Physical layer key generation against MIMO eavesdropper by exploiting full-duplex technology

Rong Jin (jinrong@hust.edu.cn)
Huazhong University of Science and Technology - Main Campus: Huazhong University of Science and Technology
https://orcid.org/0000-0001-7817-2812

Kai Zeng
George Mason University

Research Article

Keywords: full duplex radio, key generation, mutual jamming, MIMO eavesdropper, active attack detection, low cost

DOI: https://doi.org/10.21203/rs.3.rs-641396/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License
Physical layer key generation against MIMO eavesdropper by exploiting full-duplex technology

Rong Jin and Kai Zeng

Abstract
Generating a shared secret key from physical layer is an interesting topic with practical value. Inspired by the encouraging progress on full-duplex radio, a novel mechanism aiming at high and steady key generation rate with low cost is proposed in this paper. Legitimate users simultaneously send random bit sequences to actively interfere with each other. They extract those mutually jammed bits to form a secret key. A special digital modulation scheme, called Random Manchester coding is proposed. The proposed scheme achieves three goals. The first and the most important one is to prevent a MIMO eavesdropper from separating the superposed signal; the second one is to detect denial of service and key compromise attack to defend against an active attacker; the third one is to achieve design goal on low power radiation, computational complexity and memory cost. Theoretical analysis, numerical simulations and concept-proof experiments validate the effectiveness of our proposed scheme. Our solution is promising to facilitate key generation applications of nearby wireless devices such as ubiquitous smartphones, wearable devices.

Keywords: full duplex radio; key generation; mutual jamming; MIMO eavesdropper; active attack detection; low cost

1 Introduction
Generating a shared key between two parties without pre-shared secret over a public channel is a challenging problem in symmetric key cryptography systems. Physical layer key generation mechanisms (e.g. by exploiting the reciprocal and spatial diversity properties of the wireless fading channel [1–3]) are fundamentally different from traditional cryptography-based mechanisms (e.g. Diffie-Hellman (DH) key exchange) in that they do not rely on the intractability of certain computational problems and are more computationally effective. DH key exchange protocol requires extensive computational power, which is not preferable to resource constrained devices, such as sensors, RFIDs, and wearable devices. In order to keep the same security strength, DH key exchange protocol needs to increase the key space when attacker’s computing power is improved, thus leads to higher computational overhead. Physical layer key generation does not subject to these limitations and is a promising alternative for shared key generation in many applications.

While there are numbers of works being carried out [1–9], current channel based physical layer key generation mechanisms are not satisfactory in terms of key generation rate. Although techniques may evolve, the information rate of the shared randomness is fundamentally limited by the channel variation. More importantly, the key generation rate is sensitive to the environment and could be very low under stationary conditions, which is more often the case.

Inspired by the encouraging progress on full-duplex radio [10–14], a novel mechanism aiming at high and steady key generation rate and low cost, called “mutual jamming”, is proposed in this paper. Note that digital communication is subject to wireless interference at physical layer. We let legitimate users simultaneously send random bits of 0’s or 1’s to interfere with each other. While sending, the full-duplex user also listens to the superposed signal. When the bits are synchronized and different (one sends 0 and the other sends 1), they are mutually jammed and an eavesdropper cannot figure out who sent the 0 or who sent the 1. Since legitimate users know what they have sent, they can use the bits sent at either side to establish a shared key.

To transform the above idea into a practical system, we need to address the major challenge that a MIMO eavesdropper can separate the superposed digital signal with common amplitude or(and) phase modula-
Figure 1: Demonstration of key generation by mutual jamming

In mutual jamming, a special digital modulation method, called random Manchester coding is designed, by replacing common amplitude and phase modulation to what we called energy modulation. As illustrated in Fig 1, a low power noise followed by a high power noise denotes a '0', while a high power noise followed by a low power noise denotes a '1'. The major purpose is to remove the pilot symbols and information redundancy, so that a MIMO eavesdropper cannot obtain the wireless channels either by training sequence [15] or blind channel estimation [16, 17] in separation of the superposed signal. In addition, mutual jamming presents the following attractive advantages. (a) it can detect denial of service and key compromise attack in real time to defend against an active attacker without an authentication mechanism. (b) it can achieve high security strength without the need of high power radiation, computational complexity and memory cost. Numerical simulations and concept-proof experiments validate the effectiveness of our proposed scheme.

Our main contributions are as follows:

- We propose a novel physical layer key generation mechanism by exploiting full duplex technique. The method has high security strength against a single antenna or MIMO eavesdropper, can detect an active attacker and does not require high power radiation, computation or memory cost.
- We explain the basic idea of the proposed scheme in detail, analyze the security strength and evaluate the performance by simulations.
- We build a testbed based on USRP software defined radio and conduct proof-of-concept experiments to demonstrate the effectiveness of the proposed method in a real-world environment.

We make the following findings in our experiments:

- The obtained key generation rate of mutual jamming is as high as about 20kbps. For 1028 bit key, the time consumption is only about 0.05s.
- The transmitting power used by both keying parties for simultaneous random bits sending is as low as about 10dBm.

Mutual jamming is thus a practical, fast, low cost, and secure key generation mechanism for nearby wireless devices such as ubiquitous smartphones and wearable devices.

2 Related Work

In recent years, physical layer key agreement mechanisms have been proposed for establishing information-theoretical keys between two wireless devices without sharing any secret in advance.

2.1 Reciprocal channel based mechanism

There has been an increasing interest in exploiting the randomness and reciprocity of the wireless channel to generate shared keys between two parties. Most of the works have assumed passive attacks [1–7]. Early research in this area focused on theoretical analysis [3, 18], where the maximum key generation rate (assuming no information loss on key generation procedure) is bounded by the mutual information between two keying nodes [4, 19, 20]. More recent works were more interested in practical implementations of the key generation schemes using off-the-shelf wireless devices and their real-world performance [21]. Specifically, three kinds of channel characteristics are studied for measurement and quantization to generate secret keys. They are received signal strength [1, 3, 22], phase difference [23] and impulse response [24, 25]. The key generation rates considering practical communication conditions are addressed in [5, 7]. To further increase the key generation rate, multiple-antenna diversity has been exploited in [6]. Some other works discussed the multi-user case [26–28]. The work in [29] derived secrecy capacities for multiple terminals. The works in [26, 30] obtained the maximum key generation rate of simultaneous key generations and group key generation.

Some recent works have discussed interference and jamming attack [3, 31, 32] against the key agreement scheme. With the presence of jamming, the key generation rate can be seriously affected. The works in [31, 33] proposed to adaptively increase the quantization interval in accordance with the jamming signal level to mitigate the jamming effect.

As pointed out in Introduction section, channel based scheme is not satisfactory in terms of key generation rate and sensitive to the environment.

2.2 Physical proximity based mechanism

In [8, 9], physical layer features are extracted as shared secret for nearby devices. The principle is based on
that clients in the same geographic area can observe a certain shared ambient signals, such as the same normalized packet arrival time and similar received signal strengths (RSS). These physical layer features are location specific due to random wireless fading and cannot be easily estimated and forged by a client outside the proximity of half-wavelength. Therefore, users can exploit the ambient radio signals to establish spatial temporal location tags and use the location tags for authentication.

However, the method is limited to the areas with plenty of ambient radio sources, e.g. indoor environments with multiple WiFi access points (APs), bluetooth devices and FM radios. The difficulty in proximity range control is another problem. Experimental work has demonstrated that there does exist a strong correlation in measurements observed by passive eavesdroppers located significantly greater than a half-wavelength away from legitimate devices [34]. Therefore, there is not a clear safe guard distance to ensure the secrecy of the device pairing.

In [35], an NFC-based key generation method is proposed. For NFC, the operating distance is within 10cm, significantly smaller than half of a wavelength (about 11m for 13.56MHz). It is known that a MIMO eavesdropper cannot separate the superposed signal in this case. However, this method cannot be directly applied to far-field communications (e.g. WiFi) where the superposed signal can be separated once the keying devices are more than half of a wavelength (about 6.25cm at 2.4GHz) apart.

A novel physical layer key agreement mechanism by exploiting full-duplex technology is proposed in this paper, in which the shared randomness is generated by combining the user introduced randomness at both sides of the legitimate users, and the information rate for key generation is thus high and steady.

3 Preliminary

In this paper, we consider the scenario where two smart devices (typically smartphones and wearable devices), Alice and Bob, want to bootstrap a secure communication by generating a shared secret key between themselves over a wireless channel without any pre-shared secret. We assume that Alice and Bob are within a short distance (within couple of meters) so that on-demand wireless connectivity can be established conveniently by popular short range wireless communication technology and specifications, such as Bluetooth [36] or WiFi. One of them, say Alice is assumed to be full duplex enabled.

3.1 Adversary model

We consider a powerful adversary, Eve, who can launch either (1) passive attacks by eavesdropping on the communication between Alice and Bob, trying to compromise the generated key or (2) active attacks by injecting arbitrary signals over its wireless interface trying to manipulate the superposed signal. Eve may be a device having more powerful computational ability than the legitimate devices, such as a laptop or a personal computer. She may use standard or custom-built hardware to capture signals, including multi-antenna MIMO devices. She can capture baseband signals with high sensitivity and sampling rate. In this case, she can store all the overhead signals and conduct sophisticated signal processing or data analysis off-line.

We assume that the adversary is only subject to the following physical constraints: Eve could be in any location with respect to Alice and Bob but she is at least several meters away from them and not directly visible (otherwise the attacker will be physically discovered easily). In this case, the eavesdropping wireless channels are assumed to be multi-path rayleigh fading channels, and thus it is commonly agreed that there exists channel diversity among different subcarrier frequencies [37].

3.2 Mathematic model

We use $x_a(t)$ and $x_b(t)$ to denote the signal transmitted by Alice and Bob, and $y_e(t)$ and $y_a(t)$ to denote the signal received by Eve and Alice (through full-duplex ability), respectively. According to the above system configuration assumptions, $y_e(t)$ can be modeled as

$$y_e(t) = h_{A\rightarrow E}x_a(t) + h_{B\rightarrow E}x_b(t) + n(t)$$

where $h_{A\rightarrow E}$ and $h_{B\rightarrow E}$ are the channel coefficients of the eavesdropping wireless channels from Alice to Eve and Bob to Eve, respectively; $n(t)$ is the channel noise. In the similar way, $y_a(t)$ can be modeled as

$$y_a(t) = \rho x_a(t) + h_{B\rightarrow A}x_b(t) + n(t)$$

where $h_{B\rightarrow A}$ is the channel coefficient of the wireless channel from Bob to Alice; $\rho$ represents the self interference of the full duplex radio.

It is common practice to describe wireless systems in the baseband, that is after removing the carrier frequency. [1] Hence, in the rest of the paper, we use baseband signals to denote the transmitting and receiving signals (e.g. $x_a(t)$, $x_b(t)$, $y_e(t)$) if not especially specified.

[1] Wireless signals are transmitted using a carrier frequency $f_c$. At the receiver, the RF frontend removes the carrier frequency from the received signal $A\exp(j2\pi f_c t)$, which produces the baseband signal $A$. 

\[ y_e(t) = h_{A\rightarrow E}x_a(t) + h_{B\rightarrow E}x_b(t) + n(t) \]  
\[ y_a(t) = \rho x_a(t) + h_{B\rightarrow A}x_b(t) + n(t) \]
4 Method
Aiming at a physical layer key generation of high and steady key generation rate with low cost, we developed a novel solution, called mutual jamming. We introduce our design in detail and analyze its security and performance in this section.

4.1 Method introduction
The basic idea with baseband signal representation is illustrated in Fig. 1.

Alice and Bob simultaneously send random bits of 0’s or 1’s to opportunistically jam each other. The bit stream sent by Alice (or Bob) in an N-bit data frame is $C_a$ (or $C_b$).

$$C_a = [C_a(1), C_a(2), \ldots, C_a(N)]$$
$$C_b = [C_b(1), C_b(2), \ldots, C_b(N)]$$

where $C_a(i)$ and $C_b(i)$ (1 ≤ i ≤ N) are the ith bit sent by Alice and Bob, respectively.

On one hand, to tackle the major threat from MIMO eavesdropper, we propose to use Gaussian noise over wide radio spectrum in keying information exchange, so as to prevent the eavesdropper from obtaining the wireless channels (which will be detailed in the next subsection).

On the other hand, in order for the legitimate FD device to understand the information composed entirely of Gaussian noise, we design a special scheme, called Random Manchester coding to modulate the bits. A low power noise followed by a high power noise denotes a ‘0’, while a high power noise followed by a low power noise denotes a ‘1’.

- when $C(i) = 0$

$$x^i(t) = \begin{cases} n[\sigma^2_h](t) & 0 \leq t < T_0 \\ n[\sigma^2_l](t) & T_0 \leq t < 2T_0 \\ 0 & 2T_0 \leq t < T \end{cases}$$

- when $C(i) = 1$

$$x^i(t) = \begin{cases} n[\sigma^2_l](t) & 0 \leq t < T_0 \\ n[\sigma^2_h](t) & T_0 \leq t < 2T_0 \\ 0 & 2T_0 \leq t < T \end{cases}$$

where $T$ is the bit duration. $n[\sigma^2_h](t)$ and $n[\sigma^2_l](t)$ denote zero mean Gaussian noise with large variance $\sigma^2_h$ (high power) and small variance $\sigma^2_l$ (low power), respectively, and $T_0$ denotes their signal duration. We set a mute period ($T - 2T_0$) to help Alice identify the bit representation and check for synchronization (the duty cycle should be $\frac{2T_0}{T - 2T_0}$ when their signals are well synchronized).

Math Notation: we use superscript $i$ to denote the signal of the $i$th bit, and the complete signal is denoted if the superscript is not applied; we use subscript $a$, $b$ and $e$ to denote the signal sender Alice, Bob and receiver Eve, and the signal by any party is denoted if the subscript is not applied. For example, $x^i(t)$ means the $i$th bit signal sent by Alice or Bob; $y_e(t)$ means the complete signal received by Eve.

As shown in Fig. 1, there are four possible cases when the $i$th pair of bits sent by Alice and Bob are synchronized.

- Case 1: Alice sends 1, Bob sends 0.
- Case 2: Alice sends 0, Bob sends 1.
- Case 3: both Alice and Bob send 1.
- Case 4: both Alice and Bob send 0.

By inserting (4) and (5) into (1) and ignoring channel noise, we are able to make the following deductions.

For case 3, the superposed signal at Eve is the double of 1’s.

$$y_e(t|C_a^i = 1, C_b^i = 1) = \begin{cases} (h_{A\rightarrow E} + h_{B\rightarrow E})n[\sigma^2_h](t) & 0 \leq t < T_0 \\ (h_{A\rightarrow E} + h_{B\rightarrow E})n[\sigma^2_l](t) & T_0 \leq t < 2T_0 \end{cases}$$

This does not help because Eve can identify this case by comparing the energy between the first $T_0$ and the second $T_0$. As can be seen in (6), Eve can tell that both devices sent a 1 if the energy of the first $T_0$ is greater than that of the second $T_0$. The same thing happens for case 4. Eve can tell that both devices sent a 0 if the energy of the first $T_0$ is smaller than that of the second $T_0$. Alice and Bob will discard the bits of these two cases.

It gets interesting for case 1 and case 2. Note that Manchester coding has symmetric (flipped) waveform for 0 and 1. The energy relationship of the superposed RF signal between the first $T_0$ and the second $T_0$ becomes undetermined. For example, if Alice sent 1 and Bob sent 0, we have

$$y_e(t|C_a^i = 1, C_b^i = 0) = \begin{cases} h_{A\rightarrow E}n[\sigma^2_h](t) + h_{B\rightarrow E}n[\sigma^2_l](t) & 0 \leq t < T_0 \\ h_{B\rightarrow E}n[\sigma^2_h](t) + h_{A\rightarrow E}n[\sigma^2_l](t) & T_0 \leq t < 2T_0 \end{cases}$$

As demonstrated in Fig. 1, the energy of the first $T_0$ is very close to that of the second $T_0$. The same thing happens if Alice sent 0 and Bob sent 1. Therefore, these two cases are indistinguishable from the viewpoint of Eve. We call that this pair of bits are mutually jammed and either $C_a(i)$ or $C_b(i)$ can be extracted as 1 bit key.
independent quasistatic Rayleigh fading channels.

To establish a shared key, while sending \( x_a(t) \), Alice detects the receiving signal \( y_a(t) \) using its full duplex ability. To decode Bob’s bit, Alice eliminates her own signal by subtracting \( y_a(t) \) by \( px_a(t) \) (this procedure is known as SIC, self-interference cancellation). As can be seen from (2), this leads to

\[
z_a(t) = y_a(t) - px_a(t) = p_0 x_a(t) + h_{B \rightarrow A} x_b(t) + n(t)
\]

(8)

where \( p_0 \) is the residue self-interference.

Note that a high-quality full duplex radio should have \( p_0 \approx 0 \), and if we further ignore channel noise, we have

\[
z_a(t) \approx h_{B \rightarrow A} x_b(t)
\]

(9)

Alice can perform standard decoding by comparing the energy between the first \( T_0 \) and the second \( T_0 \). For example

\[
z^i_a(t|C^i_b = 1) = \begin{cases} 
  h_{B \rightarrow A} n[\sigma^2_t](t) & 0 < t < T_0 \\
  h_{B \rightarrow A} n[\sigma^2_t](t) & T_0 < t < 2T_0 
\end{cases}
\]

(10)

A detection of a relative high power noise followed by a relative low power noise can be decoded as a '1' and vice versa.

After decoding, Alice compares her bit stream with Bob’s and extracts the indexes \( L \) of all the (total number denoted by \( M \)) mutually jammed bit-pairs \( L = [l_1, l_2, l_3 \cdots l_M] \), where \( C_a(l_i) \neq C_b(l_i) \), and sends the indexes \( L \) to Bob. Alice simply takes out all the indexed values of its transmitted bit stream, \( K_A = [C_a(l_1), C_a(l_2), C_a(l_3) \cdots C_a(l_M)] \); Bob does the same operation, and flips (1 to 0 and 0 to 1) the indexed values, \( K_B = [C_b(l_1), C_b(l_2), C_b(l_3) \cdots C_b(l_M)] \). An example will be shown in Section 6 Fig 8. It can be easily verified that the M bit keys are identical, \( K_A = K_B \).

\[w_1^i = c_{ae} X \sigma^2_h \lambda_{N_e}^2 + c_{be} X \sigma^2_h \lambda_{N_e}^2\]
\[w_2^i = c_{ae} X \sigma^2_h \lambda_{N_e}^2 + c_{be} X \sigma^2_h \lambda_{N_e}^2\]

(11)

where \( w_1^i \) and \( w_2^i \) are the average energies of the first \( T_0 \) and the second \( T_0 \) of the \( i \)th bit.

\[
\begin{align*}
  w_1^i &= \frac{1}{T_0} \int_0^{T_0} y_1^i(t)dt \\
  w_2^i &= \frac{1}{2T_0} \int_{T_0}^{2T_0} y_1^i(t)dt
\end{align*}
\]

(12)

\( X \) denotes the independent exponential random variable with unit mean; \( c_{ae} = c/d_{ae}, c_{be} = c/d_{be} \) are the dimensionless constants, where \( d_{ae} \) and \( d_{be} \) are the distances between Alice and Eve and between Bob and Eve; \( \alpha \) is the pathloss exponent, and \( c \) is a normalization constant.

\( \lambda_{N_e}^2 \) denotes the independent random variable drawn from chi-squared distribution (the distribution of the square of normal random variables \([38]\)) with \( N_e \) degrees of freedom, where \( N_e = BT_0 \) approximated by time-bandwidth product denotes the number of effective sample points.

**Math Notation:** To simplify presentation, we use \( f(w_1^1, w_2^1) \) to denote \( Pr\{w_1^1, w_2^1|C_a(i) = 1, C_b(i) = 0\} \) (the probability density function for case 1) and \( g(w_1^1, w_2^1) \) to denote \( Pr\{w_1^1, w_2^1|C_a(i) = 0, C_b(i) = 1\} \).

The maximum likelihood decoding made by Eve (based on the observation of \( w_1^1 \) and \( w_2^1 \)) can be written as

\[
\begin{align*}
  C_a(i) &= 1 \quad f(w_1^1, w_2^1) > g(w_1^1, w_2^1) \\
  C_a(i) &= 0 \quad f(w_1^1, w_2^1) < g(w_1^1, w_2^1)
\end{align*}
\]

(13)

That is, for case 1, if a certain observation has \( f(w_1^1, w_2^1) < g(w_1^1, w_2^1) \), a wrong decoding will be made and vice versa. Considering that the bits transmitted by Alice(Bob) have equal probability of being '0' or '1', Eve’s bit error ratio (BER) of maximum likelihood decoding can be further calculated by

\[
p_e = \frac{1}{2} \int_{f<g} f(w_1^1, w_2^1) dw_1^1 dw_2^1 + \frac{1}{2} \int_{f>g} g(w_1^1, w_2^1) dw_1^1 dw_2^1
\]

\[
= \frac{1}{2} \int_{f<g} \min\{f(w_1^1, w_2^i), g(w_1^i, w_2^1)\} dw_1^1 dw_2^i
\]

(14)

Since the superposed signals for case 1 and case 2 are designed to be identical, we have \( f(w_1^1, w_2^1) \approx
In previous subsection, we have shown that key compromising is difficult by showing that the Eve’s decoding of keying bits is very error prone. In this subsection, we will show that key establishment is reliable by showing that Alice’s decoding has very low error rate.

Similar to the previous subsection, for a given scenario, when the bits are mutually jammed, we can write the energy of the partner’s signal extracted by Alice as follows (taking case 1 as an example)

\[
\begin{align*}
\{ w_1^i &= \rho_0 \sigma_N^2 X + c_{ab} \sigma_N^2 \chi + \sigma_N^2 \chi, \\
\{ w_2^i &= \rho_0 \sigma_N^2 X + c_{ab} \sigma_N^2 \chi + \sigma_N^2 \chi
\end{align*}
\]

where \( \sigma^2 \) is the variance of channel noise. \( c_{ab} = c/d_{ab} \) and \( d_{ab} \) is the distance between Alice and Bob.

The decoding made by Alice (based on the observation of \( w_1^i \) and \( w_2^i \)) can be written as

\[
\begin{align*}
C_b(i) &= 1 \quad w_1^i > w_2^i \\
C_b(i) &= 0 \quad w_1^i < w_2^i
\end{align*}
\]

That is, for case \( C_b(i) = 1 \), if a certain observation has \( w_1^i < w_2^i \), a wrong decoding will be made and vice versa. Considering that the bits transmitted by Bob have equal probability of being ‘0’ or ‘1’, Alice’s BER can be calculated by

\[
p_e = \frac{1}{2} \int \int f(w_1, w_2) dw_1 dw_2 + \frac{1}{2} \int \int g(w_1, w_2) dw_1 dw_2
\]

We use the same example as in subsection 4.2 to calculate Alice’s BER analytically, where we set the residue self interference to \( \rho_0 = -20 \)dB (It is stated in [10] that the receive antenna’s signal can decoded if self-interference can be removed 20dB below the transmitting signal.), and draw the BER-to-SNR curve in Fig. 3. It can be seen that the BERs are very low and less than 0.36% when SNR > 10dB.

### 4.4 Our method can defend against MIMO eavesdropper

In this subsection, we explain the mechanism of how mutual jamming defends against an emerging class of powerful adversaries: MIMO (multi-input multi-output) eavesdroppers through random Manchester coding.

We shall mention that a complete introduction requires a lot of background knowledge on MIMO and channel estimation theory, which involves complex mathematical models, technologies and numerous algorithms that it is impossible for this work to cover all the aspects (numerical security analysis against MIMO eavesdropper will be detailed in Section 5). Good descriptions of MIMO and channel estimation theory are available in [16, 41, 42] if one wishes to go for
the details. For the context of this paper, however, it is sufficient to know that the principle and theory of our design is based on the following 2 widely accepted conclusions.

(1) MIMO’s coherent decoding relies on the knowledge of wireless channels

In a MIMO system, a coherent signal detection requires a reliable estimate of the channel impulse responses between the transmit and receive antennas [16, 42].

To understand such MIMO capability, let’s recall from (1) that a 2-antenna MIMO eavesdropper will create 2 independent equations:

\[
y_{e1}(t) = h_{A\rightarrow E1}x_a(t) + h_{B\rightarrow E1}x_b(t)
\]
\[
y_{e2}(t) = h_{A\rightarrow E2}x_a(t) + h_{B\rightarrow E2}x_b(t)
\] (19)

Eve can separate 2 signals \(x_a(t)\) and \(x_b(t)\) transmitted concurrently on the wireless medium with the knowledge of wireless channels by solving the equations. In the same way, an \(n\)-antenna MIMO eavesdropper creates \(n\) independent equations, and can thus separate at most \(n\) signals. [3]

[2]MIMO communications could also be non-coherent. For example, one can exploit the structure of the codebook to recover the information without directly estimating the channel [43]. However, non-coherent MIMO communications rely on special designed precoding, which is not the case of random Manchester coding.

[3]One solution [41, 42] to address MIMO problem could be using at least as many antennas on MIMO users as there are on MIMO eavesdropper. For example, if a 2-antenna user, Alice, sends two independent signals \(x_{a1}(t), x_{a2}(t)\) concurrently to compose \(x_a(t)\), (19) can be extended to

\[
y_{e1}(t) = h_{A1\rightarrow E1}x_{a1}(t) + h_{A2\rightarrow E1}x_{a2}(t) + h_{B\rightarrow E1}x_b(t)
\]
\[
y_{e2}(t) = h_{A1\rightarrow E2}x_{a1}(t) + h_{A2\rightarrow E2}x_{a2}(t) + h_{B\rightarrow E2}x_b(t)
\]

Since the number of unknowns \(x_{a1}(t), x_{a2}(t)\) and \(x_b(t)\) is larger than the number of equations, a 2-antenna eavesdropper can no longer solve the equations in this case. This solution, however, creates a what is known as antenna battle [44] between the user and the eavesdropper, and is not preferable.

However, with the absence of channel knowledge at the MIMO receiver, the number of unknown channel coefficients increases in correspondence with the increase of the number of antennas, and so formed an underdetermined system of equation no matter how many antennas the MIMO receiver possesses.

(2) Channel estimation cannot be done without information redundancy over Gaussian noise

It is important to specify the notion that a correct identification of the channel coefficients from mixed signals is impossible without information redundancy [41], because the solution to channel coefficients is not unique. In another word, a wrong signal separation by incorrect channel coefficients does not affect the observations, as is exemplified by the following relation.

\[
y_{ek}(t) = h_{B\rightarrow Ek}x'_b(t) + h'_{A\rightarrow Ek}x'_a(t)
\] (20)

where \(x'_b(t) = x_b(t) + \rho x_a(t)\) and \(x'_a(t) = (1 - \rho)x_a(t)\) represent a wrong separation that part of the signal from Alice \(\rho x_a(t)\) is misclassified.

It can be easily verified that this wrong separation is supported by the following wrong channel coefficient at any of Eve’s antennas (the \(k\)th antenna for example).

\[
h'_{A\rightarrow Ek} = (h_{A\rightarrow Ek} - \rho h_{B\rightarrow Ek})/(1 - \rho)
\] (21)

While numerous works have put great efforts on channel estimation, they can be classified by the redundant information on which they depend. One kind of methods is based on training symbols redundancy [15]. A well designed training signal should take into consideration the channel estimation overhead, estimation error and capacity loss caused by non-ideal receive algorithm. Another kind of methods, called blind channel estimation, makes use of common redundant information in the modulated signal itself [16]. For a specific communication system, the source signal is
usually a modulated or filtered data, which either belongs to a limited set of symbols having specific amplitudes and phases, or is time/spatially correlated, or has cyclic prefix redundancy, or exists nonzero high-order statistics, etc. The last kind of methods, called semi-blind channel estimation, combines the former two.

In view of the MIMO limitation, our coding design aims at removing the information redundancy, so as to avoid these information being used by the eavesdropper, specifically.

In order to protect the secrecy of the wireless channels against training-symbols based channel estimation techniques, random Manchester coding replaces traditional amplitude and phase modulation (e.g. QAM, PSK) to energy modulation. Note that the legitimate decoding is now performed by comparing the energy between the first $T_0$ and the second $T_0$. There is no amplitude or phase information needed in this case, so that pilot symbols are not applied in data frames modulated by random Manchester coding. [5]

In order to protect the secrecy of the wireless channels against blind channel estimation techniques, random Manchester coding uses Gaussian noise over wide radio spectrum, i.e. AWGN. The wireless channel from Alice to Eve (Bob to Eve) in this case has no amplitude, phase or statistical characteristics, due to the frequency diversity and the random Gaussian signal structure. In this way, there is no potential avenues of channel estimation. [6]

4.5 Detecting active attacks

In this subsection, we explain the mechanism of how mutual jamming detects an active attack through random Manchester coding.

[4] For example, [45] proposed a subspace based blind channel estimation method for space-time coded MIMO-OFDM systems using properly designed redundant linear precoding and the noise subspace method. [46] proposed an algorithm for blind channel estimation and equalization for MIMO-OFDM systems using second-order cyclostationary statistics induced by employing a periodic nonconstant-modulus antenna precoding. [47] developed a subspace method for SISO-OFDM systems by utilizing the redundancy introduced by the cyclic prefix (CP) insertion.

[5] Frame header information (e.g. the ID of the transmitter) can be transmitted using a per-agreed alternative carrier frequency annotated by pilot symbols irrelevant to the wireless channels of the data transmitted by random Manchester coding.

[6] That both training-symbols based channel estimation and blind channel estimation cannot work certainly implies that semi-blind channel estimation cannot work.

Denial of Service Attack

In the simplest case, Eve just wants to disturb the keying process such that Alice is not able to understand the signal sent by Bob. denial of service attack can be achieved by transmitting valid frequencies of the data spectrum at a correct time. The correct time can be calculated if the attacker has a good understanding of the used modulation scheme and coding. This attack is not too complicated, but it does not allow the attacker to manipulate the actual data.

Since Manchester coding yields the same signal power on bit ‘0’ and bit ‘1’, the superposed signal exhibits an identical energy $(2T_0(\sigma_A^2 + \sigma_F^2))$ on each bit pair. Thus, Alice can simply check whether its actually received energy is in the correct range.

Key Compromise Attack

In key compromise attack, Eve wants Alice and Bob to actually receive some valid, but manipulated data, so as to control the keying process and infer portion of the key subsequently.

To counter key compromise attack, Alice can send a control frame to Bob in the beginning of key generation process, specifying (1) the beginning and the end time instant of simultaneous random bits sending, making sure that there is no time delay that could be exploited by Eve to launch a man-in-the-middle attack: (2) the power of transmitting noise $\sigma_A^2$, $\sigma_F^2$, so that Alice can perform a power detection on superposed signal.

Under regular circumstances without interference, the superposed signal detected by Alice $y_a^i(t)$ has three possibilities.

- Condition 1: a high power noise signal followed by a low power noise signal:
  \begin{align}
  y_a^i(t) &= n(2\sigma_A^2)(t) \quad 0 \leq t < T_0 \\
  y_a^i(t) &= n(2\sigma_F^2)(t) \quad T_0 \leq t < 2T_0 \\
  y_a^i(t) &= 0 \quad 2T_0 \leq t < T 
  \end{align}

  It corresponds to case 3 that both Alice and Bob sent ‘1’ on the $i$th bit.

- Condition 2: a low power noise signal followed by a high power noise signal:
  \begin{align}
  y_a^i(t) &= n(2\sigma_F^2)(t) \quad 0 \leq t < T_0 \\
  y_a^i(t) &= n(2\sigma_A^2)(t) \quad T_0 \leq t < 2T_0 \\
  y_a^i(t) &= 0 \quad 2T_0 \leq t < T 
  \end{align}

  It corresponds to case 4 that both Alice and Bob sent ‘0’ on the $i$th bit.

- Condition 3: a medium power noise signal over the time domain of $2T_0$. 

\[ y'_b(t) = n[\sigma_T^2 + \sigma_h^2](t) \quad 0 \leq t < 2T_0 \\
\quad y'_b(t) = 0 \quad 2T_0 \leq t < T \] (24)

It corresponds to case 1 and case 2 that one sent ‘0’ and the other sent ‘1’ on the rth bit.

Note that in order to let Alice and Bob decode a wrong bit, key compromise attack relies on changing the superposed signal from one condition to another, otherwise it won’t be recognized and will be detected. It can be seen from (22), (23) and (24) that the attacker must do two things: increasing the power of noise signal during one \( T_0 \) and decreasing the power of noise signal during another \( T_0 \). \[ \text{[7]} \] The former is feasible by sending compensating signal of proper power, while the latter requires signal cancellation \[ \text{[48]} \]: one should send negative RF signal of \( \pi \) phase difference with respective to the original RF signal. Note that \( y'_b(t) \) is a random noise signal, where the instantaneous phase is not known or predictable. Therefore in this case, signal cancellation is practically impossible, and so does the key compromise attack.

4.6 Cost and efficiency

In this subsection, we explain the mechanism of how mutual jamming achieves low cost through random Manchester coding.

First, the cryptographic operations of mutual jamming involves only simple computations of bit comparisons due to the physical layer design. It has low computation complexity and saves time and computational energy comparing with traditional key generation method. For example, it has been reported that the time consumption of ECDH (Elliptic Curve Diffie-Hellman key exchange method) is about 9.1s to 15.1s for low cost sensors \[ \text{[49]} \] and about 4.3s to 4.7s for smartphones \[ \text{[50]} \] due to the complex computations, while our experiments show that the time consumption of our proposed key generation method is only about 0.05s thanks to the simple computations and fast key generation rate. Moreover, it has been reported that the energy consumed by computation of the cryptographic operations is at least one order of magnitude larger than transmissions \[ \text{[49]} \]. Thus, the reduction of computations would significantly save the total energy consuming of the key generation. Second, the decoding at legitimate users involves only energy comparison between the first \( T_0 \) and the second \( T_0 \) due to the energy modulation design. Thus in mutual jamming, the FD device does not need to keep the complete waveform for self-interference cancellation (which is known as the major cost in FD communications \[ \text{[12, 13]} \]), and it saves decoding memory and energy. Finally, the key generation process of mutual jamming involves neither multi-step negotiation rounds (such as ECDH) nor information reconciliation (such as reciprocal channel based physical layer key generation method), and it is overall simple and saves transmitting and receiving energy.

4.7 How about the synchronization offset between the transmitting signals

So far, for the simplicity of our method description, we have always believed that Alice can well synchronize her transmitting signal \( x_a(t) \) with that of Bob \( x_b(t) \). However, we notice that the strict time synchronization for distributed devices is known to be difficult \[ \text{[51]} \]. A major issue causing random synchronization offset is clock skew and jitter \[ \text{[51]} \]. When an observable synchronization offset happens, the security assumption of indistinguishable superposed RF signals under case 1 and case 2 will not hold. Note that this potential weakness might be exploited by the eavesdropper if he has a good chance to know which device clock jitter happens to (e.g., the clock circuit of one device is much more unstable than that of the other device).

It is worth pointing out that this does not mean that our scheme poses strong request and high cost on synchronization. Recall that our design is based on “opportunistic jamming”. Thus, to eliminate the potential risk, Alice can simply find out all of the unsynchronized bit pairs in her received signal \( y_a(t) \) (by checking whether the superposed signal has the time length of \( 2T_0 \) at each \( y'_a(t) \) for example) and discard them in prior.

5 Results and Discussion

In this section, we conduct numerical simulations to evaluate our design, random Manchester coding, against a MIMO eavesdropper and compare it with traditional Manchester coding.

We set the center frequency to 2.4GHz, the available transmission bandwidth to 2MHz and Alice, Bob and Eve’s signal to noise ratio (SNR) to 25dB. We assume Alice and Bob simultaneously transmit digital signal as introduced in subsection 4.1 to generate a key by mutual jamming.
To simulate random Manchester coding, we let both Alice and Bob send Gaussian noise over 2MHz bandwidth. A low power noise followed by a high power noise denotes a ‘0’, while a high power noise followed by a low power noise denotes a ‘1’. We set the variance of high power noise ten times of that of low power noise \( \sigma^2_h/\sigma^2_l = 10 \). We set the bit duration to \( T = 15\mu s \); the signal width of each noise signal is \( T_0 = 5\mu s \); mute period is \( T - 2T_0 = 5\mu s \). To validate the robustness of mutual jamming, random synchronization offset uniformly distributed within 1\( \mu s \), \([8]\) random amplitude and phase deviation uniformly distributed within 1% are introduced in the simulation. The residue self interference is set to -20dB.

To simulate traditional Manchester coding for reference, we let both Alice and Bob send BPSK signal defined as follows

- when \( C(i) = 0 \)
  \[
  x^t(t) = \begin{cases} 
  0 & 0 \leq t < T/2 \\
  1 & T/2 \leq t < 2T 
  \end{cases}
  \]  
- when \( C(i) = 1 \)
  \[
  x^t(t) = \begin{cases} 
  1 & 0 \leq t < T/2 \\
  0 & T/2 \leq t < 2T 
  \end{cases}
  \]  

We set the bit rate and the total bit duration the same as that in random Manchester coding. For simplicity, we use an idealized system model in the simulation \([53]\), which does not take specific implementation issues (e.g. pulse-shaping filter) and system imperfections (e.g. intersymbol interference, imperfect orthogonality among subcarrier signals) into consideration, since they have little impact on security.

For the MIMO eavesdropper, we first assume that Eve is a normal laptop with 3 antennas being integrated. The eavesdropping channels from Alice/Bob to Eve are multi-path quasi-statistic rayleigh fading channels \([37]\). The wireless coefficients at different subcarrier frequencies are randomly and independently drawn from a complex Gaussian distribution with unit variance. We try SOBI algorithm (a classic second order blind identification algorithm \([54]\)) to separate two signal sources from Alice and Bob. After extracting only Bob’s signal, the decoding of traditional Manchester signal is performed by constellation diagram and the decoding of random Manchester signal is performed by

It is indicated that this clock synchronization accuracy of sub-microsecond range is achievable by Precision Time Protocol (PTP) \([52]\).

Figure 4 Wireless channel coefficients from Alice to Eve’s 3 antennas.

![Figure 4](image)

5.1 Effectiveness of random Manchester coding

In this simulation, Alice and Bob simultaneously transmit 1024-bit random sequences \( x_a(t) \) and \( x_b(t) \) for mutual jamming. We record channel estimation results and calculate the BERs at the MIMO eavesdropper. Fig. 4 shows an example of channel estimation result, where the channel coefficient from Alice to Eve’s first antenna is always normalized to “1”. The cross marked points are the actual channel coefficients; the circle marked points and square marked points are the 20 independent channel estimation results for traditional Manchester coding and random Manchester coding respectively. It can be seen that on one hand, the estimated channel coefficients are close to the true values for traditional Manchester coding. This is because BPSK-based signal has specific amplitudes and fits in the mathematic model described in \([54]\). On the other hand, the estimated channel coefficients are diverge from the true values for random Manchester coding. This is because Gaussian structured signal does not have the second order static characteristics described in \([54]\).

Fig. 5 further shows the cumulative distribution function (CDF) curve of the key compromising BER at Eve based on 10,000 independent random runs. Solid line represents traditional Manchester coding and dashed line represents random Manchester coding. For traditional Manchester coding, Eve’s BER is only about 8% on average. The minimum and maximum BERs are about 6% and 10%. For random Manchester coding, we use the final key compromising bit error rate (BER) at Eve as the metric of security strength, where a perfectly secure system should have a 50% BER meaning that the eavesdropper’s key compromising ability in this case is equivalent to a random guess.
coding, Eve’s BER is as high as about 46% on average, closing to a random guess. The minimum and maximum BERs are about 42% and 50%. It can be seen that random Manchester coding has much higher ratio of wrong key guessing than traditional Manchester coding. It conforms with the theoretical analysis in section 4.4 that traditional amplitude or phase modulation is vulnerable to a MIMO eavesdropper, while random Manchester coding is secure against it.

5.2 Impact of antenna number on BER

We then investigate the performance of our proposed key generation design on different number of antennas that Eve got. We keep the other simulation parameters unchanged to test the cases of single antenna, few antennas and many antennas.

Fig. 6 shows the average BER (of 10,000 independent random runs) with respect to the number of antennas. The circle marked lines represent traditional Manchester coding and square marked lines represent random Manchester coding.

As can be seen from Fig. 6 that circle marked lines locate far below square-marked lines, which indicates that random Manchester coding outperforms traditional Manchester coding in security strength against MIMO eavesdropping attack. Specifically, both traditional Manchester coding and random Manchester coding present high BERs closing to 50% at the start points of the curves, which means that both schemes are secure against single antenna eavesdroppers. However, when the number of antennas increases, circle marked line drops down rapidly as shown in Fig. 6(a). Even for only 2 antennas, the average BER decreases to about 10%. For random Manchester coding, the BERs remain almost unchanged as the the number of antennas increases. Even for 100 antennas (massive MIMO case [42]), the average BER is still larger than 40%. This confirms with the conclusion claimed in section 4.4(1) that signal separation cannot be done without channel knowledge no matter how many antennas the MIMO receiver possesses.

6 Experimental

We conduct concept-proof experiments to demonstrate the effectiveness of our proposed key generation method, mutual jamming, in this section. The experiment set up is shown in Fig 7(a). We use 2 software defined radios, USRP N210, to simulate legitimate keying parties, Alice and Bob, respectively. Another USRP is used to simulate the eavesdropper, Eve. We use Daughter board SBX-40 as the transmitting and receiving front-end, where the nominal frequency range is 400MHz - 4.4GHz, and the nominal bandwidth is 40 MHz. We use antenna VERT 2450 to send and receive RF signals at 2.4GHz. We set sampling rate to 20MHz. We set the average transmitting power by Alice (or Bob) to 10dbm.

As introduced in subsection 4.1, to implement random Manchester coding, we send Gaussian noise over the entire bandwidth of 40 MHz. A low power noise followed by a high power noise denotes a ‘0’, while a high power noise followed by a low power noise denotes a ‘1’. We set the variance of high power noise ten times of that of low power noise ($\sigma^2_h/\sigma^2_l = 10$). We set bit duration to $T = 15\mu s$; the signal width of each noise signal is $T_0 = 5\mu s$; mute period is $T - 2T_0 = 5\mu s$. 
6.1 Method validation

Fig. 8 shows the snapshot of the the superposed signal received by Eve, where the bit sequences sent by Alice and Bob are $C_a = [010101011001]$ and $C_b = [011001010101]$ during this period. It can be seen from the figure that the 3rd, 4th, 7th, 8th and 11th bit pairs are mutually jammed in this case. As expected, the superposed waveform presents a medium power noise signal over the time domain of $2T_0$. Eve cannot figure out who sent ‘0’ and who sent ‘1’ from her overheard signal.

To establish a shared key, Alice extracts the indexes of all the mutually jammed bit-pairs $L = [3, 4, 7, 8, 11]$, by performing a simple energy detection on the first $T_0$ and the second $T_0$: if these two energies are both in “acceptable” range (neither of them is larger or smaller than $\sigma_l^2 + \sigma_h^2$ by exceeding a pre-set threshold $\gamma$), the bit pair is recognized as being mutually jammed; otherwise, the bit values are the same or there could be an active attack as discussed in subsection 4.5 and the bit pair is discarded. In the experiment, we set $\gamma$ to 30% of $\sigma_l^2 + \sigma_h^2$.

Alice then sends the indexes to Bob. Alice simply takes out all the indexed values of its transmitted bit stream, $K_A = [01101]$; Bob does the same operation, and flips the indexed values, $K_B = \sim[10010] = [01101]$. It can be seen that the two sequences are identical, $K_A = K_B$, and a 5-bit key can be extracted using this time period.

6.2 MIMO evaluation

In this experiment, we apply 2 software defined radios next to each other to receive the RF signals concurrently to simulate two independent antennas of a MIMO eavesdropper, Eve1 and Eve2. For reference, we also investigate traditional Manchester coding as defined in Section 5 for simulations, where we set the traditional Manchester coding for comparison having the same bit length as random Manchester coding.

**Traditional Manchester coding vs 2-antenna Eavesdropper**

First, we let Bob send the random bit sequence $C_b$ alone to gain insight into how multiple antenna diversity on the wireless channels of amplitude modulation signal is presented.

Fig. 9(a) shows the snapshot of the strength (magnitude value) of the signal received by Eve1 $|y_{e1}(t)|$, where the bit sequence is $C_b = [110100]$ during this period. Fig. 9(b) shows the corresponding I-phase and Q-phase signals $\Re\{y_{e1}(t)\}$, $\Im\{y_{e1}(t)\}$, respectively. [9] Fig. 9(c) shows the same I-phase and Q-phase signals received by Eve2 $\Re\{y_{e2}(t)\}$, $\Im\{y_{e2}(t)\}$.

It can be seen that the I-phase, Q-phase and strength signals collected from two antennas have different amplitudes but the same waveform characteristic that

[9] Wireless signals are transmitted using a carrier frequency $f_c$. At the receiver, the RF frontend removes the carrier frequency from the received signal by $\cos(2\pi f_c t)$ and $\sin(2\pi f_c t)$, which produces the baseband signal of in-phase and quadrature components, respectively.
the voltage levels are flat. Such characteristic guarantees the uniqueness of the solution to channel coefficients because any wrong separation in (20) \( x'_b(t) = x_b(t) + \rho x_a(t) \) leads to non flat voltage levels due to the different bit structure of \( x_a(t) \) unless \( \rho = 0 \).

Then, we let Alice and Bob simultaneously send the random bit sequences \( C_a \) and \( C_b \). Fig. 10 thin line shows the snapshot of the superposed signal received by Eve1. It can be seen that the waveform also becomes unrecognizable when two bits are different due to mutual interference, which indicates that traditional Manchester coding is effective against a single-antenna eavesdropper.

We then use SOBI algorithm \( [54] \) to separate the superposed signals on two antennas Eve1 and Eve2. Fig. 10 thick line shows the snapshot of the estimated signal sent by Bob \( \hat{C}_b \). It can be seen that SOBI has successfully restored the basic shape of Bob’s transmitting signal. With a tolerable waveform distortion (mainly caused by residue channel estimation error and channel noise), the bit sequence is still readable and can be correctly decoded as \( \hat{C}_b = [110100] = C_b \) in this case, which indicates that traditional Manchester coding becomes insecure facing a multi-antenna eavesdropper.

**Random Manchester coding vs 2-antenna Eavesdropper**

We apply the same procedure to study random Manchester coding. First, we let Bob send the random bit sequence \( C_b \) alone to gain insight into how the multiple antenna diversity on the wireless channels can be covered by energy modulated noise signal.

Fig. 11(a) shows the snapshot of the strength of the signal received by Eve1 \( |y_{e1}(t)| \), where the bit sequence is \( C_b = [10101] \) during this period. Fig. 11(b) shows the corresponding I-phase and Q-phase signals \( \text{Re}\{y_{e1}(t)\}, \text{Im}\{y_{e1}(t)\} \) respectively. Fig. 11(c) shows the same I-phase and Q-phase signals received by Eve2 \( \text{Re}\{y_{e2}(t)\}, \text{Im}\{y_{e2}(t)\} \).

It can be seen that the I-phase and Q-phase signals collected from two antennas no longer present any waveform structure, since they are noise structured signal \( x_b(t) \). In this way, the uniqueness of the solution to channel coefficients cannot be guaranteed by the flatness of the voltage levels. A wrong separation in (20) \( x'_b(t) = x_b(t) + \rho x_a(t) \) is thus unable to be excluded and prevented.

Then, we let Alice and Bob send the random bit sequences \( C_a \) and \( C_b \) concurrently.

Fig. 12 thin line shows the snapshot of the superposed signal received by Eve1. It can be seen that the waveform becomes unrecognizable due to the mutual interference, which indicates that random Manchester coding is effective against a single-antenna eavesdropper.

We then use SOBI algorithm to separate the superposed signals on two antennas Eve1 and Eve2. Fig. 12 thick line shows the snapshot of the estimated signal sent by Bob \( \hat{C}_b \). It can be seen that SOBI has failed to
Figure 11 Snapshot that Bob sends a random bit sequence modulated by random Manchester coding alone to a 2-antenna eavesdropper, Eve.

Figure 12 Snapshot of random Manchester coding that Alice and Bob send random bit sequences concurrently.

6.3 BER test
We statistically validate the effectiveness of our proposed key generation method in a real-world configuration. We put Alice and Bob close to each other and put the eavesdropper in the same room 2 to 3 meters away from them at 5 different locations labelled as location A to E as illustrated in Fig 7(b). For each location, Alice and Bob simultaneously send frames of 1,000 random bits.

Table 1 shows the BERs. It can be seen that our proposed key generation method randomizes modulation waveform and causes high BER at Eve for all 5 different locations under both single antenna case and two antennas case. The BERs are from 43.8% to 57.5% with the average of 49.6% for single antenna eavesdropper, and the BERs are from 41.6% to 55.2% with the average of 47.5% for two antennas eavesdropper. The results are close to a random guess. For reference, we also test traditional Manchester coding case. The BERs are from 45.8% to 59.6% with the average of 53.6% for single antenna eavesdropper. However, the BERs decrease dramatically for two antennas eavesdropper. The BERs are from 8.3% to 21% with the average of 13.7%. The results validate that our proposed key generation method, random Manchester coding is more secure than traditional amplitude or phase coding for a MIMO eavesdropper.

We further test the key establishing performance at legitimate users. It can be seen from the table (4th column) that the BERs of key agreement are very close to 0% at all 5 different locations.

7 Conclusion
This paper proposes a physical layer key generation method, called mutual jamming, by exploiting full-
duplex technique. Legitimate devices send random bit sequences simultaneously to interfere each other and extract those mutually jammed bits to generate a secret key. A special digital modulation scheme, called Random Manchester coding is designed. A low power noise followed by a high power noise denotes a ‘0’, while a high power noise followed by a low power noise denotes a ‘1’.

With this design, mutual jamming poses high security strength against a single antenna or MIMO eavesdropper, can detect an active attacker and does not require complex computation, high power radiation or memory cost.

Numerical simulations and concept-proof experiments validate the effectiveness of our proposed scheme. Simulation results show that the average key compromising BER is always larger than 40% as we increase the number of antennas at the eavesdropper from 1 to 100. Real-world experiments show that mutual jamming randomizes modulation waveform and causes high BER at Eve for all 5 different locations under both single antenna case and two antennas case. The BERs are from 43.8% to 57.5% with the average of 49.6% for single antenna eavesdropper, and the BERs are from 41.6% to 55.2% with the average of 47.5% for two antennas eavesdropper. The results are close to a random guess.

References
1. Azimi-Sadjadi, B., Khiyias, A., Mercado, A., Yener, B.: Robust key generation from signal envelopes in wireless networks. In: CCS 07: Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 401–410 (2007)
2. Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A.: Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. MobiCom ’08, pp. 128–139 (2008)
3. Ye, C., Mathur, S., Reznik, A., Shah, Y., Trappe, W., Mandayam, N.B.: Information-theoretically secret key generation for fading wireless channels. Information Forensics and Security, IEEE Transactions on 5(2), 240–254 (2010). doi:10.1109/TIFS.2010.2043187
4. Maurer, U.M.: Secret key agreement by public discussion from common information. Information Theory, IEEE Transactions on 39(3), 733–742 (1993). doi:10.1109/18.256484
5. Liu, Y., Draper, S.C., Sayeed, A.: Exploiting channel diversity in secret key generation from multipath fading randomness. Information Forensics and Security, IEEE Transactions on 7(5), 1484–1497 (2012). doi:10.1109/TIFS.2012.2206385
6. Zeng, K., Wu, D., Chan, A., Mohapatra, P.: Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In: INFOCOM, 2010 Proceedings IEEE, pp. 1–9 (2010). doi:10.1109/INFCOM.2010.5462004
7. Wei, Y., Zeng, K., Mohapatra, P.: Adaptive wireless channel probing for shared key generation based on pid controller. Mobile Computing, IEEE Transactions on 12(9), 1842–1852 (2013). doi:10.1109/TMC.2012.144
8. Xiao, L., Yan, Q., Lou, W., Chen, G., Hou, Y.T.: Proximity-based security techniques for mobile users in wireless networks. Information Forensics and Security, IEEE Transactions on 8(12), 2089–2100 (2013). doi:10.1109/TIFS.2013.2286269
9. Mathur, S., Miller, R., Varshavsky, A., Trappe, W., Mandayam, N.: Proximate: Proximity-based secure pairing using ambient wireless signals. In: Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services. MobiSys ’11, pp. 211–224. ACM, New York, NY, USA (2011). doi:10.1145/1999995.2000016
10. Choi, J.I., Jain, M., Srinivasan, K., Levis, P., Katti, S.: Achieving single channel, full duplex wireless communication. In: International Conference on Mobile Computing and Networking, MOBICOM 2010, Chicago, Illinois, USA, September, pp. 1–12 (2010)
11. Chen, L., Zhu, Q., Meng, W., Hua, Y.: Fast power allocation for secure communication with full-duplex radio. IEEE Transactions on Signal Processing 65(14), 3846–3861 (2017)
12. Sabbarwal, A., Schniter, P., Guo, D., Bliss, D.W.: In-band full-duplex wireless: Challenges and opportunities. Selected Areas in Communications IEEE Journal on 32(9), 1637–1652 (2014)
13. Lu, H., Shao, S., Tang, Y.: A low-cost digital self-interference cancellation structure for full-duplex communications. In: Signal Processing Conference, pp. 2355–2359 (2016)
14. Bharadia, D., Mcmilen, E., Katti, S.: Full duplex radios. In: Acm Sigcomm Conference on Sigcomm (2013)
15. Biguesh, M., Geralman, A.B.: Training-based mimo channel estimation: a study of estimator tradeoffs and optimal training signals. IEEE Transactions on Signal Processing 54(3), 884–893 (2006)
16. Shin, C., Heath, R.W., Powers, E.J.: Blind channel estimation for mimo-ofdm systems. IEEE Transactions on Vehicular Technology 56(2), 670–685 (2007)
17. Janjaap, V.D.B., Edlers, O., Sandell, M., Wilson, S.K., Borjesson, P.O.: On channel estimation in ofdm systems. In: Vehicular Technology Conference, pp. 815–819 (1995)
18. Chen, C., Jensen, M.A.: Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients, pp. 205–215. IEEE Educational Activities Department, ??? (2011)
19. Cachin, C., Maurer, U.: Linking information reconciliation and privacy amplification. Journal of Cryptology 10, 97–110 (1997). doi:10.1007/s001459900023
20. Brassard, G., Savail, L.: Secret-key reconciliation by public discussion. In: Workshop on the Theory and Application of Cryptographic
Techniques on Advances in Cryptology. EUROCRYPT '93, pp. 410–423. Springer, Secaucus, NJ, USA (1994)

Zhang, J., Woods, R., Duong, T.Q., Marshall, A., Ding, Y.: Experimental study on channel reciprocity in wireless key generation. In: IEEE International Workshop on Signal Processing Advances in Wireless Communications (2016)

Liu, H., Yang, J., Wang, Y., Chen, Y.: Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In: INFOCOM, 2012 Proceedings IEEE, pp. 927–935 (2012). doi:10.1109/INFOCOM.2012.6195843

Ye, C., Reznik, A.: Group secret key generation algorithms. In: Information Theory, 2007. ISIT 2007. IEEE International Symposium On, pp. 2596–2600 (2007)

Louie, H.Y.Y., Li, Y., Vucetic, B.: Practical physical layer network coding for two-way relay channels: Performance analysis and comparison. IEEE Transactions on Wireless Communications 9(2), 764–777 (2010)

Jin, R., Du, X., Zeng, K., Huang, L.: Delay analysis of physical layer key generation in dynamic roadside-to-vehicle network. IEEE Transactions on Vehicular Technology 66(3), 2526–2535 (2016)

Saisi, T., Narayan, P.: Secrecy capacities for multiple terminals. Information Theory, IEEE Transactions on 50(12), 3047–3061 (2004). doi:10.1109/TIT.2004.838380

Lai, L., Ho, S.-W.: Simultaneously generating multiple keys and multi-commodity flow in networks. In: Proc. IEEE Info. Theory Workshop, (Lausanne, Switzerland) (2012)

Zafar, M., Agrawal, D., Srivastva, M.: Limitations of generating a secret key using wireless fading under active adversary networking. IEEE/ACM Transactions on Wireless Communications 20(5), 1440–1451 (2012). doi:10.1109/TNET.2012.2183146

Law, Y.W., Palaniswami, M., Hoesel, L.V., Doumen, J., Hartel, P., Havinga, P.: Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols. ACM Trans. Sen. Netw. 5(1), 6–1639 (2009)

Patwari, N., Croft, J., Jana, S., Kasera, S.K.: High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Transactions on Mobile Computing 9(1), 17–30 (2010)

Edman, M., Kiyajia, A., Yener, B.: On passive inference attacks against physical-layer key extraction? In: Proceedings of the Fourth European Workshop on System Security. EUROSEC ’11, pp. 8–186. ACM, New York, NY, USA (2011). doi:10.1145/1972551.1972559. http://doi.acm.org/10.1145/1972551.1972559

Jin, R., Du, X., Deng, Z., Zeng, K., Xu, J.: Practical secret key agreement for full-duplex near field communications. IEEE Transactions on Mobile Computing 15(4), 938–951 (2016). doi:10.1109/TMC.2015.2434861

Bhagwat, P.: Bluetooth: Technology for short-range wireless apps. IEEE Internet Computing 5(1), 96–103 (2001)

Liu, Z., Xin, Y., Giannakis, G.B.: Space-time-frequency coded ofdm over frequency-selective fading channels. Signal Processing IEEE Transactions on 50(10), 2465–2476 (2002)

Mood, A.M.: Introduction to the Theory of Statistics, (1963)

Vilela, J.P., Bloch, M., Barros, J., McLaughlin, S.W.: Friendly jamming for wireless secrecy. In: IEEE International Conference on Communications, pp. 1–6 (2010)

Alekseev, V.G.: Estimation of a probability density function and its derivatives. Mathematical Notes of the Academy of Sciences of the USSR 12(5), 808–811 (1972)

Chen, H.H., Guizani, M.: Fundamentals of Wireless Communications. John Wiley and Sons, Ltd

Larsson, E.G.: Fundamentals of massive mimo. In: IEEE International Workshop on Signal Processing Advances in Wireless Communications, pp. 1–1 (2016)

Inoue, T., Jr, R.W.H.: Kerdoek codes for limited feedback precoded mimo systems. IEEE Transactions on Signal Processing 57(9), 3711–3716 (2009)

Hassanien, H., Wang, J., Katabi, D., Kohno, T.: Securing rids by randomizing the modulation and channel. In: Usenix Conference on Networked Systems Design and Implementation, pp. 235–249 (2015)

Zhou, S., Muquet, B., Giannakis, G.B.: Subspace-based (semi-) blind channel estimation for block precoded space-time ofdm. IEEE Transactions on Signal Processing 50(5), 1215–1228 (2002)

Bolcskei, H., Heath, R.W., Paulraj, A.J.: Blind channel identification and equalization in ofdm-based multiantenna systems. IEEE Transactions on Signal Processing 50(1), 96–109 (2002)

Muquet, B., de Courville, M., Duhamel, P.: Subspace-based blind and semi-blind channel estimation for ofdm systems. Signal Processing IEEE Transactions on 50(7), 1699–1712 (2002)

Widrow, B., Duvall, K., Gooch, R., Newman, W.: Signal cancellation phenomena in adaptive antennas: Causes and cures. IEEE Transactions on Antennas and Propagation 30(3), 469–478 (1982). doi:10.1109/TAP.1982.1142804

de Meulenaer, G., Gosset, F., Standaert, O.-X., Pereira, O.: On the energy cost of communication and cryptography in wireless sensor networks. In: Networking and Communications, 2008. WIMOB ’08. IEEE International Conference on Wireless and Mobile Computing, pp. 580–585 (2008). doi:10.1109/WiMob.2008.16

Jin, R., Shi, L., Zeng, K., Pande, A.: Magpairing: Pairing smartphones in close proximity using magnetometers. IEEE Transactions on Information Forensics and Security 11(6), 1306–1320 (2016)

Eidson, J., Kang, L.: Ieee 1588 standard for a precision clock synchronization protocol for networked measurement and control systems. In: Sensors for Industry Conference, 2002. Isasee, pp. 98–105 (2002)

Scheiterer, R.L., Na, C., Obradovic, D., Steindl, G.: Synchronization performance of the precision time protocol in industrial automation networks. IEEE Transactions on Instrumentation and Measurement 58(6), 1849–1857 (2009)

Nee, R.V., Prasad, R.: OFDM for Wireless Multimedia Communications. Artech House, ??? (2000)

Belouchrani, A., Abed-Meraim, K., Cardoso, J.F., Moulines, E.: A blind source separation technique using second-order statistics. IEEE Transactions on Signal Processing 45(2), 434–444 (2002)

8 Figure Title and Legend

1 Demonstration of key generation by mutual jamming

2 Example of the distribution of the BER for the eavesdropper at different positions. It can be seen that all the BERs are greater than 36%.

3 Example of the BER curve for the legitimate user under different SNR. It can be seen that all the BERs are very close to 0%.

4 Wireless channel coefficients from Alice to Eve’s 3 antennas, where the first one is normalized to “1”; cross marked points: actual channel coefficients; circle marked points: estimated channel coefficients for traditional Manchester coding; square marked points: estimated channel coefficients for random Manchester coding.
|   | Description |
|---|-------------|
| 5 | CDF of BER at Eve; solid line: traditional Manchester coding; dashed line: random Manchester coding |
| 6 | Average BERs at the eavesdropper with respect to the number of antennas (a) few antennas from 1 to 10 (b) many antennas from 10 to 100 |
| 7 | Experimental demonstration. (a) Experimental equipments and setting. (b) Diagram of Eve’s location with respect to Alice and Bob |
| 8 | Snapshot of the superposed signal received by Eve |
| 9 | Snapshots that Bob sends a random bit sequence modulated by traditional Manchester coding alone to a 2-antenna eavesdropper, Eve. (a) normalized signal strength received by Eve1. (b) I-phase and Q-phase signal received by Eve1. (c) I-phase and Q-phase signal received by Eve2 |
| 10 | Snapshot of traditional Manchester coding that Alice and Bob send random bit sequences concurrently. Thin line: superposed signal received by Eve1. Thick line: estimated signal sent by Bob |
| 11 | Snapshot that Bob sends a random bit sequence modulated by random Manchester coding alone to a 2-antenna eavesdropper, Eve. (a) normalized signal strength received by Eve1. (b) I-phase and Q-phase signal received by Eve1. (c) I-phase and Q-phase signal received by Eve2 |
| 12 | Snapshot of random Manchester coding that Alice and Bob send random bit sequences concurrently. Thin line: superposed signal received by Eve1. Thick line: estimated signal sent by Bob |