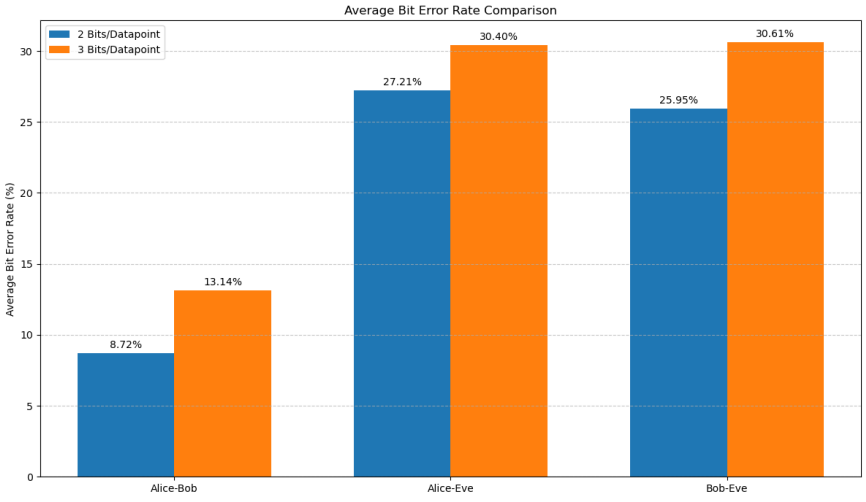



**Figure 10**: Comparison of error rates among three parties

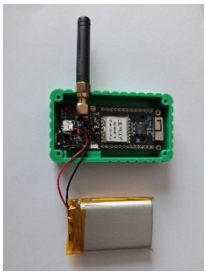
## 14 Product

Based on preliminary developments from two research projects, two software development projects were carried out in the RKD project after the appropriate components were selected. The resulting RKD software is user-friendly and can be operated without extensive technical knowledge. In the RKD product, two LoRa modules—both battery-powered and sourced from the global market—continuously collect measurement data whenever the distance permits. After any given period, users connect the RKD devices to a computer running the RKD software. The software then uses the collected measurement data to generate and distribute cryptographic keys, making them available to the user. A minimum key length of 256 bits has been defined, as this is considered quantum-computer-secure when combined with the AES-256 algorithm.

This means that the RKD product provides a fully functional RKD device, including software for both computers (Alice and Bob), which generates secure cryptographic keys on both sides of the communication via RKD (Radio-signal Key Distribution). These generated keys can then be reused for a wide variety of cryptographic applications.

The insights gained during the RKD project also open up interesting prospects for further research. In particular, a solution for key generation using satellite transmissions remains a promising field of research. The broad foundation of fundamental knowledge on secure key generation established by this project provides a solid basis.

With the present RKD device and RKD software, a product is now available for the global market for the first time. insitu software gmbh, which carried out the entire development, will offer the product on the global market starting in 2026. One of the main advantages of this solution is the separation between LoRa-based channel exploration and the rest of the key agreement protocol.



As a result, a battery-powered LoRa microcontroller responsible for the measurements can be carried by a person or even attached to a moving vehicle, for example, which improves the randomness of the keys. Key generation itself occurs automatically after users have uploaded their measurements to end devices (laptops, desktops, tablets, IoT devices) and/or servers.

## 15 Costs

The cost of RKD in the terrestrial domain using LoRa modules, as in the RKD device used here, is low due to the inexpensive, commercially available mass-market components:

- LoRa modules: $20–$50, SDR for longer ranges: up to $1,500
- Antenna, power supply, enclosure, small parts (voltage regulator, LED indicators, switches, USB port, etc.), and PCB: $40–$100
- RKD software: Due to the currently low production volume, prices here are still significantly higher, especially if certification is also required. The RKD software is customized for specific applications as needed.

## 16 Applicability in Various Wireless Technologies

This chapter discusses the applicability of RKD in various wireless technologies such as 5G, Wi-Fi, ZigBee, and LoRaWAN.

Current cellular wireless technologies such as LTE and 5G use two operating modes for transmitting data from a user device to a base station (uplink communication) and from a base station to a user device (downlink communication). The most popular is so-called Time Division Duplex (TDD), in which wireless channel access is divided into fixed time slots for uplink and downlink messages. While this mode is well-suited for RKD, since the user and the base station measure the characteristics of the same channel, the temporal separation in bidirectional communication can lead to discrepancies in the measurements, which ultimately complicates key extraction.

The alternative operating mode is frequency-, known as frequency- (FDD). Here, two different frequencies are assigned for uplink/downlink communication, meaning that a user and a base station measure the channel characteristics of two different channels. In some cases, however, when the frequency spacing between the channels is not too large—e.g., 1–10 MHz—the uplink and downlink measurements are close enough to each other to allow for key extraction. Another advantage of 5G is the use of advanced antenna techniques such as massive multiple-input multiple-output (MIMO) techniques. Such antenna systems can increase the speed of cryptographic key generation and improve privacy by making passive eavesdropping attempts more difficult.

Unlike public cellular networks, private and public wireless technologies designed for the Internet of Things offer greater potential for security applications based on RKD. Short-range protocols such as Wi-Fi, ZigBee, and Bluetooth, as well

as long-range technologies such as LoRaWAN, are suitable for this purpose. The former protocols are primarily found in portable devices and home automation products, such as smart gadgets and low-cost sensors, while long-range wireless technologies are more popular in smart city applications that require robust connectivity over greater distances. Among short-range technologies, Wi-Fi has become the most widely adopted in experimental research on wireless key agreement.

Due to low communication latency, message exchange during RF channel measurements is typically fast enough for two communicating devices to achieve a high degree of similarity during the channel measurements. Another advantage of Wi-Fi-based key agreement is a high key bit generation rate of up to 10–100 bits/s [Liu13].

However, the limited communication range of between 20 and 100 m restricts the potential applications of Wi-Fi-based key agreement. To increase the achievable range, several studies have been conducted using long-range wireless protocols. In [Ruo20], key agreement distances of one to seven kilometers were achieved using LoRa and LoRaWAN technologies. Due to LoRa's lower signal rates, key bit generation rates are typically around 1–10 bits/s. However, given the wide availability of development tools and the ability to operate on unlicensed RF bands at no cost, prototyping security functions based on key agreement for IoT applications is straightforward.

From the perspective of wireless network architecture, a direct point-to-point path is desirable, for example, for two network users who wish to use RKD. However, since many wireless services are designed for multi-user operation, various network structures are available, such as access point/gateway-based structures in Wi-Fi/5G or mesh networks like those in ZigBee. Since wireless communication in such networks does not occur directly from user to user but via a network node, users measure the characteristics of two separate radio channels (i.e., the one between the user and the access point), leading to discrepancies in the generated keys.

Furthermore, a network administrator could potentially gain access to the secret channel measurements and thus gain access to the generated secrets. These issues could compromise the privacy of potential key agreement implementations. On the other hand, security applications in which a symmetric secret key is used to enhance network security itself, such as message integrity verification, are a viable option in access point-based networks. Practical methods for applying RKD to mesh networks are still the subject of ongoing research.

## 17 Known Vulnerabilities of RKD, Their Impact, and Countermeasures

In RKD, the attack vectors for the wireless generation and distribution of cryptographic keys are primarily located at the wireless physical layer. Here, a brief overview of known attacks, their impact on system security, and possible defense techniques is provided.

The most common attack vector, which is regularly examined in the technical literature, is eavesdropping. In this attack, an attacker named Eve installs a receiver unit near Alice and Bob's RF transceivers, hoping to measure channel characteristics similar to those of the legitimate users. Although such a setup rarely reveals the entire key to Eve, some poorly chosen key agreement parameters can lead to the disclosure of the entire key.

For example, if Alice and Bob agree on an error correction capacity that is much higher than the actual number of bit errors to ensure that all keys match, Eve might be able to recover the final key from her noisy measurements as well. However, this attack is difficult to carry out in practice because Alice or Bob, or both, are at least partially in motion (without motion, no key generation occurs, or only very little).

Another vulnerability lies in a poorly implemented key agreement combined with RF measurements with low randomness. For example, Alice and Bob can sometimes measure a long sequence of individual RSSI values very well when the RF channel is not subject to changes. By applying a simple quantization rule, Alice and Bob derive keys with low randomness that consist mainly of ones or zeros. Therefore, Eve can simply assume that some of the generated keys follow very simple patterns of ones and zeros, and ultimately guess some of the extracted keys.

This attack scheme can be extended to a more sophisticated brute-force attack, in which an attacker with access to substantial computational resources can try out multiple key bit patterns within a reasonable amount of time. This attack is effectively ruled out in practice in at least one of the two solution variants selected in the RKD product (see above), because the three countermeasures listed below have been effectively implemented.

The most effective countermeasures against low randomness, eavesdropping, and brute-force attacks are: 1) moderate use of error correction, 2) rejection of measurements with low randomness (i.e., measurements with little or no dynamic range), and 3) use of privacy amplification.

More advanced attacks include the direct manipulation of measurements at the physical layer of the wireless network.

For example, an attacker can block the original channel measurement messages using broadband interference while simultaneously sending forged messages with controlled transmit power to Alice and Bob. In the worst case, an attacker can thus

send the entire key to legitimate users and later use it to eavesdrop on or manipulate the target application. This type of active attack can be prevented by using an authenticated wireless connection for channel measurements, which was also implemented in the present RKD product.