Chapter 4
RKD (Radio-Signal Key Distribution)

RKD (radio-signal key distribution) is a physical method for the secure generation and distribution of cryptographic keys. RKD uses radio signals above 30 MHz to calculate and distribute the keys and is known in the literature under various names, e.g., "physical layer key generation in wireless networks" or "wireless physical layer key agreement."

RKD exploits the unique physical properties of wireless radio channels. The method is based on two fundamental properties of high-frequency transmission: the inherent unpredictability (randomness) of channel properties and the reciprocity of radio transmission between two communication partners.

4.1 How Cryptographic Keys Are Generated and Distributed

The basic prerequisite for RKD is a direct bidirectional communication link between two wireless devices, as shown in Fig. 4.1. In everyday use, this type of communication mode is often referred to as ad hoc communication, as in WLAN networks, or simply as peer-to-peer communication. For simplicity, these two wireless devices will henceforth be referred to as Alice and Bob. While these two devices exchange wireless packets, the RF receivers [WP-RF][1] on both sides measure the characteristics of the RF channel, with the most common measure in the terrestrial domain being the received signal strength, or RSSI [WP–RSSI][2] for short. After a certain communication time, Alice and Bob have collected RF channel measurements that are *random* and show a high degree of *similarity*.

[1] https://en.wikipedia.org/wiki/High_frequency.

[2] https://en.wikipedia.org/wiki/Received_signal_strength_indicator.

E. Piller and H. Schölnast, *Data Encryption at the Intersection of Mathematics and Physics*, SpringerBriefs in Information Security and Cryptography,
https://doi.org/10.1007/978-3-032-24764-3_4

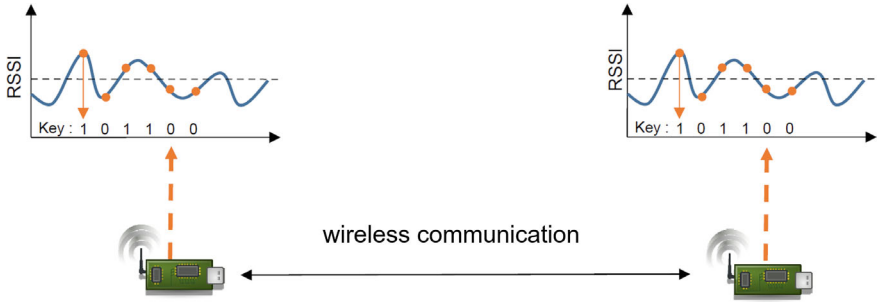

Fig. 4.1 Wireless communication

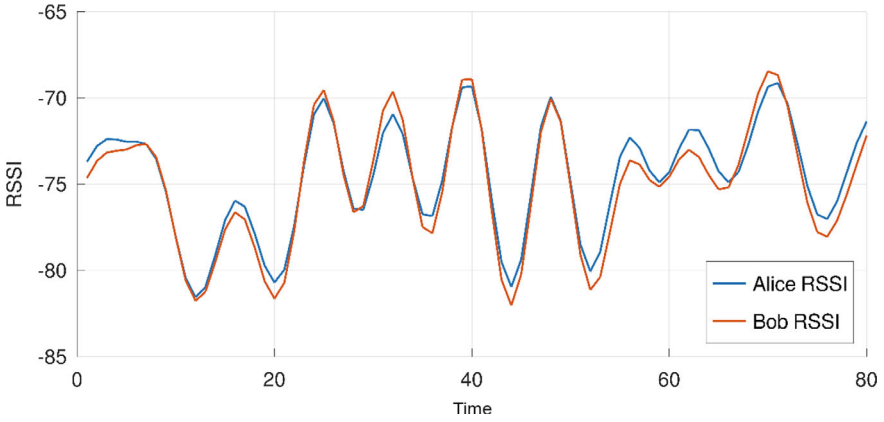

Fig. 4.2 Randomly fluctuating RSSI values for two wireless devices communicating directly with each other

Due to the similarity (see Fig. 4.2), such measurements can be converted into random bit sequences for both Alice and Bob, which differ by only a few bits. After performing error correction, Alice and Bob have the same random bit sequence, which can later be used as a secret cryptographic key on both sides. Cryptographic keys were generated and distributed based on physical properties.

The original idea of RKD dates back to 1993 [Mau93],[3] and some of the first demonstrations of its application to wireless channels took place in the early 2000s. Since the publication of this groundbreaking work, the rapid proliferation of wireless networks has led to extensive experimental research.

[3] https://doi.org/10.1109/18.256484.

4.1.1 Properties and Measurements of Wireless Channels

In order for two users to obtain similar channel measurements from which the secret key bits are derived, certain requirements must be met by a wireless channel and its measurements.

1. **The measurements must be unpredictable**. This guarantees strong, randomly generated keys that cannot be determined by an attacker. In a wireless channel, this randomness can occur in various ways. When an RF wave is transmitted from Alice's transmitting antenna, it is reflected and attenuated by various obstacles/materials, resulting in large fluctuations in the RF wave received by Bob's receiver. Thus, when Alice or Bob moves, the measured channel characteristics are subject to constant change, ultimately resulting in randomness of the secret keys. If there is no movement, changes in the environment, such as a moving object or person near a receiving/transmitting antenna, have a similar effect. In an urban environment with buildings, cars, etc., such effects are more common than in rural environments.
2. **The measured channel parameters for Alice and Bob must be nearly identical**. In point-to-point communication, i.e., when Alice talks directly to Bob and vice versa, the random channel properties are symmetric (reciprocal). In other words, reflections and attenuation are independent of the direction of propagation of the RF waves between Alice and Bob. Since Alice and Bob do not measure the channel at exactly the same time due to communication latency, their measurements show some discrepancies.
3. **An eavesdropper Eve must not be able to obtain measurements similar to those obtained by Alice or Bob**. This condition has been investigated experimentally, and it has been shown to hold true if Eve's location is at least more than a quarter of the wavelength away from both legitimate antennas (Alice's and Bob's) [Ruo18].[4] In practice, this means that for frequencies commonly used for RKD, starting at around 800 MHz, a wavelength of less than 375 cm and, consequently, a minimum distance of at least approximately 100 cm between Eve and Alice or Bob. Outside this range, i.e., at a distance of more than 100 cm from Alice and Bob—and while Alice or Bob (or both at the same time) are moving for several minutes—Eve's chances of extracting the legitimate key are practically the same as for a key generated by random guessing. At higher radio frequencies, Eve can even get closer to Alice or Bob.

As for the measurements themselves, Alice and Bob must set up a rapid exchange of wireless messages, e.g., a query from Alice to Bob and an immediate confirmation from Bob to Alice. Depending on the movement of their transceivers, the time that elapses between the two messages must not exceed a certain limit. For example, at a walking speed of 2–5 km/h, a few milliseconds are tolerable, while at speeds of moving cars (approx. 50–100 km/h), the time window for measurement is reduced

[4] https://doi.org/10.1145/3230833.3232803.

to 50–500 µs. The more time spent exchanging messages, the greater the deviation between measurements, which later leads to bit errors in the key extraction phase. It is therefore common practice to use very short user-defined wireless payloads for measurements. In addition, the center frequency for communication should be set to a fixed value, such as a specific Wi-Fi channel, in both directions.

In modern RF transceivers (WLAN/LoRa/Bluetooth), the most commonly available channel measurement is the received signal strength indicator (RSSI). It is typically calculated from the digitized RF waveform amplitude at the RF receiver and made available for each individual radio packet. The main advantage of RSSI is that it is easily accessible, as almost every radio equipment manufacturer provides RSSI querying as part of the device drivers. On the other hand, many RSSI measurements are typically required to extract a single secret key, as a single RSSI measurement corresponds to approximately one key bit. To increase the key generation rate, wireless technologies that use broadband signals such as Wi-Fi offer an alternative measurement called channel state information (CSI) [WP–CSI].[5] The original intended use of CSI is to enable an RF receiver to correct for random noise in the received signal. Since CSI contains finer amplitude information over a large bandwidth, e.g., 20 MHz, more key bits can be generated per measurement.

To provide insight into what measurements look like in real-world situations, three different RSSI curves from Alice (blue line) and Bob (red line) are shown here. In the first diagram (Fig. 4.3), Alice and Bob are stationary and their RF channel characteristics do not change. Therefore, the measurements revolve around a single RSSI value that has virtually no randomness. Keys derived from such measurements can be easily guessed by an attacker because they consist of long strings of zeros and ones. The second diagram (Fig. 4.4) shows measurements with good randomness, but the individual RSSI values between Alice and Bob differ from each other. Such deviation can be caused by rapidly changing RF channel conditions (e.g., due to rapid movement) or by noise at Alice and Bob's RF receivers. Although such deviations in the measurements can be corrected digitally to a certain extent, their presence can lead to errors in the extracted key bits, ultimately causing the key agreement to fail because the keys at Alice and Bob are not the same. Finally, Fig. 4.5 shows RSSI values that exhibit a high degree of randomness and similarity. Such measurements are best suited for key agreement because the resulting keys are random and contain few bit errors.

4.1.2 Physical Principles of Randomness

The randomness required for key generation arises, for example, when using signal strength due to continuous fluctuations in signal strength caused by a variety of physical factors:

[5] https://en.wikipedia.org/wiki/Channel_state_information.

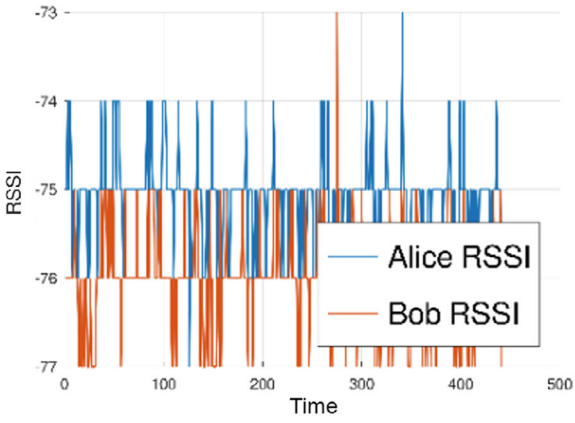

Fig. 4.3 RSSI when Alice and Bob are stationary

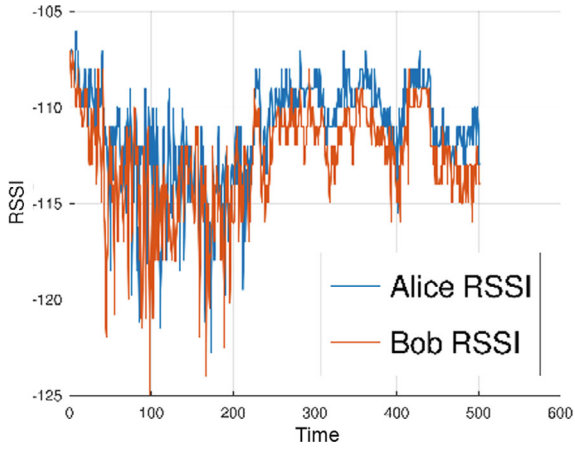

Fig. 4.4 RSSI when moving too fast

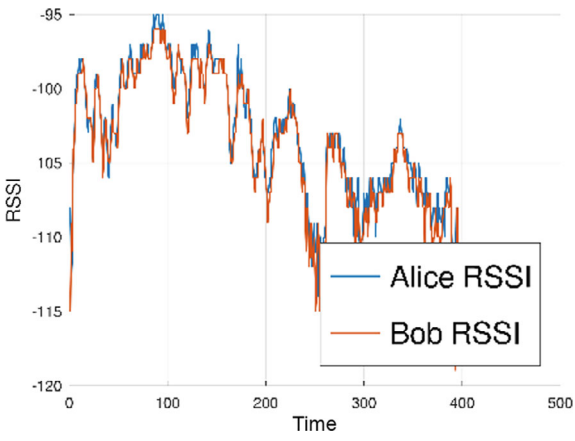

Fig. 4.5 RSSI under optimal conditions

- **Movement of Communication Devices**: Even minimal changes in position (a few centimeters) lead to measurable changes in signal strength due to altered interference patterns.
- **Dynamic Environmental Influences**: Moving devices in the radio field, such as people, vehicles, or swaying vegetation, continuously change the propagation conditions.
- **Reflection Behavior**: Changing reflections on walls, buildings, and other surfaces create complex interference patterns and thus affect signal quality.
- **Atmospheric Conditions**: Humidity, temperature, and other meteorological parameters influence radio propagation.
- **Electromagnetic Interference**: Other radio signals and electromagnetic interference create additional variability.

A cryptographic key can be calculated from these purely physical changes. The decisive advantage is that both communication partners measure the same physical conditions and can thus arrive at identical key material, while this information is not accessible to outside third parties.

The security of RKD is based on the fundamental physical principle that radio channel properties are highly location-dependent. A potential attacker (Eve) located, for example, one meter away, measures significantly different values due to the spatial decorrelation of the radio channel and therefore cannot obtain any usable information about the generated key.

The spatial diversity of the transmission and the random movement patterns create a natural source of randomness that virtually eliminates man-in-the-middle attacks.

4.1.3 Dynamic Requirements

Successful key generation requires a certain degree of dynamics in the transmission path. This occurs naturally due to changes in the distance between communication partners, movements in the environment, or changing reflection conditions. In static scenarios, this dynamic must be generated artificially in some cases, e.g., through controlled movement of one of the devices or through the use of reconfigurable antennas.

4.1.4 Summary of Findings

In RKD, two communication devices (Alice and Bob) transmit radio signals with frequencies of at least 30 MHz (usually above 800 MHz) in both directions and continuously measure the received signal characteristics. Typically, the signal strength (RSSI), phase angle, or signal propagation time are recorded. Since signal strength is usually measured in direct radio (free-space) channels, this text refers to signal

strength. An exception to this is the application with satellite connections, where signal strength can only be used for key exchange between Earth and satellite because the satellites amplify the signals with their transparent transponders.

The central principle lies in the reciprocity of the radio channel: since both devices use the same physical transmission path, they measure almost identical channel characteristics. These common measurements form the basis for generating identical cryptographic keys on both sides without having to exchange this information via a separate channel. With RKD, identical non-deterministic random numbers are generated on both sides (at Alice and Bob), which derive their entropy directly from the physical properties of the radio transmission.

RKD thus generates and distributes keys between two sides based on physical processes. These measured radio channel parameters are only available to the two devices involved in the transmission and cannot be measured by a third party (the eavesdropper, Eve). Changes in the measurements are mainly caused by the dynamics of the transmission path (changes in distance, reflections, etc.), which must be generated artificially in some cases when the devices are stationary. In the case of satellite connections, the dynamics result from the movement of the satellites in the LEO range (at an altitude of approx. 1000 km), which, however, can cause quality problems later on due to randomness. RKD is not well-suited for direct communication via a satellite because signal strength cannot be used as a signal property and the satellite always acts as a man-in-the-middle. Using runtime measurements as a signal property is hardly sufficient to defend an attacker. However, RKD could represent a cost-effective alternative to QKD for direct satellite communication between satellites and Earth, because MKD (see Chap. 5) is not applicable here and signal strength can be used as a signal property.

The advantage of RKD lies primarily in its cost and robustness, especially for moving devices. The necessary transmitting/receiving stations are available on the market at low cost as SDR (Software Defined Radio [WP–SDR][6]). These devices can be used not only for radio transmission, but also for sufficiently accurate measurements.

In contrast to free-space and satellite QKD, atmospheric influences such as aerosols, fog, clouds, etc. do not hinder or prevent key generation in RKD, but are part of the key generation process because the key is determined, among other things, from the changing attenuation.

The disadvantage of RKD is the extremely slow key generation resulting from the dynamic requirements. A maximum of a few bits per second are possible. However, this is sufficient for using AES-256 for data encryption and/or for a MAC calculation for integrity assurance. The same applies to the four new encryption methods/modes described in Sect 6.4.

[6] https://en.wikipedia.org/wiki/Software-defined_radio.

4.2 Practical Criteria

4.2.1 Economic and Technical Advantages

RKD offers exceptionally low equipment costs and very high system robustness for mobile applications. The hardware required for RKD is based on commercially available LoRa modules [WP–LoRa][7] or software-defined radios (SDRs), which are available from around $250, including power supply, housing, and software. These cost-effective components enable both radio transmission and precise recording of the channel measurements required for key generation, right through to the cryptographic key. In terms of hardware, RKD only contains robust mass-produced components from the global market, which has a very positive effect on the price, availability, deliverability, maintenance, service, and manufacturer or supplier changes.

RKD is particularly well-suited for use in mobile devices such as transport infrastructure (road, rail, water, air), mobile IoT devices, drones, military units, laptops, etc. No additional non-deterministic random number generator is required because the randomness is derived from the random measured values.

For applications with extended range requirements via satellite connections, the system costs rise to several thousand dollars per terminal, as additional signal amplifiers and high-quality antennas are required. However, the satellite-based infrastructure is already in place, as only transparent transponders are needed in LEO and GEO satellites, which already exist, meaning that no new infrastructure is required in space. However, there is still insufficient scientific, technical, and practical knowledge about RKD in conjunction with satellites.

RKD thus enables the cost-effective and mass-market-ready random generation and highly secure distribution of symmetric keys based on physical processes, followed by end-to-end data encryption.

4.2.2 System Limitations

The main limitation of RKD is the low key generation rate, which is limited to a maximum of 2–8 bits per second due to the nature of the system. This limitation results from the dynamic requirements of the system and the necessary correlation time between channel measurements. This rate is sufficient for symmetric encryption methods such as AES-256 or Message Authentication Code (MAC) calculations. However, it is not sufficient for a one-time pad, for which RKD is not suitable.

[7] https://en.wikipedia.org/wiki/LoRa.

4.2.3 Application Domains and Areas of Use

RKD is particularly suitable for applications with existing mobility, as the system requires channel dynamics for key generation. Primary areas of application include the following:

- **Transport Infrastructure**: road, rail, water, and air transport.
- **Mobile IoT Systems**: Mobile sensor networks and autonomous devices.
- **Unmanned Systems**: drones and autonomous vehicles.
- **Military and Security Applications**: Mobile communication units.

4.2.4 Security Considerations

The security analysis of RKD systems requires a differentiated consideration of various attack scenarios. Due to inherent measurement inaccuracies and the probabilistic nature of radio channel characteristics, passive man-in-the-middle attacks are theoretically possible if an attacker (Eve) can position themselves in a spatially optimal position relative to one of the legitimate communication partners.

For a successful attack from a distance (several meters away), an attacker would have to place at least three to four calibrated receivers in different spatial positions around Alice or Bob. This measurement at multiple points would be necessary to capture the three-dimensional components of the radio field distribution and to reconstruct the signal characteristics at the target location (Alice or Bob) using spatial interpolation. This scenario works without taking reflections into account, i.e., for example, in an open field without buildings, trees, etc.

The technical effort required for this attack is considerable: all receiving devices would have to be precisely synchronized in time, have identical calibration, and continuously determine their exact spatial positions relative to the target object. In moving scenarios—which are common with RKD—this complexity increases exponentially, as the entire measurement system would have to follow the movement in real time while maintaining spatial correlations. These practical limitations make coordinated spatial attacks in real environments, especially when reflections occur, unfeasible, particularly in the typical mobility scenarios for which RKD is primarily designed.

Experimental validations under controlled conditions have shown that even at distances of 50 cm to 1 m between Eve and the legitimate communication partners, significant spatial decorrelation of the channel measurements occurs. In these worst-case scenarios, Eve exhibits a two to three times higher bit error rate compared to Alice and Bob, confirming the locality of the channel characteristics.

Privacy amplification methods based on the leftover hash lemma offer information-theoretical security even in the event of partial compromise of the raw key material. An initially counterintuitive aspect of the system is its tolerance for a 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 results from the information-theoretical foundations of privacy amplification. The following example calculation illustrates this:

- Raw key: $n_{raw} = 2000\ Bits.$
- Publicly transmitted bits: $n_{pub} = n_{raw} \times 80\ \% \ = 1600\ Bits.$
- Bits not transmitted: $v = n_{raw} - n_{pub} = 400\ Bits.$
- Security margin: $s = 50\ Bits.$
- Secure key: $n_{secure} = n_{raw} - v - s = 2000 - 1600 - 50 = 350\ Bits.$

Even an attacker with knowledge of over 1600 bits (80%) 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 completely extracted into the secure key.

In satellite-based RKD implementations, the satellite acts as a transparent repeater that amplifies and retransmits received signals. By definition, this represents a man-in-the-middle scenario, making the trustworthiness of the satellite infrastructure a system requirement.

Alternative security architectures can address this problem by restricting secure communication to direct satellite-ground station connections, with end-to-end security between terrestrial endpoints ensured by downstream cryptographic protocols.

4.2.5 Market Readiness

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 there is extensive scientific literature available, only a single commercial product could be identified that enables RKD to generate and distribute cryptographic keys for end users. (Manufacturer: insitu[8]) This means that RKD lacks practical, marketable solutions. As part of this book, extensive practical tests were carried out with this single RKD product on the market in order to obtain practical data in real environments. This product is a LoRa-based RKD system and includes a complete implementation, whereby the LoRa modules autonomously collect measurement data and, after connection via the USB interface, e.g., to a laptop, RKD software, which is also part of the solution, performs key generation. The RKD hardware is housed in a small enclosure (see Fig. 4.6), is mobile, very robust, and contains a battery in addition to a USB interface for key delivery. When connected to a laptop, for example, the RKD device continuously generates key bits as soon as it is in motion (e.g., when the laptop user is on the move). When the laptop is in use, which usually happens when it is stationary, the RKD device again supplies new key material. The inner workings of the RKD device can also be integrated into other devices (e.g., IoT devices, drones, etc.)—it consists

[8] https://www.insitu.software.

Fig. 4.6 RKD device

exclusively of globally available mass-market products—or connected to mobile devices in its current form.

The software is available in two versions, which pursue different approaches. Since the current state of research covers many different approaches (see Sect. 1.8; literature analysis), all of which have their advantages and disadvantages depending on the application environment, but which are often only recognizable to a limited extent in the publications, two approaches were selected for the RKD product.

In relation to this book, this means that the extensive practical tests could be designed to be somewhat broader, resulting in even better practical data in real environments. Based on the literature analysis, this was only possible to a limited extent and with great uncertainty.

The introductory text on RKD only provided a general description of this technology. Readers who would like to learn more about how RKD works and do not want to work through the extensive scientific literature can find a more detailed description on the book's website at.[9]

4.2.6 Distance

The distance is limited to around 15 kilometers for direct radio-based RKD systems, although much greater distances are possible under excellent conditions. The LoRa-based system available as a product can reach up to several kilometers with good line of sight, although the distance is limited by the transmission power and technology standards permitted in the respective region. The range limitations result from several regulatory and technical factors: LoRa modules operate in the license-free ISM band (e.g., 863–870 MHz in Europe) [WP–ISM][10] with a maximum effective transmission power of 25 mW ERP [WP–ERP][11] according to EU regulations. This

[9] https://cryptography.study/phys/RKD.

[10] https://en.wikipedia.org/wiki/ISM_radio_band.

[11] https://en.wikipedia.org/wiki/Effective_radiated_power.

power limitation, combined with the precision of RSSI measurements required for RKD, significantly limits the practical range. Theoretically, ranges of up to 5 km are possible with high-quality antennas and optimal propagation conditions, but this reduces the measurement accuracy of the signal strength, which is essential for key generation. The spatial correlation of channel characteristics between Alice and Bob decreases with distance, causing the error rate in key generation to increase exponentially. The documented LoRa distance record is 1336 km (achieved on the open sea under perfect propagation conditions). It is not verifiable whether there would be sufficient RSSI fluctuations at such extreme distances to derive secure keys.

The ranges can be significantly improved by using more expensive SDRs (software-defined radios) instead of LoRa modules, but this also increases the cost of the RKD device.

LEO satellite connections enable global ranges of several thousand kilometers between any two points on Earth. However, for key generation, both communication partners must be able to connect via a satellite in both directions at roughly the same time, which limits the duration of the satellite connection and thus the key generation, as well as the maximum distance between the two communication partners. Furthermore, security risks arise because the satellite acts as an unavoidable man-in-the-middle and requires the trustworthiness of the satellite infrastructure. In practice, this means a connection time of around 5–15 min per satellite overflight for LEO satellites (approx. 1000 km flight altitude).

4.2.7 Cost

The costs of RKD in the terrestrial sector with LoRa modules, as used in this RKD device, are low due to the inexpensive, commercially available components on the mass market:

- Hardware: Approx. $60 to $150, for longer ranges up to $1500 (for details, see the book's website at[12]).
- RKD Software: Due to the currently low number of units, higher amounts are still required here.

4.2.8 Compatibility

Since RKD has currently only been implemented by individual research groups and a single provider, there is no established compatibility between different systems. Each implementation uses proprietary methods/technologies for synchronization, key generation, error correction, and verification.

[12] https://cryptography.study/phys/RKD.

Only the hardware components that make up the RKD hardware are mass-produced goods from the global market. They therefore do not pose a compatibility problem. The compatibility problem only applies to the RKD software. The RKD software does not run on the RKD hardware and can therefore be easily replaced.

4.2.9 Robustness/Susceptibility to Interference

RKD is highly resistant to temperature fluctuations, shocks, moisture, etc., because the hardware does not contain any mechanical components. RKD therefore does not require any maintenance of the devices, which is always security sensitive. If an RKD device ever breaks down, it can be easily and inexpensively replaced with a new one. The compatibility of the hardware also makes it easy to change manufacturers. This means that the devices can be easily replaced with other models or by other manufacturers/suppliers.

4.2.10 Suitability for Mobile End Devices

RKD systems are perfect for mobile applications, as dynamics in the system are a fundamental prerequisite for key generation. These dynamics are created by signal variations that must be generated by at least one moving communication partner. In satellite systems, this is done by the satellite itself through its orbit. The laptop example described above shows that RKD devices can generate key bits even when the device is switched off during movement because it is supplied with the necessary energy by its own battery.

4.2.11 Standardization

There is currently no formal standardization initiative for RKD technologies, and none is expected in this decade. The external interface of the only product available is a standardized USB interface. Only hardware parts from the mass market are used (the user can therefore easily exchange and replace components).

4.2.12 Certification

Certification according to [EUCC][13] is currently being prepared for the first available product.

4.3 Advantages/Disadvantages of the Technology

The main advantages are low cost and suitability for mobile applications. The technology is based on mass-market hardware.

The main disadvantages of RKD are the mandatory dynamics, the short range, and the low number of key bits per second. A maximum of 2–8 bits per second limits its applicability to mathematical encryption methods (e.g., AES-256). Long distances via satellite are conceivable, but there is no empirical data or results available yet.

4.4 Man-in-the-Middle Attacks

4.4.1 Passive Man-in-the-Middle ("Eve")

A passive eavesdropper (Eve) is theoretically able to reconstruct parts of the key material if specific spatial and environmental conditions are met.

- In urban scenarios and indoor scenarios with multiple reflective surfaces (buildings, vehicles, walls), Eve must position herself in close proximity (less than 1 m) to one of the legitimate communication partners. The complex multipath propagation patterns result in highly localized channel characteristics, whereby even small spatial distances lead to significant decorrelation. However, this condition is difficult to maintain in practice without being detected, especially if the key exchange partners move for several minutes, which is a prerequisite for key generation.
- In scenarios without significant reflections (open field, water), the requirements for Eve are less restrictive. Here, it is sufficient if the distance between Eve and one of the communication partners approximately corresponds to the distance between Alice and Bob (geometric equidistance). However, for the same reasons, an attacker can hardly maintain this state for a sufficiently long period of time.

In satellite-based RKD implementations, the satellite represents a man-in-the-middle due to the nature of the system, as it amplifies and retransmits received signals with its transparent transponder.

[13] https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en.

4.4.2 Active Man-in-the-Middle

An active man-in-the-middle can only be prevented by suitable authentication of both communication partners.

4.5 Protection Goals

4.5.1 Authentication

The same conditions apply to authentication as to QKD. RKD itself does not offer authentication of communication partners. This means that shared secrets must be used, and procedures such as the Wegman-Carter procedure [Weg81].

4.5.2 Integrity

The integrity of the key results from the algorithms used in RKD and the exchange of information between the two communication partners.

4.6 Special Challenges

The challenges lie in synchronizing the measurements between the communication partners, optimizing the parameters for different environmental conditions, and ensuring sufficient channel dynamics for continuous key generation. In addition, the complex signal and data processing steps (LOESS transformation, grid quantization, privacy amplification) require precise implementation and calibration for different application scenarios.

4.7 Brief Description of the Technology

RKD is a physical method for generating and distributing cryptographic keys that exploits the physical properties of radio channels. By measuring signal strength variations (RSSI) between two communication partners, identical random sequences are created, which are transformed into cryptographically secure 256-bit keys using algorithms (e.g., LOESS smoothing, grid quantization, cascade error correction, and Toeplitz-based privacy amplification). The system offers high security at low cost when implemented with mass-market radio modules.

4.8 Literature Analysis

RKD (radio signal key distribution) is referred to in various ways in the scientific literature, e.g., as "wireless physical layer key agreement."

If two communication partners in wireless transmission have access to a common random source, e.g., by measuring a changing channel state, they can agree on a secret key. In doing so, they convert their measured values into identical key bits. This method, also known as key agreement at the physical layer, has gained popularity, particularly in research on wireless communication security [Yener15,[14] Zeng15[15]].

The shared random source exploits two fundamental properties of radio channels: channel reciprocity and inherent unpredictability. These properties can be captured by wireless communication terminals. If an attacker does not have access to the shared measurements, they cannot extract any information about the secret keys. Security therefore lies not in assumptions, but in physical laws.

Current research on key agreement at the physical layer can be divided into five main categories:

1. Measurement techniques (not covered below).
2. Key generation algorithms.
3. Resistance to attacks.
4. Advanced key agreement methods.
5. Experimental validation efforts.

The following overview covers scientific work from the period 2007–2024.

4.8.1 The Four Basic Phases of Key Generation

The conversion of measured radio channel characteristics into secret key bits takes place in four basic phases:

- Channel exploration and synchronization.
- Key bit extraction.
- Error correction.
- Privacy enhancement.

4.8.2 Phase 1: Channel Exploration and Synchronization

In the first phase, the communication partners exchange short messages via the wireless channel and then measure the radio channel characteristics from the received signals. Various signal characteristics were examined for channel detection:

[14] https://doi.org/10.1109/JPROC.2015.2459592.

[15] https://doi.org/10.1109/MCOM.2015.7120014.

- Received signal strength (RSS) [Mathur08,[16] Premnath14,[17] Aono05[18]].
- Amplitude [Wilson07[19]].
- Phase angle [Mathur11,[20] Wang11[21]].
- Envelope [Azimi07[22]].
- Angle of arrival [Badawy15[23]].
- Time of arrival [Marino14[24]].
- Channel impulse response [Liu12[25]].
- Channel frequency response [Hon13[26]].

In addition, adaptive measurement strategies have been developed that automatically track changing channel conditions [Yas08[27]].

Since some wireless packets may be lost during channel measurements, Alice and Bob must first ensure that the individual measurements are present on both sides and that they are performed within the small measurement time window. Synchronization methods are helpful in ensuring this. The first option is to use counter values, whereby Alice adds a running integer to the channel measurement packet. If Bob can capture the packet, he stores his channel measurements along with the received integer and responds to Alice with the same integer value. Since Alice can capture Bob's packet, she now knows that she and Bob have both successfully performed a measurement, and the running integer is incremented by Alice. At the end of the measurements, Bob only needs to remove duplicate measurements, i.e., measurements associated with duplicate counter values.

Alternatively, a timestamp comparison can be used to achieve the same result. Here, Alice and Bob perform time synchronization before the channel measurements, e.g., via the Internet using an NTP server. First, a timestamp is added to each measurement value during the measurements. Bob then compares his timestamps with Alice's and discards values with large deviations. Bob informs Alice of the discarded values, whereupon Alice also removes the discarded values from her measurement set.

[16] https://doi.org/10.1145/1409944.1409960.
[17] https://doi.org/10.1145/2541289.
[18] https://doi.org/10.1109/TAP.2005.858853.
[19] https://doi.org/10.1109/TIFS.2007.902666.
[20] https://doi.org/10.1145/1999995.2000016.
[21] https://doi.org/10.1109/INFCOM.2011.5934929.
[22] https://doi.org/10.1145/1315245.1315295.
[23] https://doi.org/10.1109/VTCSpring.2015.7146072.
[24] https://doi.org/10.1109/ICUWB.2014.6958955.
[25] https://doi.org/10.1109/TIFS.2012.2206385.
[26] https://doi.org/10.1109/INFCOM.2013.6567117.
[27] https://doi.org/10.1109/ISITA.2008.4895646.

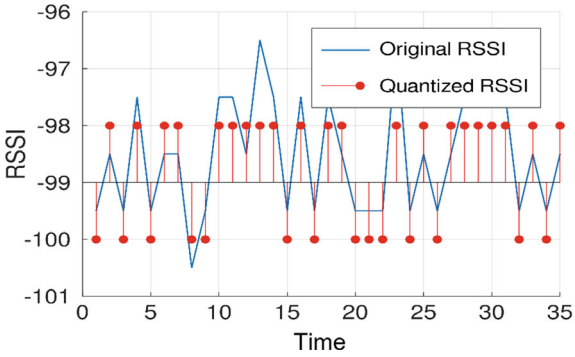

Fig. 4.7 1-bit quantizer

4.8.3 Phase 2: Key Bit Extraction

The actual process of converting RF measurements into binary values is called quantization. Here, Alice and Bob apply a quantization rule to the measured values, which converts them into secret key bits on both sides. One of the simplest rules compares a single measurement to a specified tolerance value. If a measurement is above or below the tolerance value, a key bit of one or a zero is generated. To illustrate the effect of this rule in practice, Fig. 4.7 shows a series of measured RSSI values and the corresponding quantized RSSI values after applying the above quantization rule.

On the other hand, slightly more sophisticated quantization algorithms can generate multiple bits per measurement and are robust against noise and distortion. The algorithms used include:

- Simple 1-bit quantizers with one threshold [Aono05[28]] or two thresholds [Mathur08[29]].
- Multi-bit quantizers [Patwari10,[30] Ambekar12[31]].
- Adaptive quantizers [Hamida09[32]].
- Vector quantization [Hong17[33]].
- Singular value decomposition-based quantizers [Furqan16[34]].

In addition, digital signal processing algorithms [Patwari10,[35] Yasukawa08[36]] can be used to reduce deviations between measured values caused by noise or hardware inaccuracies.

[28] https://doi.org/10.1109/TAP.2005.858853.
[29] https://doi.org/10.1145/1409944.1409960.
[30] https://doi.org/10.1109/TMC.2009.88.
[31] https://doi.org/10.1109/ISSSE.2012.6374318.
[32] https://doi.org/10.1109/NTMS.2009.5384826.
[33] https://doi.org/10.1109/TIFS.2017.2656459.
[34] https://doi.org/10.1109/ISWCS.2016.7600974.
[35] https://doi.org/10.1109/TMC.2009.88.
[36] https://doi.org/10.1109/ISITA.2008.4895646.

4.8.4 Postprocessing

Correction algorithms and privacy enhancements are then applied to ensure further error correction and resistance to eavesdropping attempts. After key bit extraction, Alice and Bob already have secret key bits that could be used for encryption and decryption. However, due to slight deviations in the measurements, some key bits on Alice's side do not match Bob's key bits. Error correction is therefore necessary. However, this reveals a small amount of information to Eve. This is counteracted by privacy amplification. For details on these procedures, see Sect. 8.3 Privacy Amplification.

Before the extracted key can be used in cryptographic algorithms, its quality, in particular the randomness of the bits, must be evaluated.

The statistical tests recommended by the US National Institute of Standards and Technology (NIST) [Rukhin10[37]] include the following:

- Mono-bit Frequency Test: Checks the ratio of zeros and ones in the key.
- Runs Test: Evaluates the independence of consecutive bit sequences.
- Spectral Test: Analyzes the discrete Fourier transform of the key stream.
- Additional tests have been developed specifically for wireless key generation:
- Maurer's Statistical Test: Particularly suitable for short key sequences [Maurer92[38]].
- Online Entropy Estimation: Designed for lightweight hardware implementations and directly monitors the randomness of channel parameters [Zenger16[39]].

4.8.5 Protection Against Attacks

More complex key generation schemes have been developed to improve resistance to various attacks. Works such as [Jana09,[40] Eberz12[41]] investigate the effects of passive and active man-in-the-middle attacks. In these scenarios, a skilled attacker takes control of the key generation process by manipulating channel conditions or injecting fake probing packets.

Similar attacks, including signal masking during channel reconnaissance and corresponding countermeasures, are discussed in [Zafer12[42]]. Further studies have shown that the so-called pilot randomization technique can successfully convert active signal injection attacks into less harmful reactive jamming attacks [Mitev19[43]].

---

[37] https://doi.org/10.6028/NIST.SP.800-22r1a.

[38] https://doi.org/10.1007/BF00193563.

[39] https://doi.org/10.1109/GLOCOMW.2016.7849064.

[40] https://doi.org/10.1145/1614320.1614356.

[41] https://doi.org/10.1007/978-3-642-33167-1_14.

[42] https://doi.org/10.1109/TNET.2012.2183146.

[43] https://doi.org/10.1109/GLOBECOM38437.2019.9013816.

This technique has also been recently investigated for advanced communication systems:

- Wireless relay communication [Letafati23[44]].
- Protection against attacks on smart reflective surfaces [Hu23[45]].

4.8.6 Advanced Key Agreement Methods

A second group of advanced methods aims to reduce the communication overhead during channel exploration. This is achieved through various advanced measurement techniques:

- Synchronized measurements in collaboration with wireless sensor networks [Premnath14[46]].
- Multiple-input multiple-output (MIMO) antennas for parallel channel detection [Wallace10[47]] and beamforming [Huang13[48]].

Both approaches have also shown improvements in key generation rates in static communication scenarios.

The MIMO concept was extended in [Jiao18[49]] to mm Wave massive MIMO configurations, as used in 5G networks. Here, angle-of-arrival interference leads to a significant increase in the secret key rate.

4.8.7 Modern Communication Technologies

Recent advances in wireless communication systems have been investigated to improve key generation:

Reconfigurable parasitic antenna arrays [Mehmood12[50]] and intelligent reflecting surfaces (IRS) can increase the randomness of channel measurements. One example is the electronically controllable parasitic array radiator antenna, which uses random beam steering for faster key generation [Aono05[51]].

Intelligent reflecting surfaces consist of large passive arrays of reflecting antenna elements and were originally used to increase channel capacity. As shown in [Ji21[52]],

---

[44] https://doi.org/10.1109/OJVT.2023.3315216.
[45] https://doi.org/10.1109/LWC.2023.3330809.
[46] https://doi.org/10.1145/2541289.
[47] https://doi.org/10.1109/TIFS.2010.2052253.
[48] https://doi.org/10.1109/INFCOM.2013.6567033.
[49] https://doi.org/10.1109/GLOCOM.2018.8647588.
[50] https://doi.org/10.1109/EuCAP.2012.6206173.
[51] https://doi.org/10.1109/TAP.2005.858853.
[52] https://doi.org/10.1109/TVT.2020.3045728.

appropriate control of the array elements can maximize the secret key capacity for users with single antennas, even in the presence of non-cooperative eavesdroppers.

This concept was extended to mmWave MIMO systems in [LiH23[53]], where IRS combined with compressive sampling outperformed conventional channel state-based methods at low signal-to-noise ratios.

4.8.8 Full-Duplex Transceivers

Wireless key generation has also been investigated for full-duplex transceivers—devices that enable simultaneous transmission and reception on the same channel [Vogt19[54]]. Under certain conditions, full-duplex mode reduces the ability of eavesdroppers to extract key material from legitimate parties, thereby strengthening attack resistance.

However, as shown in [Luo23[55]], the achievable key capacity and performance gains over half-duplex methods depend heavily on analog self-interference suppression.

4.8.9 Practical Applications

Various approaches have been developed to bring key agreement techniques closer to real-world applications:

- Low-power IoT Devices: Tailored solutions have been proposed in [Zenger14,[56] Zenger15[57]].
- Vehicle Systems: [Huth16[58]] developed key generation to secure vehicle communication.
- LoRaWAN Systems: For power-efficient wide-area networks, [Ruo20[59]] presented a reconfigurable antenna-based key transmission chain and provided extensive experimental results for indoor and outdoor scenarios.

[53] https://doi.org/10.1109/VTC2023-Fall60731.2023.10333834.
[54] https://doi.org/10.1109/TCOMM.2018.2868714.
[55] https://doi.org/10.1109/JSAC.2023.3287610.
[56] https://doi.org/10.1109/SIoT.2014.7.
[57] https://doi.org/10.1145/2841113.2841117.
[58] https://doi.org/10.1016/j.comnet.2016.06.014
[59] https://doi.org/10.1109/JIOT.2019.2946919.

References

[WP-RSSI] Wikipedia contributors, Received signal strength indicator, Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Received_signal_strength_indicator

[Mau93] U.M. Maurer, Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**(3), 733–742 (1993). https://doi.org/10.1109/18.256484

[Ruo18] H. Ruotsalainen, S. Grebeniuk, Towards wireless secret key agreement with LoRa physical layer, in *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES '18)*, (2018) https://doi.org/10.1145/3230833.3232803

[WP-CSI] Wikipedia contributors, Channel state information. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Channel_state_information

[WP-SDR] Wikipedia contributors, Software-defined radio. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Software-defined_radio

[WP-LoRa] Wikipedia contributors, LoRa. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/LoRa

[WP-ISM] Wikipedia contributors, ISM radio band. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/ISM_radio_band

[WP-ERP] Wikipedia contributors, Effective radiated power. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Effective_radiated_power

[EUCC] European Union Agency for Cybersecurity (ENISA). EUCC Certification Scheme (EU Cybersecurity Certification Scheme on Common Criteria) (certification library web page). No date. https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

[Weg81] M.N. Wegman, L. Carter, New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**, 265–279 (1981). https://doi.org/10.1016/0022-0000(81)90033-7

[Yener15] A. Yener, S. Ulukus, Wireless physical-layer security: Lessons learned from information theory. Proc. IEEE **103**(10), 1814–1825 (2015). https://doi.org/10.1109/JPROC.2015.2459592

[Zeng15] K. Zeng, Physical layer key generation in wireless networks: Challenges and opportunities. IEEE Commun. Mag. **53**(6), 33–39 (2015). https://doi.org/10.1109/MCOM.2015.7120014

[Mathur08] S. Mathur et al., Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel, in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom '08)*, (ACM, New York, NY, USA, 2008), pp. 128–139. https://doi.org/10.1145/1409944.1409960

[Premnath14] S.N. Premnath et al., Efficient high-rate secret key extraction in wireless sensor networks using collaboration. ACM Transactions on Sensor Networks **11**(1) (2014). https://doi.org/10.1145/2541289

[Aono05] T. Aono et al., Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Trans. Antennas Propag. **53**(11), 3776–3784 (2005). https://doi.org/10.1109/TAP.2005.858853

[Wilson07] R. Wilson, D. Tse, R.A. Scholtz, Channel identification: Secret sharing using reciprocity in ultrawideband channels. IEEE Trans. Inf. Forensics Security **2**(3), 364–375 (2007). https://doi.org/10.1109/TIFS.2007.902666

[Mathur11] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, N. Mandayam, ProxiMate: Proximity-based secure pairing using ambient wireless signals, in *Proc. 9th Int. Conf. Mobile Syst., Appl., Services (MobiSys)*, (Washington, DC, USA, 2011), pp. 211–224. https://doi.org/10.1145/1999995.2000016

[Wang11] Q. Wang, H. Su, K. Ren, K. Kim, Fast and scalable secret key generation exploiting channel phase randomness in wireless networks, in *Proceedings IEEE INFOCOM*, (Shanghai, China, 2011). https://doi.org/10.1109/INFCOM.2011.5934929

[Azimi07] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks, in Proceedings of the CCS '07. ACM, New York, NY, USA, 401–410, 2007. https://doi.org/10.1145/1315245.1315295

[Badawy15] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trinchero and C. -F. Chiasserini, Secret Key Generation Based on AoA Estimation for Low SNR Conditions. in 2015 IEEE 81st vehicular technology conference (VTC spring), Glasgow, UK, 2015. https://doi.org/https://doi.org/10.1109/VTCSpring.2015.7146072

[Marino14] F. Marino, E. Paolini, M. Chiani, Secret key extraction from a UWB channel: Analysis in a real environment, in *2014 IEEE International Conference on Ultra-WideBand (ICUWB)*, (Paris, France, 2014). https://doi.org/10.1109/ICUWB.2014.6958955

[Liu12] Y. Liu, S.C. Draper, A.M. Sayeed, Exploiting Channel diversity in secret key generation from multipath fading randomness. IEEE Trans. Inf. Forensics Secur. **7**(5), 1484–1497 (2012). https://doi.org/10.1109/TIFS.2012.2206385

[Hon13] H. Liu, W. Yang, J. Yang, Y. Chen, Fast and practical secret key extraction by exploiting channel response, in proceedings of IEEE INFOCOM. IEEE, Turin, Italy **3048–3056** (2013) https://doi.org/10.1109/INFCOM.2013.6567117

[Yas08] S. Yasukawa, H. Iwai, H. Sasaoka, Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM, in *Proceedings of the International Symposium on Information Theory and Its Applications, Auckland*, vol. 2008, (2008), pp. 1–6. https://doi.org/10.1109/ISITA.2008.4895646

[Patwari10] N. Patwari, J. Croft, S. Jana, 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). https://doi.org/10.1109/TMC.2009.88

[Ambekar12] A. Ambekar, M. Hassan, H.D. Schotten, Improving channel reciprocity for effective key management systems, in *Proceedings of the International Symposium on Signals, Systems, and Electronics (ISSSE)*, (Potsdam, 2012), pp. 1–4. https://doi.org/10.1109/ISSSE.2012.6374318

[Hamida09] S. Hamida, J. Pierrot, C. Castelluccia, An adaptive quantization algorithm for secret key generation using Radio Channel measurements, in *Proceedings of the 3rd International Conference on New Technologies, Mobility and Security*, (Cairo, 2009), pp. 1–5. https://doi.org/10.1109/NTMS.2009.5384826

[Hong17] P. Hong et al., Vector quantization and clustered key mapping for channel-Based secret key generation. IEEE Trans. Inf. Forensics Secur. **12**(5), 1170–1181 (2017). https://doi.org/10.1109/TIFS.2017.2656459

[Furqan16] H.M. Furqan, J.M. Hamamreh, H. Arslan, Secret key generation using channel quantization with SVD for reciprocal MIMO channels, in *2016 International Symposium on Wireless Communication Systems (ISWCS)*, (Poznan, Poland, 2016), pp. 597–602. https://doi.org/10.1109/ISWCS.2016.7600974

[Rukhin10] A. L. Rukhin & et al., A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, in Tech. Rep. of National Institution of Standards and Technology, Gaithersburg, MD, USA, 800–822, 2010. https://doi.org/https://doi.org/10.6028/NIST.SP.800-22r1a

[Maurer92] U.M. Maurer, A universal statistical test for random bit generators. J. Cryptol. **5**, 89–105 (1992). https://doi.org/10.1007/BF00193563

[Zenger16] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, The Passive Eavesdropper Afects My Channel: Secret-Key Rates under Real-World Conditions. In 2016 IEEE Globecom Workshops, 1–6, 2016. https://doi.org/10.1109/GLOCOMW.2016.7849064

[Jana09] S. Jana et al., On the effectiveness of secret key extraction from wireless signal strength in real environments, in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom '09)*, (ACM, New York, NY, USA, 2009), pp. 321–332. https://doi.org/10.1145/1614320.1614356

[Eberz12] S. Eberz et al., A practical man-in-the-middle attack on signal-Based key generation protocols, in *Proceedings of the 17th European Symposium on Research in Computer Security (ESORICS '12)*, (Springer, 2012) https://doi.org/10.1007/978-3-642-33167-1_14

[Zafer12] M. Zafer & et al. Limitations of generating a secret key using wireless fading under active adversary. IEEE/ACM Transactions of Networking, 20(5), pp. 1440–1451, 2012. https://doi.org/10.1109/TNET.2012.2183146

[Mitev19] M. Mitev, A. Chorti, E.V. Belmega, M. Reed, Man-in-the-middle and denial of service attacks in wireless secret key generation, in *2019 IEEE Global Communications Conference (GLOBECOM)*, (Waikoloa, HI, USA, 2019), pp. 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013816

[Letafati23] M. Letafati, H. Behroozi, B.H. Khalaj, E.A. Jorswieck, Learning-Based secret key generation in relay channels under adversarial attacks. IEEE Open J. Veh. Technol. **4**, 749–764 (2023). https://doi.org/10.1109/OJVT.2023.3315216

[Hu23] L. Hu, G. Li, A. Hu, D.W.K. Ng, Exploiting malicious RIS for secret key Acquisition in Physical-Layer key Generation. IEEE Wirel. Commun. Lett. (2023). https://doi.org/10.1109/LWC.2023.3330809

[Wallace10] J.W. Wallace, R.K. Sharma, Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis. IEEE Trans. Inf. Forensics Secur. **5**(3), 381–392 (2010). https://doi.org/10.1109/TIFS.2010.2052253

[Huang13] P. Huang, X. Wang, Fast secret key generation in static wireless networks: A virtual channel approach, in proceedings of IEEE INFOCOM. Turin, pp **2292–2300** (2013) https://doi.org/10.1109/INFCOM.2013.6567033

[Jiao18] L. Jiao, N. Wang, K. Zeng, Secret beam: Robust secret key agreement for mmWave massive MIMO 5G communication, in *2018 IEEE Global Communications Conference (GLOBECOM)*, (Abu Dhabi, United Arab Emirates, 2018), pp. 1–6. https://doi.org/10.1109/GLOCOM.2018.8647588

[Mehmood12] R. Mehmood, J.W. Wallace, Experimental assessment of secret key generation using parasitic reconfigurable aperture antennas, in *2012 6th European Conference on Antennas and Propagation (EUCAP)*, (Prague, 2012), pp. 1151–1155. https://doi.org/10.1109/EuCAP.2012.6206173

[Ji21] Z. Ji et al., Secret key generation for intelligent reflecting surface assisted wireless communication networks. IEEE Trans. Veh. Technol. **70**(1), 1030–1034 (2021). https://doi.org/10.1109/TVT.2020.3045728

[LiH23] H. Li, L. Chen, T. Lu, A. Hu, Angular-domain secret key generation for RIS-aided mmWave MIMO systems, in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, (Hong Kong, Hong Kong, 2023), pp. 1–6. https://doi.org/10.1109/VTC2023-Fall60731.2023.10333834

[Vogt19] H. Vogt, Z.H. Awan, A. Sezgin, Secret-key generation: Full-duplex versus half-duplex probing. IEEE Trans. Commun. **67**(1), 639–652 (2019). https://doi.org/10.1109/TCOMM.2018.2868714

[Luo23] H. Luo, N. Garg, T. Ratnarajah, A channel frequency response-Based secret key generation scheme in in-band full-duplex MIMO-OFDM systems. IEEE J Sel Areas Commun **41**(9), 2951–2965 (2023). https://doi.org/10.1109/JSAC.2023.3287610

[Zenger14] C.T. Zenger, M.J. Chur, J.F. Posielek, C. Paar, G. Wunder, A novel key generating architecture for wireless low resource devices, in *In 2014 International Workshop on Secure Internet of Things*, (2014), pp. 26–34. https://doi.org/10.1109/SIoT.2014.7

[Zenger15] C.T. Zenger, J. Zimmer, M. Pietersz, J.F. Posielek, C. Paar, Exploiting the physical environment for securing the internet of things, in *Proceedings of the 2015 New Security Paradigms Workshop*, (2015), pp. 44–58. https://doi.org/10.1145/2841113.2841117

[Hut16] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, T. Güneysu, Information reconciliation schemes in physical-layer security: A survey, in computer networks, 109, Part 1, 84–104, 2016. https://doi.org/https://doi.org/10.1016/j.comnet.2016.06.014

[Ruo20] H. Ruotsalainen, J. Zhang, S. Grebeniuk, Experimental investigation on wireless key generation for low-power wide-area networks. IEEE Internet Things J. **7**(3), 1745–1755 (2020). https://doi.org/10.1109/JIOT.2019.2946919

Further reading

Below is an excerpt from other important literature with a brief description of the content:

- Description of error correction methods, W.T. Buttler, et al., Fast, efficient error reconciliation for quantum cryptography. Phys. Rev. A **67**(5), 052303 (2003) https://doi.org/10.1103/PhysRevA.67.052303
- Description of the cascade protocol for error correction in QKD. Explains the potential performance, strengths, weaknesses, and comparison of different modified versions of this method is also very interesting for RKD: Martinez-Mateo, Jesus, et al. Demystifying the information reconciliation protocol cascade, in arXiv preprint https://arxiv.org/abs/1407.3257, 2014. https://doi.org/10.48550/arXiv.1407.3257
- Description of a key generation system based on signal strength measurement, R. Lin, et al., Efficient physical layer key generation technique in wireless communications. EURASIP Journal on Wireless Communications and Networking **2020**(1), 13 (2020) https://doi.org/10.1186/s13638-019-1634-7
- Description of the entire key generation process and an analysis of various error correction methods. This method is also very interesting for RKD, A. Yamamura, H. Ishizuka, Error detection and authentication in quantum key distribution, in *Australasian Conference on Information Security and Privacy*, (Springer Berlin Heidelberg, Berlin, Heidelberg, 2001) https://doi.org/10.1007/3-540-47719-5_22
- Key generation for smart home devices. Adaptive method based on signal strength measurement. Complex quantization method, H. Zhao, et al., A physical-layer key generation approach based on received signal strength in smart homes. IEEE Internet Things J. **9**(7), 4917–4927 (2021). https://doi.org/10.1109/JIOT.2021.3119053
- Analysis of technology in the 5G sector. Description of the advantages of 5G, because eavesdropping is made more difficult by beamforming. Furthermore, the otherwise unused channel is very well suited to minimizing errors in the key, L. Jiao, et al., Physical layer key generation in 5G wireless networks. IEEE Wirel. Commun. **26**(5), 48–54 (2019). https://doi.org/10.1109/MWC.001.1900061
- Description of the challenges in the automotive sector, Explanation of how code overhead could be reduced. Simulation with remote-controlled vehicles, L. Jiao, et al., Physical layer key generation in 5G wireless networks. IEEE Wirel. Commun. **26**(5), 48–54 (2019) https://doi.org/10.1109/MWC.001.1900061
- Explanation of how RKD can also be used in static environments. Combination of local randomness and radio channel characteristics, N. Aldaghri, H. Mahdavifar, Physical layer secret key generation in static environments. IEEE Trans. Inf. Forensics Secur. **15**, 2692–2705 (2020) https://doi.org/10.1109/TIFS.2020.2974621
- Detailed comparison of several error correction methods and the expected loss of key bits that can be intercepted by third parties, M. Miralem, et al., Error reconciliation in quantum key distribution protocols, in *Reversible Computation: Extending Horizons of Computing*, ed. by I. Ulidowski et al., vol. 12070, (Springer, Cham, 2020), pp. 222–236. https://doi.org/10.1007/978-3-030-47361-7_11