Absolute Security in Terahertz Wireless Links

Alejandro Cohen, *Member, IEEE*, Rafael G. L. D'Oliveira, *Member, IEEE*, Chia-Yi Yeh, *Member, IEEE*, Hichem Guerboukha, Rabi Shrestha, Zhaoji Fang, Edward W. Knightly, *Fellow, IEEE*, Muriel Médard, *Fellow, IEEE*, and Daniel M. Mittleman, *Fellow, IEEE*

***Abstract*—Security against eavesdropping is one of the key concerns in the design of any communication system. Many common considerations of the security of a wireless communication channel rely on comparing the signal level measured by Bob (the intended receiver) to that accessible to Eve (a single eavesdropper). Frameworks such as Wyner's wiretap model ensure the security of a link, in an average sense, when Bob's signal-to-noise ratio (SNR) exceeds Eve's. Unfortunately, because these guarantees rely on the noise realizations at Eve, statistically, Eve can still occasionally succeed in decoding information. The goal of achieving *exactly zero* probability of intercept over an engineered region of the broadcast sector, which we term absolute security, remains elusive. Here, we describe the first architecture for a wireless link with a single eavesdropper, that provides absolute security. I.e., a cryptographic deterministic and non-probabilistic security approach that does not rely on statistical assumptions about noise, shared secure key, or Eve's computational power. Our approach relies on the inherent properties of broadband and high-gain antennas, and is therefore ideally suited for implementation in millimeter-wave and terahertz wireless systems, where such antennas will generally be employed. We exploit spatial minima of the antenna pattern at different frequencies, the union of which defines a wide region where Eve is guaranteed to fail regardless of her computational capabilities, and regardless of the noise in the channels. Unlike conventional zero-forcing beam forming methods, we show that, for realistic assumptions about the antenna configuration and power budget, this absolute security guarantee can be achieved over most possible eavesdropper locations. Since we use relatively simple frequency-multiplexed coding, together with the underlying physics of a diffracting aperture, this idea is broadly applicable in many contexts.**

***Index Terms*—Absolute security, blind region, terahertz.**

Manuscript received 30 November 2022; revised 9 March 2023 and 24 June 2023; accepted 8 August 2023. Date of publication 23 August 2023; date of current version 13 October 2023. The work of Alejandro Cohen, Rafael G. L. DOliveira, and Muriel Medard was supported in part by Air Force under Grant FA8702-15-D-0001 and in part by MIT Portugal Program, Project SNOB-5G with Nr. under Grant 045929(CENTRO-01-0247-FEDER-045929). The work of Edward Knightly was supported in part by NSF under Grants CNS-1955075, CNS-1923782, CNS-1824529, and CNS-1801857, and in part by DOD: Army Research Laboratory under Grant W911NF-19-2-0269. The work of Daniel M. Mittleman was supported in part by Air Force Research Laboratory under Grant FA8750-19-1-0500 and in part by NSF under Grants NSF-1954780 and NSF-1923782. This research was supported by NSF under Grant CNS-2148132. The guest editor coordinating the review of this manuscript and approving it for publication was Dr. Chong Han. *(Corresponding author: Alejandro Cohen.)*

Alejandro Cohen is with the Faculty of Electrical, Computer Engineering, Technion, Haifa 3200003, Israel (e-mail: alecohen@technion.ac.il).

Rafael G. L. D'Oliveira is with the School of Mathematical, Statistical Sciences, Clemson University, Clemson, SC 29634 USA (e-mail: rdolive@clemson.edu).

Chia-Yi Yeh is with the Research Laboratory of Electronics, MIT, Cambridge, MA 02139 USA, and also with the School of Engineering, Brown University, Providence, RI 02912 USA (e-mail: cyyeh@mit.edu).

Hichem Guerboukha, Rabi Shrestha, Zhaoji Fang, and Daniel M. Mittleman are with the School of Engineering, Brown University, Providence, RI 02912 USA (e-mail: hichem_guerboukha@brown.edu; rabi_shrestha@brown.edu; zhaoji_fang@brown.edu; daniel_mittleman@brown.edu).

Edward W. Knightly is with the Department of Electrical, Computer Engineering, Rice University, Houston, TX 77005 USA (e-mail: knightly@rice.edu).

Muriel Médard is with the Research Laboratory of Electronics, MIT, Cambridge, MA 02139 USA (e-mail: medard@mit.edu).

Digital Object Identifier 10.1109/JSTSP.2023.3307906

I. Introduction

CONCERNS about wireless security date back to Marconi, when critics pointed out that if wireless signals propagate in all directions, then an adversary can also receive them [2]. Modern wireless technologies have now begun to employ higher frequencies, in the millimeter-wave [3], [4], [5], [6], [7], [8] and terahertz ranges [9], [10], [11], [12], [13], [14], [15], which are likely to require the use of high-gain antennas to produce directional beams [10], [11], [16], [17], [18], [19], [20]. Although this directionality inhibits eavesdropping, successful attacks are still possible since most highly directional antennas exhibit side lobe emission which sends signals in many directions. Efforts to scramble the information contained in side lobes [21], [22] can offer significant improvements, but even so, an eavesdropper (Eve) will always have a non-zero probability of intercepting and decoding the transmitted message between the sender (Alice) and the intended receiver (Bob). In essence, all such security schemes rely on noise in Eve's measurement [23], [24]. With these probabilistic information-theoretic schemes, it has been shown recently that non-negligible information could leak under reasonable finite length code constructions [25]. Despite the fact that many of these security schemes are termed in the literature as exhibiting perfect security [24], [26], [27], it is clearly more favorable if Eve has *zero* probability of intercepting the message from Alice to Bob, regardless of assumptions.

In the field of THz link security, the discussions remain in the realm of SNR discrepancy or noise realization in Eve's measurement, despite the diverse studies for various settings, including multiple eavesdroppers [28] and distributed eavesdroppers [29], and for various channel conditions including rain and snow [30] and atmospheric turbulence [31]. Likewise, the security of THz networks with wideband frequency-dependent transmissions [32], [33], orbital angular momentum (OAM) [34], or intelligent reflecting surfaces [35], [36] has also been studied under the same traditional physical layer security framework. In addition, the threat of eavesdropping that arises from a carefully engineered and placed object is also investigated [9], [37], [38], [39], [40], [41] considering the difference in SNR. To enhance the THz link security, prior works have proposed various strategies, such as transmitting artificial

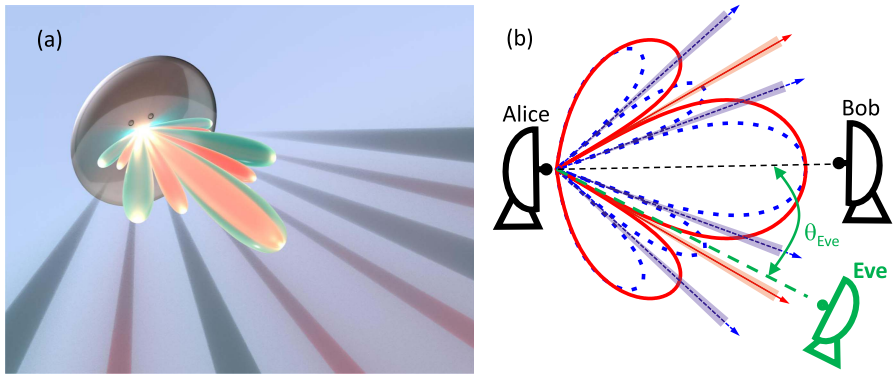


Fig. 1. (a) An illustration of radiation patterns from a parabolic dish at two different frequencies, showing the main lobe and side lobes. The minima of each pattern define angular regions where signals cannot be detected at that frequency. With many subchannel frequencies, the union of these minima creates a blind region that covers most of the possible locations for an eavesdropper. (b) Schematic diagram illustrating these minima, as Alice (the transmitter) broadcasts to Bob (the intended receiver), attempting to thwart Eve (a single eavesdropper) located at an angle θ_{Eve}.

noise [29], exploiting absorption peaks in THz bands [42], [43], and scrambling information in the unintended directions with space-time modulation [21], [22]. However, these strategies are still based on the SNR at Bob versus the SNR at Eve, which rely on statistical assumptions about noise.

In this article, we describe a new approach to realize what we call *Absolute Security*.[1] By Absolute Security we mean an information-theoretic scheme that is cryptographically (non-probabilistic) secure, and does not rely on the assumptions of a shared secure key [45] or Eve's computational ability [46]. This notion contrasts with common probabilistic security typically used in physical layer security discussions, which holds merely in an average sense over noise realizations (i.e., assumes that, on average, in the asymptotic regime, Eve's SNR is lower than Bob's SNR), thus permitting some transmissions to be insecure. In contrast, absolute security holds with probability one even for the putative case most favorable to Eve, in which her detector does not introduce noise to her measurement. Moreover, absolute security is established based on a stronger security condition than the conventional physical layer security. In essence, conventional physical layer security considers that Eve's task is to decode all the symbols despite receiving them with attenuation and additive random noise. In contrast, absolute security ensures that Eve does not receive a small portion of the transmitted symbols at all, i.e., that Eve's reception of a small portion of the symbols is below her unavoidable background thermal radiation, leaving her an insurmountable decoding task.

Our approach to achieve absolute security, in a THz communication scheme with a single Eve, relies on both the inherent properties of Alice's antenna and on an associated secure coding scheme. Many directional antennas, when driven over an ultrawide bandwidth, result in frequency-dependent minima (see Fig. 1). Since any receiver has a minimum detectable signal threshold, radiation minima create regions in space where Eve cannot even detect the signal, regardless of the noise realization. This allows us to leverage recent developments in secure communications to thwart Eve as long as some frequencies are "blind" for her (see Definitions 1 and 2 for a precise definition of the blind region and frequencies). This approach enables Alice and Bob to establish a secure wireless link (see Definitions 3 and 4 for a precise definition of the security guarantees) that cannot be broken by any adversary located in an engineered region of the broadcast space, even if she possesses arbitrarily powerful computational capabilities, even a quantum computer [47], [48], [49], [50].

Our method breaks the conventional paradigm for secure communications in which one faces a trade-off between data transmission rate and the degree of security: in our approach, increasing the transmission bandwidth (and therefore the achievable data rate) can *simultaneously* offer improved security. That is, with the proposed method, the larger the bandwidth, the larger the covered secure region in space without sacrificing the data rate. In contrast, for the conventional SNR-based physical layer secrecy capacity [23], [24], [26], [27], although the secrecy capacity scales with bandwidth, if Alice wants to protect against a stronger Eve, she must sacrifice the secrecy rate. In this sense, conventional SNR-based physical layer security has only an improvement in data rate, but not security, with increasing bandwidth. The proposed method is therefore particularly well suited for future generations of wireless technology, which will exploit ultra-wideband channels in the millimeter-wave and terahertz regions of the spectrum [10].

To demonstrate our proposed method, we perform model-driven analysis for multiple antennas suitable for millimeter-wave and terahertz bands, as well as experimental measurement with over-the-air data transmissions. With model-driven analysis, we show how the blind region increases with a larger bandwidth, when the antenna features frequency-dependent minima, including phased arrays, parabolic dishes, and leaky-wave antennas. We also show that not all antennas are suitable for our proposed method. Horn antennas, for example, do not exhibit pronounced minima, and thus increasing bandwidth does not enlarge the blind region. However, in the experiment, we show

[1]For clarity of exposition, we have narrowed the definition of absolute from cryptographic security that includes also computational security, as given in the conference version of this paper [1] and in [44], to the cryptographic information-theoretic security approach based on the concept of blind region.

that the horn antenna can still be used for our method. By placing a beam block in front of the horn antenna, we create a diffraction pattern and pronounced frequency-dependent minima. With three widely spaced frequencies (100, 200, and 400 GHz), we demonstrate a substantial blind region where Eve fails to detect at least one of the three modulated data streams, and thus achieve absolute security.

Lastly, we contrast our security scheme with a conventional method known as zero-forcing, in which a phased array is engineered to create a minima in the radiation pattern at a specific location in order to thwart an eavesdropper at that location. Our approach is quite distinct from this legacy approach for several reasons. As detailed below and in Section VI, the blind region in our method is the union of minima over all frequency channels. Thus, we do not need to know the precise location of the eavesdropper, only whether she is located in this blind region (which can realistically encompass a large fraction of the full angular range). Moreover, unlike the case of zero-forcing, if Eve fails to measure just one of the frequency channels in our approach, she is unable to decode any of them.

II. Absolute Security

A. Antenna Configuration

For many antennas, the far-field radiation pattern exhibits minima in specific directions, which depend on the details of the antenna geometry and its excitation mechanism, as well as on the frequency of the radiation [51]. For example, two commonly employed antennas in high-frequency wireless links, a linear phased array [52], [53] and a center-fed parabolic dish [16], both exhibit pronounced minima at various angles, which shift with transmission frequency (see Section III-A1). Under the assumption (discussed further below) that Eve must avoid *all* of these minima, a transmission with multiple frequency bands creates a significant excluded region for Eve. To quantify this, we consider a transmission that uses a bandwidth B from f_L to f_H, centered on $f_C = (f_L + f_H)/2$, sliced uniformly into q frequency channels, each with bandwidth $w = (f_H - f_L)/q$. Let $\mathcal{Q}$ denote the set of frequency channels. At location (r, θ), the intensity received S (in W/m^2) in the i-th frequency channel $[f_i - \frac{w}{2}, f_i + \frac{w}{2}]$ can be represented as

$$S(f_i, r, \theta) \propto \int_{f_i - \frac{w}{2}}^{f_i + \frac{w}{2}} P_T(f) \cdot \gamma(r, f) \cdot G(f, \theta) df \qquad (1)$$

where $P_T(f)$ is the transmit power spectrum (in W/Hz) employed by Alice, $\gamma(r, f)$ is the distance- and frequency-dependent channel gain from the transmitter to the receiver and $G(f, \theta)$ is the antenna radiation pattern. For simplicity, we consider only one emission plane (the H plane), although our results can readily be generalized to three dimensions.

B. Defining the Blind Region

For any receiver, there exists a minimum detectable signal threshold $\delta > 0$ (intensity per unit bandwidth), below which the receiver cannot detect a transmission. This threshold may depend on the receiver sensitivity, the receive antenna gain, the environmental noise floor, and the quantization of the digital processing (see Section II-E). The existence of this non-zero threshold δ implies that there are **blind regions** where, with probability one, Eve cannot detect the transmission. We define the blind region (Ω) for a transmission band $[f_L, f_H]$ as the set of locations (r_{Eve}, θ_{Eve}) where Eve is unable to detect signals in *at least one* of the q frequency channels. Specifically, we define the blind region as follows:

Definition 1 (Blind Region): For any $\delta > 0$ and w, the blind region for the i-th frequency channel, $\mathcal{Z}(f_i)$, is given as the set of locations for which the signal intensity at Eve, $S(f_i, r_{Eve}, \theta_{Eve})$, is below the detection threshold:

$$\mathcal{Z}(f_i) = \{(r_{Eve}, \theta_{Eve}) | S(f_i, r_{Eve}, \theta_{Eve}) < \delta \cdot w\}. \qquad (2)$$

The blind region for the total transmission band (Ω) is then the union of blind regions for each subchannel:

$$\Omega = \bigcup_{i=1}^{q} \mathcal{Z}(f_i). \qquad (3)$$

Definition 2 (Blind Frequency Channels): For each location in the blind region Ω, the number of missing frequency channels can vary from one to all q of them. Therefore, we also define Γ as the number of subchannels for which $S(f_i) < \delta \cdot w$. Each possible location for Eve can therefore be characterized as either non-blind ($\Gamma = 0$) or Γ-blind ($1 \leq \Gamma \leq q$).

As the number of subchannels q increases, Alice's broadcast includes more signals at distinct frequencies with unique radiation patterns, each exhibiting minima in distinct directions. Thus, the percentage of angular locations θ_{Eve} that are within the blind region also increases.

We emphasize that the blind region defined here is not just a function of the antenna and broadcast frequencies. It also depends on the properties of Eve's receiver, through the parameter δ defined above. As a result, different assumptions about Eve's receiver capabilities will result in somewhat different blind regions. However, even in the hypothetical best case (for Eve) that her receiver is quantum-noise limited, her ability to detect Alice's broadcast is still limited by the thermal noise of the environment which she is observing (see Section II-E). Of course, it is possible to detect signals that are well below the thermal background; this is commonly achieved, for example, in astrophysical observations, by severely restricting the spectral bandwidth of the detection and/or extended signal averaging. However, Eve cannot employ these strategies if she wishes to decode a broadband high-data-rate transmission. Thus, the value of δ cannot be infinitesimal, regardless of how Eve detects signals. An important consequence of this conclusion is that we *need not require* that Eve's location must precisely coincide with the (mathematically infinitesimal) angular position of a minimum in an antenna radiation pattern; she only needs to be *close enough* to a minimum such that her received signal is small.

This consideration emphasizes the clear distinction between our proposal and the idea of extending conventional narrowband beam forming methods based on zero forcing to a broadband context. [54], [55] With zero-forcing, one can engineer an antenna (e.g., the signals applied to each element of a phased array)

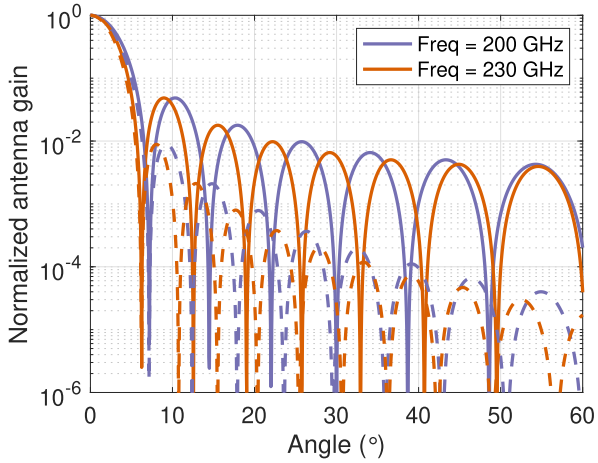


Fig. 2. Radiation patterns illustrating how the pronounced minima shift with frequency (solid: phased array, dashed: parabolic dish).

to force the broadcast wave amplitude to zero in a given direction at a given frequency. This would make it impossible for Eve to detect signals at that frequency if she is located in that direction. But she would still be able to detect signals at other frequencies, since the zero is enforced in her direction only for one particular frequency. By contrast, with our method, Eve would fail to decode any of the frequency channels, not just the one whose antenna pattern is forced to be zero at her location. Indeed, our approach does not require knowledge of Eve's location. Since the blind region defined by (3) is the *union* of minima over all frequency bands, it can quite realistically occupy a significant fraction of the total angular space. The approach described here scales favorably with increasing transmission bandwidth, while the exact opposite is true for security schemes based on zero-forcing. It is also worth noting that zero-forcing only works for phased arrays; meanwhile, our approach has the advantage of working well for many antenna configurations, including, for instance, a conventional parabolic dish antenna (see Fig. 3(b)), where zero-forcing techniques obviously cannot be applied.

It is the coordinated use of, on the one hand, the union of blind regions Ω from frequency-dependent radiation patterns and, on the other hand, a secure coding scheme, that constitutes the core of our method's novelty. Unlike legacy methods that rely on the design of minima regions for security [27], the particular subset of frequencies that Eve can detect in any of the blind regions is irrelevant to our approach. This lack of dependence on the subset of detectable channels greatly expands the notion and hence the footprint of blind regions relative to traditional beam forming methods.

C. Secure Encoding

In this section, we consider the first absolute secure encoding scheme, which we denote as Scheme 1, which assumes that Eve is within the blind region. We illustrate the ideas using a simplified situation in which Alice wants to communicate securely with Bob using only $q = 3$ subchannels, at frequencies

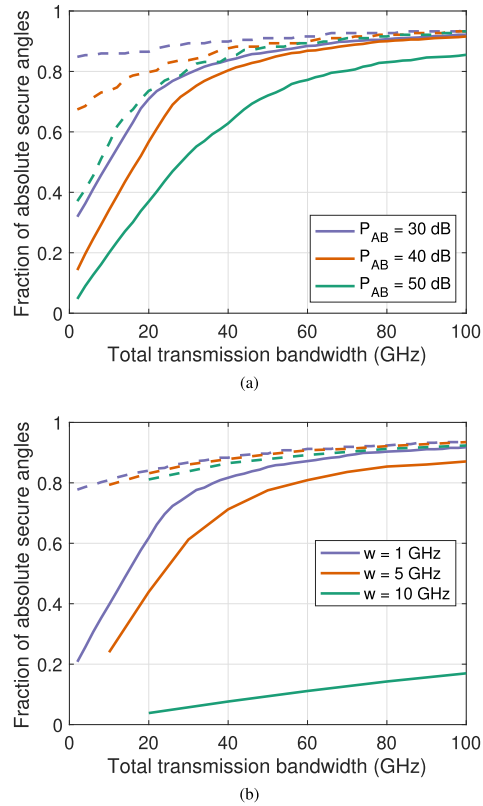


Fig. 3. Size of the blind region increases with bandwidth (solid: phased array, dashed: parabolic dish). (a) For several values of Alice's transmit power parameterized by P_{AB}. (b) For different values of subchannel bandwidth w.

f_1, f_2, and f_3. The general idea can be readily scaled to a larger number of subchannels from known constructions in the literature [56], [57], [58]. In the encoding scheme considered here, we assume that Eve is within the blind region. Our scheme operates symbolwise, so Alice must map her message into blocks and then map each block into a symbol selected from a finite field of dimension greater than 2^q [56]. For ease of exposition, here we consider a prime field. The construction can be easily generalized to operations over extensions of the binary field. Because our simplified illustration employs $q = 3$ subchannels, our illustrative example employs the finite field $\mathbb{F}_{11}$ [57], [58]. Alice first partitions her message (strings of bits) into blocks of length $\lceil \log_2(11) \rceil$, and then maps each block to a symbol of $\mathbb{F}_{11}$. To transmit a single message symbol $M \in \mathbb{F}_{11}$ securely to Bob, Alice first generates two symbols $T_1, T_2 \in \mathbb{F}_{11}$ uniformly at random. Alice then generates three encoded symbols $X_1, X_2, X_3 \in \mathbb{F}_{11}$ using her message M and the two random symbols T_1 and T_2, given by

$$\begin{aligned} X_1 &= M + T_1 + T_2, \\ X_2 &= M + 2T_1 + 4T_2, \\ X_3 &= M + 3T_1 + 9T_2. \end{aligned} \tag{4}$$

Each encoded symbol X_i is transmitted to Bob via the frequency band f_i. Since Bob is not in the blind region (i.e., his location has $\Gamma = 0$), he receives the three encoded symbols and is able to decode the message symbol M by means of a simple linear

transform that inverts (4):

$$\begin{pmatrix} M \\ T_1 \\ T_2 \end{pmatrix} = \begin{pmatrix} 3 & 8 & 1 \\ 3 & 4 & 4 \\ 6 & 10 & 6 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix}. \tag{5}$$

However, since Eve is in the blind region, she can observe at most two encoded symbols from the set $\{X_1, X_2, X_3\}$ with probability one. We can show that, regardless of which two encoded symbols Eve detects, she cannot determine M. For instance, if Eve receives X_1 and X_2, then the mutual information between her observations and the message symbol M can be computed from the entropy as:

$$\begin{aligned} I(M; X_1, X_2) &= H(X_1, X_2) - H(X_1, X_2|M) \\ &= H(X_1, X_2) - H(T_1 + T_2, 2T_1 + 4T_2) \\ &= H(X_1, X_2) - 2\log(|\mathbb{F}_{11}|) \\ &\leq H(X_1) + H(X_2) - 2\log(11) \\ &= 0. \end{aligned} \tag{6}$$

This result follows directly from the definition of mutual information and the fact that, conditioned on the messages, the only uncertainty about X_1 and X_2 is in the random variables $T_1 + T_2$ and $2T_1 + 4T_2$, which are independent and uniform. Thus, because there is zero mutual information between Eve's observation and Alice's message, Eve learns nothing about M; absolute security is guaranteed.

For the general setting given in Section V, we denote the possible matrix of message symbols by M. Furthermore, we denote the observed encoded symbol matrix at Eve in the blind region (see Definitions 1 and 2) by X_e. This matrix at Eve, contains encoded symbols transmitted over any $\mathcal{Q}_e \subset \mathcal{Q}$ frequency channels, where $|\mathcal{Q}_e| = q - \Gamma$. Thus, specifically, we define strong absolute security for Eve in the blind region as follows:

Definition 3 (Strong Absolute Security): At the eavesdropper in the blind region, observing any $\mathcal{Q}_e \subset \mathcal{Q}$ frequency channels, we have

$$I(M; X_{\mathcal{Q}_e}) = 0, \tag{7}$$

with probability one.

D. Increasing the Secure Communication Efficiency

We can define the secure communication efficiency in terms of the length of Alice's message. This efficiency η is the ratio between the size of the message and the number of bits needed to transmit it. Ideally, one would like this rate to be as close to $\eta = 1$ as possible. Generally, in previously proposed security schemes, this is not possible owing to the need to add redundancy to the transmission in order to guarantee security in the communication [23], [24], [59]. In the security scheme described in Section II-C, by noting that Alice must send $q = 3$ encoded symbols to transmit the original message symbol, we see that the secure communication efficiency is $\eta = \frac{1}{3}$. In general, the efficiency scales inversely with the number of frequency channels, $\eta \propto \frac{1}{q}$

It is easy to address this issue of the less-than-ideal efficiency of our approach, by making a small modification to the method, which we term Scheme 2: Alice can replace the $q - 1$ (in our example, two) random symbols with additional messages, M_2 and M_3, and then perform the same encoding as in (4), with the random symbols replaced by the additional messages. Alice can thus obtain an optimum secure communication efficiency of $\eta = 1$, regardless of the number of channels. That is, Alice replaces the random symbols, T_1 and T_2, with message symbols M_2 and M_3, and then transmits the three encoded symbols X_1, X_2, X_3 as in (4), i.e.,

$$\begin{aligned} X_1 &= M_1 + M_2 + M_3, \\ X_2 &= M_1 + 2M_2 + 4M_3, \\ X_3 &= M_1 + 3M_2 + 9M_3. \end{aligned}$$

As before, Bob can decode all three message symbols through a linear transform; but, the secure communication efficiency issue is now solved, since now $q = 3$ encoded symbols are sent in order to retrieve $q = 3$ message symbols, i.e., $\eta = 1$. This scheme guarantees zero mutual information with any subset of message symbols, yet may potentially allow Eve to obtain information about linear combinations of the message symbols [56]. In order to implement this approach, Alice must ensure that the message symbols M_1, M_2, M_3 are uniformly distributed. The reason for this, intuitively, is that the message symbols themselves are performing the role of the random symbols T_1 and T_2. We note that there are known techniques described in the literature [60] which can be used to enforce this uniformity condition, so this requirement is not a significant impediment. Thus, although $I(M_1, M_2, M_3; X_1, X_2)$ may not be zero, it is nevertheless possible for Alice to guarantee that the mutual information between any individual message and any two transmitted symbols is zero. That is, for any distinct $i, j, \ell \in \{1, 2, 3\}$, it follows that

$$\begin{aligned} I(M_i; X_1, X_2) &= H(X_1, X_2) - H(X_1, X_2|M_i) \\ &= H(X_1, X_2) - H(M_j + M_\ell, 2M_j + 4M_\ell) \\ &= H(X_1, X_2) - 2\log(|\mathbb{F}_{11}|) \\ &\leq H(X_1) + H(X_2) - 2\log(11) \\ &= 0. \end{aligned}$$

We stress that the information that Eve *can* obtain in this situation (which involves only linear combinations of Alice's messages) is largely trivial, and cannot in general be used to decode or decipher any meaning.

A key and, to our knowledge, unique advantage of our method is that it provides improved security as the bandwidth of the transmission increases. Indeed, as q increases, Alice is afforded more bandwidth which, because of the $\eta = 1$ communication efficiency, increases the data rate in her link with Bob while simultaneously improving the security by expanding the size of the blind region Ω. This simultaneous improvement in security and data rate has never previously been realized in wireless systems.

Specifically, we define individual absolute security for any possible message symbol M_i, and for Eve in the blind region (see Definitions 1 and 2) observing an encoded symbols matrix X_e that contains encoded symbols transmitted over any $\mathcal{Q}_e \subset \mathcal{Q}$ frequency channels, as follows:

Definition 4 (Individual Absolute Security): At the eavesdropper in the blind region, observing any $\mathcal{Q}_e \subset \mathcal{Q}$ frequency channels, for any i-th message symbol we have

$$I(M_i; X_{\mathcal{Q}_e}) = 0, \tag{8}$$

with probability one.

E. Effect of Minimum Detectable Signal Threshold

As noted, a key assumption of our approach is that a detector has a non-zero threshold δ for minimum detectable signal. This assumption is valid for any RF receiver, other than perhaps those that operate near the single-photon detection limit [61]. For the purposes of our illustrative calculations, we can consider a conservative threshold based on thermal radiation. When staring at a room temperature (300 K) blackbody, an area of 1 cm^2 intercepts 0.29 nW of power within a 1-GHz-wide frequency band from 100 GHz to 101 GHz, or 2.55 nW from 300 GHz to 301 GHz. In fact, most receivers employed in RF communication systems do not even approach this sensitivity (and this becomes increasingly true as the frequency increases into the millimeter-wave and terahertz regimes, where detectors are typically much less sensitive), so these values are something of a worst-case scenario.

For purposes of computing the channel capacity to Bob and to further illustrate its role in a communication system, let us now consider the effect of δ on the channel between Alice and Bob. Bob must be able to detect the minimum difference in fluence, δ, between any two symbols. It must be that any received symbol has, by the process of detection, a minimum detection uncertainty of energy δ Joules per meter squared, since two symbols with fluence difference less than δ could not be distinguished from each other. The effect of this uncertainty is to limit Bob's throughput. We note that, in our considerations of Eve's capabilities, we place no such limit in order to consider a very powerful eavesdropper.

Let us now consider the power per meter squared, σ^2, corresponding to this detection uncertainty. Given that we require a minimum fluence of δ to detect a signal with intensity σ^2, we require a minimum observation time τ such that $\tau\sigma^2 \geq \delta$ in order to detect the detection uncertainty inherent to a symbol. Thus $\frac{1}{\tau}$ is the fastest sampling rate for symbols.

Let the intensity of the signal be denoted by P. The Shannon capacity, if we have only the detection uncertainty, is $\frac{1}{2\tau}\ln(1+\frac{P}{\sigma^2})$, assuming the pessimum uncertainty distribution, which is Gaussian [62, Chapter 9]. Note that we should assume such a pessimum distribution since we have no guarantees on its form, only on its fluence. We may rewrite this capacity as $\frac{1}{2\tau}\ln(1+\frac{P}{\delta/\tau})$. This expression increases as τ decreases. By Nyquist, $\tau \leq 1/w$, so we obtain a capacity of $\frac{w}{2}\ln(1+\frac{P}{\delta\cdot w})$ as the maximum rate available when only the reception uncertainty is taken into account. If we have additional noise of the conventional form, that noise will further reduce capacity.

III. Absolute Security Evaluation

In this section, we evaluate the absolute security approach we propose in Section II using model-driven analysis and experimental demonstration.

A. Model-Driven Analysis

Since our method leverages antenna's frequency-dependent minima and coding to create blind regions, we examine the security performance when different types of antenna are employed. The first set of antennas features a fixed main lobe direction and frequency-dependent minima. The selected antennas in this category include a linear phased array and a parabolic dish. Next, we examine antennas whose main lobe direction shifts very strongly with frequency (in addition to frequency-dependent minima), with the example being a leaky-wave antenna. In addition, we show that not all antennas are suitable for employing the proposed absolute security approach, especially for antennas without pronounced minima, such as the horn antenna.

1) Phased Array and Parabolic Dish: In this subsection, we consider two specific antenna geometries to provide concrete illustrations of the ideas that underlie our security protocol. One of these is a 16-element linear phased array, in which each element is a vertically polarized point dipole emitter, and the elements are spaced along a horizontal line by half of the center wavelength ($\lambda = 1.5$ mm in our simulations). The other is a parabolic dish antenna, with a diameter of 16mm and a focal length of 10 mm, emitting vertically polarized radiation with a directional gain of 30.5 dBi at a frequency of 200 GHz. The phased array configuration is representative of steerable antennas that are commonly employed in today's millimeter-wave Wi-Fi and 5G standards, while the parabolic dish has often been employed in backhaul and other fixed broadband applications. In both cases, these antenna configurations scale naturally into the millimeter-wave and terahertz ranges, and have been employed for such high-frequency transmissions.

Although radiation patterns are of course three-dimensional, for simplicity we illustrate the essential idea of our approach by only considering a two-dimensional slice (the horizontal plane which is orthogonal to the polarization axis, the H-plane), for simplicity. Fig. 2 shows the radiation patterns of the two example antennas, at two different frequencies. In this figure, we observe that, even if Alice uses only the few frequency bands shown in these illustrations, many of Eve's possible locations are ruled out by the fact that she must avoid all of the minima of every frequency in Alice's transmission.

Using the phased array and the parabolic dish as described, we calculate the absolute secure angles according to (3) for a transmission with a center frequency of $f_c = 200$ GHz, a subchannel bandwidth of $w = 1$ GHz, and for several values of the parameter P_{AB} which describes Alice's transmit power to Bob. In particular, Alice's transmit power is parameterized by the intensity received by Bob, normalized to the detection threshold discussed above, $P_{AB} = S_{Bob}/(\delta \cdot w)$. For this calculation, Eve

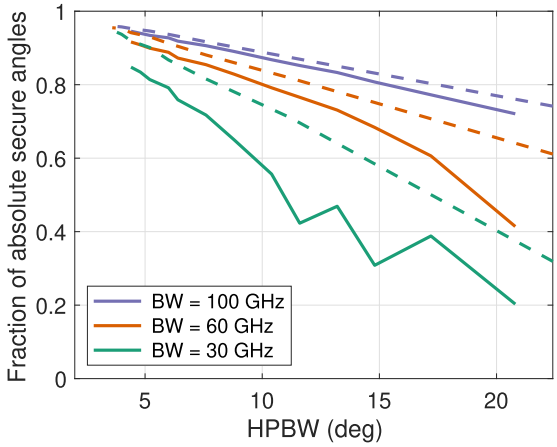


Fig. 4. Size of the blind region vs antenna HPBW at $f_C = 200$ GHz (solid: phased array, dashed: parabolic dish).

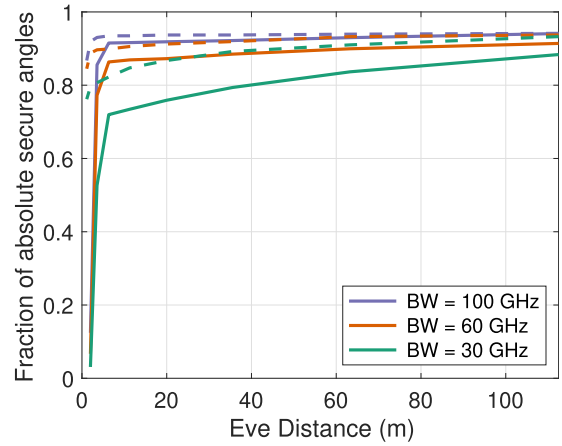


Fig. 5. Size of the blind region varies with Eve distance, using transmit power $P_{AB} = 35$ dB for Bob at 20m from Alice (solid: phased array, dashed: parabolic dish).

is at the same distance from Alice as Bob, and Alice adjusts her transmit power so that Bob receives a fixed intensity level S_{Bob} at all frequencies from f_L to f_H.

Fig. 3(a) illustrates the increase in blind region size as a function of total bandwidth B, assuming that Alice transmits to Bob using the antenna main lobe. For an increasing transmission bandwidth, as long as Eve is outside of the main antenna lobe (where Bob is located), she is increasingly likely to be within a blind region, i.e., at least one frequency channel is below her detection threshold ($\Gamma > 0$). In Fig. 3(a), the limiting value at a large bandwidth is determined by the angular width of the main lobe of the antenna pattern, where Bob is located (and which, by definition, is never within the blind region).

The width of the subchannels also impacts the size of the blind region for a given bandwidth. Using the same setup as in Fig. 3(a) with a fixed transmit power parameterized by $P_{AB} = 35$ dB, Fig. 3(b) illustrates the blind region for different subchannel bandwidths w. From Fig. 3(b), we observe that when the width of the subchannel is larger, it is harder to guarantee that the signal intensity across the subchannel is below the detection threshold, so the blind region is smaller.

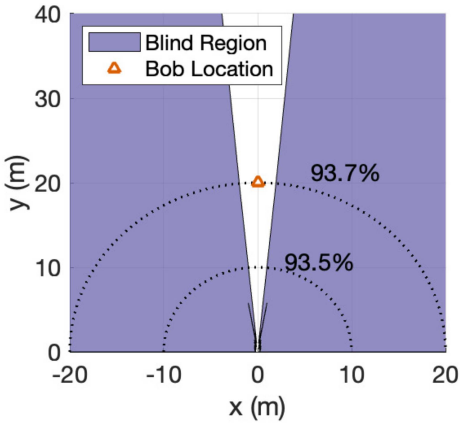
The size of the main lobe also impacts the blind region. Since the beamwidth becomes narrower with a larger antenna aperture, to explore different beamwidths, we vary the size of the linear phased array from 5 to 24 elements and the diameter of the parabolic dish antenna from 4mm to 32mm. We characterize the beamwidth using the half power beamwidth (HPBW) at the center frequency $f_C = 200$ GHz. Using the same setup as in Fig. 3 with a transmit power parameterized by $P_{AB} = 35$ dB, Fig. 4 shows how the blind region changes with HPBW for a given total bandwidth B. From Fig. 4, we observe that when the main beam is wider, the blind region becomes smaller, as we expect. Indeed, when the total bandwidth is large, the blind region is dominant by the size of the main beam, since the rest of the angular range is covered by at least one radiation minima. In addition to a wider beam, a small antenna aperture also yields fewer pronounced radiation minima for the blind region, which explains the smaller blind region when the total bandwidth is narrower.

Thus far, Eve has been assumed to be at the same distance from Alice as Bob. Here, we further examine the blind region when Eve's distance varies. Following the same settings as in Fig. 3 with transmit power parameterized by $P_{AB} = 35$ dB for Bob at 20 m, Fig. 5 shows how the blind region increases with Eve's distance from Alice, assuming that the signal attenuates with distance by an exponent of 2.

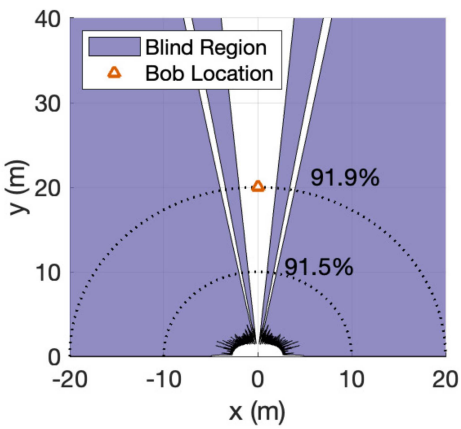
As we expect, when Eve is at a longer distance from Alice, it becomes more likely that at least one frequency channel is below Eve's detection level, and thus a larger blind region. From Fig. 5, we observe that the blind region varies slowly, except when Eve is extremely close to the transmitter Alice. Since our scheme relies on radiation minima so that Eve fails to detect at least one frequency channel, once Eve is extremely close to Alice, Eve starts to detect the frequency channels even when she is at the radiation minima, resulting in an abrupt blind region decrease when Eve is extremely close to Alice. We note that how deep the radiation minima are determines when this transition occurs. As shown in Fig. 2, the radiation minima of the parabolic dish are deeper than the minima of the phased array. Therefore, in Fig. 5, the parabolic dish (dashed lines) retains the blind region against a closer-distance Eve compared to the phased array antenna (solid lines).

While Fig. 5 explores Eve's distance in the x-axis, we can also interpret the x-axis effectively as Alice's transmit power, with Eve at a closer distance as Alice employs a larger power for Bob. Thus, Alice can design the blind region by controlling her transmit power, as we observe also in Fig. 3(a).

With the same setup as in Figs. 5 and 6 further illustrates the blind region in the 2D space when employing 100 GHz of bandwidth for the parabolic dish (Fig. 6(a)) and the phased array (Fig. 6(b)). In Fig. 6, we observe that the blind region (colored in blue) occupies most of the spatial region except for the main lobe, part of the first side lobe, and regions extremely close to the transmitter Alice. This indicates that the absolute security scheme, though achieved only when Eve is within the blind region, poses very few limitations to Eve's position once a large enough bandwidth is employed.

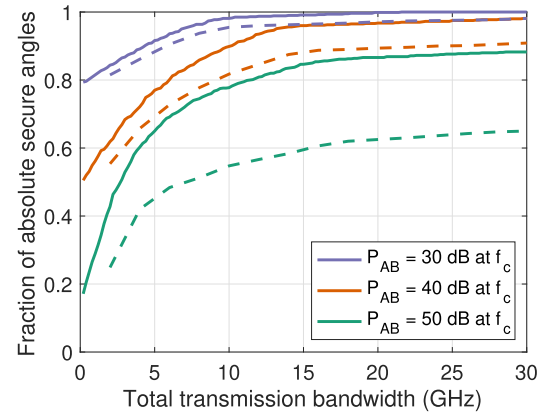


(a)

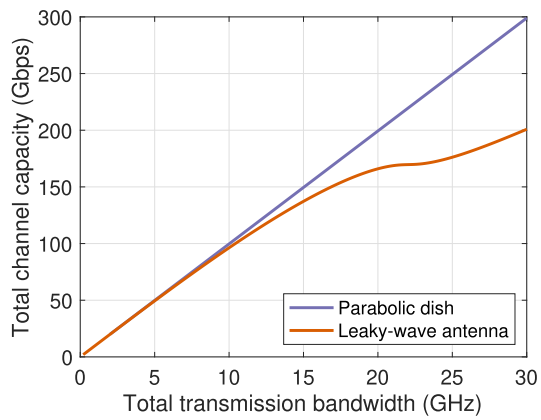


(b)

Fig. 6. Blind region in 2D space using 100 GHz of bandwidth for (a) parabolic dish and (b) phased array, with a transmit power parameterized by $P_{AB} = 35$dB.



(a)



(b)

Fig. 7. A leaky-wave antenna with strong angular dispersion. (a) The fraction of the angular range which is within the blind region ($\Gamma > 0$), and thus offers absolute security, as a function of bandwidth for several values transmit power parameterized by P_{AB} (solid: subchannel bandwidth $w = 0.1$ GHz, dashed: $w = 1$ GHz). (b) The scaling of total capacity with an increasing transmission band comparing a non-angularly dispersive antenna (parabolic dish) and an angularly dispersive link (leaky-wave antenna). $P_{AB} = 30$ dB is considered in both cases. Here, we assume Bob and Eve have the same detection threshold and an equal antenna aperture.

2) Angularly Dispersive Antennas: We address the possibility of implementing the same security scheme using a different class of antenna structure, in which the main lobe of the broadcast shifts very strongly with frequency. A prototype of such an antenna is a leaky-wave waveguide, which exhibits a very strong angular dispersion [63].

We employ a parallel-plate leaky-wave antenna with a plate separation of 1mm and an attenuation constant of 1. Bob is located at 30° and the maximum radiation frequency at this angle, 300 GHz, is the center frequency of the transmission. For the illustrative calculation, we employ two values of subchannel bandwidth, $w = \{0.1, 1\}$ GHz. As above, we assume that Eve is at the same distance from Alice as Bob. Notice that P_{AB} varies across the transmission band due to the dispersive link when Alice employs a uniform transmit power. Therefore, we use the value of P_{AB} corresponding to the center frequency to characterize the transmit power.

With angular dispersion, the available bandwidth for transmissions between Alice and Bob is restricted since widely differing frequencies propagate in very different directions. As a result, although the blind region still increases with the transmission bandwidth (Fig. 7(a)) and Scheme 2 can still be employed in the blind region, there is a limit to the improvement in the data rate (see Fig. 7(b)). This trade-off, however, may be worthwhile in view of the numerous other advantageous capabilities of leaky-wave structures, including sensing [64] and frequency multiplexing [65].

3) Horn Antenna as a Counter Example: The schemes for implementing secure communications in the case where Eve is in the blind region ($\Gamma > 0$) rely on features of the radiation patterns inherent to the antenna used by Alice, specifically the fact that, in certain broadcast directions, these patterns exhibit pronounced minima (or even analytic zeros), due to destructive interference. It is important to realize that this is not a feature of all antennas. Here, we present a counterexample to illustrate this point: a diagonal horn antenna, another commonly employed design in millimeter-wave and terahertz systems.

As in the cases discussed above, the radiation pattern from this antenna, at a given frequency, is also amenable to direct calculation [66]. In the calculation, we employ a diagonal horn with a horn length of 20mm and a diagonal aperture of 11mm. Fig. 8(a) shows one such calculation, in which it is quite clear that

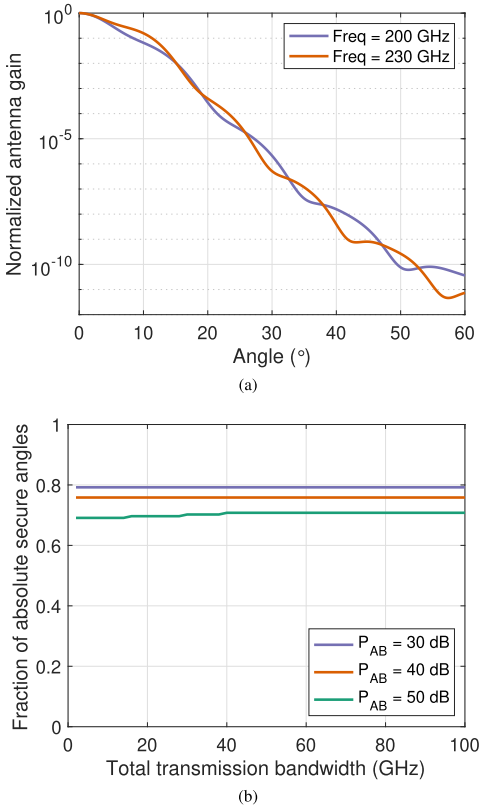


Fig. 8. Horn antenna. (a) The H-plane radiation pattern from a diagonal horn antenna, computed at two different frequencies. Unlike the antenna patterns shown in Fig. 2, this pattern exhibits no pronounced minima. (b) The fraction of secure angles, similar to Fig. 3(a), for the horn antenna. Since there are no pronounced minima, there is no improvement with increasing spectral bandwidth. As a result, the creation of blind regions is ineffective, if this antenna is employed without modification.

the 'minima' between any two side lobes (or between the main lobe and the first side lobes) are not very pronounced. Fig. 8(b) shows a blind region calculation analogous to the one shown in Fig. 3(a), for this horn antenna. This result demonstrates that the blind region does not grow with increasing transmission bandwidth. Therefore, the selection of the antenna configuration is a key aspect in implementing the proposed security protocol for the blind region.

B. Experimental Demonstration

As noted above, achieving absolute security requires the broadcast antenna to exhibit pronounced minima whose angular positions vary as a function of frequency. To illustrate the ease with which this can be accomplished, we assemble a link test bed using a horn antenna as the transmitter. Despite the lack of pronounced minima of horn antennas as observed in Fig. 8(a), it is still possible to demonstrate the feasibility of the absolute security system using a horn antenna.

As illustrated by the schematic in Fig. 9, we can place a focusing optic (a dielectric lens) in front of the horn, and focus its output onto a diffracting object, in this case a 4-mm-wide metal beam block. The far-field diffraction pattern from this illuminated beam block exhibits a strong maximum on the optic axis (the main lobe, at $\theta = 0$) and a pronounced minimum due to destructive interference at a non-zero angle. Using finite-element simulations, Fig. 9 illustrates the far-field pattern of the setup at three frequencies, 100, 200, and 400 GHz. Fig. 9 clearly shows the pronounced minimum at a small angle, followed by a subsidiary maximum (first side lobe) at a larger angle. We note that the first side lobes all peak within 10 dB of the main lobe. Thus, an eavesdropper outside of the main lobe is easily able to detect signals in the individual side lobes, but cannot decode any information from signals at the angles of the minima. Because these three minima do not coincide with each other, they collectively are expected to form a substantial (though not complete) blind region for angles outside of the main lobe.

To demonstrate the blind region, we performed the experiments employing a frequency multiplier chain in order to generate modulated signals (on-off keying at 1 Gb/sec) at the three widely spaced frequencies (100, 200, and 400 GHz). The modulated data stream is broadcast from the emitter horn antenna, and the bit error rate is measured vs. angle. Fig. 10 illustrates the experimental arrangement and shows the measured bit error rates (BER) as a function of angle for a broadcast employing three frequency channels.

At $\theta = 0°$ (Bob's location), we find BER $< 10^{-9}$ at all three frequencies. As θ increases, each frequency band passes through the minimum of the radiation pattern, where the BER increases to 0.5 (i.e., it is impossible to tell the difference between a '0' and a '1'). As θ increases further, the maximum of the first side lobe is reached, and the BER again falls to a relatively low value, before once again increasing as the angle increases beyond the edge of the diffracted beam pattern. Eye diagrams for the three frequencies are shown for a representative angle of $\theta = 8.5°$ where an eavesdropper could be located. The eye diagrams unambiguously demonstrate that an eavesdropper at this location receives information in only two of the three bands.

Based on the experiments, the blind regions (i.e., the angular locations where at least one frequency is below detection) are indicated by the orange bars along the horizontal axis in Fig. 10. This configuration, which uses only three channels, creates blind regions for $1.6° < \theta < 2.0°$ and $\theta > 3.4°$. Although only three channels are employed, we nevertheless induce a substantial (though not complete) blind region.

IV. Frequency Channels Selection

In advanced wireless communications systems, e.g., OFDMA protocols in 5G, there is a large set of frequency channels [67]. Yet, only a subset of these frequency channels is used for each particular orthogonal connection between a legitimate transmitter and a legitimate receiver. In the solution we propose, the combination of the frequency channels that Alice uses in practice to send information to Bob defines the performance of the secure communication in terms of information rate and achieved blind region. That is, by choosing the combination of different frequencies, Alice can jointly design the collective side lobe structure and the nulls to maximize the desired performance. Here we provide one example of an optimization solution to select the subset of the frequency channels at Alice by a target of performance target that we design. This optimization solution selects a subset of q frequency channels that maximize the blind

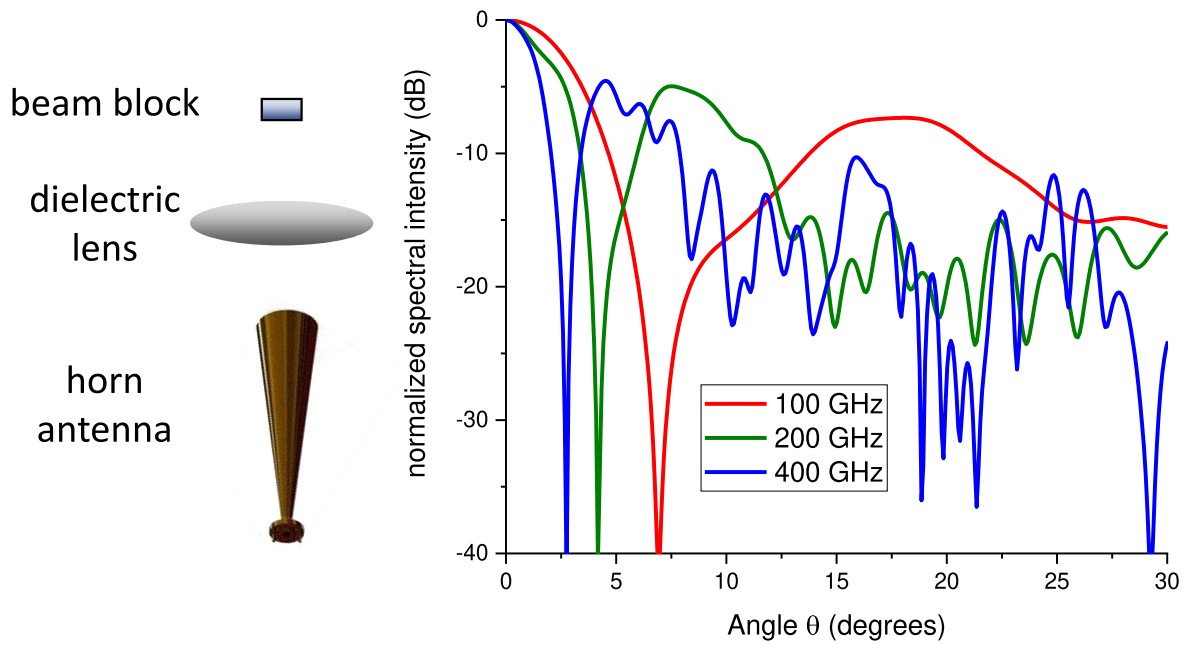


Fig. 9. Schematic of the experimental setup used in the measurements described in the above text, and also used in the simulations shown here. These are finite-element simulations of the angular dependence of the far-field diffraction pattern produced by a horn antenna focused on a 4-mm-wide metal beam block. The simulations were performed at the three different frequencies (100, 200, and 400 GHz) used in the experiments.

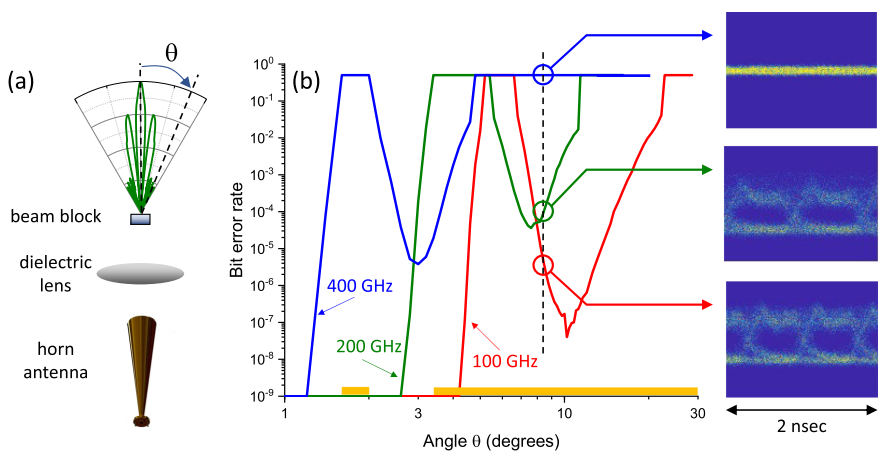


Fig. 10. Experimental realization of absolute security. (a) A schematic of the experimental setup. The emission from a horn antenna is focused onto a 4-mm wide beam block to produce a far-field radiation pattern exhibiting a pronounced minimum at an angle which depends on frequency. The pattern at 200 GHz, computed using a finite element solver, is shown. (b) At three widely spaced frequencies (100, 200, and 400 GHz), a data stream (modulated with on-off keying, at a rate of 1Gb/sec) is broadcast from the emitter horn antenna, and the bit error rate is measured vs. angle. Eye diagrams for the three frequencies are shown for a representative angle of $\theta = 8.5^\circ$ where an eavesdropper could be located. This configuration, using only three channels, creates blind regions for $1.6^\circ < \theta < 2.0^\circ$ and $\theta > 3.4^\circ$ (indicated by the orange bars along the horizontal axis).

region given in (3), while providing the information data rate needed at Bob.

We denote by $R_{m,t}$ the information data rate needed at Bob. In the setting proposed here, Alice uses q frequency channels from a large set $\mathcal{Q}$ available in the wireless communications system. Given the signal strength for each frequency channel, as given in (1), the subset of frequency channels $\mathcal{Q}_s \subset \mathcal{Q}$ selected by Alice are determined as follows:

$$\mathcal{Q}_s = \arg\max_{\mathcal{Q}_s \subset \mathcal{Q}} \bigcup_{f \in \mathcal{Q}_s} \mathcal{Z}(f), \quad \text{s.t.} \quad \sum_{f \in \mathcal{Q}_s} R_m^f \geq R_{m,t},$$

where R_m^f denotes the data rate of each frequency channel and $q = |\mathcal{Q}_s|$.

V. General Absolute Secure Coding Scheme

In this section, we describe an absolute post-quantum secure coding scheme for the general setting, illustrated in Fig. 11, [56], [57], [58]. The scheme consists of two independent stages. In the first stage, we use a secure linear code to guarantee information security. Since using a linear code is equivalent to performing a matrix multiplication on a matrix of Alice's

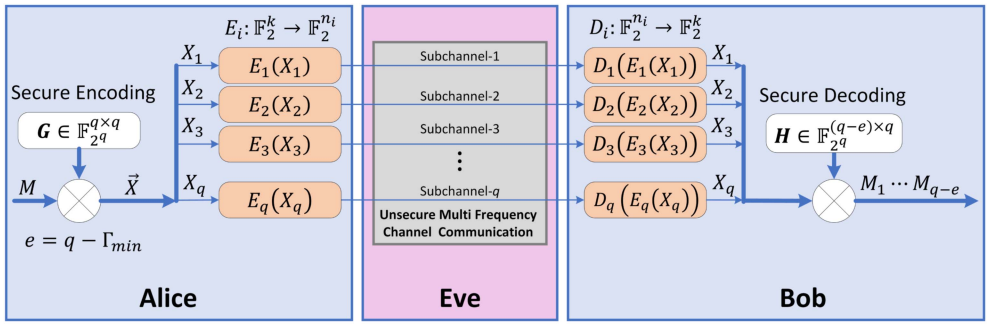


Fig. 11. Absolute post-quantum secure coding scheme.

messages, we refer to the secure linear code by its matrix $\mathbf{G} \in \mathbb{F}_{2^q}^{q\times q}$. The decoding of the secure linear code, similar to encoding, can be accomplished by matrix multiplications on the encoded messages. The encoding and decoding matrices for the proposed security schemes are further discussed below.

In the second stage, we use an error-correcting code to protect the messages from potential errors in each subchannel. For each subchannel i an error-correcting code [68] is a function $E_i : \mathbb{F}_2^k \to \mathbb{F}_2^{n_i}$ where k is such that $0 < k \leq n_i$ and varies according to the choice of scheme, as we describe below. For every error correction code E_i there is also a decoding function $D_i : \mathbb{F}_2^{n_i} \to \mathbb{F}_2^k$ that returns the messages to their original size. Intuitively, by mapping the messages into a larger space before the transmission, we are able to protect them from potential errors that might occur during the transmission. The ratio $R_i = \frac{k}{n_i}$ is called the code rate.

Alice's messages to Bob can be represented by a string of binary bits which are partitioned into blocks, each mapped to symbols of a finite field. We denote the size of each binary block by k_b and, therefore, Alice's messages can be represented over the binary field $\mathbb{F}_2^{1\times k_b}$. Since $\mathbb{F}_2^{1\times q}$ is isomorphic to $\mathbb{F}_{2^q}$ [58, Section II], Alice's messages can be represented by symbols over the finite field $\mathbb{F}_{2^q}^{1\times\lceil k_b/q\rceil}$. Finally, we define a design parameter $\Gamma_{\min} \geq 1$ that shapes the blind region so that each possible location for Eve can be characterized as either non-blind ($\Gamma < \Gamma_{\min}$) or Γ-blind ($\Gamma_{\min} \leq \Gamma \leq q$). We then denote by $e = q - \Gamma_{\min}$ the maximum number of subchannels Eve can observe in the blind region. In previous sections, we considered $\Gamma_{\min} = 1$.

Now we present a construction for a generalized version of the secure coding scheme introduced in Section II-C. It is important to note that the coding scheme is derived from known constructions in the literature [56], [57], [58]. However, in this article, the performance of the secure code depends on both the antenna design and Alice's choice of the desired blind region, represented by $\Gamma_{\min}$ and e. First, Alice forms a message symbol matrix M, which consists of $(q-e)$ message symbols and e uniformly random symbols. In particular, $M = (M_1; \ldots; M_{q-e}; T_1; \ldots; T_e) \in \mathbb{F}_{2^q}^{q\times\lceil k_b/q\rceil}$, where the M_i's in the first $(q-e)$ rows are message symbols, and the T_i's in the remaining e rows are uniformly independent random symbols. Then, to obtain the encoded symbols $X = (X_1; \ldots; X_q) \in \mathbb{F}_{2^q}^{q\times\lceil k_b/q\rceil}$, Alice multiplies each of the $\lceil k_b/q\rceil$ columns in M by a secure code $\mathbf{G} \in \mathbb{F}_{2^q}^{q\times q}$, whose construction is detailed in [69, Section V], to obtain the $\lceil k_b/q\rceil$ columns of X. The coding operation makes each encoded symbol X_i a linear combination of the $(q-e)$ message symbols and e random symbols, with the coefficients specified by the secure code $\mathbf{G}$. Also, note that X_i's can be converted to the binary field with length k_b. That is, $X = (X_1; \ldots; X_q) \in \mathbb{F}_{2^q}^{q\times\lceil k_b/q\rceil}$ can be equivalently represented over $\mathbb{F}_2^{q\times k_b}$. Before transmitting each X_i to Bob through the channel i, to ensure the reliability of the transmission, each X_i is encoded using an error-correcting code E_i with a code rate $R_i = \frac{k_b}{n_i}$, according to the maximum code rate for the error-correcting capability afforded to that subchannel [62, Chapter 9].

Bob receives a possibly erroneous version of each $E_i(X_i)$ which the decoder D_i will decode correctly if the error has not exceeded the error-correcting capability of the code. To obtain the original message symbols $(M_1; \ldots; M_{q-e})$, Bob then uses the corresponding decoding matrix $\mathbf{H} \in \mathbb{F}_{2^q}^{(q-e)\times q}$ as described in [58, Section V]. The secure encoding $\mathbf{G}$ guarantees that, if Eve detects the signal of at most e subchannels, she cannot infer any information about Alice's message symbols $(M_1; \ldots; M_{q-e})$, regardless of her computational capabilities [58]. The secure communication efficiency of the secure coding scheme is given by $\eta = \frac{\Gamma_{\min}}{q}$ (where in the main text we set $\Gamma_{\min} = 1$).

Now, we present the generalized version of Scheme 2 given in Section II-D. This scheme obtains a secure communication efficiency of $\eta = 1$ by relaxing the security guarantee from strong security to individual security. The construction is the same as above, using the secure code $\mathbf{G} \in \mathbb{F}_{2^q}^{q\times q}$ given in [56, Section V], but with two main differences. First, the e rows of the random symbols $(T_1; \ldots; T_e) \in \mathbb{F}_{2^q}^{e\times\lceil k_b/q\rceil}$ are replaced with the message symbols from Alice $(M_{q-e+1}; \ldots; M_q) \in \mathbb{F}_{2^q}^{e\times\lceil k_b/q\rceil}$. Second, Alice's message symbols $(M_1; \ldots; M_q) \in \mathbb{F}_{2^q}^{q\times\lceil k_b/q\rceil}$ must be uniformly distributed [57]. This uniformity condition can be enforced using known techniques from the literature [60]. We note that to obtain the message symbols $(M_1; \ldots; M_{q-e}) \in \mathbb{F}_{2^q}^{(q-e)\times\lceil k_b/q\rceil}$ and $(M_{q-e+1}; \ldots; M_q) \in \mathbb{F}_{2^q}^{e\times\lceil k_b/q\rceil}$, Bob must now use two decoding matrices, $\mathbf{H} \in \mathbb{F}_{2^q}^{(q-e)\times q}$ and $\tilde{\mathbf{G}} \in \mathbb{F}_{2^q}^{e\times q}$, respectively, as described in [56, Section V].

As a final comment, we address the question of how the complexity of the encoding increases with increasing number of channels. We note that the operations are performed over an extension field of binary $\mathbb{F}_{2^q}$, i.e., each symbol has q bits. The

number of bits corresponding to the finite field must thus increase with the number of channels, but only in a linear fashion. Thus, the complexity of the operation scales nearly linearly with q. For typical kilobyte-scale frames, this is a routine computation that imputes no significant complexity.

VI. Comparison With Zero-Forcing Approaches

In this section, we compare conventional zero-forcing (ZF) methods considered in the literature for wireless communication systems and information-theoretic security schemes with the absolute security approach we propose.

a) Zero-Forcing Beam Forming: Traditionally, zero-forcing utilizing beamforming techniques at the transmitter are considered in wireless communications to maximize the SNR at the receiver [70], [71], [72], [73]. As elaborated in [74], the improvement in the SNR terms in the receiver is obtained by maximizing the directed main lobe SNR by a directional beamformer. It is essential to note that the classical techniques, as presented, for example, in [70], [71], [72], [73], have not considered security constraints. However, in this setting, one can increase the security rate by applying traditional wiretap codes at the transmitter, e.g., [23], [24]. Secrecy rate is obtained using wiretap codes when Bob's SNR exceeds Eve's. Thus, by using ZF beamforming techniques which increase the SNR at Bob (when he receives the main lobe), while the SNR at the eavesdropper decreases (when he gets one of the side lobes), may increase the secrecy rate obtained. In this setting, the security guarantees obtained rely on statistical assumptions about noise.

b) Zero-Forcing Based Wiretap Channel: Recently information-theoretic coding solutions have been proposed in the literature for ZF schemes [75], [76], [77], [78]. In these wiretap ZF schemes, the transmitter intends to send the secret information in the orthogonal space of the eavesdropper channel. In this setting, secrecy rate is obtained under the assumption that the terminals have perfect channel state information (CSI). Thus, the transmitter needs to know the *precise location* of the eavesdropper. However, secrecy outage can occur when the transmitter does not have full CSI about the main channel or the eavesdropper's channel, or the transmitter has full CSI but is subject to delay constraints. Secrecy bounds for multiple-antenna with full CSI and high SNR and for finite SNR have been provided in [75], [76], and [77], respectively. Moreover, the secrecy rate of MIMO wiretap channels with ZF detectors over the uncorrelated Rayleigh fading channel is given in [78]. Compared to the classical wiretap ZF scheme, with our approach, if Eve fails to obtain information from just one of the frequency channels, she cannot get information from any of them. Finally, we note that ZF only works for multiple antenna/elements and specific codes that guarantee nulls at the eavesdropper; meanwhile, the absolute security approach has the advantage of working well for different antenna configurations and secure coding schemes. In Section III, we focus on the performance obtained with different sets of antennas and the secure coding scheme given in Section II-C. We leave the study of the combination of different secure coding schemes, as given, for example, in [26], [27], [44], [56], [79], [80], for future work.

c) Orthogonal Space Jamming: ZF beamforming strategies have been considered in the literature for a setting with a friendly jammer (or helper), James, who is interested in helping Alice and Bob achieve or increase the secure communication rate using information-theoretic security solutions. In this setting, James uses a ZF beamforming vector considering the legitimate receiver Bob. That is, the friendly jammer will transmit a random noise in the null space of his channel to Bob. By this, James decreases the SNR at Eve without impairing the channel observation at Bob. Moreover, in this setting, if the CSI of the eavesdropper channel is known to James, namely the precise location of Eve, he can utilize a beamforming vector to maximize the interference of Eve's observation. For example, the secrecy rate with ZF jammer in the MISO wiretap channel is given in [81]. Strategies with jammer applying ZF are considered for multiple eavesdroppers, for untrusted relaying, and in practical cross-layer implementations, in [82], [83], and [55], respectively. Finally, we note that those strategies with a friendly jammer can be combined with the solution offered herein for absolute security to increase the security rate. We leave this interesting direction for future study.

In summary, we note that our proposed absolute security scheme is versatile and can be applied based on different beamforming approaches, such as the one based on zero-forcing, and we expect similar security performance in the blind region regardless of the beamforming weights. We leave this interesting direction for future study.

VII. Conclusions and Future Work

It should be noted that our approach requires engineering of both the physical properties of the transmission system and the data encoding scheme. It is therefore neither purely cryptographic nor purely a physical-layer security system. The hybrid nature of this concept is, to the best of our knowledge, unique in wireless system architectures. We also note that the security guarantees described here are relatively straightforward to achieve, relying only on the assertion that Eve's ability to receive signals is limited by the thermal radiation from the scene she is observing, implying that there exists a smallest measurable signal threshold $\delta > 0$. Apart from that assertion, our analysis affords Eve every strength, such as quantum computing and quantum-noise limited detection. This is the first example of a security protocol which exploits aspects of the physical layer, but does not rely on any assumption about noise. We also note that the encoding scheme used by Alice can be known to all, including Eve, without changing any of our conclusions.

In this article, we focus on a communication model with a single eavesdropper for an idealized propagation environment (free space) to describe a new approach of absolute security. More general scenarios encompassing richer models are considered in future work, including the extension of the single eavesdropper model to the multiple eavesdropper model, as widely considered in the literature for physical layer security [26], [27]. In this

model, techniques used for SNR-based security can be considered to determine the bind region and analyze the security, as given in [84], [85], [86]. Extensions also include the study of Eve being in the same beam as Bob and Eve being equipped with a more directional antenna than Bob. For cases where potentially Eve may potentially not be in the blind region, i.e.i.e., where the probability of eavesdropping probability may be highlarger than zero, future studies also include the incorporation of the coding scheme used in this article with the techniques of partial post-quantum encryption given in [69]. Thus, potentially, at high communication data rates, it is possible to guarantee absolute security against eavesdroppers in the blind region and cryptography post-quantum security against eavesdroppersEve, which areis not in this region.

References

[1] A. Cohen et al., "Absolute security in high-frequency wireless links," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2022, pp. 46–54.

[2] M. Raboy,*Marconi the Man Who Networked the World*. London, U.K.: Oxford Univ. Press, 2016.

[3] R. Valkonen, "Compact 28-GHz phased array antenna for 5G access," in *Proc. IEEE/MTT-S Int. Microw. Symp.*, 2018, pp. 1334–1337.

[4] S. Ullah, W.-H. Yeo, H. Kim, and H. Yoo, "Development of 60-Ghz millimeter wave, electromagnetic bandgap ground planes for multiple-input multiple-output antenna applications," *Sci. Rep.*, vol. 10, no. 1, pp. 1–12, 2020.

[5] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.

[6] K. C. Ravi, J. Kumar, T. A. Elwi, and M. M. Ali, "Compact MIMO antenna for 5G applications," in *Proc. IEEE ANDESCON*, 2022, pp. 1–6.

[7] H. Zahra, M. Hussain, S. Shrestha, M. Asadnia, S. M. Abbas, and S. Mukhopadhyay, "Printed planar antenna for 28 GHz 5G millimeter wave applications," in *Proc. IEEE Int. Symp. Antennas Propag. USNC-URSI Radio Sci. Meeting*, 2022, pp. 53–54.

[8] M. Hussain, I. A. Awan, S. M. Rizvi, M. Alibakhshikenari, F. Falcone, and E. Limiti, "Simple geometry multi-bands antenna for millimeter-wave applications at 28 GHz, 38 GHz, and 55 GHz allocated to 5G systems," in *Proc. IEEE 46th Int. Conf. Infrared, Millimeter Terahertz Waves*, 2021, pp. 1–2.

[9] J. Ma et al., "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018.

[10] K. Sengupta, T. Nagatsuma, and D. M. Mittleman, "Terahertz integrated electronic and hybrid electronic–photonic systems," *Nature Electron.*, vol. 1, no. 12, pp. 622–635, 2018.

[11] J. Ma, R. Shrestha, L. Moeller, and D. M. Mittleman, "Invited article: Channel performance for indoor and outdoor terahertz wireless links," *APL Photon.*, vol. 3, no. 5, 2018, Art. no. 051601.

[12] A. Alexiou, S. Andreev, G. Fodor, and T. Nagatsuma, "THz communications: A catalyst for the wireless future," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 12–13, Nov. 2020.

[13] V. Petrov, T. Kurner, and I. Hosako, "IEEE 802.15.3d: First standardization efforts for sub-terahertz band communications toward 6G," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 28–33, Nov. 2020.

[14] X. Su et al., "Receiver aperture and multipath effects on power loss and modal crosstalk in a THz wireless link using orbital-angular-momentum multiplexing," *Sci. Rep.*, vol. 12, no. 1, pp. 1–15, 2022.

[15] P. Li et al., "Performance degradation of terahertz channels in emulated rain," *Nano Commun. Netw.*, vol. 35, 2023, Art. no. 100431.

[16] C. Castro, R. Elschner, T. Merkle, C. Schubert, and R. Freund, "Experimental demonstrations of high-capacity THz-wireless transmission systems for beyond 5G," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 41–47, Nov. 2020.

[17] J. Federici and L. Moeller, "Review of terahertz and subterahertz wireless communications," *J. Appl. Phys.*, vol. 107, 2010, Art. no. 111101.

[18] B. Peng, K. Guan, A. Kuter, S. Rey, M. Patzold, and T. Kuerner, "Channel modeling and system concepts for future terahertz communications: Getting ready for advances beyond 5G," *IEEE Veh. Technol. Mag.*, vol. 15, no. 2, pp. 136–143, Jun. 2020.

[19] H. Zhou et al., "Utilizing multiplexing of structured THz beams carrying orbital-angular-momentum for high-capacity communicationss," *Opt. Exp.*, vol. 30, no. 14, pp. 25418–25432, 2022.

[20] L. Mucchi et al., "Signal processing techniques for 6G," *J. Signal Process. Syst.*, vol. 95, pp. 1–23, 2023.

[21] K. Sengupta, X. Lu, S. Venkatesh, and B. Tang, "Physically secure Sub-THz wireless links," in *Proc. IEEE Int. Conf. Commun. Workshops*, 2020, pp. 1–7.

[22] S. Venkatesh, X. Lu, B. Tang, and K. Sengupta, "Secure space-time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks," *Nature Electron.*, vol. 4, no. 11, pp. 827–836, 2021.

[23] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[24] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[25] M. Médard and K. R. Duffy, "Physical Layer Insecurity," in *Proc. IEEE 57th Annu. Conf. on Inf. Sci. Syst.*, 2023, pp. 1–6.

[26] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Boston, MA, USA: Now Publishers Inc, 2009.

[27] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[28] Y. He, L. Zhang, S. Liu, H. Zhang, and X. Yu, "Secure transmission of terahertz signals with multiple eavesdroppers," in *Micromachines*, vol. 13, no. 8, 2022, Art. no. 1300. [Online]. Available: https://www.mdpi.com/2072-666X/13/8/1300

[29] W. Gao, C. Han, and Z. Chen, "DNN-powered SIC-free receiver artificial noise aided terahertz secure communications with randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 563–576, Jan. 2022.

[30] R. Wang, Y. Mei, X. Meng, and J. Ma, "Secrecy performance of terahertz wireless links in rain and snow," *Nano Commun. Netw.*, vol. 28, 2021, Art. no. 100350. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1878778921000119

[31] Y. Mei, Y. Ma, J. Ma, L. Moeller, and J. F. Federici, "Eavesdropping risk evaluation on terahertz wireless channels in atmospheric turbulence," *IEEE Access*, vol. 9, pp. 101916–101923, 2021.

[32] C.-Y. Yeh, Y. Ghasempour, Y. Amarasinghe, D. M. Mittleman, and E. W. Knightly, "Security in terahertz WLANs with leaky wave antennas," in *Proc. 13th Conf. Secur. Privacy Wireless Mobile Netw.*, 2020, pp. 317–327.

[33] C.-Y. Yeh, A. Cohen, R. G. L. D'Oliveira, M. Médard, D. M. Mittleman, and E. W. Knightly, "Angularly dispersive terahertz links with secure coding: From theoretical foundations to experiments," in *Proc. 15th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2022, pp. 268–273.

[34] J. Woo, M. I. W. Khan, M. I. Ibrahim, R. Han, A. P. Chandrakasan, and R. T. Yazicigil, "Physical-layer security for THz communications via orbital angular momentum waves," in *Proc. IEEE Workshop Signal Process. Syst.*, 2022, pp. 1–6.

[35] B. Ning, Z. Chen, W. Chen, and L. Li, "Improving security of THz communication with intelligent reflecting surface," in *Proc. IEEE Globecom Workshops*, 2019, pp. 1–6.

[36] J. Qiao, C. Zhang, A. Dong, J. Bian, and M.-S. Alouini, "Securing intelligent reflecting surface assisted terahertz systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8519–8533, Aug. 2022.

[37] T. Troha, T. Ostatnický, and P. Kužel, "Improving security in terahertz wireless links using beam symmetry of vortex and Gaussian beams," *Opt. Exp.*, vol. 29, no. 19, pp. 30461–30472, Sep. 2021. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-29-19-30461

[38] P. Li et al., "Scattering and eavesdropping in terahertz wireless link by wavy surfaces," *IEEE Trans. Antennas Propag.*, vol. 71, no. 4, pp. 3590–3597, Apr. 2023.

[39] Z. Shaikhanov, F. Hassan, H. Guerboukha, D. Mittleman, and E. Knightly, "Metasurface-in-the-middle attack: From theory to experiment," in *Proc. 15th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2022, pp. 257–267.

[40] J. M. Jornet, E. W. Knightly, and D. M. Mittleman, "Wireless communications sensing and security above 100GHz," *Nature Commun.*, vol. 14, no. 1, 2023, Art. no. 841.

[41] T. Doeker, C. Herold, J. M. Eckhardt, and T. Kürner, "Eavesdropping measurements for applications in office environments at low THz frequencies," *IEEE Trans. Microw. Theory Techn.*, vol. 71, no. 6, pp. 2748–2757, Jun. 2023.

[42] Z. Fang, H. Guerboukha, R. Shrestha, M. Hornbuckle, Y. Amarasinghe, and D. M. Mittleman, "Secure communication channels using atmosphere-limited line-of-sight terahertz links," *IEEE Trans. THz Sci. Technol.*, vol. 12, no. 4, pp. 363–369, Jul. 2022.

[43] W. Gao, Y. Chen, C. Han, and Z. Chen, "Distance-adaptive absorption peak modulation (DA-APM) for terahertz covert communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 2064–2077, Mar. 2021.

[44] R. G. L. D'Oliveira, A. Cohen, J. Robinson, T. Stahlbuhk, and M. Médard, "Post-quantum security for ultra-reliable low-latency heterogeneous networks," in *Proc. IEEE Mil. Commun. Conf.*, 2021, pp. 933–938.

[45] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[46] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 1–14.

[47] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999.

[48] S. Hallgren, "Fast quantum algorithms for computing the unit group and class group of a number field," in *Proc. 37th Annu. ACM Symp. Theory Comput.*, 2005, pp. 468–474.

[49] S. Hallgren, "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem," *J. ACM*, vol. 54, no. 1, pp. 1–19, 2007.

[50] A. Schmidt and U. Vollmer, "Polynomial time quantum algorithm for the computation of the unit group of a number field," in *Proc. 37th Annu. ACM Symp. Theory Comput.*, 2005, pp. 475–480.

[51] C. A. Balanis, *Antenna Theory: Analysis and Design*. Hoboken, NJ, USA: Wiley, 2016.

[52] Y. Ghasempour, C. R.C. M. da Silva, C. Cordeiro, and E. W. Knightly, "IEEE 802.11ay: Next-generation 60 GHz communication for 100 Gb/s Wi-Fi," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 186–192, Dec. 2017.

[53] T. S. Rappaport et al., "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access*, vol. 1, pp. 335–349, 2013.

[54] S. Cho, G. Chen, and J. P. Coon, "Zero-forcing beamforming for active and passive eavesdropper mitigation in visible light communication systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1495–1505, 2020.

[55] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using zero-forcing beamforming," in *Proc. IEEE INFOCOM*, 2012, pp. 720–728.

[56] A. Cohen, A. Cohen, M. Médard, and O. Gurewitz, "Secure multi-source multicast," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 708–723, Jan. 2019.

[57] D. Silva and F. R. Kschischang, "Universal weakly secure network coding," in *Proc. IEEE Inf. Theory Workshop Netw. Inf. Theory*, 2009, pp. 281–285.

[58] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.

[59] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *ATT Bell Lab. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, 1984.

[60] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2355–2409, May 2016.

[61] S. Komiyama, "Single-photon detectors in the terahertz range," *IEEE J. Sel. Top. Quantum Electron.*, vol. 17, no. 1, pp. 54–66, Jan./Feb. 2011.

[62] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2012.

[63] S. Gupta, S. Abielmona, and C. Caloz, "Microwave analog real-time spectrum analyzer (RTSA) based on the spectral–spatial decomposition property of leaky-wave structures," *IEEE Trans. Microw. Theory Techn.*, vol. 57, pp. 2989–2999, Dec. 2009.

[64] Y. Ghasempour, R. Shrestha, A. Charous, E. Knightly, and D. M. Mittleman, "Single-shot link discovery for terahertz wireless networks," *Nature Commun.*, vol. 11, 2020, Art. no. 2017.

[65] N. J. Karl, R. W. McKinney, Y. Monnai, R. Mendis, and D. M. Mittleman, "Frequency-division multiplexing in the terahertz range using a leaky-wave antenna," *Nature Photon.*, vol. 9, pp. 717–720, 2015.

[66] J. F. Johansson and N. D. Whyborn, "The diagonal horn as a sub-millimeter wave antenna," *IEEE Trans. Microw. Theory Techn.*, vol. 40, no. 5, pp. 795–800, May 1992.

[67] H. Holma, A. Toskala, and T. Nakamura, *5G Technology: 3GPP New Radio*. Hoboken, NJ, USA: Wiley, 2020.

[68] S. Lin and D. J. Costello, *Error Control Coding*, vol. 2. Englewood Cliffs, NJ, USA: Prentice Hall, 2001.

[69] A. Cohen, R. G. L. D'Oliveira, S. Salamatian, and M. Médard, "Network coding-based post-quantum cryptography," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 49–64, Mar. 2021.

[70] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1691–1706, Jul. 2003.

[71] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication-part I: Channel inversion and regularization," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.

[72] F. Rusek et al., "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.

[73] J. Jee, G. Kwon, and H. Park, "Regularized zero-forcing precoder for massive MIMO system with transceiver I/Q imbalances," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1028–1031, Aug. 2019.

[74] E. Ali, M. Ismail, R. Nordin, and N. F. Abdulah, "Beamforming techniques for massive MIMO systems in 5G: Overview, classification, and trends for future research," *Front. Inf. Technol. Electron. Eng.*, vol. 18, no. 6, pp. 753–772, 2017.

[75] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.

[76] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

[77] Z. Rezki and M.-S. Alouini, "Secure diversity-multiplexing tradeoff of zero-forcing transmit scheme at finite-SNR," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 1138–1147, Apr. 2012.

[78] L. Kong, G. Kaddoum, D. B. Da Costa, and E. Bou-Harb, "On secrecy bounds of MIMO wiretap channels with ZF detectors," in *Proc. IEEE 14th Int. Wireless Commun. Mobile Comput. Conf.*, 2018, pp. 724–729.

[79] A. Cohen, R. G. L. D'Oliveira, K. R. Duffy, and M. Médard, "Partial encryption after encoding for security and reliability in data systems," in *Proc. IEEE Int. Symp. Inf. Theory*, 2022, pp. 1779–1784.

[80] T. Q. Duong, X. Zhou, and H.V. Poor, Eds., *Trusted Communications with Physical Layer Security for 5G and Beyond*. Stevenage, U.K.: Inst. Eng. Technol., 2017.

[81] A. Wolf and E. A. Jorswieck, "On the zero forcing optimality for friendly jamming in MISO wiretap channels," in *Proc. IEEE 11th Int. Workshop Signal Process. Adv. Wireless Commun.*, 2010, pp. 1–5.

[82] H.-T. Chiang and J. S. Lehnert, "Optimal cooperative jamming for security," in *Proc. IEEE Mil. Commun. Conf.*, 2011, pp. 125–130.

[83] K.-H. Park and M.-S. Alouini, "Secure amplify-and-forward untrusted relaying networks using cooperative jamming and zero-forcing cancelation," in *Proc. IEEE 26th Annu. Inter. Symp. Pers. Indoor Mobile Radio Commun.*, 2015, pp. 234–238.

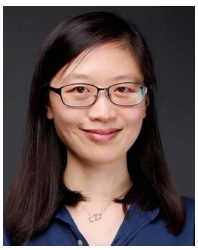
[84] Y. Ju, H.-M. Wang, T.-X. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114–2127, May 2017.

[85] Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2675–2689, Apr. 2018.

[86] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.

Alejandro Cohen (Member, IEEE) received the B.Sc. degree from the Department of Electrical Engineering, SCE College of Engineering, Ashdod, Israel, in 2010, and the M.Sc. and Ph.D. degrees from the Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Beersheba, Israel, in 2013 and 2018, respectively. He is currently an Assistant Professor with the Faculty of Electrical and Computer Engineering, Technion, Haifa, Israel. From 2019 to 2021, he was a Senior Postdoctoral Associate with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA. From 2007 to 2014, he was with DSP Group, where he worked on voice enhancement and signal processing. From 2014 to 2019, he was with Intel, Santa Clara, CA, USA, where he worked as a Research Scientist with the Innovation Group at Mobile and Wireless. His research interests include information theory, signal processing, and networks, wireless communication, security, network information theory and network coding, anomaly detection, coding, computation in networks, and speech enhancement.

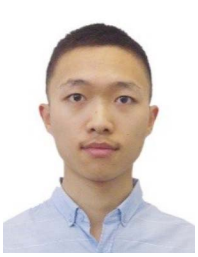
Rafael G. L. D'Oliveira (Member, IEEE) received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in applied mathematics from the University of Campinas, Campinas, Brazil, in 2009, 2012, and 2017, respectively. He is currently an Assistant Professor with the School of Mathematical and Statistical Sciences, Clemson University, Clemson, SC, USA. He was a Postdoctoral Research Associate with the Massachusetts Institute of Technology, Cambridge, MA, USA, from 2020 to 2022, and with Rutgers University, New Brunswick, NJ, USA, from 2018 to 2019, and with the Illinois Institute of Technology, Chicago, IL, USA, in 2017. From 2015 to 2016, he completed a research internship with Telecom Paristech, Paris, France. His research interests include privacy and security, distributed computing, coding theory, and information theory.



Chia-Yi Yeh (Member, IEEE) received the B.S. degree in electrical engineering from National Taiwan University, New Taipei, Taiwan, in 2014, and the M.S. and Ph.D. degrees in electrical and computer engineering from Rice University, Houston, TX, USA, in 2017 and 2021, respectively, under the supervision of Prof. Edward W. Knightly. She is currently a Postdoctoral Associate with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, and the School of Engineering, Brown University, Providence, RI, USA, under Prof. Muriel MÃ©dard and Prof. Daniel M. Mittleman. Her research interests include design, implementation, and experimental demonstration of next-generation wireless systems for communication, security, and sensing based on theoretical foundations, for systems including massive MIMO, millimeter wave, and terahertz networks.

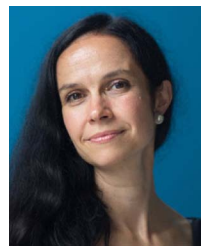
Hichem Guerboukha received the B.Sc. degree in engineering physics, the M.Sc. degree in applied science, and the Ph.D. in engineering physics from Polytechnique Montreal, Montreal, QC, Canada, in 2014, 2015 and 2019, respectively. He is currently a Postdoctoral Research Fellow with Brown University School of Engineering, Providence, RI, USA. He is currently a FRQNT Postdoctoral Research Fellow and working on THz communications, antennas, and metamaterials. His previous research interests include THz instrumentation and waveguides, THz computational imaging and THz communications. Dr. Guerboukha was the recipient of the 2015 Releve Étoile Louis-Berlinguet from Fonds de recherche – Nature et technologies. He was also the recipient of the Best M. Sc. Thesis Award and the Best Ph.D. Thesis Award from Polytechnique Montreal in 2015 and 2019, respectively.

Rabi Shrestha received the B.S. degree in electrical and computer engineering and the M.S. degree in electrical engineering from the University of Rochester, Rochester, NY, USA, in 2016 and 2017, respectively, and the Ph.D. degree in electrical engineering with Brown University, Providence, RI, USA, under the guidance of Prof. Daniel M. Mittleman, in 2022. His research focuses on terahertz wireless communication and technology.



Zhaoji Fang received the B.S. degree in electrical and information engineering from Beihang University, Beijing, China, in 2019. He is currently working toward the Ph.D. degree in electrical engineering with Brown University, Providence, RI, USA, under the direction of Dr. Daniel M. Mittleman. His research focuses on terahertz wireless communication and technology.

Edward W. Knightly (Fellow, IEEE) received the B.S. degree from Auburn University, Auburn, AL, USA, and the M.S. and Ph.D. degrees from the University of California at Berkeley, Berkeley, CA, USA. He is currently a Sheafor-Lindsay Professor of electrical and computer engineering and computer science with Rice University, Houston, TX, USA. His research interests include design, prototyping, and in-the-field demonstration of next-generation mobile and wireless networks, with a focus on networking, sensing, and security in diverse spectrum spanning from sub-6 GHz to millimeter wave and terahertz. He is an ACM Fellow and a Sloan Fellow. He was the recipient of the Dynamic Spectrum Alliance Award for Research on New Opportunities for Dynamic Spectrum Access and National Science Foundation CAREER Award., and eight best paper awards, including ACM MobiCom, ACM MobiHoc, IEEE Communications and Network Security, and IEEE INFOCOM. He has given more than 30 plenary keynote presentations, including at ACM MobiCom and IEEE INFOCOM. He was also the recipient of the George R. Brown School of Engineering Teaching + Research Excellence Award in 2021. He is an Editor-at-Large of IEEE/ACM TRANSACTIONS ON NETWORKING and serves on the scientific council of IMDEA Networks in Madrid and the scientific advisory board of INESC TEC in Porto. From 2014 to 2019, he was the Rice ECE Department Chair.



Muriel Médard (Fellow, IEEE) is currently the NEC Professor of software science and engineering with the Electrical Engineering and Computer Science Department, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, where she leads the Network Coding and Reliable Communications Group, Research Laboratory for Electronics. She has co-founded CodeOn, Steinwurf, and Chocolate Cloud for technology transfer of network coding. She was the recipient of the 2019 Best Paper Award for IEEE Transactions on Network Science and Engineering, 2009 IEEE Communication Society and Information Theory Society Joint Paper Award, 2009 William R. Bennett Prize in the Field of Communications Networking, 2002 IEEE Leon K. Kirchmayer Prize Paper Award, 2018 ACM SIGCOMM Test of Time Paper Award, and several conference paper awards. In 2007, she was named a Gilbreth Lecturer by the U.S. National Academy of Engineering. She was also the recipient of the 2016 IEEE Vehicular Technology James Evans Avant Garde Award, 2017 Aaron Wyner Distinguished Service Award from the IEEE Information Theory Society, and 2017 IEEE Communications Society Edwin Howard Armstrong Achievement Award. She was the editor of many publications of IEEE, of which she was elected Fellow, and was the Editor-in-Chief of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. She was the President of the IEEE Information Theory Society in 2012, and served on its board of governors for 11 years. She was the technical program committee co-chair of many of the major conferences in information theory, communications, and networking.

Daniel M. Mittleman (Fellow, IEEE) received the B.S. degree in physics from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1988, and the M.S. and Ph.D. degrees in physics from the University of California, Berkeley, Berkeley, CA, USA, in 1990 and 1994, respectively, under the direction of Dr. Charles Shank. He then joined AT&T Bell Laboratories as a Postdoctoral Member of the technical staff, working first for Dr. Richard Freeman on a terawatt laser system, and then for Dr. Martin Nuss on terahertz spectroscopy and imaging. In September 1996, he joined the Electrical and Computer Engineering Department, Rice University, Houston, TX, USA. In 2015, he moved to the School of Engineering, Brown University, Providence, RI, USA. His research focuses on the science and technology of terahertz radiation. He is a Fellow of the OSA and APS. He was the 2018 recipient of the Humboldt Research Award. During 2018–2020, he served a three-year term as the Chair of the International Society for Infrared Millimeter and Terahertz Waves. He was the recipient of the Society's Exceptional Service Award in 2022. In 2023, he was named a Mercator Fellow of the Deutsche Forschungsgemeinschaft (DFG), in affiliation with the Meteracom project.