BlueKey: Exploiting Bluetooth Low Energy for Enhanced Physical-Layer Key Generation

Yawen Zheng*, Fan Dang†✉, Zihao Yang‡, Jinyan Jiang§, Xu Wang†,
Lin Wang‡, Kebin Liu†, Xinlei Chen‖**††, Yunhao Liu†¶
*Department of Automation and BNRist, Tsinghua University, †Global Innovation Exchange, Tsinghua University
‡School of Information Science and Engineering, Yanshan University, §School of Software and BNRist, Tsinghua University
‖Shenzhen International Graduate School, Tsinghua University, ¶Department of Automation, Tsinghua University
**Pengcheng Laboratory, Shenzhen, China, ††RISC-V International Open Source Laboratory, Shenzhen, China
{yw-zheng21, jiangjy20}@mails.tsinghua.edu.cn, {dangfan, wangxu2020, kebinliu2021, yunhao}@tsinghua.edu.cn
Yangzihao@stumail.ysu.edu.cn, wlin@ysu.edu.cn, chen.xinlei@sz.tsinghua.edu.cn

IEEE INFOCOM 2024 - IEEE Conference on Computer Communications | 979-8-3503-8350-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/INFOCOM52122.2024.10621142

***Abstract*—Bluetooth Low Energy (BLE) is a prevalent technology in various applications due to its low power consumption and wide device compatibility. Despite its numerous advantages, the encryption methods of BLE often expose devices to potential attacks. To fortify security, we investigate the application of Physical-layer Key Generation (PKG), a promising technology that enables devices to generate a shared secret key from their shared physical environment. We propose a distinctive approach that capitalizes on the inherent characteristics of BLE to facilitate efficient PKG. We harness the constant tone extension within BLE protocols to extract comprehensive physical layer information and introduce an innovative method that employs Legendre polynomial quantization for PKG. This method facilitates the exchange of secret keys with a high key matching rate and a high key generation rate. The efficacy of our approach is validated through extensive experiments on a software-defined radio platform, underscoring its potential to enhance security in the rapidly expanding field of BLE applications.**

***Index Terms*—BLE, physical-layer key generation**

I. Introduction

Bluetooth Low Energy (BLE) has become a ubiquitous technology in various applications, ranging from IoT (Internet of Things) devices [1] to healthcare equipment [2], owing to its lower power consumption and compatibility with diverse devices. Despite these merits, one persistent challenge in the deployment of BLE is security [3]–[7].

Fortunately, the concept of Physical-layer Key Generation (PKG) [8] emerges as a potential game changer that may enhance the security profile of BLE-based systems. PKG plays a pivotal role in secure wireless communications, with its unique attribute of facilitating two devices to generate the same secret key from their common physical environment. PKG is built on *channel reciprocity*, *temporal variation*, *spatial decorrelation* [9] principles to exchange identical keys, provide wellspring information entropy for key generation, and prevent nearby eavesdroppers from snooping on essential information. These advantages position it as a promising technology, particularly for typical IoT scenarios [9].

Although extensively investigated [8]–[12], PKG is generally discussed in the context of Wi-Fi, and the application of PKG in BLE is still rare. The direct transfer of techniques from the Wi-Fi domain to the BLE domain is infeasible for significant differences in terms of *bandwidth* and *modulation*. Wi-Fi typically operates on a 20-160 MHz bandwidth and is modulated by Orthogonal Frequency Division Multiplexing (OFDM) [13], while BLE operates on a narrower 2 MHz bandwidth with Gaussian Frequency Shift Keying (GFSK) modulation [14]. Consequently, the physical layer information directly extracted in BLE is very limited. Besides, low power consumption is a necessity for BLE scenarios and any complex algorithms will conflict the principle and fail to be deployed.

Recently, Bluetooth Core Specification version 5.1 [15] released a new feature *constant tone extension* (CTE). Originally designed for direction finding [16], CTE provides finer-grained Channel State Information (CSI) [17] compared to Received Signal Strength Indication (RSSI) and could analyze the Angle of Arrival (AoA) and Angle of Departure (AoD) of BLE signals. We found an opportunity to implement PKG for BLE by taking advantage of CSI provided by CTE, which could not only increase angle accuracy but also enhance the key generation rate and key matching rate of PKG. Specifically, CSI can be divided into the dimensions of *carrier frequency* and *physical antenna*. The phase variation of each frequency is mainly due to different time of flight (ToF), and that of each antenna is mainly caused by the propagation paths of the signals [18]. Exploring the spatial dimension corresponding to antenna arrays could increase the information entropy for PKG. By analyzing CSI changes in IQ samples of CTE fields in BLE packets transmitted through spatial channels corresponding to different antennas, we can utilize BLE devices to capture the complex multi-path environment in IoT scenarios.

Insighted by the opportunity, we propose BlueKey to implement PKG for BLE (Fig. 1). BlueKey tackles the aforementioned information entropy and energy consumption bottlenecks through the following techniques. *(i) Reverse antenna scheduling* separately calculates the AoA and AoD of the signals received or transmitted by the central device, rather than measuring the AoA information from the signals received by both end devices. This reciprocal information allows for the deployment of antenna arrays only at the central device,

✉Fan Dang is the corresponding author.

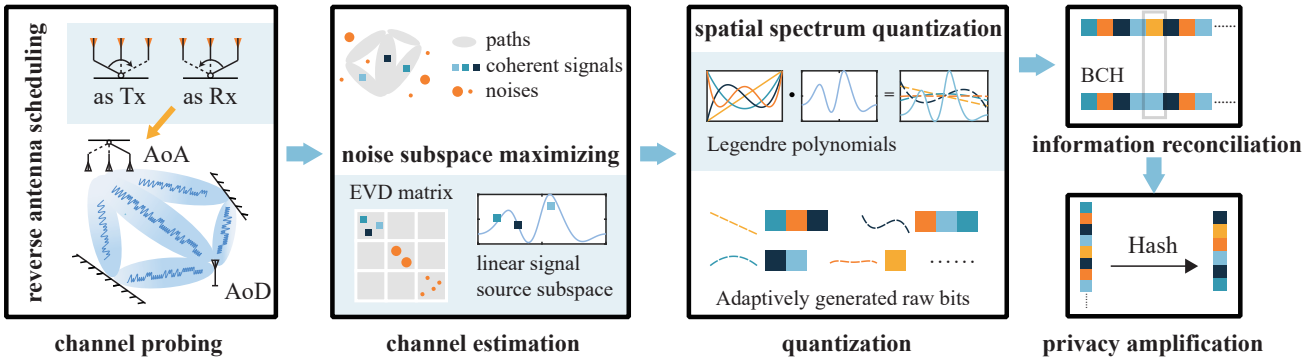


Fig. 1: The overview of BlueKey.

while users can continue using common single-antenna BLE peripheral devices for PKG. *(ii) Noise space maximizing* employs MUSIC [19] algorithms to calculate a spatial spectrum, which quantifies perturbations caused by multi-path effects and increases information entropy. This can overcome the limited resolution of BLE signals and take advantage of multi-path effects. *(iii) Spatial spectrum quantization* utilizes a series of orthogonal polynomials to fit the points of the normalized spectral curve and then transforms the corresponding coefficients into sequences of 0/1 with further adaptive quantization, which could benefit from the entire spectrum.

The contributions of this work are summarized below.

- To the best of our knowledge, this is the first study to dive into Constant Tone Extension (CTE) within BLE protocols, aiming to extract detailed information on the amplitude, phase, and other physical layer information for PKG. This approach, which leverages the existing direction-finding function in the protocols, allows for the acquisition of substantial information entropy for key generation without necessitating additional communication overhead. Furthermore, this method only requires a single antenna for peripheral devices on the user side, making it an ideal solution for low-power IoT scenarios.
- We introduced a novel method that employs Legendre polynomial quantization for PKG, informed by reverse antenna scheduling, which allows separate AoA and AoD calculations for signals at the central device, enabling continued use of single-antenna BLE peripheral devices. Our approach capitalizes on a spatial spectrum—generated by noise space maximizing, enhancing information entropy and key generation rate. Furthermore, our method utilizes spatial spectrum quantization to transform the normalized spectral curve into binary sequences, thus leveraging the entire spectrum, negating the need for complex BLE direction-finding algorithms, and ensuring its suitability for narrow-band GFSK signals.
- We conducted comprehensive experiments on a Software-Defined Radio (SDR) platform to validate the practicality of BlueKey. The experiments evaluated various aspects including information reciprocity, spatial distinction, BMR, and BGR. BlueKey significantly improved the secret bit generation rate per packet of our system, BlueKey, by 183.2× and 119.9× in indoor and outdoor scenarios, respectively, compared to state-of-the-art work. The results confirmed the feasibility of BlueKey, demonstrating its potential for real-world applications.

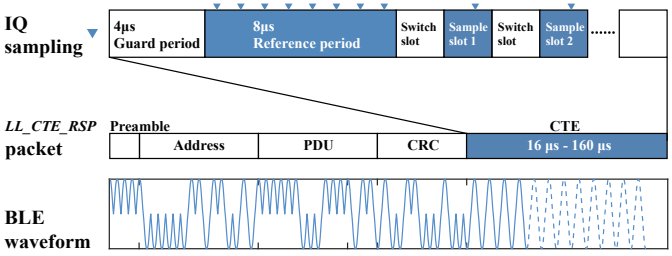


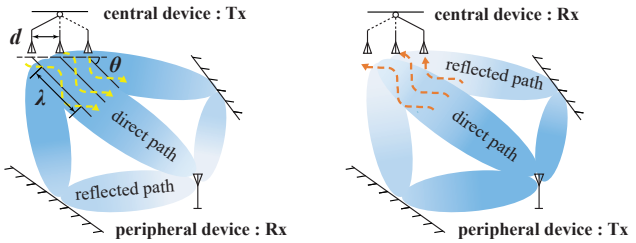
Fig. 2: The structure of BLE *LL_CTE_RSP* packet.

In the rest of the paper, we first comprehensively review the previous research in Section II, followed by a detailed description of the overall framework of the system and the design of each key module in Section III. In Section IV, we provide a thorough demonstration and discussion of a series of experimental results with the implementation of BlueKey, and the conclusions are finally drawn in Section VI.

II. Related Work

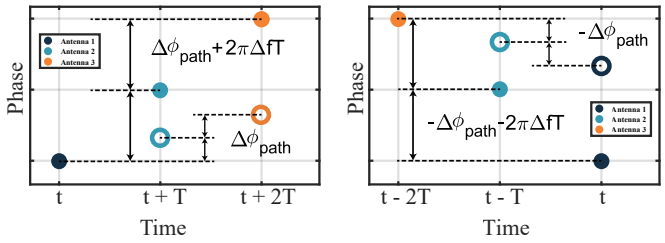
Our work is relevant to the following categories of research.

BLE Direction Finding. BLE direction finding [16] enables devices to determine the direction of a BLE signal based on AoA and AoD, making it possible to achieve centimeter-level location accuracy [20]–[25]. The most widely investigated method for the estimation of AoA and AoD is MUSIC [19] due to the high angular resolution and sensitivity achieved by separating the observation signal space into the source and noise subspaces. Channel State Information (CSI) is generally chosen as the observation signal. To measure CSI, BLoc [26] first constructed an approximate CSI of BLE devices by sending long sequences of 0s and forcing GFSK-modulated signals to converge to a specific frequency. In 2019, the



(a) angle of departure (b) angle of arrival

Fig. 3: BLE direction finding.



(a) forward switching pattern (b) backward switching pattern

Fig. 4: Phases of IQ data received the antenna array. The solid patterns depict the signal samples disturbed by the CFO while the hollow ones demonstrate those of ideal devices.

BlueTooth Core Specification version 5.1 [15] added single-tone CTE in data packets out of the same idea of BLoc, which inspires our design of BlueKey. Chip design companies have released the BLE System on Chips (SoCs) to support the AoA/AoD capabilities, such as CC2640R2F [27] provided by Texas Instruments (TI) and nRF52811 [28] provided by Nordic Semiconductor, which benefits developing IoT applications.

Physical-layer key generation. Physical-layer key generation (PKG) is a promising technique for the establishment of cryptographic keys between any two wireless users due to its attractive features of lightweight and information-theoretic security, and has received extensive research interest in recent years [8]–[12]. PKG involves four stages, including channel probing and estimation, quantization, information reconciliation, and privacy amplification. The channel probing and estimation is highly protocol specific and serves to extract randomness residing from the channel parameters, such as the received signal strength (RSS) and CSI [29]–[31]. The quantization step converts the analog measurements into binary sequences using a quantizer. Popular quantizers include the mean and standard deviation-based quantizer [29] and the cumulative distribution functions (CDF)-based quantizer [32]. The information reconciliation stage leverages the error correction code to reach an agreement [32]. The privacy amplification is used to eliminate the information revealed to eavesdroppers, which can be implemented using hash functions [33].

BlueKey also follows the procedure and introduces *reverse antenna scheduling*, *noise space maximizing*, *spatial spectrum quantization* techniques to make it practical for BLE.

III. System Design

In this section, we dive into the architecture of BlueKey as illustrated in Fig. 1. BlueKey consists of five modules: *(i) Channel probing* collects reciprocal information with the BLE direction-finding feature. *(ii) Channel estimation* extracts coherent multi-path signal groups from noise-disturbed IQ data. *(iii) Quantization* generates raw bitstreams from spatial spectra. *(iv) Information reconciliation* corrects mismatching bit errors between two communication partners. *(v) Privacy amplification* hashes raw keys into more secure secret keys. In the rest of this section, we first explain the basic procedure of AoA/AoD estimation of BLE and then present the key techniques of our work.

A. AoA/AoD Estimation of BLE

CTE [16] is an appended data field that follows the BLE Protocol Data Unit (PDU) and consists of symbols that represent only bit 1. Unlike GFSK-modulated BLE signals, CTE is not scrambled by the whitening process. Therefore, CTE is the only stable single-tone segment throughout the entire packet. Fig. 2 illustrats the packet structure.

According to the BLE Core Specification v5.1 [15], the direction-finding process in connection-oriented circumstances is described as follows. BLE device A communicates with device B. Device A is a central device, while device B is a peripheral device. Both of their PHYs support CTE. First, device A sends a packet of type `LL_CTE_REQ` to device B. The control field of the packet (`CtrData`) specifies the type of the CTE (*i.e.,* AoA or AoD) and the length of the CTE (16 - 160 µs). Subsequently, device B responds with an `LL_CTE_RSP` type packet, which contains a CTE of the corresponding type and length. Device B switches its antennas when transmitting an AoD CTE and does not perform antenna switching for an AoA CTE. Upon receiving the CTE-appended packet, device A performs the opposite behavior, switching the antennas for an AoA CTE. Finally, device A completes the IQ sampling process and reports the data to the host.

For BlueKey, the core steps of the physical-layer key exchange between two devices involve the peripheral device's measurement of the AoD of signals sent by the central device, as well as the central device's measurement of the AoA of signals transmitted in the opposite direction. In our design, BlueKey only requires the central device to perform antenna switching operations, which means that common single-antenna commercial off-the-shelf (COTS) devices could be deployed as the peripheral devices, and BlueKey could support more than one peripheral device. Since the central device serves as a base station, it can have a more complex hardware design and support synchronization and calibration.

Note that the protocol itself does not specify a particular direction-finding algorithm, providing users with the flexibility to expand in specific application scenarios. In the simplest case, consider a scenario in which a uniform linear array (ULA) receives parallel wireless signals arriving at angle θ, as shown in Fig. 3. The phase difference ϕ_{mn} between the IQ

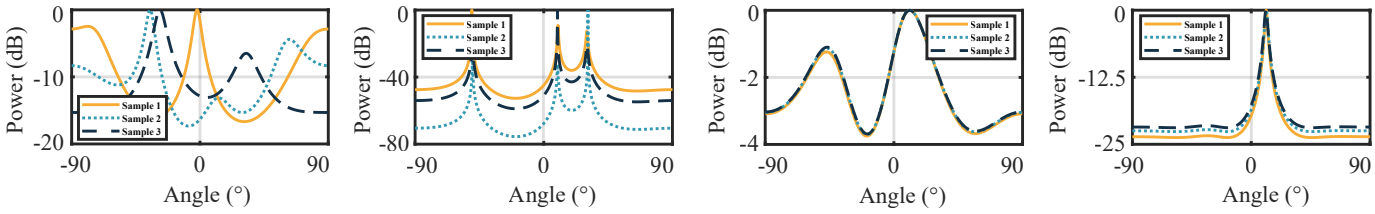


Fig. 5: Comparisons of spatial spectra generated with different noise-disturbed coherent/incoherent signal samples. For coherent signals, (a) the spectra of the class MUSIC algorithms display irregular peaks; (b) with the introduction of spatial smoothing (and extra antennas), the positions of the spectrum peaks remain fixed, but the heights still vary; (c) with the *noise subspace maximizing* method, the peaks of different spectra are highly identical; and (d) in particular, only a coherent signal group triggers multiple local maxima in spectra with the *noise subspace maximizing* method; otherwise, there is only a single peak.

samples collected by the *m-th* antenna and the *n-th* antenna simultaneously can be expressed by the following equation:

$$\phi_{mn} = 2\pi \cdot \frac{(m-n)d\sin\theta}{\lambda}, \tag{1}$$

where d represents the spacing of the antenna array, λ is the wavelength. Mentioning that a large d can lead to grating lobes [34] while a small d can cause coupling between antennas, we choose d as half of λ, as [20], [22] suggest.

The angle estimate errors could be determined with the phase measurement errors.

$$|\Delta\theta| = \left|\frac{\Delta\phi_{mn}}{(m-n)\pi\cos\theta}\right| \geq \left|\frac{\Delta\phi_{mn}}{(m-n)\pi}\right|. \tag{2}$$

Various factors contribute to phase measurement errors, *e.g.,* hardware defects, multi-path effects, and low Signal-to-Noise Ratio (SNR). Thus, it is not feasible to generate secret keys directly from erroneous direction-finding estimates. To address these problems, BlueKey proposes *reverse antenna scheduling*, *noise space maximizing*, and *spatial spectrum quantization* techniques, which will be elaborated in the rest of this section.

B. Reverse Antenna Scheduling

The most common structure of an antenna array is a combination of an RF link, a single-pole multiple-throw switch, and more than one antenna (as in TyrLoc [22], CO-SKG [35]), which is consistent with the most common COTS BLE devices. Since the multiple antennas operate asynchronously, phase errors of switch $\Delta\phi_{switch}$ are mainly caused by the Carrier Frequency Offset (CFO) Δf:

$$\Delta\phi_{switch} = 2\pi\Delta f \cdot T, \tag{3}$$

where T denotes the switching interval, Δf is the CFO between a transmitter/receiver pair, which is essentially caused by inherent hardware defects of the inaccurate Local Oscillator (LO). However, here we have an important observation that most of the COTS BLE peripheral devices shared one LO between the transmission link and the reception link to generate carrier signals and therefore the biased carrier frequency $f_{peri,tx}$ and $f_{peri,rx}$ should be consistent. And for a single central device fixed in position, even if the transmission and reception link rely on independent LOs, the difference can be amended by more resource-consuming methods, such as external clock sources or power-on/real-time calibration, so that identical $f_{ctr,tx}$ and $f_{ctr,rx}$ are provided. As a result, the CFO of the AoA/AoD estimate process can be written as

$$\Delta f_{AoA} = f_{peri,tx} - f_{ctr,rx} = f_{ctr,tx} - f_{peri,rx} = -\Delta f_{AoD}. \tag{4}$$

To make full use of this inverse numerical relationship, we proposed a *reverse antenna scheduling* method to implement two opposite antenna switching patterns when performing AoA and AoD estimates.

Specifically, according to Eq. (3) and Eq. (4), when the transmitting and receiving sides are switched, the phase difference $\Delta\phi_{switch}$ caused by the CFO is negative of each other. Meanwhile, the $\Delta\phi_{path}$ derived from the propagation path difference remains the same. Based on these two rules, the overall $\Delta\phi_{mn}$ generated by different antennas in the array will lose reciprocity when the central device serves as a transmitter or receiver, respectively, jeopardizing channel probings.

However, a turning point emerges from the fact that the sign of $\Delta\phi_{switch}$ depends not only on that of the CFO but also on the sequence of antenna scheduling. As shown in Fig. 4, if we implement two exactly opposite switching patterns for the AoA/AoD probing process respectively, the values of the overall phase difference $\Delta\phi_{mn}$ become identical with the sign of $\Delta\phi_{switch}$ reversed. Consequently, the phase measurement error caused by antenna switching and CFO can be reciprocal when estimating AoA/AoD with the same device pair.

C. Noise Space Maximizing

In practical IoT scenarios, the trivial algorithm given by Eq. (1) struggles to deal with issues like low SNR and signal aliasing caused by multiple signal sources/propagation. Therefore, a variety of direction-finding algorithms have been widely proposed and applied, out of which stands *MUSIC* [19].

MUSIC calculates the eigenvectors of the received signal covariance matrix as the first step, and then employs a method of signal-noise subspace separation. Subsequently, it iterates over an omnidirectional steering vector of the antenna array to obtain a spatial spectrum. The peaks of the spectrum, the

number of which corresponds to the signal subspace rank n, provide an estimate of AoA or AoD.

One of the essential assumptions of MUSIC for correctly separating multiple signals is that $N > m > n$, where N is the number of data snapshots, m is the number of antennas, and n is the number of signals to be separated specifically referring to incoherent signal sources. Otherwise, coherent signals with different AoA/AoD angles will not be resolvable in the spatial spectrum, unless more IQ data from extra antennas are provided [36].

However, most commercially available BLE antenna arrays could not meet the assumptions as they usually possess only less than 4 ULA antennas, which is often insufficient to effectively handle most indoor multi-path scenarios. Consequently, under these conditions, estimates of AoA and AoD are prone to be erroneous, biased, and neglectful of the abundant environmental variations. Such limitations can ultimately jeopardize the performance of key generation and exchange.

Our key insight towards this challenge is that the necessary condition for generating matched raw keys is not to improve the accuracy of direction finding, but to enhance and exploit the reciprocity of entropy sources. Since the signal propagation paths of AoA and AoD estimates are strictly identical, the disturbance caused by coherent signals should be reproducible as a result. Therefore, the main factor that impairs reciprocity is noise in low-SNR scenarios.

Based on the analysis above, we propose the method of *noise space maximizing* to address the challenge of characterizing multiple coherent signals propagating along different paths from the same source. With a limited number of antennas, our goal is not to accurately resolve the different directions of each path, but to extract all the reciprocal fluctuations in the spectrum. Specifically, we expand the noise subspace with as many eigenvectors of the covariance matrix as possible, while leaving only the one corresponding to the dominant eigenvalue to represent the coherent signal group. This approach results in an equivalent signal source number of 1, allowing even a 2-antenna array to be used effectively for exchanging BlueKey. In addition, it is important to note that with more antennas in the array, the characterization of the noise subspace and spectrum becomes more fine-grained, thus increasing the beneficial information entropy.

As shown in Fig. 5, simulation results reveal that the *MUSIC* spectrum exhibited multiple local maxima due to interference of multi-path effects, compared to a single peak in the case of incoherent sources without a coherent group. Furthermore, the local maxima of the coherent signal spectrum remain stable with the *noise space maximizing* even in low-SNR circumstances, but vary significantly when the signal subspace is expanded with more than one basis vector.

D. Spatial Spectrum Quantization

As discussed above, the design of *noise space maximizing* reveals the presence of multiple local maxima in the *MUSIC* spectrum, indicating interference caused by coherent signals propagating in different AoA or AoD. However, classical

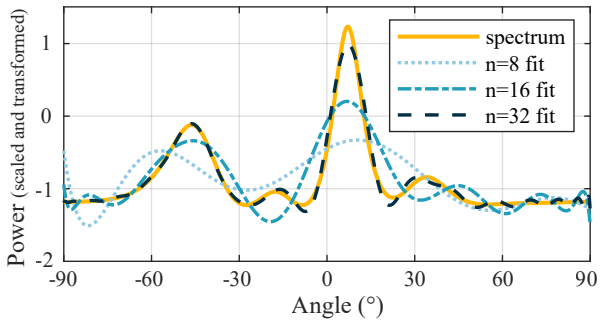


Fig. 6: Spectrum fitting with n-degree Legendre polynomials.

MUSIC only searches for peak points corresponding to the dimension of the signal subspace, yielding only one estimate for the angle, as is the case with BlueKey. Consequently, a significant portion of the spectral features remain underutilized by using this approach.

Previous works that achieve PKG based solely on AoA collected only the peak data as raw information [8]. To ensure sufficient entropy, additional efforts are required in the form of longer probing periods, a pre-shared codebook, or the establishment of a massive MIMO system [37]. However, these methods are found to be rather inefficient. In contrast, BlueKey effectively captures multi-path variations in the environment, even by stably reflecting the lesser local maxima. Therefore, we propose the design of *spatial spectrum quantization* to extract more characteristics from the entire spectrum. Specifically, we utilize a series of orthogonal polynomials to fit the spectral curve points and then transform the corresponding coefficients into 0/1 sequences with further adaptive quantization. Notably, due to the large variation in the range of normalized power (in dB) of spatial spectra generated with the experimental data (which is one manifestation of environmental diversity), we have scaled some of the smaller spectral data to maintain consistency in the quantization process.

Orthogonal polynomials are a class of basis functions that span a Hilbert space, with the inner product defined as

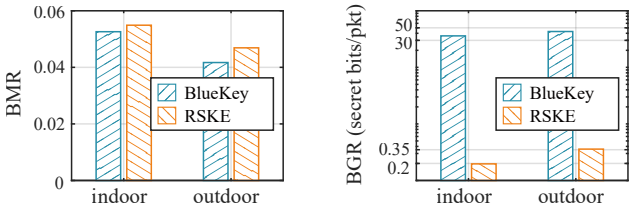
$$f(x) \cdot g(x) = \int_a^b f(x)g(x)W(x)dx. \tag{5}$$

If we set the integration interval $[a, b]$ to $[-1, 1]$, and let the weight function $W(x) = 1$, the orthogonal polynomials defined in this manner are known as Legendre polynomials [38]. Utilizing Legendre polynomials for data fitting can be highly advantageous due to their orthogonality feature.

Taking into account the spectral curve $P(x)$, expressed as $\sum_1^{N+1} c_k q_k(x)$, where N represents the maximum degree of polynomials, and c_k represents the coefficient of each function, to calculate c_k, we only need to project $P(x)$ onto q_k. This can be achieved by multiplying $P(x)$ with q_k, as in

$$P(x) \cdot q_k = \left(\sum_1^{N+1} c_k q_k(x) \right) \cdot q_k = c_k (q_k \cdot q_k). \tag{6}$$

This allows for estimating the coefficient of each polynomial term independently. Furthermore, the approximation of $P(x)$



(a) BMR (b) BGR

Fig. 7: PKG performance.

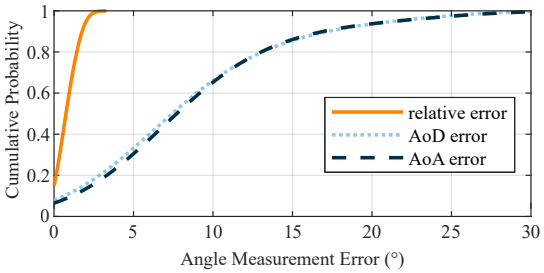


Fig. 8: AoA/AoD estimation.

derived in this manner can be mathematically proven to be the best fit for a least-squares error problem.

Another advantage of Legendre polynomials is that q_k can be easily generated through a recursive relationship, as illustrated in Eq. (7).

$$q_{n+1}(x) = \frac{2n+1}{n+1} x q_n(x) - \frac{n}{n+1} q_{n-1}(x), \tag{7}$$

which is computationally efficient. Moreover, as the degree of q_k increases, the fitting results converge to the spectral curve, as demonstrated in Fig. 6.

Subsequently, adaptive quantization schemes are utilized to perform Gray code quantization [39] on coefficients corresponding to polynomials of varying degrees, ultimately obtaining the raw key bits.

E. Information Reconciliation and Privacy Amplification

BlueKey adopts the widely used BCH code [40] for information reconciliation. To address information leakage during the reconciliation stage, corrected bits can be transformed into a more secure key using digest functions such as SHA2 or SHA3. As the aforementioned two methods do not differ significantly from previous PKG work [41], we will not delve into a more detailed explanation in this paper.

IV. Evaluation

A. Experimental Setup

To evaluate the performance of BlueKey in practical application scenarios, we set up a testbed using the Software Defined Radio (SDR) platform USRP-N210 with UBX40 daughterboards. We adopted another structure to emulate the *reverse antenna scheduling* stated in Sec. III-B. In this particular structure, the central device consists of three USRPs that serve as RF links of a 3-antenna array, while another USRP is utilized as a single-antenna peripheral device. To ensure proper spacing of the antenna array, we utilized laser-cut acrylic boards, which fix the spacing at half a wavelength of the BLE signals. The USRPs were connected to a network switch and from there to a PC workstation. All IQ data were transferred to the PC for examination and processing.

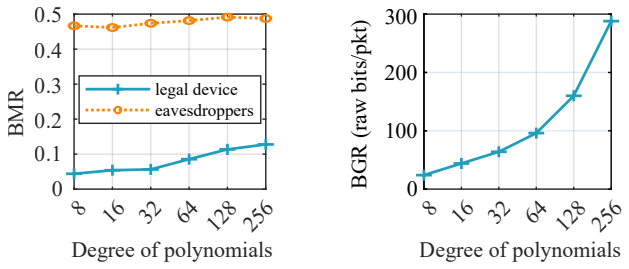
Regarding Section III-B, we acknowledge that the multi-RF-chain hardware architecture introduces phase measurement errors due to the variances in frequencies and initial phases of the carrier signals generated by each RF chain. To address this hardware limitation, specifically, we incorporated an OctoClock distribution module to ensure the synchronization of the PPS and reference signals. This synchronization guarantees that the three antennas within the central device array share an identical carrier frequency. To further mitigate any initial phase differences, we conducted calibration using an attenuator, coaxial cables, and a multi-way power divider. For USRPs, this phase difference is a result of the random initial state of a delta-sigma modulator in the Frac-N divider PLL, which remains unchanged even after power-up. It is noteworthy that BlueKey only requires the central device for an antenna array, so there is no need to calibrate the peripheral device.

We specified BLE packet signals with the parameters *ConnectionCTE* as the direction-finding packet type and *LE1M* as the PHY transmission mode. We generated and sampled IQ data of the CTE field with the settings of 72 µs length, 2 µs slot duration, and 8 µs sample offset. Simulations and signal processing were implemented using Matlab, and USRPs were controlled by UHD-based programs. We conducted a series of experiments in three typical scenarios: meeting rooms, hallways, and outdoors. Throughout all the experiments, we had people moving around to introduce dynamic and ever-changing multi-path effects.

The metrics used to evaluate the BlueKey system mainly include the bit mismatch rate (BMR), *a.k.a.,* the correctness, and the (secret) bit generation rate (BGR), *a.k.a.,* the speed. The BMR refers to the rate at which the raw key bits do not match before the information reconciliation step, and the BGR measures the number of raw key bits generated per BLE packet. When comparing BlueKey with the state-of-the-art robust secret key extraction (RSKE) [41], we followed the same definition as the baseline, which is "secret bits per packet." This definition takes information leaks during reconciliation into consideration.

B. Experimental Results

PKG performance. We compare BlueKey with the previous RSSI-based Bluetooth PKG method RSKE and select the baseline with parameter settings that yield the highest BGR at a distance of 5 ft, which is the closest to our experimental scenario. As shown in Fig. 7, the BMR of BlueKey decreases by 4.19% and 11.09% in indoor and outdoor scenarios, respectively. The number of erroneous bits is determined by the BMR



(a) BMR (b) BGR

Fig. 9: Impact of Legendre degrees.

in indoor and outdoor scenarios, and we subtract the BCH code's check bit length from the raw key bits, thus eliminating the impact of information leakage during the reconciliation stage. As a result, the secret bit generation rate per packet of BlueKey increased by 183.2× and 119.9× in indoor and outdoor scenarios, respectively, compared to RSKE.

AoA/AoD estimation. We first confirm the reciprocity of the AoA/AoD spatial spectrum, regardless of the accuracy of the angle measurement. We used a protractor board to ensure precise calibration and alignment of the antenna positions, maintaining a communication distance of exactly 1 meter. Next, we measured the AoD of the transmitted signals from the antenna array and the AoA of the received signals in the antenna array, covering a range of 0° to 90°.

As shown in Fig. 8, by selecting the maximum peak of the spatial spectrum as the angle measurement result, the median error of AoA/AoD compared to the actual directions can reach 7.37° and 7.91°, respectively. However, the median error of AoD/AoA measured at each location is only 0.73°. This confirms that the spatial reciprocity of wireless channels can be utilized effectively for the generation and exchange of raw key bits, even in cases where the angle measurement results are significantly inaccurate.

Legendre fitting degree. We assessed the impact of the highest degree, denoted as n, of Legendre polynomials used in the quantization stage on the BMR of raw key bits. This evaluation was based on experimental data collected from real-world scenarios. As depicted in Fig. 9a, when the highest degree $n \leq 32$, we achieved a legitimate BMR of approximately 0.5% or lower, together with an eavesdropper BMR close to 50%. However, when $n \geq 64$, the legitimate BMR exhibits a more significant increase. This can be attributed to the fact that as the degree of polynomials increases, the coefficient values gradually approach zero. Consequently, the bits generated in a later sequence become more susceptible to errors in spectra.

On the other hand, as shown in Fig. 9b, the adaptive quantization schemes in BlueKey cause a linear increase of the BGR with the highest degree n of the polynomial, albeit asymptotically. However, it should be noted that the time complexity for calculating the Legendre polynomial coefficients increases exponentially with the highest degree ($O(n^3)$ or $O(pn^2)$, where n is the highest degree and p is the number of signal samples), depending on the different algorithms. Thus, polynomials with large n cannot be used unrestrictedly for quantization even with a higher BGR. Consequently, we have chosen to use Legendre polynomials with $n = 32$ in our experiments to quantize the spatial spectrum of each packet into 64 raw bits.

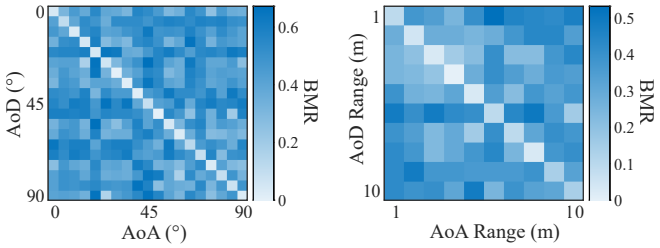
Angular positions. We set the communication distance to 1 m and collected the spectra of AoA and AoD in the range of [0, 90°] at 5° intervals in the multi-path scenario of a meeting room. We use the BlueKey methods to calculate the BMR for a pair of devices. As shown in Fig. 10a, the average BMR of the pair of devices on the diagonal (where the relative angular positions of the central and peripheral devices are the same) is significantly lower than that of the pair of non-diagonal devices (where the transmitter and receiver locations differ). Furthermore, even when the angular difference is only 5° (which corresponds to a distance of approximately 8.73 cm, slightly larger than half the wavelength of 6.25 cm), there is a noticeable difference in the BMR of the generated raw bits. The result indicates that BlueKey has a high spatial resolution when the angular position of the device changes. Specifically, the Legendre polynomial quantization method is sensitive to changes in the peak positions of the spatial spectra.

Communication ranges. We adjust the signal direction to approximately 30° and collect the AoA and AoD spectra within the range of 1 m to 10 m, with intervals of approximately 1 m. This is done in a narrow indoor hallway displaying another multi-path scenario. Using the BlueKey method, we then calculated the BMR for each pair of spectra. As shown in Fig. 10b, the average BMR for device pairs on the diagonal line (within the same range) is noticeably lower than that of the nondiagonal pairs (within different ranges). However, the difference between adjacent positions is not as significant as in the case when the signal direction changes.

This indicates that BlueKey has a moderate spatial resolution when the device direction is fixed and the distance changes. This is because the Legendre polynomial quantization method shows relative insensitivity to the peak height and the width of the main lobe of the spatial spectrum compared to the peak positions. In other words, if an eavesdropper is positioned exactly along the line connecting the central device and a peripheral device, they might obtain a larger number of accurate raw bits compared to other positions. However, it is important to note that achieving such uniquely positioned eavesdropping is not typically feasible in real-world scenarios, especially when the peripheral devices are moving. Furthermore, a resolution of approximately 1 m is sufficient to mitigate the majority of eavesdropping attacks.

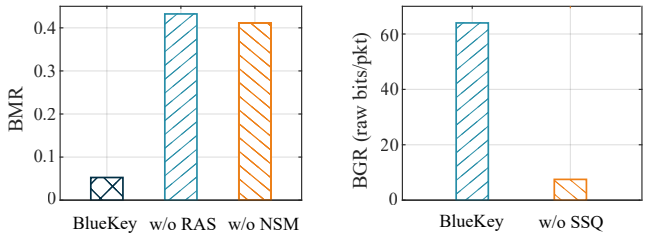
C. Component Study of BlueKey

We conducted an ablation test on the three main modules of BlueKey: *reverse antenna scheduling*, *noise subspace maximizing*, and *spatial spectrum quantization*. As shown in



(a) Angular positions (b) Communication ranges

Fig. 10: BMR resolutions of device positions.



(a) BMR (b) BGR

Fig. 11: Ablation test of BlueKey. (RAS, NSM, and SSQ are abbreviations of the key components)

Fig. 11, the first two modules primarily affect the BMR, while the latter module primarily affects the BGR.

Reverse antenna scheduling. Unlike most commercially available BLE devices, the RF transmission and reception links of the USRP N210 do not share the same LO. To align with real-world application premises, we manually introduced an approximate 10 kHz CFO between the central and peripheral devices using a clock source. This would result in a phase difference of 40π given a 2 ms slot duration setting. It is important to note that the clock source cannot precisely generate a frequency offset of exactly 10 kHz. Therefore, the actual phase difference is not an integer multiple of 2π. However, this offset remains consistent for both the transmission and reception links thanks to the use of the same reference signal. Without the *reverse antenna scheduling module*, the BMR of the raw key bits generated by a pair of legitimate devices would approach 50%, which is essentially like making random guesses. This means that the PKG system would not be able to successfully exchange matching keys.

Noise subspace maximizing. After conducting the experiment using only a three-antenna array, the number of signal sources in the classical MUSIC algorithm was set to 2. As observed in the simulation results discussed in Sect. III, the AoA/AoD spectrum is greatly affected by environmental noise, making it impossible to generate reciprocal data. Under these circumstances, the BMR of the raw key bits generated by a pair of legitimate devices exceeds 40%.

Spatial spectrum quantization. According to the experiments carried out in AoA/AoD estimation, the median relative error in estimating the single peak angle of AoA / AoD is less than 1°. Given this result, it is reasonable to quantify the range of single angle estimates from -90° to 90°, with a resolution of 1°. This approach yields 7-8 bits, which is more than $8\times$ lower than the original *spatial spectrum quantization* method, which required a BGR of 64 raw bits/packet. Another important point to highlight is that the use of Gray codes in the quantization method leads to a significant decrease in the spatial distinction between adjacent angular positions when single-peak quantization is employed.

D. Security Analysis

We conducted experiments in both indoor and outdoor scenarios, as shown in Fig. 12, to analyze the most common attacks, such as eavesdropping, position replay attack, predictable channel attack, and out-of-band attack. The results are presented in Fig. 13.

Eavesdropping. We first fix the position and direction of the antenna array as the central device, and then randomly select a series of locations as potential peripheral devices. At each spot, we measured the AoA/AoD spectra and generated raw key bits in pairs. The key pairs generated at the same location correspond to the BMR of the legitimate devices Alice and Bob, while all other locations are considered as the eavesdropper Eve. The BMRs of the eavesdropping devices in the indoor and outdoor scenarios are 47.26% and 50.09%, respectively. This indicates that BlueKey is robust against eavesdropping attacks.

Position replay attack. In the two scenarios, we carefully select two specific locations to exchange spatial spectra between the legitimate devices Alice and Bob. Afterward, we measured Eve's spatial spectrum again at the same location where Bob used to be, after a short time. Since there are movements of people and objects, the multi-path environment has changed between these two measurements. Additionally, the carrier frequency generated by Eve's device most likely diverges from that generated by Bob's because of distinctive hardware fingerprints [42], which leads to dissimilar transform on the spatial spectra with the *reverse antenna scheduling* module. As a result, even if Eve and the legitimate peripheral device Bob are in the same location, the number, position, height, and width of their spatial spectrum peaks differ. Under these conditions, the BMRs of malicious devices in indoor and outdoor scenarios are 49.11% and 26.79%, respectively. Although the multi-path outdoor environment is not as diverse and dynamic as the indoor environment, Eve still unintentionally acquired a sufficient number of mismatched bits. Therefore, BlueKey proves effective in resisting position replay attacks.

Predictable channel attack. Predictable channel attacks mainly target RSSI-based PKG methods. A common strategy of Eve is to create regular alternating line-of-sight (LoS) and

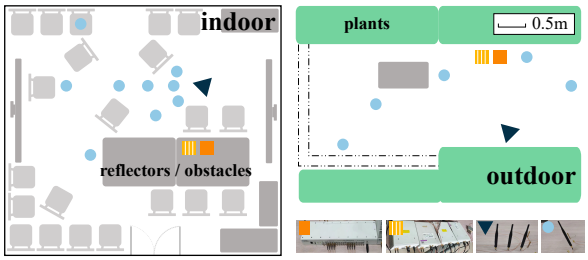


Fig. 12: Scenes of security analysis.

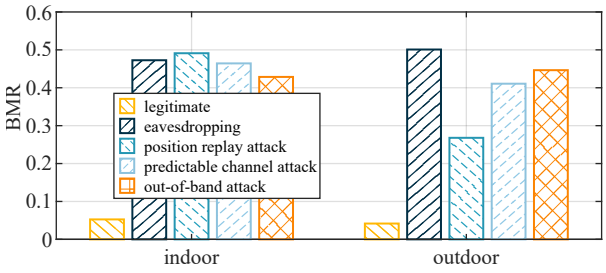


Fig. 13: Security analysis.

non-line-of-sight (NLoS) channels between legitimate devices, which results in predictable changes in the physical layer signals. In the case of BlueKey, when Eve successfully blocks the direct LOS channel, the most reasonable prediction is that the spatial spectra will have no peak values. However, noticeable fluctuations still exist in the actual AoA/AoD spectra due to signal multi-path propagation. In this situation, the BMRs obtained by Eve in indoor and outdoor scenarios are 46.43% and 41.07%, respectively. These values are not significant enough to jeopardize the security of BlueKey.

Out-of-band attack. We assume that Eve obtains the relative angular position information of Alice and Bob using out-of-band methods, such as vision monitoring. Then, she directly uses algorithms like Gaussian functions to create a forged set of single-peak spatial spectrum data. However, in reality, due to the utilization of the *reverse antenna scheduling* and *noise subspace maximizing* module, the positions of the maximum peak for Alice and Bob do not correspond to the direction of the direct LOS path in the actual scenario. Additionally, legitimate devices exhibit multiple peaks in their spectra due to the multi-path effects. Even if Eve continuously adjusts the height and width of the single peak through brute force, the BMRs achieved by Eve in indoor and outdoor scenarios are only 42.86% and 44.64%, respectively.

V. Discussion

2.4G concurrent transmissions. BLE devices share the 2.4 GHz frequency band with common Wi-Fi devices, necessitating measures to avoid signal interference during communication. Common strategies include: 1. If both Wi-Fi and BLE functionalities are activated on the same device, time-division multiplexing is employed by the software to prevent channel interference. 2. Standalone BLE devices use a frequency-hopping strategy, adaptively avoiding Wi-Fi channels across 40 channels of 2 MHz each. The first scenario is also applicable to BlueKey. However, for the second scenario, concurrent transmissions might not affect decoding, but could interfere with the lower-level physical layer information in the CTE field, which obfuscates the frequency-agnostic spatial spectra. Existing research [43] also indicates that concurrent transmissions can affect BLE signals with different parameters of the physical layer in varying ways. Future work in the PKG domain could involve more detailed experimentation and analysis in this regard.

Mobility of transceivers. In common IoT scenarios, the movement of both people and objects in the environment, as well as the devices engaged in physical-layer key exchange, creates a dynamic multi-path setting. Although Bluetooth data packet exchanges are brief (on the order of milliseconds), minimizing the impact of spatial position changes, the movement of the transmitter and receiver introduces more complex challenges by causing a Doppler shift. These Doppler effects, although resulting in relatively stable frequency shifts at constant speeds, add complexity to PKG, especially in real-world scenarios where device movement is not uniformly linear. Nevertheless, some PKG works [44] leverage active manipulation by swinging device antennas to introduce richer information entropy. Future work should spotlight the effects of device movement speed and patterns within specific time windows on the key generation process.

VI. Conclusion

This paper presents a pioneering approach to enhancing security in Bluetooth Low Energy applications by leveraging the constant tone extension for physical-layer key generation. We introduce a novel method that employs Legendre polynomial quantization for PKG, utilizing the spatial spectrum generated by antenna arrays. This approach enables the exchange of secret keys with a high key matching rate and key generation rate within a confined space, providing a unique solution for low-power IoT scenarios. The practicality of our proposed system is validated through comprehensive experiments on a software-defined radio platform, confirming its potential for real-world applications. This research marks a significant step forward in the field of BLE security, opening up new possibilities for secure wireless communication.

VII. Acknowledgement

This work is supported in part by the National Key R&D Program of China under grant No. 2021YFB2900100, the Natural Science Foundation of China under Grant No. 62302259, 62371269, 62202263 and 61772453, and the Guangdong Innovative and Entrepreneurial Research Team Program No. 2021ZT09L197.

REFERENCES

[1] J. Yin, Z. Yang, H. Cao, T. Liu, Z. Zhou, and C. Wu, "A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT," *ACM Transactions on Sensor Networks*, vol. 15, no. 3, pp. 1–29, 2019.

[2] L. Ott, "The Evolution of Bluetooth® in Wireless Medical Devices," *Socket Mobile, Inc. White Papers*, 2010.

[3] J. Wang, F. Hu, Y. Zhou, Y. Liu, H. Zhang, and Z. Liu, "BlueDoor: Breaking the Secure Information Flow via BLE Vulnerability," in *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, 2020, pp. 286–298.

[4] M. Cäsar, T. Pawelke, J. Steffan, and G. Terhorst, "A Survey on Bluetooth Low Energy Security and Privacy," *Computer Networks*, vol. 205, p. 108712, 2022.

[5] Q. Zhang and Z. Liang, "Security Analysis of Bluetooth Low Energy Based Smart Wristbands," in *Proceedings of the 2nd International Conference on Frontiers of Sensors Technologies*. IEEE, 2017, pp. 421–425.

[6] A. C. Santos, J. L. S. Filho, Á. Í. Silva, V. Nigam, and I. E. Fonseca, "Ble Injection-Free Attack: A Novel Attack on Bluetooth Low Energy Devices," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–11, 2019.

[7] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "Low Entropy Key Negotiation Attacks on Bluetooth and Bluetooth Low Energy," *Cryptology ePrint Archive*, 2019.

[8] K. Zeng, "Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[9] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing Wireless Communications of the Internet of Things from the Physical Layer, an Overview," *Entropy*, vol. 19, no. 8, p. 420, 2017.

[10] 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 *Proceedings of 2014 International Workshop on Secure Internet of Things*. IEEE, 2014, pp. 26–34.

[11] J. Wallace, "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits," in *Proceedings of 2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–5.

[12] N. Aldaghri and H. Mahdavifar, "Physical Layer Secret Key Generation in Static Environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.

[13] Y. G. Li and G. L. Stuber, *Orthogonal Frequency Division Multiplexing for Wireless Communications*. Springer Science & Business Media, 2006.

[14] B. Xia, C. Xin, W. Sheng, A. Y. Valero-Lopez, and E. Sánchez-Sinencio, "A GFSK Demodulator for Low-IF Bluetooth Receiver," *IEEE Journal of Solid-State Circuits*, vol. 38, no. 8, pp. 1397–1400, 2003.

[15] M. Woolley, "Bluetooth Core Specification V5.1," *Bluetooth Special Interest Group*, 2019.

[16] M. Woolley, "Bluetooth Direction Finding," *A Technical Overview*, 2019.

[17] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor Localization via Channel Response," *ACM Computing Surveys*, vol. 46, no. 2, pp. 1–32, 2013.

[18] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "Spotfi: Decimeter Level Localization Using WiFi," in *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, 2015, pp. 269–282.

[19] R. Schmidt, "Multiple Emitter Location and Signal Parameter Estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, no. 3, pp. 276–280, 1986.

[20] M. Cominelli, P. Patras, and F. Gringoli, "Dead on Arrival: An Empirical Study of the Bluetooth 5.1 Positioning System," in *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, 2019, pp. 13–20.

[21] P. Sambu and M. Won, "An Experimental Study on Direction Finding of Bluetooth 5.1: Indoor vs Outdoor," in *Proceedings of the 2022 IEEE Wireless Communications and Networking Conference*. IEEE, 2022, pp. 1934–1939.

[22] Z. Gu, T. He, J. Yin, Y. Xu, and J. Wu, "TyrLoc: A Low-Cost Multi-Technology MIMO Localization System with a Single RF Chain," in *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, 2021, pp. 228–240.

[23] H. Ye, B. Yang, Z. Long, and C. Dai, "A Method of Indoor Positioning by Signal Fitting and PDDA Algorithm Using BLE AOA Device," *IEEE Sensors Journal*, vol. 22, no. 8, pp. 7877–7887, 2022.

[24] X. Qiu, B. Wang, J. Wang, and Y. Shen, "AOA-Based BLE Localization With Carrier Frequency Offset Mitigation," in *Proceedings of the 2020 IEEE International Conference on Communications Workshops*. IEEE, 2020, pp. 1–5.

[25] Z. HajiAkhondi-Meybodi, M. Salimibeni, A. Mohammadi, and K. N. Plataniotis, "Bluetooth Low Energy and CNN-Based Angle of Arrival Localization in Presence of Rayleigh Fading," in *Proceedings of 2021 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2021, pp. 7913–7917.

[26] R. Ayyalasomayajula, D. Vasisht, and D. Bharadia, "BLoc: CSI-Based Accurate Localization for BLE Tags," in *Proceedings of the 14th International Conference on Emerging Networking EXperiments and Technologies*, 2018, pp. 126–138.

[27] T. Instruments. CC2640R2F data sheet, product information and support | TI.com. Accessed on: July 29, 2023. [Online]. Available: https://www.ti.com/product/CC2640R2F

[28] N. Semiconductor, "nRF52811 Datasheet," 2019.

[29] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-Telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 128–139.

[30] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient Key Generation by Exploiting Randomness from Channel Responses of Individual OFDM Subcarriers," *IEEE Transactions on Communications*, vol. 64, no. 6, pp. 2578–2588, 2016.

[31] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks," in *Proceedings of the 29th IEEE International Conference on Computer Communications*. IEEE, 2010, pp. 1–9.

[32] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2009.

[33] 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.

[34] R. Mailloux, "Array Grating Lobes Due to Periodic Phase, Amplitude, and Time Delay Quantization," *IEEE Transactions on Antennas and Propagation*, vol. 32, no. 12, pp. 1364–1368, 1984.

[35] G. Li, H. Yang, J. Zhang, H. Liu, and A. Hu, "Fast and Secure Key Generation with Channel Obfuscation in Slowly Varying Environments," in *Proceedings of the 41st IEEE International Conference on Computer Communications*. IEEE, 2022, pp. 1–10.

[36] T.-J. Shan, M. Wax, and T. Kailath, "On Spatial Smoothing for Direction-of-Arrival Estimation of Coherent Signals," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 33, no. 4, pp. 806–811, 1985.

[37] L. Jiao, J. Tang, and K. Zeng, "Physical Layer Key Generation Using Virtual AoA and AoD of mmWave Massive MIMO Channel," in *Proceedings of 2018 IEEE Conference on Communications and Network Security*. IEEE, 2018, pp. 1–9.

[38] A. M. Legendre, *Essai Sur La Theorie Des Nombres*. chez Courcier, imprimeur-libraire pour les mathematiques, quai des Augustins, 1808.

[39] F. Gray, "Pulse Code Communication," *United States Patent Number 2632058*, 1953.

[40] R. C. Bose and D. K. Ray-Chaudhuri, "On a Class of Error Correcting Binary Group Codes," *Information and control*, vol. 3, no. 1, pp. 68–79, 1960.

[41] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, and R. Ricci, "Secret Key Extraction Using Bluetooth Wireless Signal Strength Measurements," in *Proceedings of the 2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking*. IEEE, 2014, pp. 293–301.

[42] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information," in *Proceedings of the 37th IEEE International Conference on Computer Communications*. IEEE, 2018, pp. 1700–1708.

[43] M. Baddeley, C. A. Boano, A. Escobar-Molero, Y. Liu, X. Ma, U. Raza, K. Römer, M. Schuß, and A. Stanoev, "The impact of the physical layer on the performance of concurrent transmissions," in *2020 IEEE 28th International Conference on Network Protocols (ICNP)*. IEEE, 2020, pp. 1–12.

[44] L. Wang, H. An, H. Zhu, and W. Liu, "MobiKey: Mobility-Based Secret Key Generation in Smart Home," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7590–7600, 2020.