Security Analysis of Triangle Channel-based Physical Layer Key Generation in Wireless Backscatter Communications

Jiajun Li, *Student Member, IEEE,* Pu Wang, *Student Member, IEEE,* Long Jiao, *Student Member, IEEE,* Zheng Yan, *Senior Member, IEEE,* Kai Zeng, *Member, IEEE,* Yishan Yang, *Student Member, IEEE*

***Abstract*—Ambient backscatter communication (AmBC) enables ultra-low-power communications by backscattering ambient radio frequency (RF) signals and harvesting energy simultaneously. It has emerged as a cutting-edge technology for supporting a variety of Internet of Things (IoT) applications. However, existing research lacks effective secret key sharing schemes for safeguarding communications between resource-constrained backscatter devices (BDs) in AmBC systems. In this paper, we present, Tri-Channel, a novel physical layer key generation scheme between two BDs by multiplying downlink signals and backscatter signals to obtain the information of a triangle channel as a shared random secret source for key generation. In particular, we analyze the security of our scheme under both passive and active attacks, concretely Eavesdropping Attack (EA), Control Channel Attack (CCA), Signal Manipulative Attack (SMA), and Untrusted RF-Source Attack (URSA). Through theoretical analysis and simulations by comparing with a traditional scheme (named Tradi-Channel), we found that our scheme consistently outperforms the Tradi-Channel under the EA and two active attacks (CCA and SMA). In addition, it shows better security performance under URSA, which is proposed based on the unauthenticated characteristic of BDs in Tri-Channel, even though URSA is more vital than SMA. Concretely, Tri-Channel's secret key rate (SKR) outperforms Tradi-Channel's under the above four passive and active attacks. This implies that our scheme is advanced in terms of both security and efficiency of key generation. Numerous extensive simulations further prove our theoretical analysis results.**

***Index Terms*—Backscatter Communication, Physical Layer Key Generation, Passive Eavesdropping, Active Attacking**

I. Introduction

AMBIENT backscatter communication (AmBC) is considered as a promising communication technology for enabling various Internet of Things (IoT) applications due to its ultra-low-power consumption and energy harvesting capability [1]. In an AmBC system, backscatter devices (BDs) can transmit data by reflecting radio frequency (RF) signals in the air, such as TV and Wi-Fi signals, rather than generating power-hungry RF signals [2], [3]. In addition to backscattering signals via the uplink channel between the BD and a dedicated RF source, device-to-device (D2D) communication can also be realized [4]–[7]. One of the attractive applications of AmBC is implanted and wearable sensor systems for physiological and medical treatment. These sensors are resource-limited, making AmBC a suitable technology for data transmission and battery replenishment. However, due to the broadcast nature of backscatter, it is extremely easy for illegal devices to obtain backscattered communication information, which causes severe data interception and privacy leakage. But the limitations of energy and computational resources of BDs make implementing complex security schemes extremely challenging. Thus, it is urgent to devise a practical security scheme to protect the backscatter communications among BDs.

Traditional schemes for securing backscatter communications are mainly based on lightweight symmetric cryptography [8], [9]. They utilize a shared secret session key to encrypt/decrypt messages between BDs. The session key could be derived from a long-term master secret key or generated with the Diffie-Hellman (D-H) key exchange protocol. The former method suffers from complex key distribution and heavy management overhead, especially in ad-hoc scenarios where two BDs without any pre-shared secrets need to establish a secure communication channel. Once the long-term master secret key is compromised, all past communications are cracked. That is, the schemes based on a long-term master key cannot guarantee forward secrecy. It is also easily subjected to various attacks, such as impersonation and man-in-the-middle [10]. Regarding the D-H key exchange protocol, although it can provide forward secrecy, it introduces significant computational overhead, making it impractical to be applied into the AmBC system due to resource-constrained BDs. And with the dense deployment of BDs, the secret key distribution and management might become even complex and hard. Besides, cryptographic credentials are exchanged over backscatter channels, which can be intercepted by an eavesdropper, even if encrypted.

Alternatively, for resource-constrained systems, physical layer (PHY) key generation has been considered as a promising technology to provide lightweight and information-theoretically secure key sharing with forward secrecy [11], [12]. Based upon reciprocal randomness in a wireless fading channel, this method generates shared secret keys between devices without incurring significant computation overhead [13], [14]. In theory, the secrecy of the shared key is ensured by the fact that an adversary who is kept at a distance from the key generating device (larger than coherence distance) observes highly uncorrelated channel characteristics, thus unable to derive the same key. PHY key generation provides complete flexibility and scalability by supporting independent key establishment on demand, rather than relying on central servers or infrastructures.

Despite this, existing PHY key generation schemes cannot be directly applied to BD communications. The existing schemes usually require two devices to send channel probing signals to one another in order to measure highly correlated channel characteristics, such as received signal strengths (RSS) [15], at both ends for key generation [16]–[18]. However, BDs are not capable of generating channel probing signals by themselves, making channel probing between two BDs

J.J. Li, P. Wang, Y.S. Yang is with the State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, Shaanxi, 710026 China. (email: jiajunli1204@stu.xidian.edu.cn, wangpu@stu.xidian.edu.cn, ysyangxd@stu.xidian.edu.cn)

Z. Yan (corresponding author) is with the State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, Shaanxi, 710026 China. (email: zyan@xidian.edu.cn)

L. Jiao and K. Zeng are with the Department of Electrical and Computer Engineering, Cyber Security Engineering, and the Department of Computer Science, George Mason University, Fairfax, VA, 22030 USA (email: ljiao@gmu.edu, kzeng2@gmu.edu)

fundamentally different from traditional channel probing. The literature still lacks an effective physical layer key generation scheme to secure the communication between two BDs.

In this paper, we propose a novel PHY key generation scheme for two paired BDs in an AmBC system, named Tri-Channel, by multiplying downlink signals and backscatter signals to obtain the information of a triangle channel as a shared random secret source for key generation. Concretely in our working AmBC system, there is an RF source that transmits RF signals continuously, and two paired BDs communicate with each other in a time-division manner. Tri-Channel exploits the superposed ambient RF signal received by a BD, which contains the downlink signal from the RF source to the BD and the backscatter signal that is the signal of a concatenation channel of the other BD's downlink channel and the inward reflecting channel between the two BDs. Then by multiplying the downlink channel and the cascade backscatter channel, we can obtain a triangle channel, a multiplication of the two downlink channels and the inward reflecting channel at each BD, like three sides of a triangle formed by the RF source and the two BDs. The multiplications on both BDs are highly correlated if the reciprocity of the BD-to-BD channel holds well. Therefore, a random secret source can be established for key generation between the two BDs over ambient RF signals.

In order to evaluate the security of the Tri-Channel, we study its security performance under four types of attacks, either passive or active, and compare it with a traditional key generation scheme (named Tradi-Channel) that uses a channel probing signal to measure (estimate) channel information for key generation. Regarding active attacks, we introduce two popular types of attacks: Channel Control Attack (CCA) [18], Signal Manipulative Attack (SMA) [19], and propose a novel active attack, Untrusted RF-source Attack (URSA). For passive attacks, we consider a traditional eavesdropping attack (EA). URSA is actually a particular SMA that targets the Tri-Channel, but does not influence the Tradi-Channel. We analyze the security performance of the Tri-Channel in contrast to the Tradi-Channel under the EA and the first two active attacks. Since SMA and URSA are relative, we can distinguish these two attacks by analyzing the impact of them on the key generation and security performance of the Tri-Channel, respectively. In addition, we examine the impact of attack strength on the upper bound of the mutual information of generated keys under three types of active attacks. It is interesting to find that although the Tradi-Channel scheme has higher mutual information, a metric to measure key generation performance, than the Tri-Channel under all attacks, the secret key rate (SKR), which is a metric to jointly indicate both key generation security and efficiency, of Tri-Channel is higher than that of Tradi-Channel. Moreover, we find that Tri-Channel is sensitive to signal-to-noise ratio (SNR). When SNR is increased, the advantage of the Tri-Channel against CCA becomes obvious, compared with the Tradi-Channel.

In [20], we proposed BCAuth to allow the RF source to authenticate a BD to ensure its eligibility. After BDs' authentication, it is essential to setup a secure communication channel between two BDs in order to support their confidential information exchange. However, this has not yet been discussed in [20]. Compared with our early work [21], this paper provides a number of additional research results with experimental evaluation. First, we introduce two more typical active attacks (CCA and SMA) and further propose a new type of active attack URSA based on the non-authentication characteristic of the Tri-Channel. Second, we analyze the security performance of the Tri-Channel in contrast to the Tradi-Channel under EA, CCA and SMA. We further analyze and compare the security of Tri-Channel under SMA and URSA. Through analysis, we draw some valuable and interesting conclusions to show the advance of Tri-Channel. Third, we analyze the upper bound of mutual information of Tri-Channel under three active attacks. Fourth, we conduct numerical simulations to verify the conclusions drawn from theoretical security performance analysis. Finally, we compare the key generation performance between a joint transceiver design method and a channel estimation method with regard to the Tri-Channel.

The main contributions of this paper are summarized as below:

- We propose Tri-Channel, a novel PHY key generation scheme for two BDs by constructing a multiplication of three channels (i.e., the three sides of a triangle formed by the RF signal source and the two BDs) as shared randomness. To the best of our knowledge, this is the first work tackling the problem of BD communication session key generation in physical layer in an AmBC system.
- We evaluate the Tri-Channel's security performance with regard to the EA, the two typical active attacks (CCA and SMA), and the novel URSA, and compare it with that of the benchmark scheme, Tradi-Channel.
- We examine how the upper bound of the mutual information of generated keys changes under three types of active attacks when the attacks are strengthened. We prove that the upper bound of mutual information is monotonically increased, following the increase of attack strength.
- We conduct extensive numerical simulations to evaluate the security performance of Tri-Channel to show the correctness of our theoretical analysis and discuss its security merits and drawbacks.

II. Related Works

A. Lightweight Cryptography

In the existing literature, most security solutions tailored for backscatter communication are based on lightweight cryptography, such as lightweight data encryption standard (DESL), Present, Salsa20, Leak EXtraction (LEX) and lightweight elliptic curves cryptography (ECC) [8], [9]. Chine [22] presented an ultra-lightweight protocol that only requires simple bit-wise operations to provide authentication and integrity with reduced computational cost. While these algorithms provide good security against some attacks, they also exhibit unexpected limitations [23]–[25], such as reliance on key generation, distribution and management. They require resources to exchange cryptographical credentials over a backscatter channel, which could be intercepted by an eavesdropper, even if they are encrypted. Besides, the above solutions only support traditional backscatter systems with a dedicated RF reader and a tag with sufficient computational capability. However, the significant computational overhead of lightweight cryptography makes it problematic and undesirable for resource-constrained BDs. Whether it can be applied to AmBC to secure communications between two BDs requests additional investigation.

B. Physical Layer Security

Another way to secure backscatter systems while overcoming the limitations of cryptography is to apply PHY security schemes. Unlike the computational nature of cryptography, PHY security exploits the inherent randomness of a wireless channel to achieve communication confidentiality [26]. Apart from secure backscatter channel establishment with the help of proper coding, signal design and power allocation [27]–[29], PHY key generation has gained much attention in the literature [12], [30]. PHY Key Generation exploits the randomness and reciprocity of a wireless channel as a shared source to generate

secret keys. For example, channel state information (CSI), such as amplitude and phase, can be estimated by sending probing signals for key generation between two devices [17], [18]. In [31], the received signal strength (RSS) trajectories of two moving wearable devices are exploited to generate a secret key. Besides, secret group key generation schemes were proposed by exploiting different channel information and considering various topologies in multi-device systems [32]–[34].

In the current literature, all existing PHY key generation schemes require two communication parties to measure the channel properties by alternately transmitting probing signals. However, in the AmBC systems, BDs backscatter ambient RF signals in the air to transmit information. They are unable to estimate channel characteristics by transmitting probing signals, as required by the traditional PHY key generation schemes. Besides, BDs receive RF signals from RF sources and other BDs that pass different wireless channels, making it impossible to apply the RSS of RF signals or other channel state information as a random source. Therefore, it is impossible to apply existing schemes of physical key generation to AmBC systems, especially for D2D communications based on backscattering. The literature still lacks such an effective scheme.

III. System and Security Model

A. System Model

Fig. 1 illustrates the system model of our work with four types of attack models. Fig. 1(a) shows an AmBC system that consists of multiple BDs, which can communicate with each other in a time-division manner by backscattering the ambient RF signals emitted by the RF source (e.g., TV tower and Wi-Fi access point). We are interested in the physical layer key generation between two paired BDs in the AmBC system, which is trivial to be extended to multiple BDs scenarios [34]. We assume that there are only one legacy RF source and two passive (or semi-passive) BDs with a single antenna in the AmBC system. The BDs contain a backscatter modulator (i.e., a switched load impedance) and an information receiver. BDs can operate in a backscattering mode or a listening mode. The working mode can be shifted by switching the modulator. In the backscattering mode, BDs transmit information by reflecting incident signals and intentionally altering their amplitude and/or phase. To receive information, the antenna of BDs is switched to the listening mode, and BDs decode information from a part of received signals [6].

Since the AmBC system is often deployed in a crowded space, such as a warehouse or a house, the main channels (downlink or backscatter channels) are often blocked by some obstacles and therefore follow the Rayleigh channel model. Let h_i denote the multi-path Rayleigh fading channels between the RF source, BD A_i, and Eve or Mallory. And $h_{i,j}$ denotes the channel between A_i and A_j ($i, j \in \{1, 2, e$ (Eve) ,m (Mallory)$\}$, $i \neq j$), respectively. A channel is given in the form of $h = \vartheta d^{-\frac{\lambda}{2}}$, where ϑ is a circularly symmetric complex Gaussian (CSCG) variable, d is the distance between the considered transmitter and receiver, and λ is a path-loss exponent. For convenience subsequently, we define that the downlink channel of A_i is h_i and the inward channel of A_i and A_j is $h_{i,j}$, and the cascade backscatter channel $h_i h_{i,j}$, which is a concatenation of h_i and $h_{i,j}$, as shown in Fig. 1(a). All relevant channels are mutually independent and assumed to remain unchanged during the period of time slots, i.e., coherence time T_{ch} [12], [35].

B. Security Model

We introduce one passive attack and three active attacks to evaluate the security performance of the Tri-Channel under various attacks. In the security model, we assume the attacker can choose to launch a passive attack or different active attacks. In what follows, we respectively specify the passive attack, i.e., eavesdropping attack (EA) and two prevalent active attacks, CCA and SMA, as well as one specific SMA targeting on the Tri-Channel, i.e., URSA.

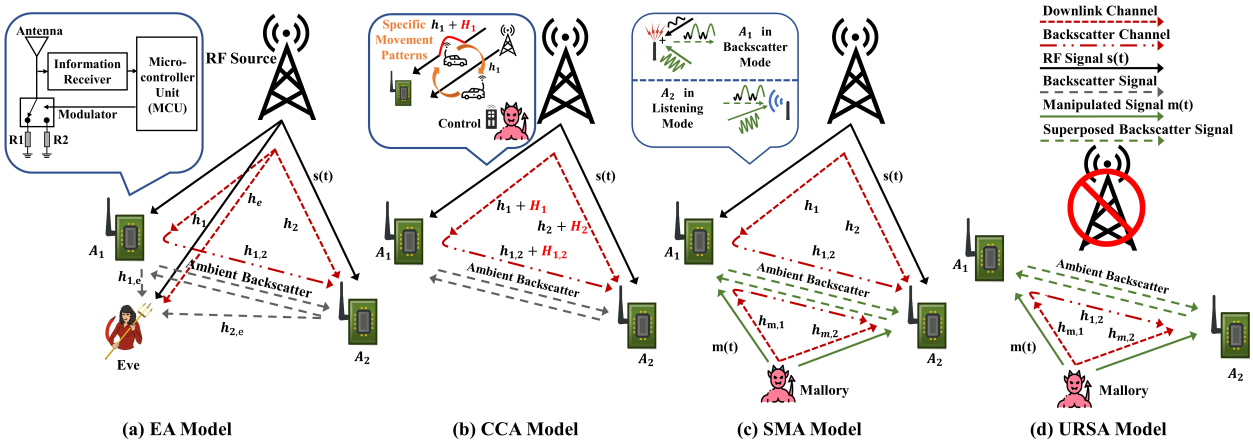
1) Eavesdropping Attack: We assume a passive eavesdropper named Eve, who only overhears all communications between BDs and tries to infer information about the generated key. This assumption implies that Eve is not interested in disrupting key establishment, neither jamming the communication channel nor modifying any message between BDs. As illustrated in Fig. 1(a), Eve measures the characteristics of the channels from all received signals while BDs are backscattering information to other BDs for key extraction. Thus, Eve can obtain the channel information from the original ambient signals of the RF source and the backscattered signals of BDs. However, we assume that Eve cannot be very close (less than a few multiples of the wavelength) to any BDs. This implies that Eve measures different and uncorrelated wireless channels. [12].

2) Channel Control Attack: As shown in [18], [19], an active attacker named Mallory can make a desired change in the channel between a receiver and a sender by designing specific movement patterns of intermediate objects to launch CCA. It may lead to variations in channel characteristics like path loss exponent. Mallory's objective involves making the involved key generating devices agree on some valid, but manipulated bits. Parts of the controlled information are contained in a generated key, and Mallory can utilize sequence similarities to infer portions of the key [36]. We use the symbol H_i shown in Fig. 1(b) to represent the variation of the channel. When launching the CCA, Mallory blocks the main channel with controlled intermediate objects or moves them away from the main channel. Furthermore, these movements result in the increase or decrease of the path loss exponent and further influence the channel gain.

3) Signal Manipulative Attack: An active attacker is capable of injecting signals and can perform two possible ways of attack: (1) the attacker injects different signals to two BDs to jam their communication; (2) the attacker injects similar signals to those of the two BDs and is interested in agreeing on some valid but manipulated key bits. The first is referred as jamming attack, which can be alleviated by adopting frequency hopping (FH) technique by randomly hopping to any one of multiple sub-channels in each time slot no matter the adversary jammer is equipped with a single antenna [37] or multiple antennas [38]. In this paper, we center our attention on the latter case. The second way of attack is called signal manipulative attack (SMA). Some existing works show that Mallory can inject equaled signals to both A_1 and A_2 and this constitutes an opportunity to control some bits of the key generated between A_1 and A_2 in the quantization phase [19], [39]. Mallory only needs to wait for an 'attack opportunity' when the attack channels are reciprocal.

As illustrated in Fig. 1(c), the 'attack opportunity' mentioned above refers to $h_{m,1} \approx h_{m,2}$. In this case, we let the manipulated signal sent from Mallory as $m(t)$, then the received signals at A_1 and A_2 are $P_1(t) = m(t)h_{m,1}$ and $P_2(t) = m(t)h_{m,2}$. Since the attack channels are reciprocal under the 'attack opportunity', we have $P(t) = P_1(t) = P_2(t)$. On the other hand, Mallory can manipulate some key bits since the generated key contains the manipulated signal $P(t)$.

4) Untrusted RF Source Attack: This attack is raised based on the non-authentication characteristic of the BDs in the Tri-Channel since the BDs unconditionally receive or backscatter



(a) EA Model (b) CCA Model (c) SMA Model (d) URSA Model

Fig. 1: System models under various attacks.

any arriving signals and generate a shared key based on these signals. Mallory can disguise itself as a signal source and send a signal to the backscatter device to manipulate the result of the key generation.

URSA is a particular case of SMA and is more vital than SMA. As shown in Fig. 1(c), when under SMA, the received signal of BDs is composed of the signal sent by a trusted RF source $s(t)$ and the signal sent by Mallory $m(t)$. Whereas when under URSA shown in Fig. 1(d), Mallory disguises itself as an RF source, the received signal of BDs is only composed of $m(t)$. This means that the key generated by the received signal is dominated by the signal $m(t)$ under URSA. Thus when Mallory launches URSA, it can manipulate more bits of keys to compromise more information than SMA.

C. Signal Model in AmBC Systems

Denote a bandpass signal transmitted from the RF source during a symbol interval as

$$\tilde{s}(t) = \Re\{\sqrt{p}s(t)e^{j2\pi f_c t}\}, \tag{1}$$

where $s(t)$ is a unit baseband signal with transmission power p, and f_c represents carrier frequency. The ambient signal received at A_i can be represented as [40]

$$\tilde{c}_i(t) = \Re\{[\sqrt{p}h_i(t)s(t)]e^{j2\pi f_c t}\}, \tag{2}$$

where $c_i(t) = \sqrt{p}h_i(t)s(t)$ is the baseband representation of $\tilde{c}_i(t)$.

Let $b_i(t)$ be the signal of A_i to be transmitted. By denoting α as the reflection coefficient at BDs, the signal backscattered from A_i is $\alpha\tilde{c}_i(t)b_i(t)$. This modulation technique exempts BDs from generating RF signals locally and thus significantly reduces their power consumption [3].

The received superposed signal at A_j can be expressed as,

$$\tilde{y}_j(t) = \alpha h_{i,j}(t)\tilde{c}_i(t)b_i(t) + h_j(t)\tilde{s}(t) + \tilde{n}_j(t), \tag{3}$$

where $\tilde{n}_j(t)$ is the received passband additive white Gaussian noise (AWGN) at A_j. The baseband representation of (3) is

$$y_j(t) = y_j^b(t) + y_j^d(t) + n_j(t), \tag{4}$$

where $y_j^b(t) = \alpha h_{i,j}(t)c_i(t)b_i(t)$ is the backscatter signal reflected from A_i, $y_j^d(t) = \sqrt{p}h_j(t)s(t)$ is the original ambient signal directly from the RF source, and $n_j(t)$ is the baseband representation of $\tilde{n}_j(t)$ with power σ_j^2, i.e., $n_j(t)\sim\mathcal{CN}(0,\sigma_j^2)$.

Let $h_i[n]$, $h_j[n]$ and $h_{i,j}[n]$ denote the discrete-time representation of $h_i(t)$, $h_j(t)$ and $h_{i,j}(t)$, respectively. For convenience, we write the discrete-time representation of the received signal at A_j as

$$y_j[n] = y_j^b[n] + y_j^d[n] + w_j[n], \tag{5}$$

where $y_j^b[n] = \alpha h_{i,j}[n]c_i[n]b_i[n]$, $y_j^d[n] = \sqrt{p}h_j[n]s[n]$ and $w_j[n]\sim\mathcal{CN}(0,\sigma_j^2)$.

IV. The Proposed Key Generation Scheme

In this section, we first provide an overview of the Tradi-Channel and explain why it is not applicable in the AmBC systems. Then, we describe the design of the Tri-Channel and show the challenge to extract a secret randomness from the received RF signals between two paired BDs. Furthermore, we provide the process and technique brief of the key generation procedures (i.e., quantization, information reconciliation and privacy amplification).

A. Traditional Secrecy Extraction

In the traditional point-to-point key generation scheme, i.e., Tradi-Channel, there are two devices, A_1 and A_2, which wish to agree on a secret key through a wireless channel. Three main steps are needed to generate a shared key: (1) shared randomness extraction, (2) information reconciliation, (3) privacy amplification [12].

To extract the shared randomness, A_1 and A_2 successively transmit a probing signal x to the other. The received signal at A_1 sent from A_2 at time t is

$$y_1(t) = h_{2,1}(t)x(t) + n_1(t). \tag{6}$$

Similarly, the received signal at A_2 sent from A_1 at time t' is

$$y_2(t') = h_{1,2}(t')x(t') + n_2(t'), \tag{7}$$

where $h_{2,1}(t)$ and $h_{1,2}(t')$ are the inward channels between A_1 and A_2, respectively, $n_1(t)$ and $n_2(t')$ are additive white Gaussian noise (AWGN). After all the above procedures, we assume there is no noise to explain the Tradi-Channel more clearly. Then A_1 and A_2 can conduct a channel estimation to obtain the inward channel information.

$$v_1 = h_{2,1}(t), \tag{8a}$$

$$v_2 = h_{1,2}(t'). \tag{8b}$$

If $(t' - t) < T_{ch}$, then due to channel reciprocity, $h_{1,2} \approx h_{2,1}$. Variables $V_1 = \{v_1(1), v_1(2), \ldots, v_1(k)\}$ and $V_2 = \{v_2(1), v_2(2), \ldots, v_2(k)\}$ and k is the length of the key, measured by A_1 and A_2 for a period of time, are highly correlated in statistics, thus can be used as the shared randomness for key generation.

However, the traditional key generation scheme cannot be applied to the AmBC systems for BDs, since BDs cannot

directly estimate the inward channel information between them. They cannot generate determined RF signals as probing pilots, only relying on the ambient RF signals, which are uncontrollable, even unknown to BDs. In the AmBC systems, BDs receive either the downlink signal from the RF source while no backscattering, or the superposed signals, which is the superposition of the downlink signal and the backscattered signal from the other BD.

The downlink signals at two BDs are uncorrelated due to passing through different downlink channels. The received signals at BDs are much uncorrelated because of the superposition of uncorrelated downlink signals and backscattered signals. Thus, the measurement of such superposed received signals cannot be directly used as shared common randomness. Nevertheless, the superposed signal includes the information of three channels, including the downlink channels h_1 and h_2, and the inward channel $h_{1,2}$ (or $h_{2,1}$), which are common and identical for two paired BDs. Therefore, we can exploit the superposed signal to construct the shared randomness for key generation.

B. Tri-Channel Design

This subsection introduces our physical layer key generation scheme between two paired BDs, Tri-Channel. The system consists of one RF source and two paired BDs, A_1 and A_2. Two BDs communicate in a time-division manner and want to generate a shared secret key without involving the the RF source by extracting physical layer features of wireless channels. The scheme proceeds in three time slots can be described as below:

Step 1: In the first time slot t_1, A_1 and A_2 both operate in the listening mode to receive RF signals $s(t)$ directly from the RF source. The signals are received by A_1 and A_2, respectively, as

$$c_1(t_1) = y_1^d(t_1) = h_1 s(t_1) + n_1(t_1), \tag{9a}$$

$$c_2(t_1) = y_2^d(t_1) = h_2 s(t_1) + n_2(t_1). \tag{9b}$$

Step 2: In the second time slot t_2, the RF source continuously transmits the RF signals and A_2 operates in the backscattering mode to reflect the signals to A_1. The received superposed signal, including the backscattered signal y_1^b from A_2 and the downlink signal y_1^d directly sent from the RF source, at A_1 in the listening mode is given by

$$\begin{aligned} y_1(t_2) &= y_1^d(t_2) + y_1^b(t_2) + n_1(t_2) \\ &= h_1(t_2)s(t_2) + \alpha_2 h_{2,1}(t_2)h_2(t_2)s(t_2) + n_1(t_2), \end{aligned} \tag{10}$$

where α_2 is the backscatter coefficient of A_2.

Step 3: Similarly, in the third time slot t_3, A_2 operates in the listening mode when A_1 is backscattering. The superposed signals received at A_2 is

$$\begin{aligned} y_2(t_3) &= y_2^d(t_3) + y_2^b(t_3) + n_2(t_3) \\ &= h_2(t_3)s(t_3) + \alpha_1 h_{1,2}(t_3)h_1(t_3)s(t_3) + n_2(t_3), \end{aligned} \tag{11}$$

where α_1 is the backscatter coefficient of A_1. After all procedures above, if we assume there is no noise in all BDs for simplicity and the signal $s(t)$ are known by all system parties, A_1 and A_2 can estimate the respective channels in each step as

$$C_1 = h_1, C_2 = h_2, \tag{12a}$$

$$Y_1 = \alpha_2 h_{2,1} h_2 + h_1, \tag{12b}$$

$$Y_2 = \alpha_1 h_{1,2} h_1 + h_2. \tag{12c}$$

With the estimated channels, A_1 and A_2 can construct an end-to-end channel information between them by computing the following equations:

$$v_1 = (Y_1 - C_1)C_1 = \alpha_2 h_{2,1} h_2 h_1, \tag{13a}$$

$$v_2 = (Y_2 - C_2)C_2 = \alpha_1 h_{1,2} h_1 h_2. \tag{13b}$$

The constructed channel information between A_1 and A_2 are theoretically equal to each other as $v_1 = v_2$, if $h_{2,1} = h_{1,2}$ holds and all channels, h_1, h_2, $h_{1,2}$, $h_{2,1}$ keep unchanged. In practice, if the whole procedure is completed in a time duration less than channel coherence time, the channel reciprocity holds (i.e., $h_{2,1} = h_{1,2}$) and all channels remain unchanged. It should be noted that the backscatter coefficients of A_1 and A_2 are required to remain unchanged during key generation, which does not introduce additional unknowns to the system and thus guarantees that v_1 and v_2 can serve as the shared randomness of A_1 and A_2. If the backscatter coefficients are time varied, then $v_1 = v_2$ no longer holds. In this case, each BD needs to know their own time-varied backscatter coefficient and multiply it to their triangle channel measurements. Then the measurement of A_1 and A_2 turn to $v_1' = \alpha_1(t) \cdot \alpha_2(t) h_{2,1}(t) h_2(t) h_1(t)$ and $v_2' = \alpha_2(t') \cdot \alpha_1(t') h_{1,2}(t') h_2(t') h_1(t')$, where $\alpha_1(t) = \alpha_1(t')$ and $\alpha_2(t) = \alpha_2(t')$. By multiplying the time-varied backscatter coefficient, the measurements can obtain more randomness and make the generated key more robust under various attacks than multiplying a static backscatter coefficient. Thus, using the time-varied backscatter coefficient is applicable to the static environment (as discussed in Section VII)

However, how to design an appropriate time-variant function of $\alpha_1(t)$ and $\alpha_2(t)$ is still an open question since it should take a trade-off between the rate of secret key generation and harvested energy [21], [41]. Therefore, we only consider the case of fixed backscatter coefficients of BDs.

With the system model in Fig. 1, where there are two BDs A_1 and A_2 located at two vertices of a triangle, the channel information constructed by A_1 and A_2 is the product of three sides of this triangle and the backscatter coefficients α_1 and α_2. Although different BDs have different backscatter coefficients, the correlation of the shared randomness equals 1 consistently (as proved in *Appendix A*). For simplicity, we set the backscatter coefficients of the two BDs as α in the following. We define the constructed channel information as the triangle channel information. Since the three channels of the triangle formed by A_1 and A_2 and the RF source and the backscatter coefficient of the triangle are shared between two BDs, the two triangle channel information obtained by A_1 and A_2 are highly correlated in practice. Thus, two BDs can exploit this triangle channel information as shared randomness and obtain a sequence of the triangle channel information ($V_1 = \{v_1(1), ..., v_1(k)\}$ at A_1 and $V_2 = \{v_2(1), ..., v_2(k)\}$ at A_2) with a sequence of measurements and k is the length of the key, respectively in order to generate a shared secret key. After channel measurements and randomness extraction, BDs can conduct quantization, information reconciliation and privacy amplification to generate the shared key.

C. Quantization

Quantization is a method to extract analog measurements into binary bits in the key generation. Two parameters affect the quantizer, quantization level and threshold, respectively. The quantization level is the number of key bits quantified from each measurement. A high quantization level increases the key generation rate while deteriorating the bit disagreement ratio (BDR) between keys [42]. The threshold is the reference level that divides the measurements into different groups. A distribution-based threshold method is based on the estimated value of statistics (mean value or standard

deviation) of the channel estimation [43], [44]. In Section VI we use a distribution-based threshold method in quantization and discuss the impact of different quantization levels on the performance of key generation.

D. Information Reconciliation

Although pre-processing can improve the correlation between channel measurements, the measurements between legitimate BDs may still have key disagreements after quantization. Many information reconciliation techniques can be implemented for mismatch correction, such as low-density parity-check (LDPC) [45], [46] and Golay code [47], etc. We use Cascade for information reconciliation since it leaks less information [46] and with lower complexity than LDPC [48].

E. Privacy Amplification

Privacy amplification reduces the amount of information that an attacker can obtain about the derived key [13], [49]. It is then employed to remove the exposed information from the shared key sequence between BDs. It can be implemented by using universal hash functions, chosen at random from a publicly known set of hash functions, to transform the reconciled bit stream into a nearly perfect random bitstream.

V. Security Analysis

This section performs security analysis on Tri-Channel under four attacks as described above. We first propose three metrics to measure the security performance of Tri-Channel. Then we analyze the variation trend of each metric when SNR changes or the strength of attack changes under different attacks by comparing Tri-Channel with Tradi-Channel. Furthermore, we analyze the upper bound of mutual information (MI) in the shared key when the underlying AmBC system is under three different active attacks.

A. Evaluation Metrics

Mutual Information (MI): MI is the general measure of dependence between two random variables. Furthermore, in Tri-Channel, it helps verify the feasibility of the constructed triangle channels as shared randomness. A larger MI value indicates a higher key generation rate and reflects the efficiency of key generation.

Leaked information (LI): LI measures the mutual information among A_1's estimated sequence, A_2's estimated sequence and Eve's overheard sequence. It represents the information that could be eavesdropped by Eve.

Secret Key Rate (SKR): SKR represents the mutual information of the message (keys) that cannot be eavesdropped on when there is an eavesdropper. Since MI can only evaluate the key generation performance and LI can only evaluate the robustness against attacks, we need to evaluate key security performance by synthesizing both MI and LI for comprehensive evaluation. The value of SKR is equal to the difference between the MI of the generated key and LI.

The three metrics presented above are used in our security analysis. In particular, MI is the metric that is used to measure the efficiency of key generation, while LI and SKR are the metrics used to measure the security of the generated key.

B. Eavesdropping Attack

1) Tradi-Channel: During eavesdropping, Eve can eavesdrop the probing signal x sent from A_1, A_2. Since the probing signal between A_1 and A_2 is trained and open to the public before key generation, Eve also knows the probing signal x. Therefore, Eve can conduct the channel estimation with probing signal x to obtain the eavesdropping channel.

$$v_e^1 = y_e^2(t)/x(t) = (x(t)h_{2,e}(t))/x(t) = h_{2,e}(t), \tag{14a}$$

$$v_e^2 = y_e^1(t')/x(t') = (x(t')h_{1,e}(t'))/x(t') = h_{1,e}(t'). \tag{14b}$$

where $h_{i,e}$ is the channel between A_i and Eve, $y_e^i(t)$ is the eavesdropped signals of Eve by eavesdropping A_i. Thus, with channel estimation sequences V_1, V_2 at A_1, A_2 and $V_e^1 = \{v_e^1(1), ..., v_e^1(k)\}$, $V_e^2 = \{v_e^2(1), ..., v_e^2(k)\}$ at Eve, the achievable SKR of the Tradi-Channel key generation model is given by

$$SKR = \min\{I(V_1; V_2|V_e^1), I(V_1; V_2|V_e^2)\}, \tag{15}$$

where I stands for the function to calculate MI. If Eve is located at a sufficient distance d ($> \frac{\lambda}{2}$, where λ is the applied wavelength) from A_1 and A_2, we have $h_{2,e}(t) \neq h_{2,1}(t)$ and $h_{1,e}(t') \neq h_{1,2}(t')$. Therefore, V_e^1 is uncorrelated with V_1 and so does V_e^2 and V_2, that is the generated key of Eve is uncorrelated with the generated key of BDs.

Nevertheless, if Eve is very close to A_1, Eve can obatin some information of the inward channels of $h_{2,1}(h_{1,2})$, which can be modeled with a cross-correlation coefficient cor between $h_{2,1}$ and $h_{2,e}$ [50]. The actual effect of the cross-correlation coefficient on information leakage is analyzed in Subsection VI-B2.

2) Tri-Channel: In Tri-Channel, Eve can eavesdrop the backscattered signals from A_1, A_2 and the RF signal from the RF source. Furthermore, we assume that Eve knows the RF signal s and is able to utilize signal s to estimate channels. Since, $t' - t < T_{ch}$, the signals or channels can be considered as unchanged, so we eliminate t in the latter formulas in this subsection. Similar to the procedures of BDs to estimate the channels in (12), the channels estimated by Eve can be expressed as

$$C_e = h_e, \tag{16a}$$

$$Y_{1,e} = \alpha h_{1,e} h_1 + h_e, \tag{16b}$$

$$Y_{2,e} = \alpha h_{2,e} h_2 + h_e. \tag{16c}$$

The observation of C_e represents the estimation of downlink channel h_e when Tri-Channel operates the *Step 1* of the key generation. $Y_{1,e}$ represents the estimation of the superposed cascade channel $h_{1,e}h_1$ and downlink channel h_e when Tri-Channel operates the *Step 2* of the key generation. While $Y_{2,e}$ is the estimation when Tri-Channel operates the *Step 3* of the key generation. If Eve wants to obtain the information of the cascade backscatter channel (i.e., $\alpha h_{1,e}h_1$ or $\alpha h_{2,e}h_2$), it needs to deduct (16a) from (16b) or (16c) (i.e., $\alpha h_{1,e}h_1 + h_e - h_e$). In this case, Eve does not need to know the backscatter coefficient since the downlink signal from the RF source is not backscattered from BDs (or say multiplied by α). The only condition of Eve needs to know the backscatter coefficient is that Eve wants to deduct $\alpha h_{1,e}h_1$ from $\alpha h_{1,e}h_1 + h_e$ to obtain h_e when it only knows $h_{1,e}$ and h_1. However, this circumstance does not occur in Tradi-Channel or Tri-Channel. Furthermore, as shown in *Appendix A*, the backscatter coefficients does not affect the quantization result of the bit sequence since it is a constant value during key generation. Therefore, there is no need for Eve to know the backscatter coefficients of A_1 and A_2. Then, Eve can obtain the information as below:

$$v_e^1 = (Y_{1,e} - C_e)C_e = \alpha h_{2,e} h_2 h_e, \tag{17a}$$

$$v_e^2 = (Y_{1,e} - C_e)(Y_{2,e} - C_e) = \alpha h_{1,e} h_1 \cdot \alpha h_{2,e} h_2. \tag{17b}$$

There are two overhear modes of Eve to eavesdrop shared information. The first mode (i.e., v_e^1) is to just simply construct triangle channel between itself, A_2 and RF source. While in

the second mode (i.e., v_e^2), Eve uses the backscatter signals from A_1 and A_2 to concatenate and form eavesdropped information.

If Eve is located at a sufficient distance ($d > \frac{\lambda}{2}$) from A_1 and A_2, $h_{1,e}$ and $h_{2,e}$ are uncorrelated with $h_{1,2}$, and h_e is uncorrelated with h_1 and h_2. In this case, both the sequences V_e^1 and V_e^2 at Eve are independent with V_1 or V_2. Thus, Eve cannot intercept any information of the shared secret information V_1 or V_2. If Eve is much close to A_1 ($d < \frac{\lambda}{2}$), Eve could intercept some information of the triangle channel, since h_e and h_1 are highly correlated, so as between $h_{2,e}$ and $h_{2,1}$ [50]. Therefore, we can also use the cross-correlation coefficient cor to model the reciprocity (similarity) between h_1 and h_e or $h_{2,1}$ and $h_{2,e}$. The actual effects of the cross-correlation coefficient on information leakage in Tradi-Channel and Tri-Channel are analyzed in Subsection VI-B2.

3) Comparison: In the Tradi-Channel, when Eve is at a sufficient distance from A_1 and A_2, the eavesdropping channels $h_{1,e}$ and $h_{2,e}$ obtained by Eve using channel estimation are uncorrelated with the inward channel $h_{1,2}$ or $h_{2,1}$ between two BDs. However, if Eve is within half-wavelength distance of A_1 or A_2, $h_{2,e}$ is correlated to $h_{2,1}$, thus it could crack the key entirely.

The conditions under which the Tri-Channel and the Tradi-Channel can be completely compromised are identical. When Eve eavesdrops, it can obtain the information of the downlink channels h_1 and h_2. However, it cannot get the information of the inward channel $h_{2,1}(h_{1,2})$ if Eve is half-wavelength away from A_1 or A_2. Thereby, Eve cannot completely crack the key under this condition. Comparing Tri-Channel with Tradi-Channel under EA, the LI of Tri-Channel is lower since the triangle channel brings more randomness (i.e., h_1, h_2), making Eve more difficult to eavesdrop. On the contrary, the MI of Tri-Channel is lower than Tradi-Channel since the BD works in the backscatter mode backscatters its received AWGN to the BD that works in the listening mode. It means that the BD who works in the listening mode receives AWGN from both the environment and another BD. Moreover, this circumstance introduces more noises to the generated keys. Therefore, theoretical analysis is difficult to evaluate which scheme has higher key security. For simplicity, in the consequent theoretical analysis of security, only the difference of LI between the two schemes is discussed.

In Tri-Channel, the cross-correlation coefficient measures the correlation between h_1 and h_e (denoted as cor_{h_1,h_e}), h_2 and h_e (denoted as cor_{h_2,h_e}), $h_{1,2}$ and $h_{1,e}$ (denoted as $cor_{h_{1,2},h_{1,e}}$), $h_{2,1}$ and $h_{2,e}$ (denoted as $cor_{h_{2,1},h_{2,e}}$). When Eve is close to A_1 (away from A_2), we have $cor_{h_{1,2},h_{1,e}} = 0$ and $cor_{h_2,h_e} = 0$, $cor_{h_{2,1},h_{2,e}} > 0$ and $cor_{h_1,h_e} > 0$. In Tradi-Channel, the cross-correlation coefficient is to measure the correlation between $h_{1,e}$ and $h_{1,2}$, $h_{2,e}$ and $h_{2,1}$. When Eve is close to A_1 (away from A_2), $cor_{h_{1,2},h_{1,e}} = 0$ and $cor_{h_{2,1},h_{2,e}} > 0$. We can observe that in Tradi-Channel, the only one main channel (i.e., inward channel $h_{2,1}$) between legitimate BDs has some correlation with the eavesdropping channel $h_{2,e}$. While in Tri-Channel, among three main channels, only two of the main channels (i.e., downlink channel h_1 and inward channel $h_{2,e}$) have some correlation with the eavesdropping channel. This means that the measurements in Tradi-Channel have higher correlation with eavesdropped measurements than in Tri-Channel since there remains one downlink channel h_2, from which Eve cannot obtain any information (i.e., $cor_{h_2,h_e} = 0$) when Eve eavesdrops on Tri-Channel.

Conclusion 1: **From the perspective of LI, Tri-Channel has stronger robustness to resist EA than Tradi-Channel** no matter Eve is located at a sufficient distance ($d > \frac{\lambda}{2}$) or even very close to ($d < \frac{\lambda}{2}$) A_1 and A_2.

4) Multiple Antenna Scenario: We first discuss the eavesdropping attack when Eve has a single antenna. However, without hardware limitations like BDs, the eavesdropping devices of Eve can be equipped with multiple antennas. In this subsection, we discuss two cases, one is Eve has only one multi-antenna device, and another is Eve has more than two devices, i.e., distributed devices (antennas).

Case 1: One Multi-antenna Device

In the previous section, we have two modes of eavesdropping attack $v_e^1 = h_e h_{2,e} h_2$ and $v_e^2 = h_1 h_{1,e} \cdot h_2 h_{2,e}$ (when Eve is very close to A_1), respectively. If Eve has m antennas, the eavesdropped information of i-th antenna can be expressed as $v_{e_i}^1 = h_{a_i} h_{2,a_i} h_2$ and $v_{e_i}^2 = h_1 h_{1,a_i} \cdot h_2 h_{2,a_i}$, where h_{a_i} represents the downlink channel between RF source and the i-th antenna of Eve and h_{1,a_i} represents the inward channel between BD A_1 and the i-th antenna of Eve. In this case, the leaked information of the above two eavesdropping modes can be expressed as $max\{I(v; v_{e_1}^1), I(v; v_{e_2}^1), ..., I(v; v_{e_m}^1)\}$ and $max\{I(v; v_{e_1}^2), I(v; v_{e_2}^2), ..., I(v; v_{e_m}^2)\}$, respectively. Since Eve cannot be too close to A_1, we have $cor_{h_{ai},h_1} = 0$ (the cross-correlation between h_{a_i} and h_1) and $cor_{h_{2,a_i},h_{2,1}} > 0$ (no greater than 0.1 in practice [51]). This means that whatever the number of Eve's antennas is, it has no impact on eavesdropping. However, Eve can select the antenna closest to A_1 among all the antennas for eavesdropping.

Case 2: Distributed Antennas

In this case, we assume that Eve can deploy two antennas a_1 and a_2 that close to A_1 and A_2, respectively. Since in the second attack mode with a single antenna (i.e., $v_e^2 = h_1 h_{1,e} \cdot h_2 h_{2,e}$), we have $cor_{h_{1,2},h_{1,e}} = 0$ since Eve is close to A_1, $h_{1,e}$ introduces additional randomness to the eavesdropping information and corrupting Eve to obtain extra information. Therefore, in the distributed antennas scenario, Eve can multiply the backscattered signal received at a_2 from A_1 (i.e., $h_1 h_{1,a_2}$) with the backscattered signal received at a_1 from A_2 (i.e., $h_2 h_{2,a_1}$). And the observation can be expressed as $v_e^3 = h_1 h_{1,a_2} \cdot h_2 h_{2,a_1}$, where the superscript 3 represents the third attack mode. We can observe that $h_{1,e}$ in v_e^2 is replaced by h_{1,a_2} in v_e^3. Since a_2 is close to A_2, we have $cor_{h_{1,2},h_{2,e}} \approx cor_{h_{1,2},h_{2,a_1}} \approx cor_{h_{1,2},h_{2,a_2}} \geq cor_{h_{1,2},h_{1,e}}$. Therefore, the third attack mode can eavesdrop more information on keys. The influence of two attack modes when Eve equips with one single antenna and multiple distributed antennas is further analyzed in Subsection VI-B2.

C. Channel Control Attack

1) Tradi-Channel: Under CCA, the channel between A_1 and A_2 changes from h to $h+H$. We define H as a controlled channel, and the absolute value $|H|$ is the controlled channel strength (CCS), representing the controlled channel's intensity. To make it easier to understand the impact of the Tradi-Channel under CCA, suppose that there is no noise. In Tradi-Channel, A_1 and A_2 can directly utilize the estimation of the inward channel as secret shared randomness. Similar to the analysis processed above, the estimation of the inward channel of A_1 and A_2 can be expressed as

$$v_1 = y_1(t)/x(t) = (h_{2,1}(t) + H)x(t)/x(t), \tag{18a}$$

$$v_2 = y_2(t')/x(t') = (h_{1,2}(t') + H)x(t')/x(t'), \tag{18b}$$

where, $/$ represents the process after conducting a channel estimation. We use a Least-Square (LS) channel estimation method in our simulations when conducting a channel estimation. Since the Rayleigh channel is modelled by one dimension

vector, the result of applying the LS or Minimum Mean Square Error (MMSE) channel estimation method is the same. Since Mallory causes desired changes in channels, it manipulates the changes of channel $v_e = H$. Compare two formulas (18) and $v_e = H$, the channel estimation v_1 and v_2 consist of H, which is correlated with v_e controlled by Mallory. This implies that in Tradi-Channel when CSS increases, channel estimation v_1 and v_2 is more correlated with v_e and more bits of key sequence can be compromised by Mallory.

2) Tri-Channel: Tri-Channel performs similarly to Tradi-Channel under CCA. The only distinction is there are three communication channels in the Tri-Channel. Therefore, Mallory can attack one or more channels arbitrarily. To make it easier to explain the influence of CCA on the Tri-Channel, suppose that there is no noise and BDs (A_1 and A_2) can estimate the appropriate channels given signal $s(t)$. Since, $t' - t < T_{ch}$, the signals or channels can be considered as unchanged, so we eliminate t in the latter formulas in this subsection. The shared randomness of A_1 and A_2 can be expressed as:

$$v_1 = [(h_{2,1} + H_{2,1})(h_2 + H_2)] \cdot (h_1 + H_1), \tag{19a}$$
$$v_2 = [(h_{1,2} + H_{1,2})(h_1 + H_1)] \cdot (h_2 + H_2), \tag{19b}$$

where H_i or $H_{i,j}$ represents the controlled channel in channel h_i or $h_{i,j}$. If Mallory only wants to attack channel h_1, other controlled channels except for H_1 (like H_2) are zero. As mentioned above, Mallory can choose any number of channels to launch CCA. Consequently, we discuss three cases when Mallory attacks one, two, or three channels, respectively. The influence on the observation of A_1 or A_2 can be expressed similarly regardless of how many channels or which channel Mallory attacks. We take attacking h_1 as an example to illustrate the situation when Mallory attacks one channel, and take attacking h_1 and h_2 as a concrete example to illustrate the situation when Mallory attacks two channels. Since v_1 and v_2 are identical, we take v_1 as an example.

$$v_{One} = (h_{2,1}h_2) \cdot (h_1 + H_1) = h_1h_2h_{2,1} + H_1h_2h_{2,1}, \tag{20a}$$
$$\begin{aligned} v_{Two} = [h_{2,1}(h_2 + H_2)] \cdot (h_1 + H_1) = h_1h_2h_{2,1} \\ + H_1h_2h_{2,1} + H_2h_1h_{2,1} + H_1H_2h_{2,1}, \end{aligned} \tag{20b}$$
$$\begin{aligned} v_{Three} = [(h_{2,1} + H_{2,1})(h_2 + H_2)] \cdot (h_1 + H_1) = h_1h_2h_{2,1} \\ + H_1h_2h_{2,1} + H_2h_1h_{2,1} + H_{2,1}h_1h_2 + H_1H_2h_{2,1} \\ + H_1H_{2,1}h_2 + H_2H_{2,1}h_1 + H_1H_2H_{2,1}. \end{aligned} \tag{20c}$$

When attacking one channel (h_1), Mallory cannot master the information of other channels (h_2 and $h_{2,1}$), and therefore H_1 is uncorrelated with $H_1h_2h_{2,1}$. Similarly, when attacking two channels (h_1 and h_2), Mallory cannot master the information of the other channel ($h_{2,1}$) and H_1H_2 is uncorrelated with $H_1H_2h_{2,1}$. So, we can conclude that when only one channel or two channels are under CCA, the information mastered by Mallory is uncorrelated to the shared randomness between BDs. Whereas when all three channels are under attack, Mallory masters the information of $H_1H_2H_{2,1}$. This means that the information mastered by Mallory is partially correlated to the shared information between legitimate BDs. Based on the above analysis, we can conclude that as CCS increases, since the entire key is uncorrelated to the information mastered by Mallory, the LI is still relatively low unless Mallory attacks all three channels simultaneously.

3) Comparison: In Tri-Channel, Mallory can only achieve the purpose of compromising the information of shared randomness when attacking three channels simultaneously. However, in Tradi-Channel, Mallory only needs to attack one channel to achieve the same objective. Obviously, it is rather tough to control three channels than a single channel.

Conclusion 2: **From the perspective of LI, Tri-Channel has stronger robustness to withstand CCA than Tradi-Channel.**

4) Mutual Information Upper Bound: In this subsection, we reintroduce noise to study the precise impact on the MI of the shared key when CCS increases. We redefine the controlled channel as βH, where H is a vector and β (scalar) denotes a coefficient to adjust CCS. Therefore, the CCS is $|\beta H|$. Consequently, the observation of A_1 and A_2 can be expressed as:

$$v_1 = (h_1 + \beta_1H_1)(h_2 + \beta_2H_2)(h_{2,1} + \beta_{2,1}H_{2,1}) + w_1, \tag{21a}$$
$$v_2 = (h_1 + \beta_1H_1)(h_2 + \beta_2H_2)(h_{1,2} + \beta_{1,2}H_{1,2}) + w_2, \tag{21b}$$
$$\begin{aligned} w_1 = (h_{2,1} + \beta_{2,1}H_{2,1})[(h_1 + \beta_1H_1)n_1/s \\ + (h_2 + \beta_2H_2)n_2/s + n_1n_2/s^2], \end{aligned} \tag{21c}$$
$$\begin{aligned} w_2 = (h_{1,2} + \beta_{1,2}H_{1,2})[(h_1 + \beta_1H_1)n_3/s \\ + (h_2 + \beta_2H_2)n_4/s + n_3n_4/s^2]. \end{aligned} \tag{21d}$$

In (21), w_1 and w_2 represent the polynomials containing noises and they serve as the noises corrupting the channel observation by A_1 or A_2, respectively. n_i represents the AWGN. From the above formulas, we can see that the influence of both two AWGNs (n_1 and n_2) on the shared randomness v_1 amplifies as $\beta_{1,2}$ or $\beta_{2,1}$ increases. Whereas when only β_1 or β_2 increases, only one of the AWGN (n_1 or n_2) on the shared observation v_1 is amplified. Therefore, we focus on the worst case regarding the MI of the shared key, when Mallory imposes CCA on the inward channel $h_{2,1}$ ($h_{1,2}$).

$$\begin{aligned} v_1 = h_1h_2(h_{2,1} + \beta_{2,1}H_{2,1}) + (h_{2,1} + \beta_{2,1}H_{2,1}) \\ \cdot (h_1n_1/s + h_2n_2/s + n_1n_2/s^2), \end{aligned} \tag{22a}$$
$$\begin{aligned} v_2 = h_1h_2(h_{1,2} + \beta_{1,2}H_{1,2}) + (h_{1,2} + \beta_{1,2}H_{1,2}) \\ \cdot (h_1n_3/s + h_2n_4/s + n_3n_4/s^2). \end{aligned} \tag{22b}$$

In (22), the polynomials like $h_1h_2(h_{2,1} + \beta_{2,1}H_{2,1})$ is obtained by multiplying multiple Rayleigh-distributed variables, and therefore v_1 and v_2 do not obey the Gaussian distribution. Shown in [52], [53], the upper bound of $I(v_1, v_2)$ is when v_1 and v_2 are both Gaussian variables. To obtain the expression of mutual information upper bound, some assumptions about the variance of variables are listed below. Since assumptions on v_1 and v_2 are the same, we only describe the assumptions made on v_1.

- We assume $h_{2,1} + \beta_{2,1}H_{2,1} \approx (\beta + 1)h_{2,1}$ and $\beta = h_1h_2h_{2,1}$, where the variance of X is T.
- We can further assume $W_1 = h_{21}(h_1n_1/s + h_2n_2/s)$ and $W_2 = h_{2,1}n_1n_2/s^2$, where the variance of W_1 and W_2 is $4N_1$ and N_2, respectively.
- The observation of A_1 is $v_1 = (\beta+1)X+(\beta+1)W_1+W_2$, while A_2 observes $v_2 = (\beta + 1)X + (\beta + 1)W_3 + W_4$, where X,N_1,N_2,N_3,N_4 are independent between each other.

Then, the upper bound of MI in Tri-Channel under CCA can be obtained [16], [54].

$$I(v_1, v_2) = -log_2(1 - \rho^2) = -log_2(1 - \frac{Cov(v_1, v_2)^2}{Var(v_1)Var(v_2)}), \tag{23a}$$
$$Cov(v_1, v_2) = (\beta + 1)^2P, \tag{23b}$$
$$Var(v_1) = (\beta + 1)^2P + 4(\beta + 1)^2N_1 + N_2, \tag{23c}$$
$$Var(v_2) = (\beta + 1)^2P + 4(\beta + 1)^2N_3 + N_4. \tag{23d}$$

If we let $N_1 = N_2 = N_3 = N_4 = N$ in this setting, we get a natural definition of SNR as $SNR = \frac{T}{N}$, and (23(a)) can be simplified as

$$I(SNR, \beta) = -log_2(1 - \frac{SNR^2(\beta + 1)^4}{[SNR(\beta + 1)^2 + 4(\beta + 1)^2 + 1]^2}). \tag{24}$$

Conclusion 3: From (24), we can tell that the upper bound of MI is affected by both SNR and β, and the change of β represents the variation of CCS in numerical terms. Therefore to discuss the effect of CCS on the upper bound of MI, we can study the partial derivative $\frac{\partial I(SNR,\beta)}{\beta}$ for the above equation. A simple calculation provided in *Appendix B* shows that $\forall SNR > 0$, $\frac{\partial I(SNR,\beta)}{\beta} > 0$ still holds. Consequently, we can conclude that when β increases, that is, **when Mallory augments CCS, the upper bound of MI of the key shared between A_1 and A_2 rises.**

D. Signal Manipulative Attack

1) Tradi-Channel: When Mallory imposes SMA, both A_1 and A_2 receive a manipulated signal $P(t)$ from Mallory. And we define manipulated signal strength (MSS) as the average power of $P(t)$. The channel estimation of A_1 and A_2 is

$$\begin{aligned} v_1 &= y_1(t)/x(t) = (x(t)h_{2,1}(t) + P(t))/x(t) \\ &= h_{2,1}(t) + P(t)/x(t), \end{aligned} \tag{25a}$$

$$\begin{aligned} v_2 &= y_2(t')/x(t') = (x(t')h_{1,2}(t') + P(t'))/x(t') \\ &= h_{1,2}(t') + P(t')/x(t'), \end{aligned} \tag{25b}$$

where $/$ represents the process after we conduct a channel estimation and y_i is the received signal of A_i. Mallory aims at manipulating some bits of the keys instead of jamming the communication between A_1 and A_2. And it is apparent that $v_1 \approx v_2$ still holds when $t' - t < T_{ch}$. Since the probing signal between A_1 and A_2 is trained and open to the public before the key generation, Mallory also knows the probing signal $x(t)$. Furthermore, Mallory controls the manipulated signal $P(t)$, it knows $P(t)/x(t)$. It is worth noting that, the channel estimation v_1 and v_2 are correlated with the $P(t)/x(t)$ controlled by Mallory. This implies that when MSS increases under SMA, more bits of keys are compromised by Mallory in Tradi-Channel.

2) Tri-Channel: In Tri-Channel, as illustrated in Fig.1(c), legitimate devices A_1 and A_2 backscatter the received signal $s(t)$ sent by the RF source and the manipulated signal P sent by Mallory at the same time. To easily understand the influence of MSS on the Tri-Channel Scheme, let us assume there is no noise and BDs (A_1 and A_2) can estimate their corresponding channels with the known signal $s(t)$. Since, $t' - t < T_{ch}$, the signals or channels can be considered as unchanged, so we eliminate t in the latter formulas in this subsection. According to the three steps proposed in Tri-Channel to obtain shared information (Section IV-B), A_1 and A_2 can estimate the respective channels in each step as

$$C_1 = h_1 + P/s, C_2 = h_2 + P/s, \tag{26a}$$

$$Y_1 = \alpha h_{2,1}(h_2 + P/s) + h_1 + P/s, \tag{26b}$$

$$Y_2 = \alpha h_{1,2}(h_1 + P/s) + h_2 + P/s. \tag{26c}$$

With the estimated channels, A_1 and A_2 can construct the shared information between them by computing the following equations:

$$\begin{aligned} v_1 &= (Y_1 - C_1)C_1 = [\alpha h_{2,1}(h_2 + P/s)] \cdot (h_1 + P/s) \\ &= \alpha[h_1h_2h_{2,1} + P/s(h_1h_{2,1} + h_2h_{2,1}) + P^2/s^2h_{2,1}], \end{aligned} \tag{27a}$$

$$\begin{aligned} v_2 &= (Y_2 - C_2)C_2 = [\alpha h_{1,2}(h_2 + P/s)] \cdot (h_1 + P/s) \\ &= \alpha[h_1h_2h_{1,2} + P/s(h_1h_{1,2} + h_2h_{1,2}) + P^2/s^2h_{1,2}]. \end{aligned} \tag{27b}$$

In the adversary model of SMA, Mallory controls the manipulated signal P and can estimate the downlink channel between the RF source and itself to obtain the signal s sent from the RF source. The estimation of the cascade backscatter channel of Mallory by eavesdropping the backscattered signal from A_1 and A_2 can be expressed as:

$$Y_{1,m} = \alpha h_{1,m}h_1 s, \tag{28a}$$

$$Y_{2,m} = \alpha h_{2,m}h_2 s. \tag{28b}$$

Since $h_{1,m} \approx h_{m,1}$ and $h_{2,m} \approx h_{m,2}$, Mallory knows $h_{1,m}$, $h_{2,m}$, P and s in the above equations. Consequently, it can master the information of h_1 and h_2 by conducting channel estimation. Furthermore, Mallory combines the information it masters to get a result as close as possible to the shared information between two BDs according to (28(a)) and (28(b)). The information Mallory masters can be expressed as

$$v_{1,m} = \alpha h_{1,m}(h_2 + P/s)(h_1 + P/s), \tag{29a}$$

$$v_{2,m} = \alpha h_{2,m}(h_1 + P/s)(h_2 + P/s). \tag{29b}$$

As shown in (29), since Mallory is more than half-wavelength away from A_1 or A_2, the attack channels $h_{1,m}$ or $h_{2,m}$ are uncorrelated with $h_{2,1}(h_{1,2})$. Hence, $v_{1,m}$ and $v_{2,m}$ mastered by Mallory are uncorrelated with v_1 or v_2 since all items including h_1, h_2, P are multiplied by $h_{2,1}$ or $h_{1,2}$.

3) Comparison: In the Tradi-Channel, the shared information between two BDs is correlated to the manipulated signal P. This means that Mallory can compromise more bits of keys when MSS increases. Whereas in the Tri-Channel, even though Mallory knows the downlink channels h_1 and h_2, RF signal s and manipulated signal P, it does not know $h_{2,1}(h_{1,2})$. This means that the information mastered by Mallory is uncorrelated with the shared information between two BDs. Consequently, LI is not severe in Tri-Channel but turns out to be opposite in Tradi-Channel with the increase of MSS.

When Mallory is very close ($d < \frac{\lambda}{2}$) to A_1 or A_2, Mallory knows the inward and downlink channel, and can crack the whole key in both Tradi-Channel and Tri-Channel.

Conclusion 4: After comparison, it can be seen that **the robustness of Tri-Channel against SMA is much stronger than that of Tradi-Channel**.

4) Mutual Information Upper Bound: In this subsection, we reintroduce noise to study the actual impact of increased MSS on the MI of the shared key. This subsection redefines the manipulated signal and MSS to describe the relationship between manipulated signal and MSS. The manipulated signal is redefined as γP, where P is a vector and γ (scalar) denotes a coefficient to adjust MSS. Therefore, the MSS can be expressed as $|\gamma P|$. Consequently, the shared randomness of A_1 and A_2 can be reformed as:

$$\begin{aligned} v_1 &= \alpha[h_1h_2h_{2,1} + \gamma P/s(h_1h_{2,1} + h_2h_{2,1}) \\ &\quad + \gamma^2P^2/s^2h_{2,1}] + w_1, \end{aligned} \tag{30a}$$

$$\begin{aligned} v_2 &= \alpha[h_1h_2h_{1,2} + \gamma P/s(h_1h_{1,2} + h_2h_{1,2}) \\ &\quad + \gamma^2P^2/s^2h_{1,2}] + w_2, \end{aligned} \tag{30b}$$

$$\begin{aligned} w_1 &= \gamma P/s(h_{2,1}n_1/s + h_{2,1}n_2/s) + h_{2,1}(h_1n_1/s \\ &\quad + h_2n_2/s + n_1n_2/s^2), \end{aligned} \tag{30c}$$

$$\begin{aligned} w_2 &= \gamma P/s(h_{1,2}n_3/s + h_{1,2}n_4/s) + h_{1,2}(h_1n_3/s \\ &\quad + h_2n_4/s + n_3n_4/s^2). \end{aligned} \tag{30d}$$

The process of making assumptions about the variance of variables in v_1 and v_2 is the same, so we only describe the assumptions made on v_1.

- We assume $X_1 = h_1h_2h_{2,1}$, $X_2 = P/s(h_1h_{2,1} + h_2h_{2,1})$, $X_3 = P^2/s^2h_{2,1}$, where the variance of X_1,X_2 and X_3 is T_1, $4T_2$ and T_3 respectively.
- We assume $W_1 = P/s(h_{2,1}n_1/s + h_{2,1}n_2/s)$ and $W_2 = h_{2,1}(h_1n_1/s + h_2n_2/s + n_1n_2/s^2)$, where the variance of W_1,W_2 is $4N_1$ $9N_2$ respectively.
- The observation in A_1 is $v_1 = X_1 + 4\gamma X_2 + \gamma^2 X_3 + 4\gamma W_1 + 9W_2$, while A_2 observes $v_2 = X_1 + 4\gamma X_2 +$

$\gamma^2 X_3 + 4\gamma W_3 + 9W_4$, where X_1,X_2,X_3,W_1,W_2,W_3,W_4 are independent with each other.

If we let $N_1 = N_2 = N_3 = N_4 = N, T_1 = T_2 = T_3 = T$ in this setting, we get a natural definition of SNR as $SNR = \frac{T}{N}$, the upper bound of MI in our key generation scheme under SMA can be expressed as:

$$I(SNR, \gamma) = -log_2(1 - \frac{SNR^2(\gamma^4 + 4\gamma^2 + 1)^2}{[SNR \cdot (\gamma^4 + 4\gamma^2 + 1) + 4\gamma^2 + 9]^2}). \tag{31}$$

Conclusion 5: From (31), we can tell the upper bound of the MI is affected by both SNR and γ, and the change of γ represents the variation of MSS in numerical terms. Therefore to discuss the effect of MSS on the upper bound of MI, we can study the partial derivative $\frac{\partial I(SNR,\gamma)}{\gamma}$ for the above equation. A simple calculation provided in *Appendix C* shows that $\forall SNR > 0$, $\frac{\partial I(SNR,\gamma)}{\gamma} > 0$ still holds. Consequently, we can conclude that when γ increases, that is, **when Mallory augments MSS during SMA, the upper bound of the MI of the key between A_1 and A_2 rises.**

E. Untrusted RF Source Attack

The URSA is proposed based on the non-authentication characteristic of Tri-Channel, and therefore this attack is not suitable for Tradi-Channel. Therefore, we only analyze the influence of URSA on the Tri-Channel scheme herein. In addition, since URSA is a specific SMA, we compare the performance of Tri-Channel under these two attacks.

1) Comparison: Under URSA, there are no other signal sources, so we can obtain the observation between A_1 and A_2 by replacing the signal s in Subsection IV-B with the signal m controlled by Mallory and changing the h_1 and h_2 channels to $h_{m,1}$ and $h_{m,2}$ channels. Furthermore, to easily understand the influence of URSA on Tri-Channel, we first assume there is no noise. Similar to SMA, $h_{m,1} \approx h_{m,2}$ also holds in URSA, since this can help Mallory obtain most key information. In this case, we have $P = mh_{m,1} = mh_{m,2}$. Therefore, the observation between A_1 and A_2 can be expressed as

$$v_1 = \alpha h_{2,1} h_{m,1} h_{m,2} m^2 = \alpha h_{2,1} P^2, \tag{32a}$$

$$v_2 = \alpha h_{2,1} h_{m,1} h_{m,2} m^2 = \alpha h_{1,2} P^2. \tag{32b}$$

On the premise that Mallory is more than half-wavelength away from A_1 or A_2, it does not know the information of channel $h_{2,1}(h_{1,2})$. Hence, the information mastered by Mallory is uncorrelated with v_1 or v_2 since all items in (32) related to P are multiplied by $h_{2,1}$ or $h_{1,2}$. Consequently, LI does not become more severe with the increase of MSS.

Conclusion 6: Comparing the observations of A_1 and A_2 under SMA and URSA, (27) and (32) show that Mallory controls all other information under URSA except the inward channel $h_{2,1}(h_{1,2})$. While under SMA, in addition to the channel $h_{2,1}(h_{1,2})$, the RF signal s is also unknown to Mallory. Since more information is mastered by Mallory under URSA, **launching URSA can compromise more key information than launching SMA**.

2) Mutual Information Upper Bound: In this subsection, we reintroduce noise to study the precise impact of increased MSS on the MI of the shared key. The definitions of P, γ in Subsection V-D4 still hold herein since URSA is a particular SMA. Consequently, the observation of A_1 and A_2 can be expressed as:

$$v_1 = \alpha h_{2,1} P^2 + w_1, \tag{33a}$$

$$v_2 = \alpha h_{1,2} P^2 + w_2, \tag{33b}$$

$$w_1 = h_{2,1}(Pn_1 + Pn_2) + h_{2,1} n_1 n_2, \tag{33c}$$

$$w_2 = h_{1,2}(Pn_1 + Pn_2) + h_{1,2} n_1 n_2. \tag{33d}$$

TABLE I: Default simulation parameters

Channel and key generation parameters:	
Wireless Channel	Rayleigh fading channel
Path-loss exponent	$\lambda = 6$
Distance between A_i and the RF source A_0	$d_{0,1} = 8$ $d_{0,2} = 7$
Distance between A_1 and A_2	$d_{1,2} = 3$
Muti-path spread	$\tau_{0,1} = 8$,$\tau_{0,2} = 7$,$\tau_{1,2} = 3$
Backscatter coefficient	$\alpha = 0.5$
Signal to noise ratio	1dB
Bits of key	50000
Quantization Level	1 bit
Attack parameters:	
Distance between Eve and A_i	$d_{e,1} = 1$,$d_{e,2} = 3$
Distance between Mallory and A_i	$d_{m,1} = d_{m,2} = 2$
Controlled channel strength ratio	$[0, 1]$
Manipulated signal strength	$[0, 10]$

The process of making assumptions about the variance of variables in v_1 and v_2 is the same, so we only describe the assumptions made on v_1.

- We assume $X = h_{2,1}P^2$ and the variance of X is T.
- We assume $W_1 = h_{2,1}(Pn_1 + Pn_2)$ and $W_2 = h_{2,1}n_1n_2$, where the variance of W_1 and W_2 is $4N_1$ and N_2 respectively.
- The observation in A_1 is $v_1 = \gamma^2 X + \gamma W_1 + W_2$, while A_2 observes $v_2 = \gamma^2 X + \gamma W_3 + W_4$, where X,W_1,W_2,W_3,W_4 are independent with each other.

If we let $N_1 = N_2 = N_3 = N_4 = N$ in this setting, then we get a natural definition of SNR as $SNR = \frac{T}{N}$, the upper bound of MI in Tri-Channel under URSA can be expressed as:

$$I(SNR, \gamma) = -log_2(1 - \frac{SNR^2\gamma^8}{[SNR\gamma^4 + 4\gamma^2 + 1]^2}). \tag{34}$$

Conclusion 7: To discuss the effect of MSS on the upper bound of MI, we can study the partial derivative $\frac{\partial I(SNR,\gamma)}{\gamma}$ for the above equation. A simple calculation provided in *Appendix D* shows that $\forall SNR > 0$, $\frac{\partial I(SNR,\gamma)}{\gamma} > 0$ still holds. Consequently, we can conclude that when γ increases, that is, **when Mallory augments MSS during URSA, the upper bound of the MI of the key between A_1 and A_2 rises.**

VI. Performance Evaluation

In this section, we carry out Monte Carlo simulations to show the performance of key generation with different settings and to verify the conclusions drawn in Section V when Tradi-Channel and Tri-Channel are under EA, CCA, SMA, and URSA, respectively. Moreover, we analyze the variation of SKR by analyzing the changing trend of MI and LI through simulations under four types of attacks as mentioned above.

A. Experimental Settings and Assumptions

1) Configuration: We model each channel tap as an independent complex Gaussian random variable (Rayleigh fading) with its average power that follows an exponentially decaying power delay profile, refer to the system model specified in Section III. Some basic simulation parameters are listed in TABLE I. It is worth noting that SNR = 1dB, which is meant to prove that the conclusions drawn before still hold even SNR is low. Different from the work in [19], we set a limitation of the max value of H_i. Since BDs are often used in storage systems and indoor medical diagnoses, the value range of the path-loss exponent in the building can be obtained according to a empirical formula, which is $\lambda = [4, 6]$ [55]. For simplicity, we assume the path loss exponent $\lambda = 6$ and Mallory just can move away intermediate objects to further increase the path loss exponent. Since we set the multi-path spread in each channel as $\tau_{01} = 8$, $\tau_{02} = 7$ and $\tau_{12} = 3$, which implies the maximum multi-path spread is $L = 10$ [21]. Since the channel

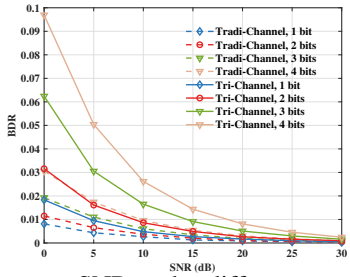


Fig. 2: BDR versus SNR under different quantization levels.

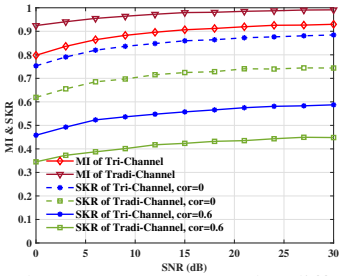


Fig. 3: SKR and MI versus SNR under different correlation coefficient.

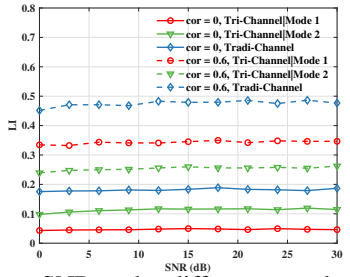


Fig. 4: LI versus SNR under different correlation coefficient.

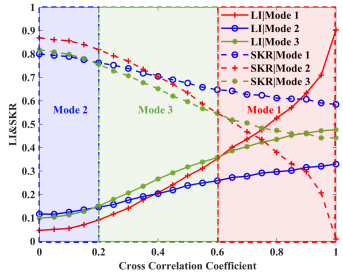


Fig. 5: LI and SKR of three kinds of attack modes in Tri-Channel versus different cross correlation coefficient.

is modelled by $h = \vartheta d^{-\frac{\lambda}{2}}$ and the minimum value of path loss exponent is 4 [55], the ratio of the maximum channel gain to the minimum channel gain is $\frac{\vartheta d^{-\frac{4}{2}}}{\vartheta d^{-\frac{6}{2}}} = d$. And therefore, we have $H_{max}/h_i = d_i$, where d_i is the distance between the considered transmitter and receiver that communicate via channel h_i. Since the communication distance of each channel is different, the maximum CCS is different when Mallory controls different channels, we define $\frac{H}{H_{max}}$ as the CCS ratio (ranges from 0 to 1) with unification.

Section IV mentions that A_1 and A_2 obtain k rounds of the triangle channel information. Next, the estimated sequences are mapped to binary bits with a level crossing algorithm as described in [12]. Once we have the secret bits, we can use MI, LI, and SKR as metrics to measure the security performance of key generation.

2) Channel Estimation and Joint Transceiver Design: When analyzing the security and efficiency of Tri-Channel, we assume that BDs can use a channel estimation method to estimate the downlink and cascade backscatter channels with the known RF signal s. However, due to the restriction of the circuit configuration inside the BD and its resource-limited characteristics, the current BDs cannot use the channel estimation method to generate a secret shared key since this method needs to send a probing signal and apply high computation consumption channel estimation algorithms. Therefore, our previous work proposed a method that enables BD to generate shared keys without sending probing signals or using computation exhausted channel estimation algorithms. In our previous work, we proposed a cyclic prefix (CP) in orthogonal frequency division multiplexing (OFDM) transmission scheme based BD joint transceiver design method, named JointTrans [21].

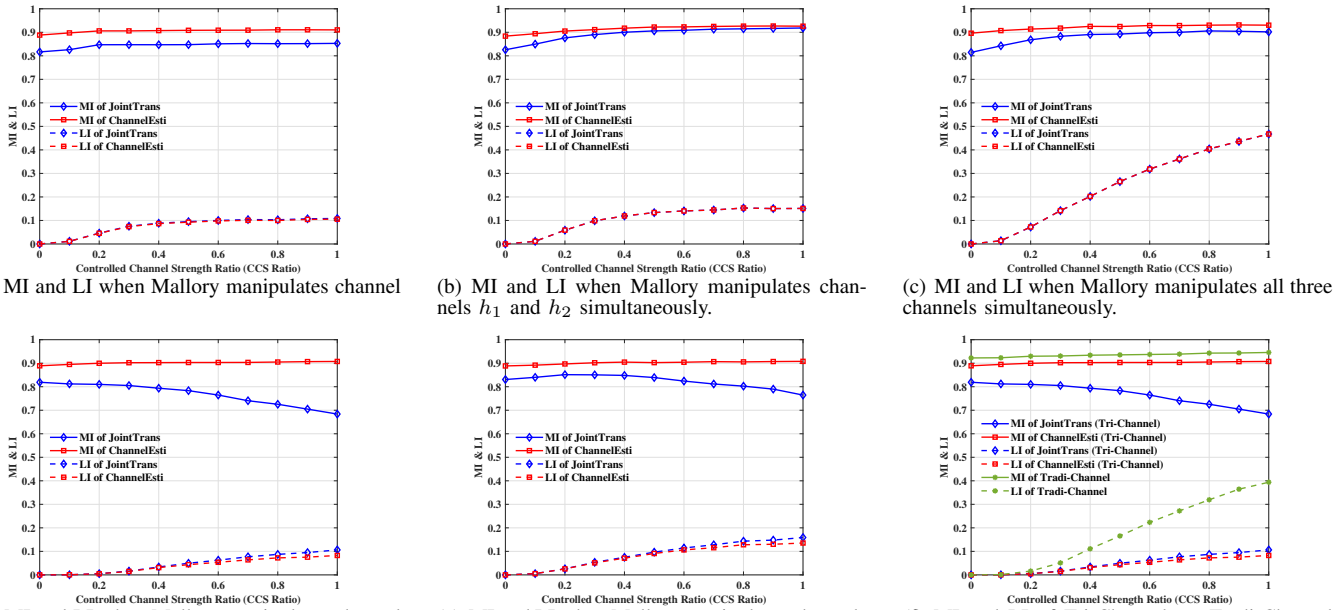
Compared with the channel estimation method used in Tri-Channel, named ChannelEsti, JointTrans is certainly weaker in key generation performance. However, JointTrans is a lightweight method that does not require many computational resources and therefore it is very suitable for resource-constrained BDs. Next, we compare the performance of both ChannelEsti and JointTrans in key generation efficiency and security through numerical simulations.

B. Simulation Results

1) Performance of KGR and BDR: In this subsection, we discuss the performance of key generation rate (KGR) and bit disagreement ratio (BDR) of key generation with a quasi-static indoor channel.

Table II presents the KGR of Tri-Channel and Tradi-Channel with different parameters, including the symbol duration K, the length of the OFDM frame and the cyclic prefix (CP) part of N, and the maximum multi-path spread L. The KGR of both schemes increases with the growth of SNR under all parameter settings. When increasing N or K , the length of CP part ($N_{cp} = \frac{1}{4}N$) can be extended and the KGR of both schemes are increased. These indicate that KGR improves as the length of the repeated CP part increases, i.e., extending OFDM symbol N or symbol duration K. Furthermore, when we decrease the maximum spread by reducing the multi-path channel spread of each channel (by setting $\tau_{01} = 4$, $\tau_{02} = 3$, $\tau_{12} = 2$ which implies $L = 5$ in Tri-Channel and $L = 1$ in Tradi-Channel), KGR can be improved in the cases with the long length of the CP part. This is because more samples of the CP part can be exploited for obtaining the triangle channel information, which reduces the influence of noise and varied power of CP samples. For example, when $L = 10$, only 6 samples of the CP part ($N_{cp} = 16$) are available as common triangle information since inter-symbol interference (ISI) deteriorates the information in the first ten symbol bits. While when $L = 5$, 11 samples are available, more than the available samples when $L = 10$.

Fig. 2 presents the BDR of Tri-Channel and Tradi-Channel versus SNR under different bit quantization levels in the phase of quantization. We can observe that BDR decreases with the increase of SNR in all settings. Increasing the quantization level increases the number of bits per sample quantified by the quantizer in the quantization phase, thus increasing the rate of key generation. However, a high quantization level also increases BDR since additional information in the key measurements is considered. Therefore, the influence of noise grows. Then, we can observe that BDR decreases as the quantization level increases in both Tri-Channel and Tradi-Channel. However, the BDR of Tradi-Channel is lower than Tri-Channel's under the same quantization level. Although the



(a) MI and LI when Mallory manipulates channel h_1.

(b) MI and LI when Mallory manipulates channels h_1 and h_2 simultaneously.

(c) MI and LI when Mallory manipulates all three channels simultaneously.

(d) MI and LI when Mallory manipulates channel $h_{2,1}$.

(e) MI and LI when Mallory manipulates channels h_1 and $h_{2,1}$ simultaneously.

(f) MI and LI of Tri-Channel vs. Tradi-Channel when Mallory manipulates channels $h_{2,1}$.

Fig. 6: MI and LI when Mallory manipulates one, two, or three channels

TABLE II: KGR of Tri-Channel and Tradi-Channel under various experiment settings.

BPCU \ SNR / Scheme	0dB	10dB	20dB	30dB	Setting
Tri-Channel	0.98876	0.99726	0.99920	0.99962	K=3; N=256; L=10
	0.98448	0.99528	0.99862	0.99956	K=1; N=256; L=10
	0.95234	0.98690	0.99566	0.99868	K=1; N=64; L=10
	0.98190	0.99521	0.99857	0.99951	K=1; N=64; L=5
Tradi-Channel	0.99498	0.99838	0.99950	0.99992	K=3; N=256; L=2
	0.99114	0.99714	0.99894	0.99976	K=1; N=256; L=2
	0.98314	0.99490	0.99870	0.99954	K=1; N=64; L=2
	0.99090	0.99704	0.99887	0.99973	K=1; N=64; L=1

K: symbol duration; N: number of FFT and CP; L: maximum multi-path spread

key quality of Tri-Channel is worse than Tradi-Channel, its secrecy is better.

2) Performance under EA: Eve is a passive attacker, and therefore, its communication environment and eavesdropping location determine eavesdropped information. The change of the eavesdropping position causes a change in the correlation coefficient between Eve's attack channel and the inward channel. Therefore, we discuss the influence on MI and SKR when SNR and the correlation coefficient between the attack channel and the inward channel change simultaneously.

We use different cross-correlation coefficients to illustrate the actual impact of the cross-correlation coefficient to LI and SKR of Tradi-Channel and Tri-Channel. For simplicity, we set $cor_{h_1,h_e} = cor_{h_{2,1},h_{2,e}} = cor$ in our simulation. Fig.3 shows that both MI and SKR increase as SNR rises due to the disturbance of noises to the generated key is alleviated. Furthermore, the MI of the key in Tradi-Channel outperforms Tri-Channel in every condition. In Tri-Channel, the BD works in the backscatter mode backscatters its received AWGN to the BD that works in the listening mode. This means that the BD works in the listening mode not only receives AWGN from its environment but also receives AWGN from another BD. This means more noises are included in Tri-Channel than Tradi-Channel. When we observe the SKR of the two schemes, it is evident that the SKR of Tri-Channel is always higher than that of Tradi-Channel. From Fig. 3 and 4, we can see that even though the MI in Tradi-Channel is higher, its LI is more severe than that of Tri-Channel, which makes its SKR is lower than that of Tri-Channel. Therefore, we can infer that the higher MI of Tradi-Channel cannot sufficiently compensate LI, which causes poor security performance (SKR).

It is worth noting that the SKR of Tri-Channel is taken in the mode with the most leaked information in the two eavesdropping modes (i.e., Mode 1 is $v_e^1 = h_e h_{2,e} h_2$ and the Mode 2 is $v_e^2 = h_{1,e} h_1 h_{2,e} h_2$) in Mode 2 in the previous Subsection V-B With $cor = 0$, the eavesdropping capability of Eve with Mode 2 is superior to that of Mode 1, as shown in Fig. 4, making LI under Mode 2 more than Mode 1. This is because eavesdropping channels $h_{1,e}$ and $h_{2,e}$ with short distance bring less randomness compared with $h_{2,e}$ and h_e, which makes $h_{1,e} h_1 h_{2,e} h_2$ selected by Eve more correlated with the triangle channel $h_1 h_{2,1} h_2$ than $h_e h_{2,e} h_2$. When $cor = 0.6$, $h_{2,e}$ and h_e become more correlated with $h_{2,1}$ and h_1, respectively, Eve with eavesdropping Mode 1 has a better eavesdropping capability than Mode 2. This is because it still has an independent channel $h_{1,e}$ in $h_{1,e} h_1 h_{2,e} h_2$ to introduce additional randomness. However, no matter Eve adopts which eavesdropping mode in Tri-Channel, the LI of Tri-Channel is always lower than that of Tradi-Channel in every conditions. Thus, these simulation results in Fig. 4 verify ***Conclusion 1***.

Fig. 5 shows the LI of three different attack methods versus cross correlation coefficients. We can observe that when the correlation is small (between 0 and 0.2), Mode 2 obtains more LI than Mode 3 since the multi-path spread in h_{1,a_2} is more severe than $h_{1,e}$($d_{A_1,a_1} = 1m$ and $d_{A_1,a_2} = 3m$). Note that this correlation range is commonly taken in reality [51]. This figure also gives the LI and SKR that Eve can achieve if the correlation coefficient is very high by some means. However, when the correlation rises (between 0.2 and 0.6), the LI of Mode 3 is the highest among three modes. When the correlation is very high (between 0.6 and 1), Mode 1 can obtain the highest LI since it is more like the triangle channel constructed by BDs as it does not multiply the inward channel one more time like Mode 3.

3) Performance under CCA: Since there are three communication channels used in the Tri-Channel, Mallory can

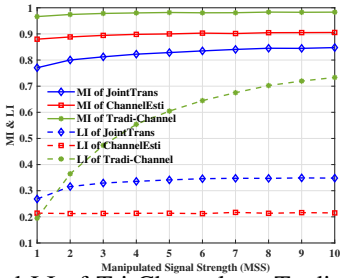


Fig. 7: MI and LI of Tri-Channel vs. Tradi-Channel under SMA.

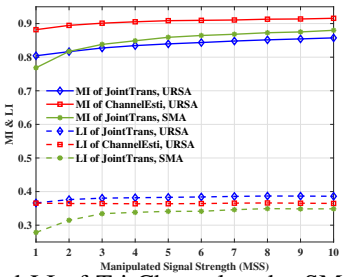


Fig. 8: MI and LI of Tri-Channel under SMA and URSA.

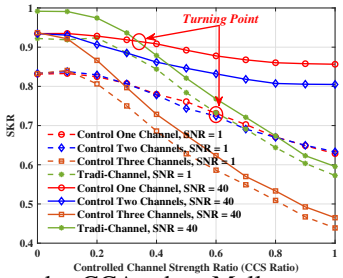


Fig. 9: SKR under CCA when Mallory manipulates one, two or three channels when SNR = 1 and SNR = 40.

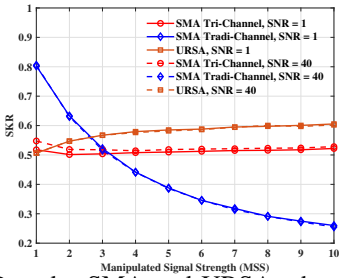


Fig. 10: SKR under SMA and URSA when SNR = 1 and SNR = 40.

arbitrarily attack one, two or all three channels. This subsection discusses the MI and LI of Tri-Channel when attacking a single channel, two channels, and all channels, respectively. Moreover, we compare Tri-Channel with Tradi-Channel and analyze the corresponding performance of key generation and security.

Since both h_1 and h_2 are downlink channels, the effect when Mallory controls h_1 or h_2 is similar. Consequently, when analyzing the effect of Mallory that controls a single channel, we only need to discuss the situation when it controls downlink channel h_1 or inward channel $h_{2,1}(h_{1,2})$. As shown in Fig. 6(a) and (d), it is quite different when Mallory controls the downlink channel and controls the inward channel. In both cases, the LI eventually becomes stable with a bit rise, while ChannelEsti's MI has an imperceptible climb as the the CCS ratio grows. The MI of JointTrans rises when Mallory manipulates the downlink channel h_1, but decreases when Mallory manipulates the inward channel $h_{2,1}$. In JointTrans, using cyclic preflix to generate shared information unintentionally amplifies the disturbance of noise on the key. To avoid the situation that MI drops in JointTrans, we can increase the length of cyclic preflix or augment the SNR to reduce noise (as analyzed in our previous work and proved with simulations results in Fig. 4(a) [21]). Moreover, it is shown that when SNR increases, the MI of JointTrans gets closer to the MI of ChannelEsti and bith become stable instead of dropping (shown in *Appendix E*).

As shown in Fig. 6(b), when Mallory controls two downlink channels h_1 and h_2 simultaneously, as an overall trend with the increase of CCS ratio, both ChannelEsti and JointTrans's MI rise as CCS ratio grows. It is worth noting that, as the CCS ratios grow, the MI of JointTrans is getting closer to the MI of ChannelEsti. From the perspective of LI, the trend of LI is the same as when only one channel is controlled. Nevertheless, when controlling two channels, the LI stabilizes at 0.15, slightly higher than controlling a single channel (0.1). In general, instead of enlarging the LI, the CCS ratio increment enhances MI, which is beneficial for key generation security and efficiency.

Similarly to controlling a single channel, it is nearly the same when Mallory controls $h_1, h_{2,1}$ or $h_2, h_{2,1}$. Therefore, we only discuss the former case. Fig. 6(e) shows a completely different change of the MI of JointTrans compared to Fig. 6(b). When the CCS ratio ranges from 0 to 0.3, there is a slight increase of the MI of JointTrans. When the CCS ratio ranges from 0.3 to 1, the upward trend turns into a downward trend. It can be seen from Fig. 6(a) that when h_1 is controlled, MI of JointTrans stops rising when the CCS ratio increases to 0.3. However, in Fig. 6(d) when $h_{2,1}$ is controlled, the MI of JointTrans continues to decrease with the rise of the CCS ratio. And this leads to MI rising first and then falling. The drop of MI of the key can be alleviated, like the situation when only one $h_{2,1}$ channel is controlled, as long as SNR rises.

Fig. 6(c) shows the situation when Mallory attacks three channels simultaneously. With the increase of the CCS ratio, the MI of both ChannelEsti and JointTrans raises. From the perspective of LI, the LI of both ChannelEsti and JointTrans ascend dramatically. This is because when Mallory controls three channels simultaneously, the information it manipulated is partially correlated to the shared information between legitimate BDs. Comparing all the cases of CCA, Mallory can only compromise more information when it controls three channels simultaneously. Under the three types of CCA attack scenarios, we see a slight climb of the MI of ChannelEsti with the increase of CCS ratio (although it is not obvious when only one channel is controlled), which verifies ***Conclusion 3***.

Finally we compare Tri-Channel with Tradi-Channel when Mallory controls the inward channel $h_{2,1}(h_{1,2})$. As shown in Fig. 6(f), the MI of Tradi-Channel keeps increasing as the CCS ratio grows. From the perspective of MI, the Tradi-Channel outperforms the Tri-Channel since the Tri-Channel introduces more noises and more fading channels. From the perspective of LI, the robustness of Tri-Channel is stronger than that of Tradi-Channel. In Tradi-Channel, the controlled channel $H_{2,1}$ is correlated to the generated key and therefore, the LI becomes severe as the CCS ratio grows. While in Tri-Channel, when Mallory only controls a single channel, the controlled channel $H_{2,1}$ is uncorrelated with the generated key, and therefore the LI keeps stable as the CCS ratio grows. And these results verify ***Conclusion 2***.

4) Performance under SMA: We further compare Tri-Channel with Tradi-Channel under SMA and uses the met-

rics MI, LI, and SKR to evaluate their performance of key generation rate and key security.

Fig. 7 shows the variation of MI and LI concerning MSS. As shown from the figure, the MI of Tradi-Channel increases with the growth of MSS, the same for MI of both JointTrans and ChannelEsti. The MI of JointTrans is getting closer to ChannelEsti's as MSS increases. This means that the improvement of MSS has a enhancement on the key generation efficiency of JointTrans. Furthermore, Tradi-Channel outperforms Tri-Channel since the latter scheme introduce more noises and more fading channels and therefore decrease the efficiency of the key. From the perspective of LI, the LI of Tradi-Channel keeps elevating as the MSS grows while the LI of Tri-Channel keeps still after a slight rise. In Tradi-Channel, the manipulated signal is correlated with the generated key. In contrast, the manipulated signal is multiplied with the inward channel in the generated key in the Tri-Channel, resulting in the manipulated signal being uncorrelated with the generated key. The above simulation results verifies ***Conclusion 4 and 5***.

5) Performance under URSA: Since URSA is a particular SMA, we compare these two attacks and use MI and LI to measure the influence of URSA and SMA, respectively. As an overall trend in Fig. 8, MI and LI increase as MSS rises. From the simulation results of the MI in the figure, we can see that the MI under URSA is closer to that of SMA. Shown in (33), there is one item of URSA serving the key consistency and three noise items disrupting key consistency. Shown in (30), SMA has three items serving key consistency and five items of noise disrupting key consistency. The difference of MI between URSA and SMA is not mentioned in V-E1 since it is unnoticeable, but in the simulation results, it can be seen that the MI under SMA is slightly larger than that under URSA. From the perspective of LI, the performance of Tri-Channel under SMA outperforms that under URSA. Shown in (31) and (33), the reason is that under SMA, both RF signal s and manipulated signal P participate in the key generation, while only the manipulated signal P participates in key generation under URSA. And this results to a higher SNR when under SMA. Furthermore, Mallory controls all part of ambient signals in the system, which helps Mallory obtain a higher LI when launching URSA. The above simulation results verifies ***Conclusion 6 and 7***.

6) SKR Analysis: In particular, we analyze the trend SKR of Tri-Channel under CCA, SMA, and URSA when attack capability is strengthened. In the following simulations, the SKR of Tri-Channel are all obtained using the JointTrans.

Fig. 9 shows the SKR under CCA when Mallory manipulates different amounts of channels. As an overall trend, SKR drops as the CCS ratio increases in any case. Furthermore, when Mallory manipulates one or two channels, SKR become stable after a period of descent while the SKR of Tradi-Channel and the SKR of Tri-Channel when three channels are manipulated keep decreasing. The *Turning Point* in the figure when controlling only the inward channel represents the point at which the SKR of Tri-Channel is higher than the SKR of Tradi-Channel. When SNR increases (from 1 to 40), the appearance of a *Turning Point* with regard to CCS ratio gradually moves ahead (i.e., becomes smaller) from 0.6 to 0.3. This means that with the increase of SNR, the security performance of the Tri-Channel gradually surpass the Tradi-Channel.

Unlike EA and CCA, as shown in Fig. 10, SKR does not have much difference with different SNR under URSA and SMA. This is because under URSA and SMA, increasing the attack strength is equivalent to increasing the SNR. As the SNR is increased further, the effect is not so obvious. Fig. 10 reflects the significant difference between Tradi-Channel and Tri-Channel under SMA. In Tradi-Channel, the SKR drops significantly, while in Tri-Channel, there is a decreasing trend followed by a slightly increasing trend. Refer to Fig. 7, in Tradi-Channel, the rising rate of LI is greater than that of MI. While in Tri-Channel, the rising rate of MI is gradually greater than the rising rate of LI. Also, Fig. 10 demonstrates the difference of the trend of SKR under URSA and SMA in Tri-Channel. Although the LI of URSA is higher than that of SMA, Tri-Channel under URSA still outperforms SMA in terms of SKR.

VII. Further Discussion

A. Static Environment

Wireless channels are naturally modeled to be dynamic in most of the PHY key generation schemes, including our scheme. These schemes depend on the rapid variation of wireless channel to generate shared randomness. However, these schemes may have ultra-low secret key rates in a static environment, such as in door IoT networks. In [56], a direct link key generation scheme utilizes randomly generated symbols exchange between two devices to address such a problem that an inward channel cannot be used directly as a shared randomness in the static environment. Song et al. [57] designed a transmitter to create an "artificial multi-path effect" by using time-delayed signal copies to mimic multi-path component with different arrival time.

These two methods can be implemented in the Tri-Channel by relying on the RF source to create an "artificial multi-path" effect or to continuously generate a new random signal sequence in each time slot. However, the RF source can master the whole key information in these cases and could impose significant information leakage in the system when suffering from URSA. A novel way to introduce randomness to the system is that BDs can use a time-variant backscatter coefficient (i.e., $\alpha_1(t)$ of A_1 and $\alpha_2(t)$ of A_2) in the backscatter phase. And in the construction phase, each BD needs to multiply the backscatter coefficient with the triangle channel measurement (i.e., $v_1 = \alpha_1(t) \cdot \alpha_2(t) h_1 h_2 h_{2,1}$ of A_1 and $v_2 = \alpha_2(t') \cdot \alpha_1(t') h_1 h_2 h_{1,2}$ of A_2). In this case, the RF source cannot master most of the key information. However, how to design an appropriate time-variant function of $\alpha_1(t)$ and $\alpha_2(t)$ is still an open question since it needs to take a trade-off between the rate of secret key generation and harvested energy [21], [41].

B. Multiple Antenna Scenario

MIMO technique is considered as a promising technology of communications. Although MIMO systems may outperform SISO systems, it is accompanied with high complexity. Some existing works have shown the opportunities for an AmBC system to obtain high communication efficiency and accuracy by implementing multiple antennas into RF sources and BDs [58], [59]. A dyadic backscatter channel was proposed in the AmBC system, which characterizes with multiple backscatter channels enabled by multiple antennas, e.g., M antennas at an RF source, L antennas at a backscatter transmitter, and N antennas at a backscatter receiver. As demonstrated, by using multiple antennas at the backscatter transmitter and the backscatter receiver, the communication range is significantly extended since small-scale fading effects can be reduced by adopting the dyadic backscatter channel [60], [61]. Hence, equipping multiple antennas can improve the performance of Tri-Channel as derived in Table II that the KGR improves when reducing the multi-path spread.

VIII. Conclusions

This paper proposed and analyzed the security of Tri-Channel, a novel scheme of physical secret key generation for two paired BDs over ambient RF signals. BDs can obtain the triangle channel information to generate a shared secret key by multiplying two downlink signals and inward backscatter signals. In particular, we theoretically analyze the security of Tri-Channel by comparing it with a traditional scheme named Tradi-Channel when both are under EA and three types of active attacks (i.e, CCA, SMA, and URSA). Finally, the performance of the above two schemes was evaluated under various signals or environment settings through numerical simulations. The results show that although the key generation performance of the Tri-Channel is slightly lower than the Tradi-Channel, the security performance of Tri-Channel outperforms Tradi-Channel under EA, CCA, and SMA. Interestingly, when Tri-Channel suffers from URSA, a more vital SMA, its SKR is conversely higher than that when it suffers from SMA. Under URSA, even though the attacker enhances its attack by increasing the power of manipulated signals, the SKR rises instead. Noteworthy to mention that, when SNR increases, the SKR of Tri-Channel improves when suffering from all kinds of attacks. Thus, we can conclude that Tri-Channel exhibits advanced security than Tradi-Channel with regard to robustness under analyzed four attacks. Notably, Tri-Channel can play as a foundation for group key generation to support secure multi-BD communications, which has been studied in another line of our work.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Academy of Finland under Grant 345072 and Grant 350464; in part by the Open Project of Zhejiang Lab under Grant 2021PD0AB01; and in part by the 111 Project under Grant B16037; and in part by the U.S. National Science of Foundation through the Networking Technology and Systems (NeTS) Program under Award 2131507.

References

[1] W. Liu, K. Huang, X. Zhou, and S. Durrani, "Next generation backscatter communication: systems, techniques, and applications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–11, 2019.

[2] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Communications surveys & tutorials*, vol. 20, no. 4, pp. 2889–2922, 2018.

[3] G. Yang, Y.-C. Liang, R. Zhang, and Y. Pei, "Modulation in the air: Backscatter communication over ambient OFDM carrier," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1219–1233, 2018.

[4] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 39–50, 2013.

[5] K. Han and K. Huang, "Wirelessly powered backscatter communication networks: Modeling, coverage, and capacity," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2548–2561, 2017.

[6] X. Lu, H. Jiang, D. Niyato, D. I. Kim, and Z. Han, "Wireless-powered device-to-device communications with ambient backscattering: Performance modeling and analysis," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1528–1544, 2018.

[7] S. Gong, L. Gao, J. Xu, Y. Guo, D. T. Hoang, and D. Niyato, "Exploiting backscatter-aided relay communications with hybrid access model in device-to-device networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 4, pp. 835–848, 2019.

[8] A. Juels, "RFID security and privacy: A research survey," *IEEE journal on selected areas in communications*, vol. 24, no. 2, pp. 381–394, 2006.

[9] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522–533, 2007.

[10] E. Vahedi, R. K. Ward, and I. F. Blake, "Security analysis and complexity comparison of some recent lightweight rfid protocols," in *CISIS*. Springer, Conference Proceedings, pp. 92–99.

[11] T. Chou, S. C. Draper, and A. M. Sayeed, "Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1751–1764, 2013.

[12] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[13] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[14] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015.

[15] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 3048–3056.

[16] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[17] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM journal on computing*, vol. 38, no. 1, pp. 97–139, 2008.

[18] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.

[19] R. Jin and K. Zeng, "Manipulative attack against physical layer key agreement and countermeasure," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[20] P. Wang, Z. Yan, and K. Zeng, "Bcauth: Physical layer enhanced authentication and attack tracing for backscatter communications," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2818–2834, 2022.

[21] P. Wang, L. Jiao, K. Zeng, and Z. Yan, "Physical layer key generation between backscatter devices over ambient RF signals," in *IEEE INFOCOM 2021-IEEE International Conference on Computer Communications*, 2021.

[22] M. Chen, S. Chen, and Y. Fang, "Lightweight anonymous authentication protocols for RFID systems," *IEEE/ACM Transactions on Networking*, vol. 25, no. 3, pp. 1475–1488, 2017.

[23] X. Wang, Z. Su, and G. Wang, "Relay selection for secure backscatter wireless communications," *Electronics Letters*, vol. 51, no. 12, pp. 951–952, 2015.

[24] B. Defend, K. Fu, and A. Juels, "Cryptanalysis of two lightweight RFID authentication schemes," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*. IEEE, 2007, pp. 211–216.

[25] H.-J. Chae, M. Salajegheh, D. J. Yeager, J. R. Smith, and K. Fu, *Maximalist cryptography and computation on the WISP UHF RFID tag*. Springer, 2013, pp. 175–187.

[26] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[27] Q. Yang, H.-M. Wang, Y. Zhang, and Z. Han, "Physical layer security in MIMO backscatter wireless systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7547–7560, 2016.

[28] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE transactions on wireless communications*, vol. 13, no. 6, pp. 3442–3451, 2014.

[29] B. Zhao, H. Wang, and P. Liu, "Safeguarding RFID wireless communication against proactive eavesdropping," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 587–11 600, 2020.

[30] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. Part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[31] Z. Li, Q. Pei, I. Markwood, Y. Liu, and H. Zhu, "Secret key establishment via RSS trajectory matching between wearable devices," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 802–817, 2018.

[32] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2820–2835, 2014.

[33] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: Algorithms and rate optimization," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1831–1846, 2016.

[34] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 18–33, 2019.

[35] C. Boyer and S. Roy, "Space time coding for backscatter RFID," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2272–2280, 2013.

[36] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proceedings of the Fourth European Workshop on System Security*, 2011, pp. 1–6.

[37] M. Letafati, A. Kuhestani, D. W. Kwan Ng, and M. R. Ahmadi Beshkani, "Physical layer secrecy and transmission resiliency of device-to-device communications," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1–6.

[38] M. Letafati, A. Kuhestani, H. Behroozi, and D. W. K. Ng, "Jamming-resilient frequency hopping-aided secure communication for internet-of-things in the presence of an untrusted relay," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6771–6785, 2020.

[39] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *European symposium on research in computer security*. Springer, 2012, pp. 235–252.

[40] S. Haykin, *Digital communications*. Wiley New York, 1988.

[41] P. Wang, Z. Yan, N. Wang, and K. Zeng, "Resource allocation optimization for secure multidevice wirelessly powered backscatter communication with artificial noise," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7794–7809, 2022.

[42] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2009.

[43] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 128–139.

[44] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th annual international conference on Mobile computing and networking*, 2009, pp. 321–332.

[45] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[46] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 410–423.

[47] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*, 2011, pp. 211–224.

[48] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[49] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[50] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Communications Letters*, vol. 21, no. 4, pp. 961–964, 2017.

[51] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, pp. 1–9.

[52] T. M. Cover and J. A. Thomas, "Elements of information theory. wiley, new-york," 2006.

[53] L. Batina, B. Gierlichs, E. Prouff, M. Rivain, F. X. Standaert, and N. Veyrat-Charvillon, "Mutual information analysis: a comprehensive study," *Journal of Cryptology*, vol. 24, no. 2, pp. 269–291, 2011.

[54] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 480–490, 2012.

[55] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM wireless communications with MATLAB*. John Wiley & Sons, 2010.

[56] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.

[57] S. Fang, I. Markwood, and Y. Liu, "Wireless-assisted key establishment leveraging channel manipulation," *IEEE Transactions on Mobile Computing*, vol. 20, no. 1, pp. 263–275, 2019.

[58] J. D. Griffin, *High-frequency modulated-backscatter communication using multiple antennas*. Georgia Institute of Technology, 2009.

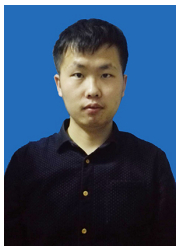
[59] J. D. Griffin and G. D. Durgin, "Gains for rf tags using multiple antennas," *IEEE Transactions on Antennas and Propagation*, vol. 56, no. 2, pp. 563–570, 2008.

[60] M. A. Ingram, M. F. Demirkol, and D. Kim, "Transmit diversity and spatial multiplexing for rf links using modulated backscatter," *Signal*, vol. 10, no. 3, 2001.

[61] J. D. Griffin and G. D. Durgin, "Reduced fading for rfid tags with multiple antennas," in *2007 IEEE Antennas and Propagation Society International Symposium*. IEEE, 2007, pp. 1201–1204.

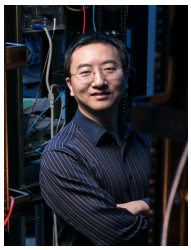
Jiajun Li (Student Member, IEEE) received the bachelor degree in computer science from Xidian University in 2022. He is currently pursuing the master degree in cyberspace security Xidian University. His research interests are in wireless backscatter communication, physical layer security and key generation.

Pu Wang (Graduate Student Member, IEEE) received the Ph.D. degree in cyberspace security from Xidian University in 2021. His research interests are in backscatter communication, wireless information and power transfer, physical layer security, and information security in the Internet of Things.



Long Jiao (Graduate Student Member, IEEE) received the B.Sc. degree in information security from Xidian University, Xi'an, China, in 2016. He is currently pursuing the Ph.D. degree with George Mason University, Fairfax, VA, USA.,His current fields of interest include 5G physical layer security, millimeter-wave communication, and deep learning.

Zheng Yan (Senior Member, IEEE) received the doctor of science in technology in electrical engineering from Helsinki University of Technology, Helsinki, Finland, in 2007. She is currently a Professor in the School of Cyber Engineering, Xidian University, Xi'an, China. Her research interests are in trust, security, privacy, and data analytics. Dr. Yan is an area editor or an associate Editor of IEEE INTERNET OF THINGS JOURNAL, Information Fusion, Information Sciences, IEEE NETWORK MAGAZINE, etc. She served as a General Chair or Program Chair for numerous international conferences, including IEEE TrustCom 2015 and IFIP Networking 2021. She is a Founding Steering Committee co-chair of IEEE Blockchain conference. Her recent achieved awards include 2021 N²Women: Stars in Computer Networking and Communications, Nokia Distinguished Inventor Award, Aalto ELEC Impact Award, the Best Journal Paper Award issued by IEEE Communication Society Technical Committee on Big Data and the Outstanding Associate Editor of 2017 and 2018 for IEEE Access.



Kai Zeng (Member, IEEE) received the PhD degree in electrical and computer engineering from Worcester Polytechnic Institute (WPI), in 2008. He is an associate professor with the Department of Electrical and Computer Engineering, Department of Computer Science, and Center for Secure Information Systems, George Mason University. He was a postdoctoral scholar with the Department of Computer Science, University of California, Davis (UCD) from 2008 to 2011. He worked with the Department of Computer and Information Science, University of Michigan - Dearborn as an assistant professor from 2011 to 2014. He was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) award in 2012. He won Excellence in Postdoctoral Research Award at UCD in 2011 and Sigma Xi Outstanding PhD Dissertation Award at WPI in 2008. He is an editor of the IEEE Transactions on Wireless Communications. His current research interests include cyber-physical system security and privacy, physical layer security, network forensics, and cognitive radio networks.

Yishan Yang (Student Member, IEEE) received a master's degree in cyberspace security from Xidian University in 2021. She is currently pursuing the Ph.D degree with Xidian University. Her research interests include backscatter communication and physical layer security.

APPENDICES

APPENDIX A

Although different BDs will have slightly different backscatter coefficients, this does not affect the consistency of the shared randomness.

$$v_1 = \alpha_2 h_{2,1} h_2 h_1,$$
$$v_2 = \alpha_1 h_{1,2} h_1 h_2 = (\theta \cdot \alpha_2) h_{1,2} h_1 h_2 = \theta \cdot v_1,$$

where $\theta = \alpha_1/\alpha_2$, α_1 and α_2 are the backscatter coefficient of A_1 and A_2, respectively ($\alpha_1 \neq \alpha_2$, $\alpha_1 \neq 0$, $\alpha_2 \neq 0$). Therefore, the correlation of v_1 and v_2 is

$$\begin{aligned} Cor(v_1, v_2) &= \frac{Cov(v_1, v_2)}{\sqrt{Var(v_1)}\sqrt{Var(v_2)}} \\ &= \frac{\theta \cdot Var(v_1)}{\sqrt{Var(v_1)}\sqrt{\theta^2 Var(v_1)}} = 1 \end{aligned}$$

Therefore, even if the backscatter coefficients are different, the correlation of the shared randomness equals to 1 constantly. Then, we prove that the same key sequence can be obtained after the quantization step even when the two measurements are not equal if the correlation coefficient is 1. For simplicity, we assume that there is no noise in the system. The measurements of A_1 and A_2 can be expressed as follows:

$$V_1 = \{v_1(1), v_1(2), \cdots, v_1(k)\} = \alpha_2 \cdot \{T_1(1), T_1(2), \cdots, T_1(k)\},$$
$$(where \quad T_1 = h_1 h_2 h_{2,1}),$$
$$V_2 = \{v_2(1), v_2(2), \cdots, v_2(k)\} = \alpha_1 \cdot \{T_2(1), T_2(2), \cdots, T_2(k)\},$$
$$(where \quad T_2 = h_1 h_2 h_{1,2}),$$

where T_1 and T_2 represent the triangle channel measurement of A_1 and A_2. In the quantization phase of key generation, take 1 bit quantization as an example. For A_1, it needs quantify each sample $v_1(i)$ in the measurement V_1. And quantifying each sample $v_1(i)$ is equal to quantifying $v_1(i)/a_2$ since α_2 is a constant number.

$$v_1(i) = \begin{cases} 1, & if \quad v_1(i) \geq \frac{\sum_{i=1}^{m} v_1(i)}{m} = \alpha_2 \frac{\sum_{i=1}^{m} T_1(i)}{m} \\ 0, & if \quad v_1(i) < \frac{\sum_{i=1}^{m} v_1(i)}{m} = \alpha_2 \frac{\sum_{i=1}^{m} T_1(i)}{m} \end{cases} \leftrightarrow$$
$$\frac{v_1(i)}{a_2} = \begin{cases} 1, & if \quad v_1(i) \geq \frac{\sum_{i=1}^{m} T_1(i)}{m} \\ 0, & if \quad v_1(i) < \frac{\sum_{i=1}^{m} T_1(i)}{m} \end{cases} = T_1(i)$$

Therefore, to quantify $\{v_1(1), v_1(2), \cdots, v_1(k)\}$ is equivalent to quantify $\{T_1(1), T_1(2), \cdots, T_1(k)\}$ and to quantify $\{v_2(1), v_2(2), \cdots, v_2(k)\}$ is equivalent to quantify $\{T_2(1), T_2(2), \cdots, T_2(k)\}$. Since two triangle channel measurements (i.e., $T_1(i)$ and $T_2(i)$) are measured within coherence time, we have $T_1(i) = T_2(i)$. Therefore, even though the bit sequences measured by A_1 and A_2 are not equal since $\alpha_1 \neq \alpha_2$, the bit sequences that turn into 0–1-bit sequences after quantization phase are eventually identical. This implies that A_1 and A_2 do not need to know their own backscatter coefficients or other BDs' backscatter coefficients to obtain identical key sequences.

APPENDIX B

To study the variation of $I(SNR, \beta)$ with β (monotonicity), we only need to study the monotonicity of ρ^2 as β increases. ρ^2 can be transformed into the following expression:

$$\begin{aligned} \rho^2 = f(SNR, \beta) &= \frac{SNR(\beta+1)^2}{SNR(\beta+1)^2 + 4(\beta+1)^2 + 1} \\ &= \frac{1}{1 + \frac{4}{SNR} + \frac{1}{SNR(\beta+1)^2}} \end{aligned}$$

Obviously, $1 + \frac{4}{SNR} + \frac{1}{SNR(\beta+1)^2}$ is monotonically decreasing for $\forall SNR > 0, \beta > 0$ with respect to β. Hence, when β increases and $\forall \beta > 0, SNR > 0$, $f(SNR, \beta)$ increases monotonically. Furthermore, when β increases and $\forall \beta > 0, SNR > 0$, $I(SNR, \beta)$ increases monotonically.

APPENDIX C

To study the variation of $I(SNR, \gamma)$ with γ (monotonicity), we only need to study the monotonicity of ρ^2 as γ increases. Since $\gamma > 0, SNR > 0$, then $\frac{SNR^2(\gamma^4+4\gamma^2+1)^2}{[SNR\cdot(\gamma^4+4\gamma^2+1)+4\gamma^2+9]^2}$ monotonicity and $\frac{SNR(\gamma^4+4\gamma^2+1)}{SNR\cdot(\gamma^4+4\gamma^2+1)+4\gamma^2+9} = \frac{1}{1+\frac{4\gamma^2+9}{SNR(\gamma^4+4\gamma^2+1)}} = \frac{1}{1+f(SNR,\gamma)}$ is the same. Furthermore, the monotonicity of ρ^2 is the opposite of the monotonicity of $f(SNR, \gamma)$, and therefore we just need to study the monotonicity of $f(SNR, \gamma)$. We can further transform $f(SNR, \gamma)$ into the following expression:

$$\begin{aligned} \rho^2 = f(SNR, \gamma) &= \frac{4\gamma^2 + 9}{SNR(\gamma^4 + 4\gamma^2 + 1)} \\ &= \frac{4\gamma^2 + 8 + 1}{SNR(\gamma^4 + 4\gamma^2 + 4) - 3SNR} = \frac{4(\gamma^2+2)+1}{SNR(\gamma^2+2)^2 - 3SNR} \\ &= \frac{4}{SNR(\gamma^2+2) - \frac{3SNR}{(\gamma^2+2)}} + \frac{1}{SNR(\gamma^2+2)^2 - 3SNR} \end{aligned}$$

Since $\gamma > 0$, we make $t = \gamma^2 + 2, t > 2$, and we can transform $f(SNR, \gamma)$ into the following expression:

$$\begin{aligned} &\frac{4}{SNR(\gamma^2+2) - \frac{3SNR}{(\gamma^2+2)}} + \frac{1}{SNR(\gamma^2+2)^2 - 3SNR} \\ &= \frac{4}{SNR \cdot t - \frac{3SNR}{t}} + \frac{1}{SNR \cdot (t^2 - 3)} \end{aligned}$$

Obviously, under the premise of $t > 2$ and $SNR > 0$, as t increases, $\frac{1}{SNR\cdot(t^2-3)}$ decreases monotonically. Moreover, $\frac{4}{SNR\cdot t - \frac{3SNR}{t}}$ decreases monotonically as t increases. By taking the partial derivative of the term's denominator, it can be proved that the term is also monotonically decreasing.

$$\frac{\partial(SNR \cdot t - \frac{3SNR}{t})}{t} = SNR + \frac{3 \cdot SNR}{t^2} > 0$$

Adding two subtractive functions is still a subtracting function. Hence, when γ increases and $\forall \gamma > 0, SNR > 0$, $f(SNR, \gamma)$ decreases monotonically. Furthermore, when γ increases and $\forall \gamma > 0, SNR > 0$, $I(SNR, \gamma)$ increases monotonically.

APPENDIX D

To study the variation of $I(SNR, \gamma)$ with γ (monotonicity), we only need to study the monotonicity of ρ^2 as γ increases. ρ^2 can be transformed into the following expression:

$$\rho^2 = f(SNR, \gamma) = \frac{SNR\gamma^4}{SNR\gamma^4 + 4\gamma^2 + 1} = \frac{1}{1 + \frac{4}{SNR\cdot\gamma^2} + \frac{1}{SNR\cdot\gamma^4}}$$

Obviously, $1 + \frac{4}{SNR\cdot\gamma^2} + \frac{1}{SNR\cdot\gamma^4}$ is monotonically decreasing for $\forall SNR > 0, \gamma > 0$ with respect to γ. Hence, when γ increases and $\forall \gamma > 0, SNR > 0$, $f(SNR, \gamma)$ increases monotonically. Furthermore, when γ increases and $\forall \gamma > 0, SNR > 0$, $I(SNR, \gamma)$ increases monotonically.

APPENDIX E