This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

A 60-GHz Antenna-Duplexed Modular Front-End for Channel Sounding and Physical Layer Security

Muhammad Umar, Axel Schmidt, Martin Laabs, Niels Neumann, and Dirk Plettemeier, *Member, IEEE*

***Abstract*— Distinctive propagation characteristics of millimeter wave (mmWave) bands require channel sounding for link management. Reported mmWave channel-sounder setups support only simplex operation while depending on bulky and expensive lab equipment; especially for frequency domain channel sounding (FCS), which can be performed with simple hardware. This work presents a solution in the form of a 60 GHz modular front-end designed using off-the-shelf components with tailor-made passive circuits and high-frequency interconnections, all compatible with printed circuit technology. An FCS setup is developed using two units of the designed transceiver front-ends, which can sweep 6 GHz bandwidth with 1 MHz resolution. An antenna duplexing circuitry is also presented, which enables each front-end unit to use a single transmit-receive antenna ensuring a high correlation between the round-trip channels. To the best of the authors' knowledge, this work reports the first FCS setup, which preserves channel reciprocity in round-trip sounding. The application of the designed system is showcased through a channel reciprocity key generation (CRKG) algorithm, which exploits the high correlation between the forward and receive channels to demonstrate a physical layer security system functional at 60 GHz.**

***Index Terms*— Antenna duplexer, channel sounder, channel reciprocity, modular 60 GHz front-end, balun, bias-tee, DC-block, bond wire, millimeter wave PCB, millimeter wave packaging, physical layer security, secret key generation, TRL calibration.**

I. Introduction

ELECTROMAGNETIC (EM) propagation at 60 GHz suffers relatively higher attenuation through free space and building materials, making this band relevant for short-range communications. The distinguished propagation properties make channel state information necessary to adapt the link parameters. This information can be acquired through channel emulators or channel sounding systems; however, channel sounders provide real-time information at the cost of hardware complexity [1], [2], [3], [4]. Channel sounding can be performed in the time or frequency domain. Time-domain channel sounding utilizes impulses, spread spectrum, or orthogonal frequency division multiplexing waveforms requiring compatible hardware for high peak-to-average power, dynamic range, and complex baseband processing [2]. On the other hand, frequency-domain channel sounding (FCS), aka vector network analyzer (VNA) sounding, sweeps a wide bandwidth to get frequency-dependent path loss. Time domain parameters, e.g., power delay profile and unambiguous time range, are extracted from this information through signal processing algorithms [5], [6]. It is a slow process compared to time domain sounding, nevertheless feasible for slow varying or static channels using comparatively simple hardware [7]. However, in contemporary research, FCS has been predominately demonstrated using bulky and expensive lab equipment, justifying the need for economical and portable hardware [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18].

Another critical aspect attaining research attention is wireless link security. Especially for a wireless sensor network (WSN), where a single malfunctioning device can expose others to cyber-attacks. Physical layer security (PhySec) has emerged as a potential solution for this challenge [19]. Channel reciprocity key generation (CRKG) is a variant of PhySec that utilizes reciprocity of the channel characteristics between transmitter (Tx) and receiver (Rx) for encryption key generation, assuming legitimate and wire-tap channels remain uncorrelated [20], [21]. This correlation increases when the eavesdropper comes physically closer to the legitimate receiver but can be decreased by increasing electrical distance between them through shorter wavelength carriers, i.e., mmWaves [22]. However, shorter wavelength applies further constraints to the hardware, such as complexity in antenna-duplexing, which is required to ensure channel reciprocity within a round-trip path [23], [24], [25]. The advancements in physical layer research calls for compatible hardware to endorse its contemporary PhySec proposals in a real wireless environment.

The contemporary research in the 60 GHz band shows a high dependency on a few commercially available off-the-shelf (COTS) front-ends for link-level experiments [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36]. Their downsides are simplex transmission, non-sweepable carrier, and unavailability of agent-mode operation, making them non-compatible with FCS and CRKG [37], [38]. A survey

Manuscript received 31 January 2024; revised 12 April 2024, 3 June 2024, and 24 June 2024; accepted 30 June 2024. This work was supported in part by the Project "Fast Secure" of German Federal Ministry of Education and Research (BMBF) under Grant 03ZZ0522B; and in part by the Institute of Communication Technology (IfN), Technische Universität Dresden (TU Dresden), Germany. This article was recommended by Associate Editor R. Gomez-Garcia. *(Corresponding author: Muhammad Umar.)*

Muhammad Umar is with the RF Design Enablement Group, Barkhausen-Institut gGmbH, 01067 Dresden, Germany (e-mail: muhammad.umar@barkhauseninstitut.org).

Axel Schmidt, Martin Laabs, and Dirk Plettemeier are with the Institute of Communication Technologies (iFN), Technische Universität Dresden (TU Dresden), 01069 Dresden, Germany (e-mail: axel.schmidt@tu-dresden.de; martin.laabs@tu-dresden.de; dirk.plettemeier@tu-dresden.de).

Niels Neumann is with the Institute of Electrical Information Technology, Technical University of Clausthal, 38678 Clausthal-Zellerfeld, Germany (e-mail: niels.neumann@tu-clausthal.de).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSI.2024.3428609.

Digital Object Identifier 10.1109/TCSI.2024.3428609

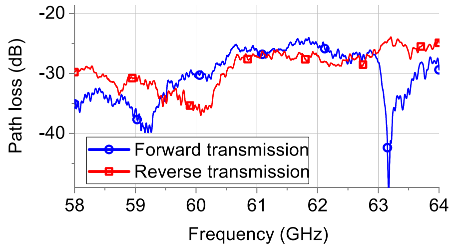


Fig. 1. Round-trip channel response in a multipath environment measured using seperate Tx and Rx antennas [50].

TABLE I

FEATURES OFFERED BY STATE-OF-THE-ART 60 GHz FRONTENDS

Feature	**COTS**		**Published articles**			**Proposed**
	[37]	[38]	[41]	[42]	[43]	
Mode	Sx*	Sx*	Sx*	Sx*	Sx*	H.Dx**
BW (GHz)	7	7	7	3	6	6
Carrier step (MHz)	500	500	500	Fixed carrier	Fixed carrier	1
Carrier sweep	✗	✗	✗	✗	✗	✓
Agent mode	✗	✗	✓	✗	✗	✓

(∗) Sx.= simplex (∗∗) H.Dx.= half duplex

reports the variety of 60 GHz COTS front-ends and their provided features as a bottleneck for seamless continuation of modern research [39]. Designing a tailor-made integrated circuit for mmWave front-end presents formidable challenges at various design stages followed by time taking production cycles [40]. On the other hand, scholarly articles unveiling the modular front-end construction using mmWave circuits with chip-on-board approach are also scarce and lack the features discussed above [41], [42], [43], [44], [45]. The modular integration involves application-specific redesigning of passive circuits because simple frequency scaling of low-frequency components is seldom practical. High-frequency interconnects, e.g., bondwires, exhibit dominant parasitics. Furthermore, the unavailability of lumped surface mount devices (SMDs) and susceptibility towards manufacturing process tolerance adds to the challenges. Therefore, the modular construction of a standalone mmWave front-end needs considerable work compared to the legacy chip-on-board approach for lower microwave bands. To develop a modular front-end, authors have already contributed several essential mmWave blocks and interconnects in [46], [47], [48], and [49].

This paper reports a 60 GHz planar modular front-end constructed using COTS chipsets and tailormade passive blocks, all compatible with standard printed circuit technology (PCT). The front-end is reconfigurable for its carrier frequency within 58 – 64 GHz with 1 MHz of frequency step. The prominent features are antenna-duplexed two-way communication, frequency sweeping, and agent-mode operation. Two front-end units are used to demonstrate digital data transmission and round-trip FCS providing a platform to CRKG. An encryption key generation algorithm is implemented to demonstrate CRKG at 60 GHz. The design criteria and technology choice of the hardware is given in Section II. Section III presents building blocks followed by their integration in Section IV. Utilization of the front-end in FCS setup and the PhySec are given in Section V and VI, respectively.

TABLE II

SUBSTRATE PROPERTIES AND PCB PROCESS RESOLUTION

Substrate		**Process**	
Relative permitivity	3.66	Metal & gap resolution	0.1 mm
Substrate height	254 µm	Min. via diameter	0.1 mm
Metallization	35 µm	Min. via pitch	0.35 mm
Loss tangent	0.0021	Min. via pad diameter	0.3 mm

II. DESIGN CRITERIA AND TECHNOLOGY CHOICE

Wireless channel reciprocity, which is a prerequisite for CRKG, can not be ensured in a multipath environment if a transceiver's Tx and Rx antennas are more than half a wavelength apart [20]. It has been demonstrated by the FCS results in Figure 1 generated by separate Tx and Rx antennas reported by the authors in [50]. Separate antennas transmit and receive the waves in different paths in a multipath environment. Therefore, an antenna duplexer is required to route Tx and Rx signals through a single antenna and wireless path. To the best of the authors' knowledge, this feature is unavailable in COTS mmWave front-ends and unaddressed in contemporary research as summarized in Table I.

A. Design Technology

The choice of components is critical for the application-specific utilization of COTS chipsets. The 60 GHz transceiver chipset is selected from the "Infineon BGT" chipset family for its inbuilt Tx and Rx chains. This chipset has been used by the authors before for a comparably simple front-end design [50]. However, its downside in the current application is non-duplexed (separate) Tx and Rx antennas. This work presents and utilizes the additional building blocks, necessary for single antenna operation. Therefore, the architecture differs from [50] in the radio frequency (RF) chain, which fetches the 60 GHz signal between the chip and the antenna. At mmWave frequencies, ferrite-based circulators are not available for antenna duplexing, while planar quasi-circulators provide load-dependent isolation with high insertion loss [51]. The alternative option is an antenna switch, used in this work, providing time-division-based antenna-duplexing. A single pole double throw (SPDT) MACOM-MA4AGSW2 PIN-diode switch is selected for its bandwidth coverage. The switch die requires bondwire connectivity and a DC biasing network. Based on the requirements, a simplified block diagram of the front-end is presented in Figure 2. The planar integration of the building blocks is accomplished using PCT for its economical and rapid prototyping. However, mmWave circuits on printed circuit boards (PCB) need particular attention due to layout resolution cap, higher manufacturing tolerance, and substrate parameters' deviation, as discussed in [50]. The substrate and process properties are given in Table II.

B. Measurement Setup

The designed PCB blocks are characterized by probing with 400 μ m pitch ground-signal-ground (GSG) probes and Rohde & Schwarz ZVA67 4-port vector network analyzer (VNA). A probe launch-pad is designed for probe contact to

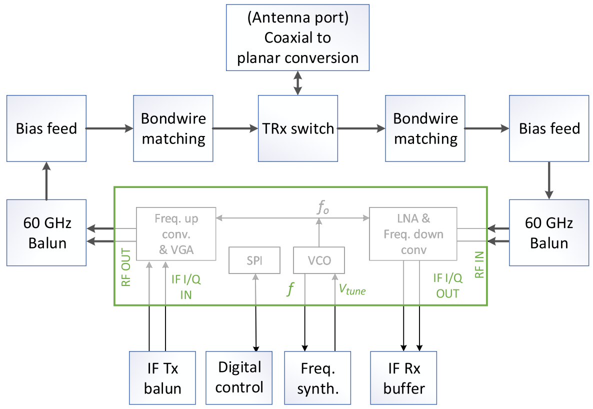
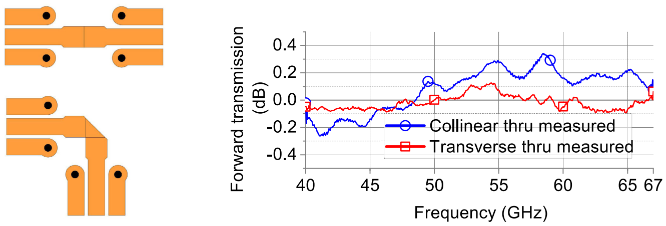


Fig. 2. System block diagram. Transceiver chipset is shown with green border.



(a) Thru standard (b) Post calibration measurement

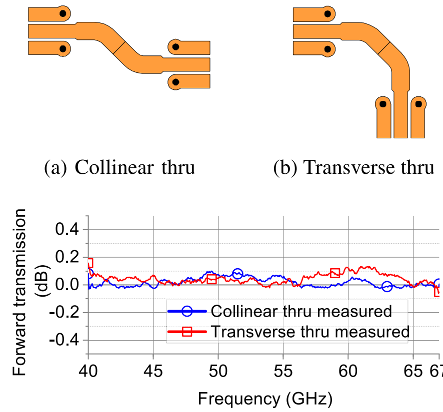
Fig. 3. On-substrate (a) collinear and transverse thru standards for 3-port calibration and (b) calibration verification.

on-substrate thru-reflect-line (TRL) calibration standard. The integration stages of our front-end requires several three-port RF structures requiring compatible calibration. The third port on the probe station is only possible at a transverse angle to two collinear ports introducing non-uniform delays between collinear and transverse lengths due to an additional bend, as notable in Figure 3a. It disturbs the reference plane during the calibration and a solution for this problem is not provided by the commercial calibration substrates and software. A post-calibration measurement of the thru standards is plotted in Figure 3b showing 0.6 dB (±0.3 dB) of calibration deviation. Delay compensation through EM simulations or approximating equations may require several manufacturing iterations. The innovative technique applied in this work is introducing a 45° bend in the probe launch pad [52]. In this way, collinear and transverse thrus and lines undergo equal bends, as shown in Figure 4a and 4b. Measurement of thru standards after the proposed 3-port TRL calibration is plotted in Figure 4c showing relatively flat behavior. The curve deviation from 0 dB is ≤ 0.1 dB which is an acceptable calibration error due to manufacturing variations and known challenges with probe contact repeatability.

III. Building Blocks

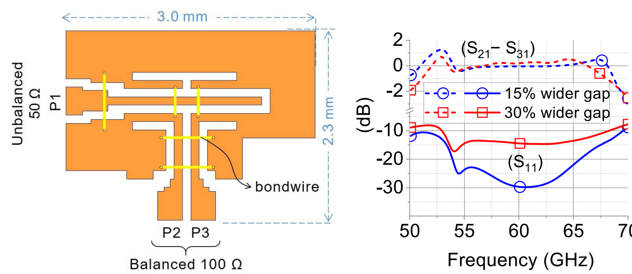
A. Balun

This work utilizes the wideband double-edge coupled Marchand balun configuration from [47], shown in Figure 5a. A fine-tuning of the layout and bondwire loop profiles is performed to obtain a flat amplitude response over the



(c) Post calibration measurement

Fig. 4. (a & b) Proposed on-substrate thru standards with 45° bended probe launch-pad and (c) calibration verification.



(a) Layout (b) Effect of etching tolorance

Fig. 5. Marchand balun layout and etching impact analysis.

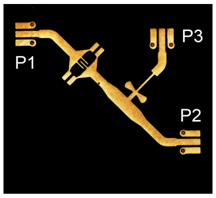
selected bandwidth 58 – 64 GHz. This work also includes a simulation-based performance analysis of the design toward manufacturing process tolerance to ensure its performance with the low-cost PCB processing. A 10 dB matched input response with amplitude imbalance <1 dB is verified for an over-etching of up to 30%, as plotted in Figure 5b, indicating the balun can be used in the intended system with standard PCB process.

B. Bias Feed

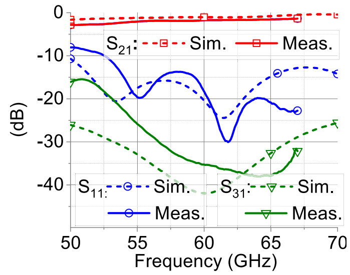
In this work, the design from [48] is validated through laboratory measurements and then utilized. For this purpose, the bias-tee prototype has been remanufactured with 45° bends in probe launch pads (see Figure 6) and 3-port RF-probing setup is used from Section II-B. Measurement curves in Figure 6b largely agree with simulation results. However, the proximity of the probes impacts the measured isolation level because a minor over-the-air coupling affects these low decibel scale values. Nevertheless, measured DC-to-RF isolation is >30 dB over the bandwidth of use, sufficient for our application.

C. Bondwire Interconnects

The switch die (MACOM-MA4AGSW2) requires bondwire connectivity. To evaluate the bondwire parasitics, we utilize the lump element model presented in [49], which is then used as a seed for matching network design, notable in Figure 7a, and its

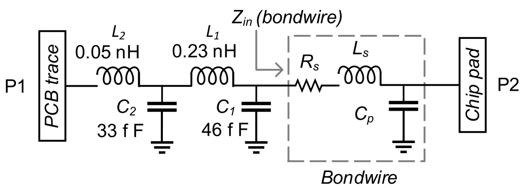


(a) Manufactured

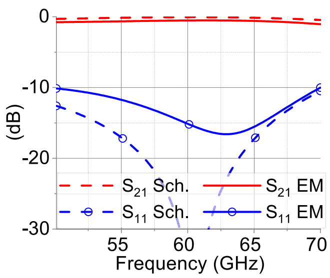


(b) Loss (S21), matching (S11), isolat. (S31)

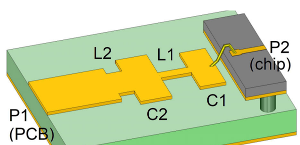
Fig. 6. 60 GHz DC-blocking bias-tee (a) prototype and (b) results.



(a) Two stage LC network for bondwire parasitics' compensation.

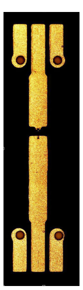


(b) Simulated response

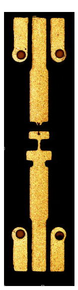


(c) PCB layout

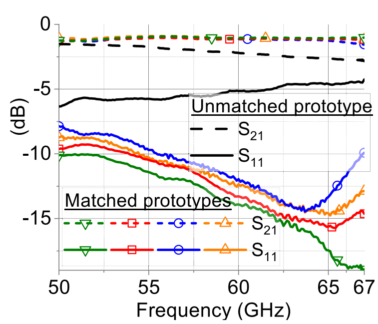
Fig. 7. Bondwire matching network (a) design, (b) simulation resutls and (c) layout implementation.



(a)



(b)

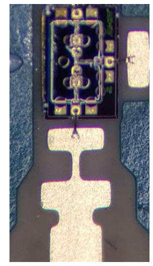


(c)

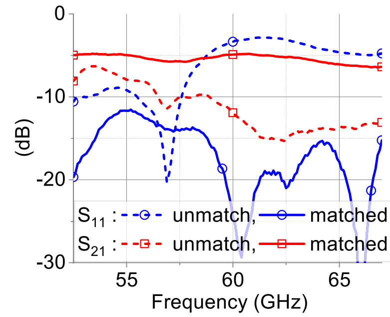
Fig. 8. (a) Unmatched, (b) matched prototype for PCB-to-PCB bondwire and (c) their measured response. Each curve represents one matched prototype.

response plotted with dash curves in Figure 7b. Its layout realization (depicted in Figure 7c) is performed in planar lumped fashion by exploiting narrow traces' inductance and large traces' ground capacitance [53]. However, the downside of the planar-lumped approach is the presence of parasitic inductance and capacitance in capacitive and inductive traces, respectively. It reduces the matching on the layout level, as notable from EM layout simulation results given in Figure 7b using solid curves.

For laboratory validation, PCB-to-PCB matched bondwire interconnects are designed as presented in Figure 8. In this

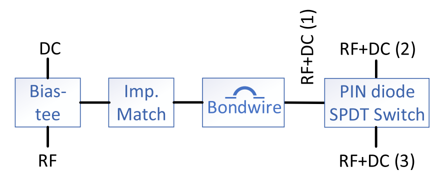


(a) Prototype

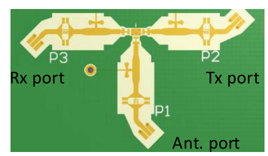


(b) Measured response

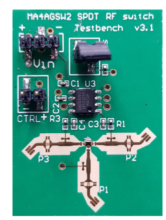
Fig. 9. (a) Matched chip-to-PCB bondwire interconnects and (b) measured input reflection coefficient (Γin) and insertion loss (I.L.).



(a) Block diagram of one of the three chains of antenna duplexer.



(b) Layout zoom-in



(c) Manufactured

Fig. 10. Antenna-switching duplexer (a) block diagram, (b) layout, and (c) manufactured prototype.

work we have verified the repeatability of the technique by developing several PCB-to-PCB prototypes, each containing a natural variation in the bondwire loop profile. Prototypes are bonded with 25 μ m gold wires using a semi-automatic bonder "TPT HB-16". Figure 8c shows the measured response of various prototypes. It is noticeable that the general behavior of all curves is the same and 10 dB of input matching is obtained for over 10 GHz bandwidth for the least performing interconnect. Finally, chip-to-PCB interconnects are verified by bonding the switch die to biasing networks through bondwires, without and with bondwire matching networks as visible in Figure 9. The plotted response verifies the interconnect performance. The insertion loss includes a pair of bias-tees, bondwires, and on-chip passive circuitry.

D. Antenna Duplexer

Using the aforementioned RF components, an antenna duplexer is manufactured and validated before integrating into the system. Figure 10a indicates the required blocks. MADR007097 chipset is utilized for the biasing generation. Switching action is performed through the control voltage of the driver chip, i.e., 0 or +5 V. The zoom-in of the layout and a manufactured prototype are also shown in Figure 10. P1 (antenna port) is switched between P2 (Tx port) or P3 (Rx port), depending on the control voltage. Measurements are

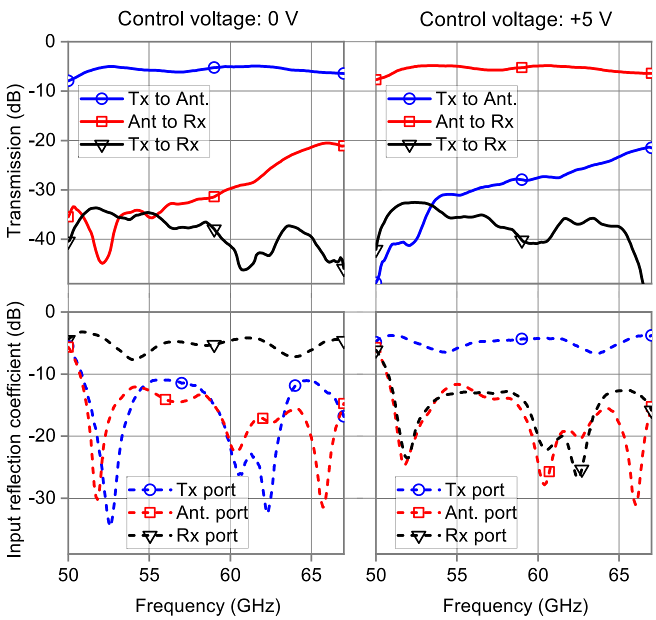


Fig. 11. Measured results by 3-port probing of the antenna duplexer.

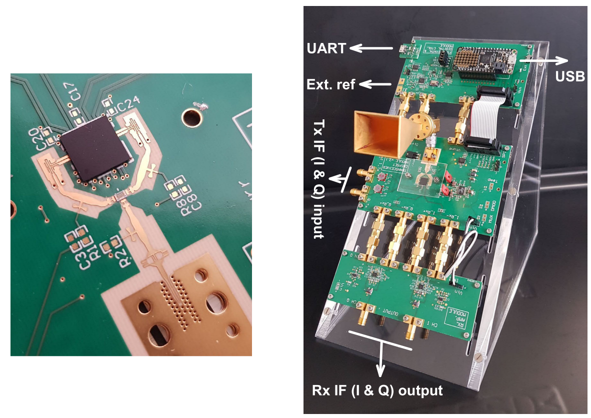
taken using simultaneous three-port probing and switching the control voltage to validate both transmission paths.

Measurement results are plotted in Figure 11. Insertion loss of 5 dB is noted for each transmission path, including insertion loss of two bias-tees, two bondwire matchings, and a passive on-chip network. The disconnected port remains isolated from the antenna by $>$ 20 dB. The input reflection coefficient at the connected ports remains below -10 dB for 52 – 67 GHz in both transmission paths. The isolated port reflects the input signal as noticeable from reflection coefficient curves. Leakage from Tx to Rx port is plotted with solid black curves, showing isolation better than 30 dB. Both transmission paths show similar curve trends verifying circuits' symmetry and equipment calibration.

IV. System Integration and Characterization

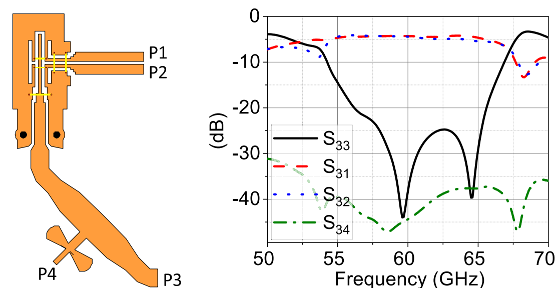
The interconnection of all RF blocks of Figure 2 forms a Y-shaped chain with a switch chip in the center, as depicted in Figure 12a. A photograph of the complete front-end is visible in Figure 12b. Baluns in the upper two arms of the Y-shaped chain connect to differential Tx and Rx ports of the mmWave chipset. Interestingly, both upper arms do not need DC-blocks (unlike the duplexer prototype in Section III-D) because the designed baluns already provide a DC-blocking function. The upper arm becomes a 4-port network, as shown in Figure 13 along with the simulation results. It has an insertion loss of almost 4 dB from each RF port to the choke output with DC/RF isolation $>$ 30 dB. On-substrate probing of this structure is not possible without modifying the structure shape, hence, only the simulation results are given here.

A DC-block is deployed in the lower arm to allow interfacing lab equipment or active antenna systems. The lower arm is common for Tx and Rx chain ending in the landing pad of Rosenberger 08K80A-40ML5 1.85mm V-band connector for planar-to-coaxial transition. The discussed blocks are



(a) RF-chain zoom-in (b) A photograph of the complete front-end. Size : 21 cm × 11 cm.

Fig. 12. Developed 60 GHz frontend.



(a) (b)

Fig. 13. (a) Upper arm of the RF-chain and (b) the simulation response.

integrated on 4 layered PCB stack up with Isola "I-Tera MT" prepregs and FR4 core. This PCB module is named as RF-board and is the middle one of the three boards visible in Figure 12b. It further contains switch driving circuitry, baluns for Tx intermediate frequency (IF) inputs, and a power supply.

A frequency synthesizer board is developed using an ADF4175 phase-frequency detector chipset, as explained in [50]. The board is redesigned for interfacing with the RF-board and is visible in Figure 12b as the top one of the three boards. A third PCB module is developed to buffer and amplify receiver IF output using Texas Instruments THS4509 fully differential amplifiers. The modular realization facilitates individual characterization and troubleshooting. PCB modules are connected with SMA connectors and ribbon cables for IF and digital signaling, respectively. The front end is equipped with an off-the-shelf 23 dBi SAR-2309-15-S2 horn antenna from Sage Millimeter, Inc. Figure 12b presents a photograph of the front-end.

The developed front-end can reconfigure its system parameters e.g. frequency, output power, switching between transmitter and receiver, I/Q modulation calibration, and local oscillator (LO) switching during run time through a command line user interface (UI) with defined commands. In addition, the loop filter bandwidth can be adjusted on the hardware accessible on the PCB. The microcontroller can be reprogrammed to implement complex procedures and algorithms in the front-end. Furthermore, a universal asynchronous

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

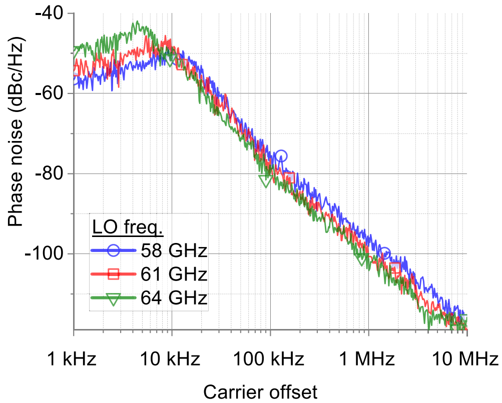


Fig. 14. Measured LO phase noise of the front-end.

transmit-receive (UART) port is provided which can be used to control the front-end externally, e.g., for agent-mode operation in a system of devices. To the best of the authors' knowledge, this front-end outstands the existing COTS and published designs at 60 GHz in terms of the degree of reconfigurability. The presented modular architecture also supports future expension opportunities, e.g., equipping it with a passive beamformer module controlled through the existing digital control circuitry, etc.

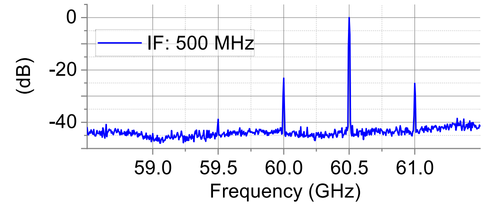
A. LO Generation

Generated LO purity is characterized by Rohde & Schwarz FSW67 spectrum analyzer (SA) for various LO frequencies generated by reconfiguring the frequency divider in the ADF4157 chipset. Measured phase noise for minimum, center, and maximum LO frequencies is plotted in Figure 14 showing approximately −100 dBc/Hz double sideband noise at 1 MHz carrier offset.

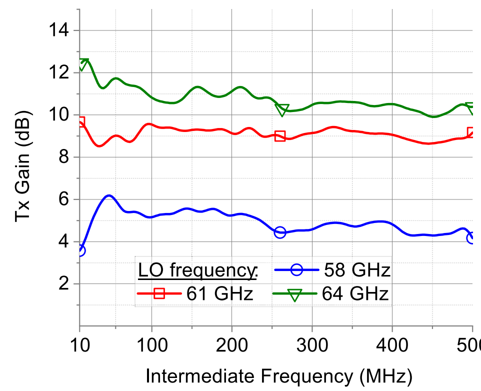
B. Front-End as Transmitter

In Tx mode, the front-end performs quadrature upconversion of the applied I and Q signals for a maximum IF of 500 MHz recommended by the chipset in use. An up-converted spectrum is presented in Figure 15a as an example. Carrier suppression is achieved by adjusting the mixer current, while lower sideband (LSB) suppression is done through I-to-Q phase adjustment of the applied IF signals on the cost of an additional harmonic component at $LO + 2IF$. Nevertheless, the harmonic remains 25 dB weaker than the upper sideband (USB). In contrast to Ref. [50], the spectrum does not contain any undesired frequency components due to separating the RF routing on the PCB from digital and IF signals. Tx-chain gain is measured using Rohde & Schwarz ZVA67 VNA. One port of the VNA generates sweeping IF input, and the other measures the upconverted output, while the front-end generates LO internally. Figure 15b presents Tx gain for swept IF with various LO frequencies showing a LO dependency of gain.

Digital modulation is demonstrated by quadrature upconversion of two baseband data waveforms generated by the Anritsu 3710A vector signal generator (VSG). From VSG operational limits, waveforms are generated at 200 MHz IF,

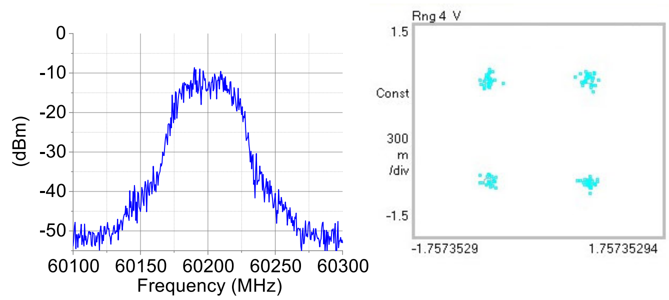


(a) Normalized up-converted spectrum for IF = 500 MHz and LO = 60 GHz.



(b) Up-conversion gain of the transmitter chain.

Fig. 15. Measured characteristics of the Tx-chain.



(a)

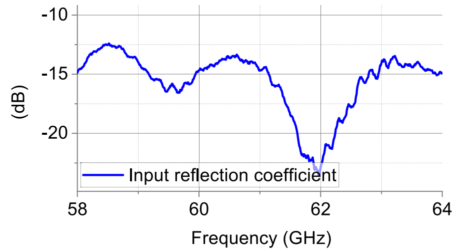
(b)

Fig. 16. (a) Modulated signal spectrum at 60 GHz (captured with SA resolution BW of 3 MHz) and (b) IQ-constellation as on the DSA screen.

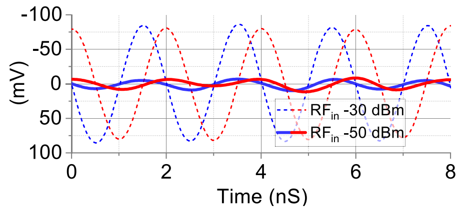
each carrying 50 Mbps data. Figure 16a shows the upconverted output spectrum of a 100 Mbps quadrature phase shift keying (QPSK) signal. The modulated signal is analyzed by Agilent DSA90804A digital signal analyzer (DSA) supported by Agilent 89600VSA software. Figure 16b shows the recovered IQ constellation. The DSA reports an error vector magnitude (EVM) of 9.2 %rms.

C. Front-End as Receiver

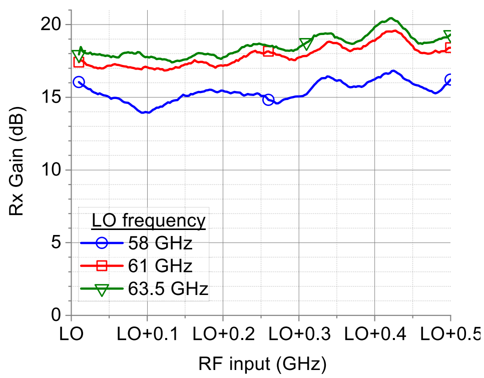
In Rx mode, the front-end performs quadrature downconversion of the RF signal and outputs the IF I and Q components. The chipset supports maximum input power of 0 dBm and a signal bandwidth of 500 MHz. The input matching of the receiver chain is measured with a VNA, which is better than −13 dB for overall working bandwidth as presented by Figure 17a. Figure 17b presents an example of downconverted waveforms for RF input frequency higher than LO, producing $IF = RF - LO$. Rx-chain gain is measured



(a) Input matching of the receiver chain.



(b) Frequency down-converted I and Q components with RFin = 60.5 GHz and LO = 60 GHz.



(c) Down-conversion gain

Fig. 17. Measured characteristics of the Rx-chain.

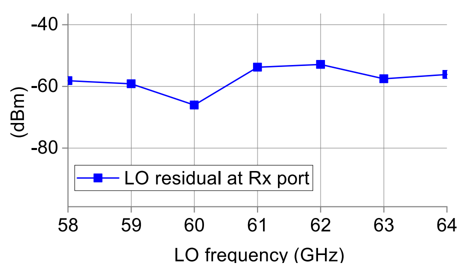


Fig. 18. LO residual at the receiver port.

using the same setup explained for Tx-gain, which is plotted in Figure 17c. The LO residual at the RF input port is measured using SA and manually varying LO from the user interface, plotted in Figure 18 and noted < -50 dBm.

The receiver chain is further used for digital data demodulation. Due to the unavailability of 60 GHz VSG in the authors' lab, two front-end units are connected back to back through their RF ports, one operated as a modulator, as explained earlier, producing 100 Mbps QPSK signal at 60 GHz. The receiving front-end downconverts the received signal to 200 MHz which DSA then analyzes. Automatic clock recovery and equalization of the DSA are used, reporting the

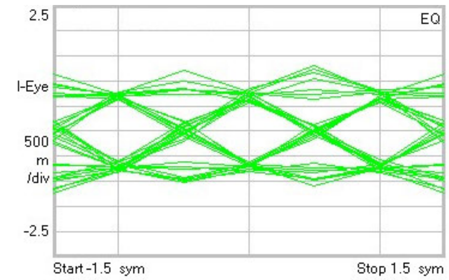


Fig. 19. Recovered eye-diagram for I-component from the down-converted signal, as shown on DSA screen.

EVM of 9.9 %rms. As an example, the recovered eye diagram of the I channel is plotted here in Figure 19.

V. Application as Channel Sounder

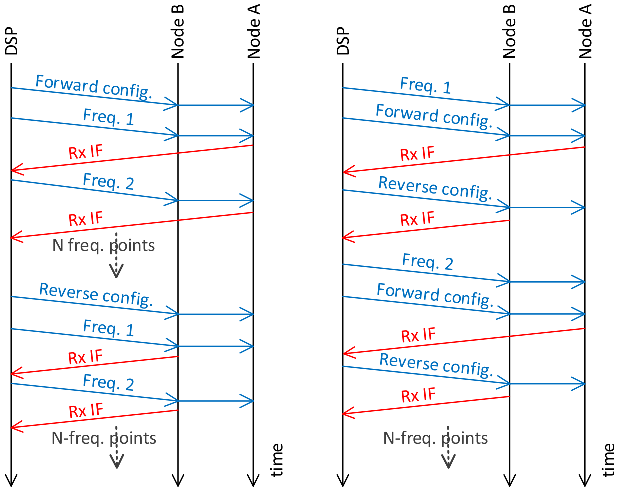
Two front-end units are employed in round-trip (forward and reverse channel) FCS within 58 – 64 GHz. Red Pitaya STEMlab 125-14, an economical COTS digital signal processor (DSP), is used for IF generation, baseband processing and synchronization. It has two Tx and two Rx channels with 14-bit 125 MS/s digital-to-analog converters (DACs) and analog-to-digital converters (ADCs) supporting signals up to 50 MHz.

There can be two strategies for round-trip channel sounding: i) Sounding the forward channel with a frequency sweep followed by the reverse channel, here referred to as continual sweep. ii) round-trip sounding of one frequency point before moving to the next, here referred to as alternating sweep. The command flow of both schemes is given in Figure 20. Continual sweep reduces the synchronization command overhead for rapid switching of the front-end between Tx and Rx operation; hence, completing the process faster. On the other hand, an alternating sweep reduces the time delay between the forward and reverse sounding of each frequency point and preserves the channel reciprocity in varying channels. Since the target application is CRKG, therefore alternating sweep sounding is considered in this work.

A. Sounding Process

Two Tx channels of the Redpitaya generate I and Q IF signals. 20 MHz is selected for IF as experiments show a better voltage accuracy of Redpitaya DAC and ADC at this frequency. LO frequency of the front-ends is tuned 20 MHz lower than required to use USB after up-conversion. LSB suppression is achieved by IF I-to-Q phase adjustment in the Redpitaya source code. LSB suppression is necessary as it acts as an image frequency for the receiver LO, adding a response of a channel 40 MHz away from the desired. Redpitaya sends a 16-bit command through UART connection to both units specifying the next frequency point for sounding and assigning each unit Tx or Rx operation. Implemented frequency sweep resolution is 1 MHz. The front-ends can support more refined resolutions; however, lengthy UART commands are required to specify values in kilohertz.

Redpitaya generates a frequency sweep by regularly sending UART commands to front-end units to increase the LO



(a) (b)

Fig. 20. Command flow for (a) continual sweep and (b) alternating sweep.

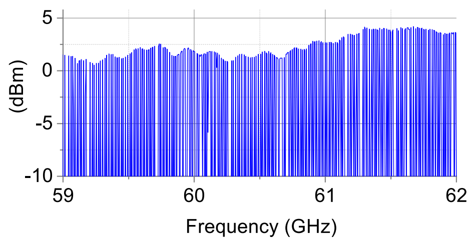


Fig. 21. Frequency sweep generated by the front-end and captured by SA.

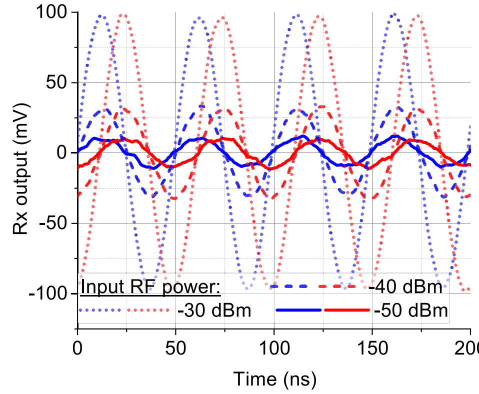


Fig. 22. Downconverted I (black) and Q (red) waveforms for different RF input power levels captured using digital oscilloscope.

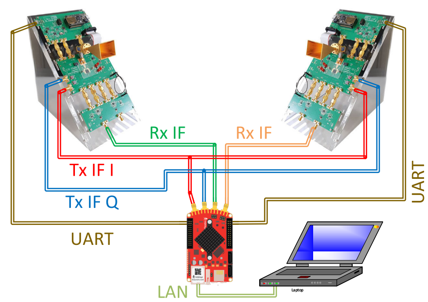
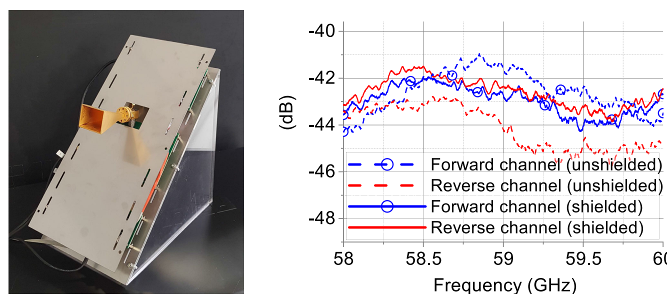


Fig. 23. Channel sounder setup using two 60 GHz front-end units, a Redpitaya STEMlab and a computer terminal.



(a) (b)

Fig. 24. (a) Photograph of the front-end with EMI shielding. (b) Round-trip channel sounding results with and without EMI shielding.

frequency in the defined step. Figure 21 shows an example of a frequency sweep captured by SA with a relatively larger (15 MHz) step size for plot clarity. It is difficult for SA to capture a sweeping signal perfectly as it also works on the sweeping principle. Therefore the plot shows some missing frequency points. This sweep signal is transmitted over the wireless channel and received by the synchronized Rx front-end unit. RF wave at each frequency point is down-converted to a 20 MHz IF wave carrying path loss information of that RF. Figure 22 shows signals downconverted to 20 MHz for various RF input powers. The ADC of the Redpitaya samples the IF signal and calculates the signal power as

$$P = \frac{1}{N}\sum_{n=1}^{N}|x(n)|^2 \tag{1}$$

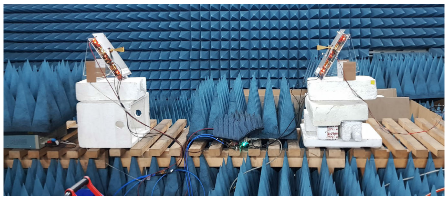
where x is the value of n^{th} sample and N is the sample space, 16384 maximum for Redpitaya. Path loss for each frequency point is stored in CSV format.

B. Assembly and Calibration

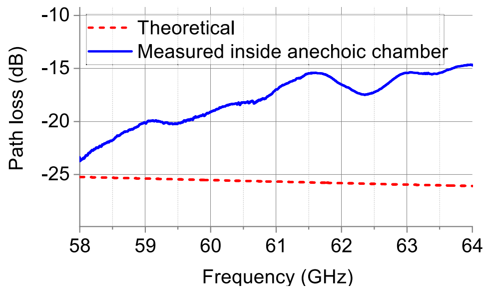
A single Redpitaya feeds I and Q IFs to both units as depicted in Figure 23. However, only the Tx unit uses the IF. The Rx unit downconverts the received 60 GHz signal to IF I and Q components. Only I component is used for further processing because both I and Q are affected by path loss similarly. Using both I and Q components can of course increase system performance against noise but requires an advanced DSP kit with four Rx channels. Both units share the UART connection to receive the commands simultaneously.

Experiments show EM interference distorting the channel response when Tx signal hits bare boards of the Rx unit, coupling the energy into PCB traces, bondwires, and dies. It introduces the mismatch between forward and reverse channel response, e.g., as plotted in Figure 24. To mitigate this problem, the PCBs are enclosed between two metal plates.

For setup calibration, the frequency response of the front-ends is determined by link-level measurements of a line-of-sight (LOS) link inside an anechoic chamber. The measured result consists of the hardware response as well as the LOS path loss. Since the latter is already known theoretically, the hardware response can be determined for all frequency points which is the error magnitude in the measurements. The



(a) Photograph of measurement setup inside the anechoic chamber.



(b) Theoratical vs. measured LOS response with 1.5 m distance.

Fig. 25. Channel sounder calibration (a) setup and (b) result.

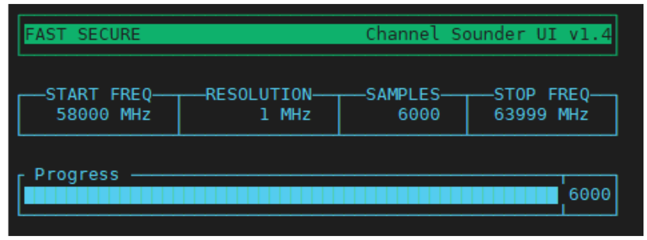


Fig. 26. Screen shot of the command line interface of channel sounder.

measurement result taken inside an anechoic chamber using 23 dBi antennas on each side over a 1.5 m LOS link is plotted in Figure 25 against the theoretical value of the path loss for the same distance, including additional oxygen absorption in the 60 GHz band. The deviation between the two curves provides the hardware response that will be subtracted from each channel measurement.

C. Short Distance Channel Sounding

The channel sounder setup can round-trip FCS within 58 to 64 GHz band with a maximum 1 MHz resolution. A command-line UI is designed to input the start, stop, and resolution frequency, shown in Figure 26. The output of the process is amplitude-frequency response of the forward and reverse channels made available in csv file format. The hardware has been used to measure indoor channels up to 5.5 m distance. Measured channels include LOS, reflected and multipath environments created by metal sheets, and a random assembly of Teflon rods in the free space.

A few examples of the measured amplitude frequency response by channel-sounder are given in Figure 27. The measurements show a high level of agreement in the forward and reverse channel response, which indicates that the hardware ensures the channel reciprocity at 60 GHz, in contrast to the sounding results obtained with separate antennas for transmission and reception on a single node, as plotted in Figure 1. Unlike the previously reported channel-sounding setups, this setup does not require bulky lab equipment or COTS modules as compared in Table III. Except for reference [8], [9], and [10], who completely rely on lab equipment, the swept bandwidth of our hardware is higher than all the previously reported setups which incorporated customized circuits with a VNA or PXI system. The published channel sounding campaigns report an unambiguous time range of 200 ns being enough for reliable indoor channel characterizations [18]; this setup allows a five-fold better time range. Moreover, it fairly competes with the other references for frequency resolution despite their exploitation of VNAs for sweep generation. Furthermore, the presented channel sounder has comparatively the smallest form factor and is unique in terms of permitting round-trip sounding. To the best of the authors' knowledge, this work is the first contribution towards frequency-swept round-trip mmWave channel sounding while preserving channel reciprocity. This feature makes this front-end compatible with the applications depending on round-trip channel reciprocity, e.g., reciprocity-based MIMO channel training and CRKG, etc., which are still demonstrated on classical centimeter-wave frequency bands.

VI. Physical Layer Security

One use-case for the channel sounder described in Section V is the PhySec approach of key generation out of channel measurement data, which will be detailed in this section. This approach can complement the security architecture of wireless systems by adding a safe and easy way to provide encryption keys. In combination with the channel sounder now reasonably-priced investigations could be carried out, which were not feasible up to now.

A. Scenario and System Model

We consider a wireless communication system where two legitimate transceivers, Alice and Bob, generate the secret key based on their common source of randomness, which is the channel characteristics between them, acquired through the channel sounder explained in the previous chapters. Assuming Eve is a passive eavesdropper, she might overhear the measurement procedure without being noticed. However, there is no realistic scenario for Eve to estimate the channel characteristics between Alice and Bob correctly because due to the wavelength of a few millimeters only, she will overhear the transmission through an uncorrelated channel in a multipath environement [20]. This scenario is known as the source-type or source model introduced in [55] and [56].

B. Bit Extraction

Raw data for key generation is determined by the channel sounder mentioned above, which will execute channel measurements bi-directional in this case. Despite the channel's reciprocity, Alice and Bob's measurement results contain variation due to noise, hardware variation, and possible interference (e.g., see Figure 27), resulting in an unidentical bit sequence at Alice's and Bob's sides. To ease the following information reconciliation phase, minimizing the number of

TABLE III
STATE-OF-THE-ART SETUPS FOR FCS IN MMWAVE BANDS

Ref.	Bandwidth (GHz)		Freq. Res. (MHz)	τ_{res}* (ns)	τ_{amb}** (µs)	Range (m)	Cal.	Hardware / (portability)	Sounding mode / Ch. reciprocity
[8]	35	[75.0 – 110.0]	1	0.02	1	3.6	Thru	VNA+Ext./(no)	One way/ (no)
[9]	20	[90 – 110]	3.3	0.05	0.30	2.25	Thru	VNA+Ext./(no)	One way/ (no)
[10]	15	[3 – 18]	0.5	0.06	2	53	Thru	PXI system / (no)	One way/ (no)
[54]	6	[58.0 – 64.0]	Chirp	0.16	–	38	Anechoic	Coax modular / (yes)	One way/ (no)
[50]	6	[58.0 – 64.0]	1	0.16	1	5.5	Thru	PCB modular / (yes)	Round trip/ (no)
[11]	4	[26 – 30]	2.6	0.25	2.6	41	Thru	VNA / (no)	One way/ (no)
[12]	3.5	[60.5 – 64.0]	7	0.28	0.14	4.3	N.A.	VNA+synth./ (no)	One way/ (no)
[13]	3.5	[26.5 – 30]	0.5	0.28	2	46	Anechoic	VNA+optical/ (no)	One way/ (no)
[14]	2	[59 – 61]	5	0.5	0.2	6	–	VNA /(no)	One way/ (no)
[15]	2	[57.0 – 59.0]	2.5	0.5	0.4	12	Anechoic	VNA+mixer/ (no)	One way/ (no)
[16]	2	[28 – 30]	2	0.5	0.5	43	Thru	VNA+optical/ (no)	One way/ (no)
[17]	1	[59.6 – 60.6]	0.1	1	10	>100	Thru	PXI system/ (no)	One way/ (no)
[18]	1	[63.4 – 64.4]	0.625	1	1.6	50	Anechoic	VNA+mixer/ (no)	One way/ (no)
This work	6	[58 – 64]	1	0.16	1	5.5	Anechoic	PCB modular/ (yes)	Round trip/ (YES)

*τ_{res} is the equivalent multipath resolution, **τ_{amb} is the equivalent unambiguous time range

non-identical bits by optimal design of the bit extraction procedure is important. The bit extraction we implemented is based on a proposal of the project partners from IHP Frankfurt Oder [57]. The algorithm consists mainly of four steps:

1) Averaging: An (optional) smoothing of measured results through a sliding window of configurable size. The number of samples for further processing is reduced.
2) Partitioning: The whole channel response is partitioned in sections of configurable size, illustrated in Figure 28.
3) Mean: Within each section, the mean value is calculated, in Figure 28 shown as black line. All values above the mean are interpreted as "1", and all values below as "0".
4) Guard interval: Around the mean value in each section, a guard interval can be defined, shown as blue bar in Figure 28. All values within that guard interval can be either discarded (along with the transmission of their index to the opposite side) or randomly substituted by equally distributed "0" and "1".

Extracted bits are combined into a single bit-sequence for information reconciliation. The number of these bits might be fixed for all measurement cycles or varying, depending on the options chosen.

C. Information Reconciliation

The information reconciliation, i.e., the elimination of the remaining differences in the bit sequences extracted by Alice and Bob, consists of three steps:

1) Parity 1: The bits are parted in small groups of adjustable size. The parity is calculated for each group and transmitted to the opposite side. Only the groups with identical parity are kept. For each kept group, one bit is eliminated to avoid information disclosing to Eve.
2) Parity 2: Optionally, there can be a second parity round by choosing a different group size.
3) Error correction: The remaining errors in the bit sequences at Alice's and Bob's sides are corrected utilizing a BCH code. An appropriate code can be generated depending on the remaining bit number, and the error correction capability can be set as a parameter. Alice then interprets the bit sequence as a code word, which can be decoded. The syndrom calculated in the decoding process is transmitted to Bob, who now can also decode a code word. The decoding will be successful as long as the error correction capability is chosen well, i.e., at least the number of remaining errors in the bit sequence. After decoding the code words, the information bits are the key bits we generated out of the channel amplitude frequency response.

A cryptographic hash function can verify the identity of the generated bit sequences at Alice's and Bob's sides. Those functions are non-reversible; Eve cannot calculate any key information from an overheard hash information. Identical key bits are stored; an encryption function might use as many bits as necessary.

D. Demonstration and Results

The key-generator UI is shown in Figure 29. The input values are limited to the following values, estimated from tests:

1) Average: 3 to 7
2) Mean period: 6, 12, 24, 36, 48
3) Guard interval: 0 to 20
4) Parity 1 / Parity 2: 2 to 10
5) Error correction capability: 10 to 70

The UI connects to the Red Pitaya and can reconfigure the channel sounder hardware by:

1) start frequency: in steps of 500 MHz
2) resolution: 1/2/5/10/20 MHz
3) number of samples: 100/200/500/1000/2000/../6000

For the used platform, no real communication is necessary within the demonstrator script between Alice and Bob from an algorithmic point of view. Where required, Alice and Bob can easily be separated with a communication protocol for bit-sequence reconciliation. Every measurement for channel amplitude frequency response is processed up to the final key bits; the remaining bits in the last BCH step are kept and included in the next run.

After verifying the identity of the bit sequences at Alice's and Bob's sides, the first 40 bits are shown in the UI to have an optical impression of the results. The whole sequence is

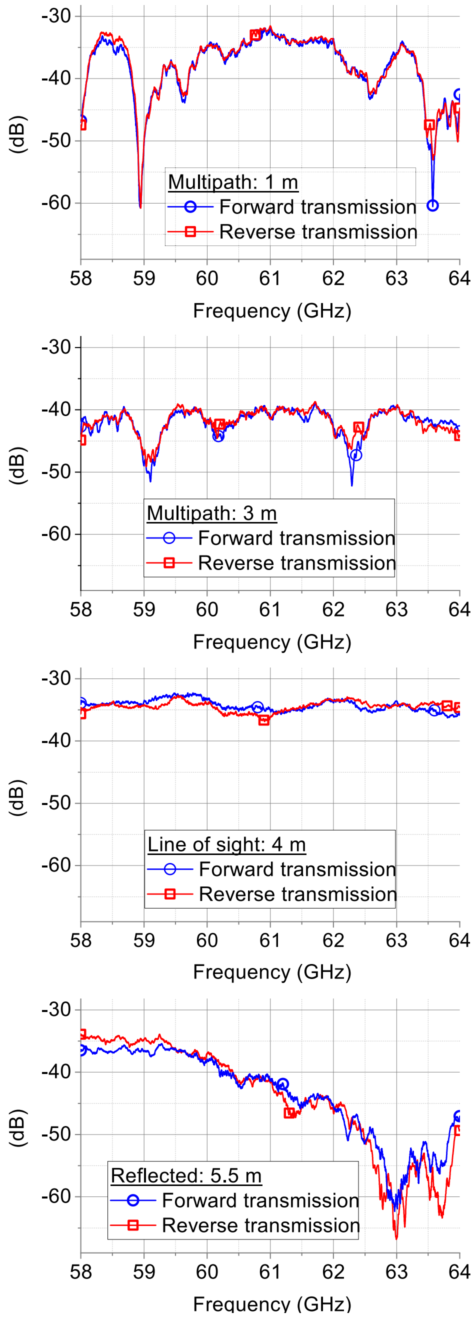


Fig. 27. Round-trip FCS results in various indoor environments.

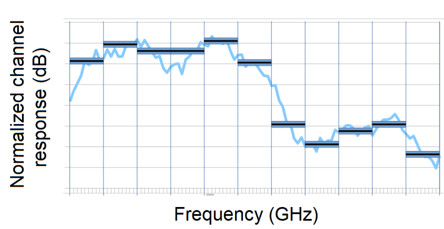


Fig. 28. Principle of bit extraction.

stored for further analysis. With the integration of hardware and software, the maximum bandwidth (6 GHz) and resolution (1 MHz) generate, on average, 584 key bits per measured channel response, sufficient to be used in a commercial system.

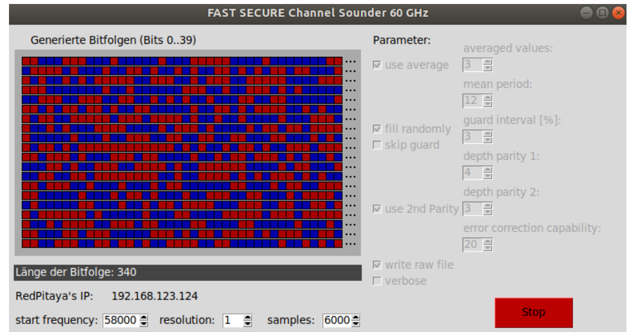


Fig. 29. PhySec demonstrator's user interface.

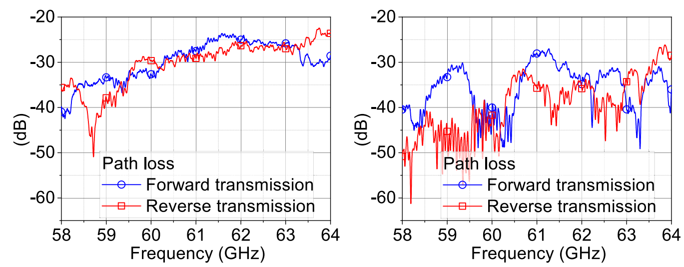


Fig. 30. Two-way channel sounding results using the hardware introduced in [50] in a multipath environment.

E. Discussion

The ultimate key rate of the proposed CRKG approach strongly depends on the level of agreement between forward and reverse channel measurements, i.e., Alice's and Bob's measurements. Since the wavelength of the RF system is a few millimeters only, the separate transmit and receive antennas at each node will result in a deviation between Alice's and Bob's measurement results. To elaborate on the situation, the exemplar two-way channel sounding results are presented in Figure 30, taken through the setup reported in [50], which uses separate Tx and Rx antennas. It is noticeable through visual inspection that forward and reverse channels may have very different frequency responses in some parts of the spectrum. Anyway, we continued by applying the above-mentioned key generation algorithm to the collected channel response data:

- After the bit extraction, the guard interval is checked in Step B(4) to identify the values close to the mean value, for which, a slight deviation between Alice' and Bob's measurements would lead to different bit extraction. In the duplex-sounding case, that results in a slight deviation of values. In the un-duplexed case, due to the very different measurement results, the guard interval becomes very large and a lot of values have to be treated as lying inside the guard interval.
- If the values within the guard interval are skipped, the number of remaining bits (after Step B4), in some un-duplexed sounding scenarios, is reduced by a factor of 3, while in some other scenarios even by a factor of 100, i.e., much less bits are remaining than in the duplexed case.
- If the values within the guard interval are filled randomly, it introduces more bit errors. This increased number of errors has to be corrected afterwards (Step C), which

decreases the final number of key bits substantially as well.

For a reasonable key rate, it is essential to use a single antenna for Tx and Rx on each transceiver node, thus enabling Alice and Bob to obtain channel measurement data as identical as possible. Based on such data only, one can generate a key rate as described in this paper, which seems applicable in a commercial encryption system.

Towards a real-time hardware implementation of CRKG, very few publication have been reported. Ref. [58] reports it using a sub-6 GHz Universal Software Radio Peripheral (USRP) with an antenna-duplexed TRx interface. While [59] uses a 60 GHz COTS hardware for LOS links without antenna duplexing; however, the flat LOS channel response will generate the same key bit sequence every time, which is undesirable in a commercial encryption system. Ref. [59] does not demonstrate a use case in a multipath environment. To the best of the authors' knowledge, this work is the first report for a real-time CRKG demonstration using a millimeter wave band in a multipath indoor environment.

Not part of the project was the verification of the randomness of the generated bits. This point must be addressed for practical usage, even if the results so far look promising. If the randomness is not satisfactory after the generation of the bits, a privacy amplification (see, e.g., [60]) might be included in the algorithm to randomize the generated bits.

VII. Conclusion

Distinct propagation characteristics of mmWave channels call for channels sounding in each deployment scenario. When performed in the frequency domain, round-trip channel sounding becomes useful for CRKG, provided the wireless channel remains reciprocal. A single transmit-receive antenna system is a prerequisite to preserve channel reciprocity by routing forward and reverse propagation through the same path in a multipath environment. This work showcases that constructing such a channel-sounding front-end is possible at 60 GHz using COTS chipsets and custom-designed planar RF blocks, e.g., Marchand balun and biasing networks. Bondwire interconnections have a primary role in the modular integration of RF blocks and require special attention for parasitics compensation networks. An antenna duplexing is made possible through an RF switch which enables transmission and reception through a single antenna, preserving the channel reciprocity. The reported front-end can transmit and receive digital data in half-duplex mode and supports indoor round-trip channel sounding within 58-64 GHz with 1 MHz resolution. FCS campaigns in various indoor multipath environments show that the reciprocal amplitude-frequency response of the channel is achieved between two transceiver units, usable for PhySec implementation. An encryption key generation algorithm extracts key bits from the measured channel response and reconciles it with the other legitimate transceiver. CRKG is successfully tested at 60 GHz, enabling real-time parameters estimation for PhySec, e.g., mean period, guard interval, parity, and error correction capability. The developed system can serve as a platform for advancements of PhySec algorithms and hardware, e.g., privacy amplification protocols and a pathway towards multi-carrier mmWave front-ends.

References

[1] A. Al-Saman, M. Cheffena, O. Elijah, Y. A. Al-Gumaei, S. K. A. Rahim, and T. Al-Hadhrami, "Survey of millimeter-wave propagation measurements and models in indoor environments," *Electronics*, vol. 10, no. 14, p. 1653, Jul. 2021.

[2] G. R. MacCartney and T. S. Rappaport, "A flexible millimeter-wave channel sounder with absolute timing," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1402–1418, Jun. 2017.

[3] P. K. Chundi, X. Wang, and M. Seok, "Channel estimation using deep learning on an FPGA for 5G millimeter-wave communication systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 2, pp. 908–918, Feb. 2022.

[4] Q. Zhu, Z. Zhao, K. Mao, X. Chen, W. Liu, and Q. Wu, "A real-time hardware emulator for 3D non-stationary U2V channels," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 9, pp. 3951–3964, Sep. 2021.

[5] X. H. Mao, Y. H. Lee, and B. C. Ng, "Comparison of wideband channel sounding techniques," in *Proc. PIERS*, 2009, pp. 400–404.

[6] T. Yucek and H. Arslan, "Time dispersion and delay spread estimation for adaptive OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 57, no. 3, pp. 1715–1722, May 2008.

[7] K. A. Remley, C. Gentile, A. Zajic, and J. T. Quimby, "Methods for channel sounder measurement verification," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–4.

[8] M.-T. Martinez-Ingles et al., "Channel sounding and indoor radio channel characteristics in the W-band," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 30, Dec. 2016.

[9] Y. Lyu, P. Kyösti, and W. Fan, "Sub-THz VNA-based channel sounder structure and channel measurements at 100 and 300 GHz," in *Proc. IEEE 32nd Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Helsinki, Finland, Sep. 2021, pp. 1–5.

[10] C. U. Bas, V. Kristem, R. Wang, and A. F. Molisch, "Real-time ultra-wideband channel sounder design for 3–18 GHz," *IEEE Trans. Commun.*, vol. 67, no. 4, pp. 2995–3008, Apr. 2019.

[11] J. Hejselbaek, Y. Ji, W. Fan, and G. F. Pedersen, "Channel sounding system for MM-wave bands and characterization of indoor propagation at 28 GHz," *Int. J. Wireless Inf. Netw.*, vol. 24, no. 3, pp. 204–216, Sep. 2017.

[12] S. Ranvier, M. Kyro, K. Haneda, T. Mustonen, C. Icheln, and P. Vainikainen, "VNA-based wideband 60 GHz MIMO channel sounder with 3-D arrays," in *Proc. IEEE Radio Wireless Symp.*, Jan. 2009, pp. 308–311.

[13] A. W. Mbugua, W. Fan, K. Olesen, X. Cai, and G. F. Pedersen, "Phase-compensated optical fiber-based ultrawideband channel sounder," *IEEE Trans. Microw. Theory Techn.*, vol. 68, no. 2, pp. 636–647, Feb. 2020.

[14] X. Wu et al., "60-GHz millimeter-wave channel measurements and modeling for indoor office environments," *IEEE Trans. Antennas Propag.*, vol. 65, no. 4, pp. 1912–1924, Apr. 2017.

[15] P. F. M. Smulders and A. G. Wagemans, "Frequency-domain measurement of the millimeter wave indoor radio channel," *IEEE Trans. Instrum. Meas.*, vol. 44, no. 6, pp. 1017–1022, Dec. 1995.

[16] M. Bengtson, Y. Lyu, and W. Fan, "Long-range VNA-based channel sounder: Design and measurement validation at mmWave and sub-THz frequency bands," *China Commun.*, vol. 19, no. 11, pp. 47–59, Nov. 2022.

[17] L. Talbi and J. LeBel, "Broadband 60 GHz sounder for propagation channel measurements over short/medium distances," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 2, pp. 343–351, Feb. 2014.

[18] A. G. Siamarou and M. Al-Nuaimi, "A wideband frequency-domain channel-sounding system and delay-spread measurements at the license-free 57- to 64-GHz band," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 3, pp. 519–526, Mar. 2010.

[19] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6G security," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 375–388, 2023.

[20] M. Zoli, A. N. Barreto, S. Köpsell, P. Sen, and G. Fettweis, "Physical-layer-security box: A concept for time-frequency channel-reciprocity key generation," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, p. 114, Dec. 2020.

[21] P. Walther et al., "Improving quantization for channel reciprocity based key generation," in *Proc. IEEE 43rd Conf. Local Comput. Netw. (LCN)*, Oct. 2018, pp. 545–552.

[22] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[23] D. Regev et al., "Analysis and design of quasi-circulating quadrature hybrid for full-duplex wireless," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 12, pp. 5168–5181, Dec. 2021.

[24] Z. Deng, H. Qian, and X. Luo, "Tunable quasi-circulator based on a compact fully-reconfigurable 180° hybrid for full-duplex transceivers," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 8, pp. 2949–2962, Aug. 2019.

[25] A. Goel, B. Analui, and H. Hashemi, "Tunable duplexer with passive feed-forward cancellation to improve the RX-TX isolation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 2, pp. 536–544, Feb. 2015.

[26] H. Boeglen, "A 60 GHz digital link with GNU Radio and USRP radios," in *Proc. GNU Radio Conf.*, vol. 2, no. 1, Jan. 2021. Accessed: Jul. 29, 2024. [Online]. Available: https://pubs.gnuradio.org/index.php/grcon/article/view/87

[27] A. Quadri, H. Zeng, and Y. T. Hou, "A real-time mmWave communication testbed with phase noise cancellation," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Paris, France, Apr. 2019, pp. 455–460.

[28] W. Khawaja, O. Ozdemir, and I. Guvenc, "UAV air-to-ground channel characterization for mmWave systems," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–5.

[29] J. Zhang, X. Zhang, P. Kulkarni, and P. Ramanathan, "OpenMili: A 60 GHz software radio platform with a reconfigurable phased-array antenna," in *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MOBICOM)*, 2016, pp. 162–175.

[30] T. Wei and X. Zhang, "mTrack: High-precision passive tracking using millimeter wave radios," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, 2015, pp. 117–129.

[31] Y. Zeng, P. H. Pathak, Z. Yang, and P. Mohapatra, "Poster abstract: Human tracking and activity monitoring using 60 GHz mmWave," in *Proc. 15th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2016, pp. 1–2.

[32] Y. Ghasempour, M. K. Haider, and E. W. Knightly, "Decoupling beam steering and user selection for MU-MIMO 60-GHz WLANs," *IEEE/ACM Trans. Netw.*, vol. 26, no. 5, pp. 2390–2403, Oct. 2018.

[33] Y. Ghasempour and E. W. Knightly, "Decoupling beam steering and user selection for scaling multi-user 60 GHz WLANs," in *Proc. 18th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, New York, NY, USA, Jul. 2017, pp. 1–10.

[34] R. Foster et al., "Beam-steering performance of flat Luneburg lens at 60 GHz for future wireless communications," *Int. J. Antennas Propag.*, vol. 2017, pp. 1–8, Jan. 2017.

[35] T. Nitsche, G. Bielsa, I. Tejado, A. Loch, and J. Widmer, "Boon and bane of 60 GHz networks," in *Proc. 11th ACM Conf. Emerg. Netw. Experiments Technol.*, New York, NY, USA, Dec. 2015, pp. 1–13.

[36] M. KIM, H. Kinh, Y. CHANG, and J.-i. TAKADA, "Development of low-cost 60-GHz millimeter-wave MIMO channel sounding system," in *Proc. 6th Global Symp. Millim. Waves (GSMM)*, Sendai, Japan, 2013, pp. 18–21.

[37] *60 GHz Transmit/Receive (Tx/Rx) Development System*. Accessed: Nov. 1, 2023. [Online]. Available: https://www.pasternack.com/images/ProductPDF/PEM009-KIT.pdf

[38] Hittite Microwave Corp., Chelmsford, MA, USA. Accessed: Nov. 1, 2023. [Online]. Available: https://www.microwavejournal.com/articles/17871-highly-integrated-60-ghz-radio-transceiver-chipset

[39] R. Gomes et al., "Will COTS RF front-ends really cope with 5G requirements at mmWave?" *IEEE Access*, vol. 6, pp. 38745–38769, 2018.

[40] B. Razavi, "Design of millimeter-wave CMOS radios: A tutorial," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 56, no. 1, pp. 4–16, Jan. 2009.

[41] P. Zetterberg and R. Fardi, "Open source SDR frontend and measurements for 60-GHz wireless experimentation," *IEEE Access*, vol. 3, pp. 445–456, 2015.

[42] L. Duarte, R. Gomes, C. Ribeiro, and R. F. S. Caldeirinha, "A software-defined radio for future wireless communication systems at 60 GHz," *Electronics*, vol. 8, no. 12, p. 1490, Dec. 2019.

[43] M. J. Horst, M. T. Ghasr, and R. Zoughi, "Design of a compact V-band transceiver and antenna for millimeter-wave imaging systems," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 11, pp. 4400–4411, Nov. 2019.

[44] K. C. Eun et al., "LTCC SoP integration of 60 GHz transmitter and receiver radios," in *Proc. Asia–Pacific Microw. Conf.*, Dec. 2008, pp. 1–4.

[45] W. Hong, K.-H. Baek, and A. Goudelev, "Grid assembly-free 60-GHz antenna module embedded in FR-4 transceiver carrier board," *IEEE Trans. Antennas Propag.*, vol. 61, no. 4, pp. 1573–1580, Apr. 2013.

[46] M. Umar, M. Laabs, N. Neumann, and D. Plettemeier, "60 GHz double edge coupled Marchand balun for PCB implementation," in *Proc. 49th Eur. Microw. Conf. (EuMC)*, Oct. 2019, pp. 332–335.

[47] M. Umar, M. Laabs, J. Damas, N. Neumann, and D. Plettemeier, "Analysis of substrate parameters' variations in a PCB-based 60 GHz GCPW Marchand balun design," in *Proc. 14th Eur. Conf. Antennas Propag. (EuCAP)*, Mar. 2020, pp. 1–5.

[48] M. Umar, M. Laabs, N. Neumann, and D. Plettemeier, "Design of DC-blocks and bias-tee on PCB for V-band," *IEEE Microw. Wireless Compon. Lett.*, vol. 31, no. 10, pp. 1107–1110, Oct. 2021.

[49] M. Umar, M. Laabs, N. Neumann, and D. Plettemeier, "Bondwire model and compensation network for 60 GHz chip-to-PCB interconnects," *IEEE Antennas Wireless Propag. Lett.*, vol. 20, no. 11, pp. 2196–2200, Nov. 2021.

[50] M. Umar, M. Laabs, N. Neumann, and D. Plettemeier, "A low-cost 60-GHz modular front-end design for channel sounding," *IEEE Trans. Compon., Packag., Manuf. Technol.*, vol. 14, no. 2, pp. 277–290, Feb. 2024.

[51] M. Umar and P. Sen, "Antenna-duplexed passive beamforming front-end for joint communication and sensing," in *Proc. IEEE 3rd Int. Symp. Joint Commun. Sens. (JC&S)*, Mar. 2023, pp. 1–6.

[52] E. Leipner, "Entwurf und aufbau eines synchronen mehrkanal-downconverters fuer 28 GHz," M.S. thesis, Technische Universitaet Dresden, Dresden, Germany, 2020. [Online]. Available: https://tu-dresden.de/ing/elektrotechnik/ifn/hf/studium/studien-und-diplomarbeiten/copy_of_index

[53] C. R. Paul, *Inductance: Loop Partial*. Hoboken, NJ, USA: Wiley, Dec. 2009.

[54] S. Salous, S. M. Feeney, X. Raimundo, and A. A. Cheema, "Wideband MIMO Channel Sounder for Radio Measurements in the 60 GHz Band," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2825–2832, Apr. 2016.

[55] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[56] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

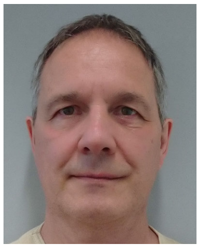
[57] N. Felkaroski and M. Petri, "Secret key generation based on channel state information in a mmWave communication system," in *Proc. SCC 12th Int. ITG Conf. Syst., Commun. Coding*, Feb. 2019, pp. 1–6.

[58] A. Mayya, M. Mitev, A. Chorti, and G. Fettweis, "A SKG security challenge: Indoor SKG under an on-the-shoulder eavesdropping attack," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Kuala Lumpur, Malaysia, Dec. 2023, pp. 1–6.

[59] N. C. Manjappa, L. Wimmer, N. Maletic, and E. Grass, "Real-time physical layer secure key generation in a mmWave communication system," in *Proc. 17th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Sep. 2021, pp. 1–6.

[60] W. Yang, R. F. Schaefer, and H. V. Poor, "Privacy amplification: Recent developments and applications," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Oct. 2018, pp. 120–124.

Muhammad Umar received the B.E. degree from Air University, Pakistan, in 2009, the M.S. degree from Linköping University, Sweden, in 2012, and the Ph.D. degree in electrical engineering from Technische Universität Dresden (TU Dresden), Dresden, Germany, in 2023. From 2016 to 2021, he was associated with the Chair of RF and Photonics Engineering, TU Dresden. Since 2021, he has been a Senior Researcher with the Barkhausen-Institut gGmbH, Dresden. He has contributed to several European and German-funded research projects. His research interests include RF systems, millimeter wave circuits, RF packaging, and integrated sensing and communication (ISAC) technologies.



Axel Schmidt received the Dipl.-Ing. degree from the Communications Laboratory, Technische Universität Dresden (TU Dresden), Germany, in 1995. Since then, he worked there with a research focus mainly on UWB and physical layer security.

Martin Laabs is currently a Research Associate with the Chair of Radio Frequency and Photonics, Technische Universität Dresden (TU Dresden), Germany, focusing on RF measurement and radar systems. His work includes the development of advanced antenna technologies and radar systems for various applications. He holds several patents in the area of over-the-air testing of antenna arrays and innovative frequency comb radar systems and has made several biomedical radar-related inventions. His research plays a critical role in the advancement of space and biomedical technologies, ensuring the reliable performance of electronic systems.

Niels Neumann received the Dipl.-Ing., Dr.-Ing., and Dr.-Ing. (Habilitation) degrees from Technische Universität Dresden (TU Dresden), Germany, in 2005, 2010, and 2020 respectively. Since 2011, he has been with the Microwave Photonics Group, Chair for RF and Photonics Engineering, TU Dresden. In 2022, he became a Full Professor of communication technology for the Industrial Internet of Things at Technical University of Clausthal (TU Clausthal). His interdisciplinary research interests in RF and communications engineering include the modeling and characterization of frontends as well as EM and propagation scenarios for RF and optical systems.

Dirk Plettemeier (Member, IEEE) received the Ph.D. degree in electrical engineering from Ruhr-Universität Bochum, Bochum, Germany. Since 2011, he has been a Full Professor with the Chair of Radio Frequency and Photonics Engineering, Technische Universität Dresden (TU Dresden), Dresden, Germany. He has been involved in several international scientific activities, as a Co-Investigator for ESA and NASA Space Missions, such as Cassini-Huygens, Rosetta, and ExoMars, mainly focusing on subsurface imaging. He is currently with the Centre for Tactile Internet with Human-in-the-Loop and 6G-Life Research Hub, TU Dresden, where he is involved in electronics for next-generation sensor and communications systems. His research interests include millimeter-wave and terahertz systems, antennas and chip-integrated applications, microwave photonics, wave propagation, remote sensing, and imaging solutions for radar applications.