# A Novel Approach to Secure Communication in Physical Layer via Coupled Dynamical Systems

Najme Ebrahimi, Hessam Mahdavifar, and Ehsan Afshari
Department of Electrical and Computer Engineering, University of Michigan, Ann Arbor, MI 48109, USA
Email: najme@umich.edu, hessam@umich.edu, afshari@umich.edu

***Abstract*—A new framework for secure communication in physical layer is proposed. A network of users equipped with coupled dynamical systems is considered. The aim is to securely exchange messages between network nodes in the presence of an eavesdropper, referred to as Eve. Unlike a traditional wireless system, the messages to be conveyed are not sent directly through the medium. Instead, they are mapped to initial conditions of the dynamical system. Once the system converges to a steady state, conditions of the local system at each node is measured to recover the sent messages. A fundamental property of the proposed system which makes it secure is that if Eve tries to eavesdrop messages by acting as a node of the coupled network, her presence will change the dynamics of the system and hence, it will be detected by the network nodes. In particular, a situation with two users is considered. The proposed system is then modeled as a two-way wiretap channel and the secrecy capacity region is derived under various conditions. Furthermore, a radio frequency (RF) system is proposed to realize this model in a wireless setting by means of local coupled oscillators. In particular, a unidirectional master-slave coupling architecture is considered where a power-constrained slave node synchronizes its phase and frequency with a high-power master node. It is shown how the coupling mechanism, realized by transmitting and receiving power between the RF front-ends of the master and the slave node, can be used by the slave node to securely send messages or to share secret keys with the master node. To the best of our knowledge, this is the first architecture providing physical layer secret key generation fully designed in the RF front-end. The proposed RF system is simulated using Advanced Design System (ADS). The simulation results are shown for a 10 m channel link and confirm the security condition. The secret key generation rate is 2 bits per synchronization time-frame which is dominated by the wave propagation delay between the two nodes.**

## I. Introduction

The forecast of tremendous growth of wireless networks in future systems, e.g., the fifth generation of wireless networks (5G) and the Internet of Things (IoT) poses a higher risk of malicious attacks against message confidentiality in communication systems. The conventional cryptographic techniques currently deployed in wireless systems, such as SNOW 3G algorithms in Long-Term Evolution (LTE) [1], are based on point-to-point encryption and decryption protocols. These protocols require a shared secret key that is only known to the legitimate parties. However, as wireless networks become more distributed, e.g., with the incorporation of Device-to-Device (D2D) communications into cellular protocols [2], there is a need to implement methods for securely sharing keys between individual users without the help of a central entity. Furthermore, Internet-of-Things (IoT) devices are severely constrained by low power consumption and low device unit costs. This makes it inefficient for such devices to have separate hardware for encryption and decryption at higher layers. Therefore, developing new methods for secure communication in the physical layer is inevitable for future communications and networking technologies.

In contrast to conventional cryptographic algorithms, physical layer security methods are keyless, where the noise level of the wireless link is utilized to provide security [3]. Also, no computational restrictions are placed on the adversary, and hence, there is no need for unproven assumptions of computational hardness. In this framework, security is measured in terms of information-theoretic security, in the sense defined by Wyner [4]. However, an arguable assumption is that the channel from the transmitter to the eavesdropper is somewhat weaker than the channel from the transmitter to the legitimate receiver. This has become a major barrier in implementing physical layer security protocols in practical settings.

Physical layer security methods can be also deployed to exchange secret keys efficiently and hence, to complement the higher layer cryptographic security protocols. With the fundamental work of [5] to use common randomness for secret communication, secret key agreement protocols using the characteristics of physical layer channel have recently received significant attention [6]. A common assumption in such protocols is the channel reciprocity between legitimate parties [7]–[9]. However, transmitted and received signals in the front-end antennas of communicating devices are generated by separate local oscillators (LO). The traveling signals between two nodes could experience frequency mismatch and its associated phase variation, which is neglected in the reciprocity assumption. In other words, the phase and frequency mismatch between two wireless nodes disturb the reciprocity assumption. In fact, LO phase noise is one of the critical sources of asynchronous frequency and phase error [10], [11]. Consequently, carrier synchronization is essential in physical-layer secret key generation to accurately estimate the channel and suppress the reliability error.

In this paper, we establish a new framework to provide security in the physical layer by means of coupled dynamical systems. To this end, a network of coupled dynamical systems is considered. Such network can be realized by exploiting RF local oscillators deployed at each node of the network. The messages are not directly sent through the wireless channel. Instead, each network node encodes its message into an initial condition, such as its free-running frequency. Then the network nodes enter a transition phase and within nanoseconds converge to a steady-state condition provided that initial free-running frequencies are within a certain range referred to as *locking range*, [12]. Each node then observes its steady-state condition such as the synchronized frequency and its phase difference with other nodes. Then the initial conditions and the steady-state conditions are compared in order to recover messages. This protocol can be used repeatedly by adjusting the free-running frequencies as the initial conditions for a new transmission. The security of the proposed protocol is based upon the fact that the eavesdropper, referred to as Eve, is not part of the dynamical

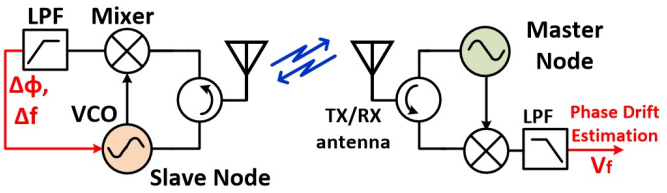


Fig. 1: Conceptual block diagram of a master-slave RF coupled oscillator used for synchronization.

system and hence, she does not observe the initial conditions of the nodes. If she tries to act as a node coupled with other nodes, then the dynamics of the system changes, thereby enabling network nodes to detect such malicious attacks. This provides a new framework for keyless secure communications in physical layer that works regardless of Eve's location and how strong her receiver is. An analytical approach to study a network of two legitimate parties using two-way wiretap channel is provided and secrecy capacity regions are derived.

In order to put the proposed protocol in a practical setting, a system of RF local oscillators using a *master-slave* architecture is designed and simulated in ADS Keysight simulator. This system is inspired by synchronized networks such as the one shown in Fig. 1. The advantage of the proposed architecture is two fold: It serves as means of frequency synchronization of the slave node to the master node, and also enables the slave node to secretly share a random sequence with the central master node. To the best of our knowledge, this is the first architecture providing physical layer secret key generation fully designed in the RF front-end. Consequently, it does not have a back-end processing delay and is resilient to digital software hack. Simulation results in ADS confirm the security and the reliability of the proposed protocol.

The rest of this paper is organized as follows. In Section II some background on coupled dynamical systems, coupling mechanisms in wireless networks, and physical layer security are provided. A theoretical framework to model the proposed system as a two-way wiretap channel together with the analysis of secrecy capacity region is provided in Section III. An RF system implementation of the proposed protocol for secret key generation together with simulation results is discussed in Section IV. Finally, the paper is concluded in Section V.

## II. Preliminaries

### A. Coupled dynamical systems

A coupled dynamical system is modeled as a network of nodes with dynamical states that evolve according to certain differential equations. Parameters of such differential equations at each node depend on the states of other nodes as well as some inherent properties of the underlying node.

The best way to describe a coupled dynamical system is by a graph with weighted edges. Let $\mathcal{G} = (\mathscr{V}, A)$ denote the graph, where $\mathscr{V} = \{\mathcal{V}_1, \ldots, \mathcal{V}_n\}$ is the set of nodes. Also, $A = [A_{i,j}]_{n\times n}$, where $A_{i,j} \in \mathbb{R}^+ \in \{0\}$, is the weighted adjacency matrix for $\mathcal{G}$. In fact, $A_{i,j}$ denotes the coupling coefficient of node $j$ towards node $i$. In particular, $A_{i,j} = 0$ implies that the state of node $j$ does not affect the evolution of node $i$'s state. One may assume that $A_{i,i} = 0$. Let $\theta_i(t) \in \mathbb{R}$ denote the state of node $i$ at time $t$. Then the dynamical system at node $i$ evolves according to the following equation:

$$\frac{d\theta_i(t)}{dt} = g\big(\theta_i(t)\big) - \alpha_i \sum_{j\neq i} A_{i,j} f\big(\theta_j(t) - \theta_i(t)\big). \qquad (1)$$

In many applications, the nodes are oscillators with $\omega_i$ as the corresponding initial frequencies, $\alpha_i$ is an inherent positive constant associated with the $i$-th oscillator , $g(\theta_i(t)) = \omega_i$, $f(.) = \sin(.)$, and $\theta_i$'s are linear functions in steady state. Assuming that $f(.)$ is the sin function, (1) reduces to a weighted version of the well-known Kuramoto model [13]:

$$\frac{d\theta_i(t)}{dt} = \omega_i - \alpha_i \sum_{j\neq i} A_{i,j} \sin\big(\theta_j(t) - \theta_i(t)\big), \qquad (2)$$

We say that the system described by (2) synchronizes if oscillators operate at the same frequency $\tilde{\omega}$ in the steady state. Also, we say that the initial frequencies are within the *locking range*, if the system described by (2) synchronizes in the steady state.

*Definition 1:* Let $\Pi = [0, 2\pi)$ denote the set of possible phases. Assuming that the initial frequencies of the nodes are within the locking range, we describe the system as a function

$$\mathcal{D} : (\mathbb{R}^+ \times \Pi)^n \to \mathbb{R}^+ \times \Pi^n. \qquad (3)$$

The input to $\mathcal{D}$ is $\{(\omega_i, \varphi_i); i \in [n]\}$, where $\varphi_i$ is the initial phase of nodes $i$ at time 0, and $[n] = \{1, 2, \ldots, n\}$. The output of $\mathcal{D}$ is $\big(\tilde{\omega}, \{\tilde{\varphi}_i, i \in [n]\}\big)$, where $\tilde{\omega}$ in the steady-state frequency of all the nodes, and $\tilde{\varphi}_i$'s are the steady-state phases of the nodes, whose differences can be derived from (2) assuming the nodes are synchronized to frequency $\tilde{\omega}$.

In our proposed protocol, we will use the relation between the initial conditions of oscillators and their steady-state condition, described by the function $\mathcal{D}$ defined above, for secure communication.

### B. Coupling mechanism for synchronization in wireless communications

Synchronization between wireless network nodes can be obtained via a bidirectional architecture [11] or a master-slave architecture [10]. For wireless coupled oscillators, such as the one shown in Fig. 1, the coupling coefficient $A_{i,j}$ is given by

$$A_{i,j} = \frac{P_{r,j}}{P_i}, \qquad (4)$$

where $P_{r,j}$ is the average received power from $\mathcal{V}_j$ by $\mathcal{V}_i$ and $P_i$ is the transmitted power by node $\mathcal{V}_i$ to $\mathcal{V}_j$. It can be observed that

$$A_{i,j}A_{j,i} = \frac{P_{r,j}}{P_j} \times \frac{P_{r,i}}{P_i} = |G_{ch}|^2, \qquad (5)$$

where $G_{ch}$ represents the path loss of the channel between $\mathcal{V}_i$ by $\mathcal{V}_j$.

The conceptual block diagram of a master-slave architecture for wireless coupled oscillator synchronization is shown in Fig. 1. In this architecture, simultaneous transmitting and receiving powers is enabled by a $180^0$ hybrid balun between two front-end local oscillators. In master-slave architectures, the central master node has a reference frequency and phase, and other nodes, such as user equipments (UE), are slave nodes. The slave nodes lock their frequency to the frequency of master's node and then use a feedback to synchronize their phases to the phase of master node as well. However, in our proposed protocol there is no feedback loop from the mixer to oscillators, comparing to the architecture in Fig. 1. In other words, only the frequencies are locked through the unidirectional coupling mechanism and the resulting phase difference will be used for secret key generation.

Let $\mathcal{V}_c$ denote the central master node. The master node has a dominating power comparing to slave nodes. In terms of coupling coefficients, this translates to $A_{c,i} = 0$, for $i \neq c$. Therefore, in the steady state, the master's frequency $\omega_c$, which is also referred to as carrier frequency, and its phase remain the same, and slave nodes $\mathcal{V}_i$'s lock their frequency to $\omega_c$. Then, assuming $\omega_i$ is within the locking range, by (1)

$$\Delta\varphi \stackrel{\text{def}}{=} \tilde{\varphi}_i - \tilde{\varphi}_c = \tilde{\varphi}_i - \varphi_c = f^{-1}\big(\frac{1}{\alpha_i}\frac{P_i}{P_{r,c}}(\omega_i - \omega_c)\big), \quad (6)$$

where $\tilde{\varphi}_i$ is the phase of $\mathcal{V}_i$ in steady state, $\tilde{\varphi}_c = \varphi_c$ is assumed, $P_{r,c}$ is the power received by $\mathcal{V}_i$ at the carrier frequency $\omega_c$, $\Delta\varphi$ is referred to as the phase shift, and $\omega_i - \omega_c$ is referred to as frequency drift. Also, for the LC tank oscillators the function $f$ is the $\sin$ function and consequently $f^{-1}$ is the arc $\sin$ function [14]. The locking range of $\omega_i$ is then given by

$$|\omega_i - \omega_c| \leqslant \alpha_i \frac{P_{r,c}}{P_i} \quad (7)$$

In the RF implementation of our proposed protocol, free-running frequency $\omega_i$ serves as the initial condition, and the locked frequency $\omega_c$ and $\Delta\varphi$ are the steady state conditions. The relation between frequency drift $\omega_i - \omega_c$ and phase shift $\Delta\varphi$, stated in (6), is the main component of our protocol to provide secure communication.

### C. Physical layer security: wiretap channel

The notion of wiretap channels was introduced by Wyner [4]. In this setting, Alice wishes to send messages to Bob but her transmissions also reach an adversary Eve. Let $X \in \mathscr{X}$ denote the transmitted message by Alice, $Y \in \mathscr{Y}$ denote the received message by Bob, and $Z \in \mathscr{Z}$ denotes Eve's observation. The system is denoted by $(\mathscr{X}, \mathscr{Y}, \mathscr{Z}, \{p_{YZ|X}\})$, where $\{p_{YZ|X}(y, z|x)\}$ denotes the channel transition probabilities. By convention, capital letters denote random variables and small letters denote their instances. The goal is to design a coding scheme that makes it possible for Eve to communicate both *reliably* and *securely* with Bob. Reliability is often measured in terms of the probability of error of decoding $X$ at Bob's side. Security is usually measured in terms of the mutual information $I(X; Z)$, often normalized by the code block length.

Wyner characterized the fundamental limit of communication, referred to as secrecy capacity $C_s$, for the wiretap channel and showed achievability using random-type arguments [4]. The best known expression for the secrecy capacity $C_s$ is given in [15] as

$$C_s = \max_U \big(I(U; Y) - I(U; Z)\big), \quad (8)$$

where the maximum is taken over all random variables $U$ such that $U \to X \to (Y, Z)$ is a Markov chain. Explicit coding schemes have been shown to achieve the secrecy capacity of wiretap channels [16]. Also, a model of two-way wiretap channel was introduced in [17]. In this setting, Alice and Bob communicate over a noisy bidirectional channel while an eavesdropper observes interfering signals.

## III. Security via Coupled Dynamical Systems: The Proposed Approach and Security Analysis

In this section, we discuss our proposed protocol and show how the channel modeling can be described as a two-way wiretap channel. Then the secrecy capacity region of the underlying channel is derived under various conditions.

### A. A two-way wiretap channel: system model and the proposed protocol

We consider a system of two oscillators $\mathcal{V}_1$ and $\mathcal{V}_2$ with coupled dynamical system as described in (2). Suppose that the oscillators are initially locked at the same frequency and are synchronized. Since they are synchronized, they can agree, according to some a priori protocol to start a new session simultaneously. Suppose that $\mathcal{V}_1$, also referred to as Alice, wishes to transmit message symbol $m_1 \in \mathcal{M}_1$ to $\mathcal{V}_2$, also referred to as Bob, and $\mathcal{V}_2$ wishes to transmit message symbol $m_2 \in \mathcal{M}_2$ to $\mathcal{V}_1$. At the beginning of the new session, $\mathcal{V}_i$ maps $m_i$ to the frequency $\omega_i$. Then it switches its frequency to $\omega_i$. It is also assumed that nodes are aware of their locking range and hence, $\omega_1$ and $\omega_2$ are within the locking range. Once the oscillators switch their frequency, they enter a transition phase, also known as the *chaos* phase and then reach a steady state. The aim is to convey messages through the conditions of the oscillators in the steady state. Note that the transition time is very short, and, in practice, it is in the order of nanoseconds [12]. It is assumed that Eve does not obtain any meaningful information from the transition phase and hence, her channel observation is limited to the steady state. In fact, the randomness of coupled oscillators in chaotic phase have been studied in the literature for secure communications [18], however, this is different comparing our approach since we aim at secure communication using the conditions of steady states.

Our proposed protocol can be best described using a two-way wiretap channel model. Let $\omega_i, \tilde{\omega}, \varphi_i, \tilde{\varphi}_i$, for $i = 1, 2$, be as defined in Definition 1. Let also $\Delta\varphi = \tilde{\varphi}_2 - \tilde{\varphi}_1$ (in this network of two oscillators, only the difference between phases $\Delta\varphi$ matters in steady state). A two-way wiretap channel model associated to the proposed protocol is denoted by

$$W_{\mathcal{D}} = \big(\mathscr{X}_1, \mathscr{X}_2, \mathscr{Y}_1, \mathscr{Y}_2, \mathscr{Z}, \{p_{Y_1Y_2Z|X_1X_2}\}\big). \quad (9)$$

The inputs to $W_{\mathcal{D}}$ are $x_1 \in \mathscr{X}_1$ and $x_2 \in \mathscr{X}_2$ for Alice and Bob, respectively, and the outputs observed by $\mathcal{V}_1$, $\mathcal{V}_2$, and Eve are $y_1 \in \mathscr{Y}_1$, $y_2 \in \mathscr{Y}_2$, and $z \in \mathscr{Z}$, respectively, where

$$x_i = (\omega_i, \varphi_i), y_i = (\tilde{\omega}, \Delta\varphi), z = \big(\tilde{\omega}, h_1 e^{j\tilde{\varphi}_1} + h_2 e^{j\tilde{\varphi}_2} + n\big), \quad (10)$$

and $h_1$ and $h_2$ are received powers by Eve from Alice and Bob, respectively, reflecting their antenna and channel gain, and $n = n_x + jn_y$, where $N_x, N_y \sim \mathcal{N}(0, \sigma_n^2)$, is the additive Gaussian noise. We assume that Eve has perfect knowledge of her channel with Alice and Bob and hence, for simplicity we assume $h_1 = h_2 = 1$. Also, it is assumed that $A_{1,2}$ and $A_{2,1}$ are non-zero. The situation will be different in the next section, when one of the users is dominant. Note that $\mathcal{V}_1$ and $\mathcal{V}_2$ can perfectly measure their phase difference $\Delta\varphi$ in the feedback loop of of steady state.

*Lemma 1:* There is a one-to-one mapping between $(\omega_1, \omega_2)$ and $(\tilde{\omega}, \Delta\varphi)$. In particular, in the channel $W_{\mathcal{D}}$ defined in (9), the outputs $y_1, y_2$ are deterministic given inputs $x_1$ and $x_2$ of the channel.

*Proof:* The input-output relation for this channel model is described through the function $\mathcal{D}$ defined in Definition 1. More specifically, the following equations holds in the steady state:

$$\begin{aligned} \tilde{\omega} &= \omega_1 - \alpha_1 A_{1,2} \sin\big(\Delta\varphi\big) \\ \tilde{\omega} &= \omega_2 + \alpha_2 A_{2,1} \sin\big(\Delta\varphi\big) \end{aligned} \quad (11)$$

This system has a unique solution provided that the frequencies

$\omega_1$ and $\omega_2$ are within the locking range. In fact,

$$\tilde{\omega} = \frac{\alpha_2 A_{2,1}\omega_1 + \alpha_1 A_{1,2}\omega_2}{\alpha_2 A_{2,1} + \alpha_1 A_{1,2}}$$
$$\Delta\varphi = \text{arc sin}\, \frac{\omega_1 - \omega_2}{\alpha_2 A_{2,1} + \alpha_1 A_{1,2}} \tag{12}$$

■

Note that $\alpha_1$ and $\alpha_2$ are fixed constants and are assumed to be publicly known. However, the coupling coefficients $A_{1,2}$ and $A_{2,1}$ depend on the powers of the oscillators and can change. But in wireless settings, (5) can be invoked, which shows $A_{1,2}A_{2,1} = |G_{ch}|^2$ is fixed as long as nodes do not move. Therefore, we assume that $A_{1,2}A_{2,1}$ is known at Alice and Bob. For the analysis of security we consider different scenarios for Eve in the next subsection. With this assumption, the one-to-one mapping between $(\omega_1, \omega_2)$ and $(\tilde{\omega}, \Delta\varphi)$ derived in Lemma 1 is invoked by Alice and Bob as follows:

*Corollary 2:* Alice can recover $\omega_2$ using her channel observation $y_1$. Similarly, Bob can recover $\omega_1$ using his channel observation $y_2$.

*Proof:* By Lemma 1 $y_2$ is deterministic given the inputs. Also, Alice knows $\omega_1, \tilde{\omega}, \Delta\varphi$. Then a system of three equations given by (11) together with (5) involves three unknowns $\omega_2, A_{12}, A_{21}$ and can be solved to uniquely determine $\omega_2$. The same applies to Bob. ■

The transition probabilities $p_{Y_1Y_2Z|X_1X_2}(y_1y_2z|x_1x_2)$ are then reduced to $p_{Z|X_1X_2}(z|x_1x_2)$ provided that $y_1 = y_2 = (\tilde{\omega}, \Delta\varphi)$ with probability 1, as derived in Lemma 1. Then $p_{Z|X_1X_2}(z|x_1x_2)$, where $x_1, x_2, z$ are given in (10) is characterized in terms of distributions of $h_1$, $h_2$, and $n$.

After Alice and Bob recover the initial frequencies of the other party, i.e., $\omega_1$ and $\omega_2$, respectively, they map them back to the message symbols $m_1$ and $m_2$. The security of the protocol against Eve and the achievable rates are discussed in the next subsection.

### *B. Secrecy capacity region*

The achievable secrecy rates of the proposed protocol depends on prior information that Eve has about the oscillator constants $\alpha_1, \alpha_2$ as well as the coupling coefficients $A_{1,2}, A_{2,1}$. Since $\alpha_1$ and $\alpha_2$ are fixed constants, we assume that they are publicly known. However, the coupling coefficients $A_{1,2}$ and $A_{2,1}$ depend on the transmitted and received powers of the oscillators and can change. In practice, these parameters are difficult to estimate for Eve. To analyze the achievable rate region, we consider two extreme cases: the first case is when Eve does not have any prior knowledge and the second case is when she has full knowledge of these parameters.

*Definition 2:* Assuming that each synchronizing session is considered as one channel use, the rates $R_1$ and $R_2$ are defined as the transmission rates of Alice to Bob, and Bob to Alice, respectively. Let $C_{s,\mathcal{D}}$ denote the set of all possible achievable rate-tuples $(R_1, R_2)$ while guaranteeing information-theoretic security.

*Theorem 3:* Suppose that Eve has no prior knowledge about the coupling coefficients $A_{1,2}, A_{2,1}$. Then

$$C_{s,\mathcal{D}} = \{(R_1, R_2) : R_1 \leqslant \max_{p_{\Omega_1}} H(\Omega_1), R_2 \leqslant \max_{p_{\Omega_2}} H(\Omega_2)\},$$

where $H(.)$ is the entropy function and the maximizations are over all the possible distributions $p_{\Omega_1}(\omega_1)$ and $p_{\Omega_2}(\omega_2)$ over their locking range.

*Proof:* Note that even if Eve can perfectly estimate $\tilde{\omega}, \Delta\varphi$, given her noisy observation $z$ described in (10), then $\omega_1$ and $\omega_2$ are independent from $\tilde{\omega}, \Delta\varphi$. This holds by (12) and the assumption that Eve has no prior knowledge about $A_{1,2}, A_{2,1}$. Therefore, the secrecy capacity is just limited by the source entropies $H(\Omega_1)$ and $H(\Omega_2)$, and maximizing these over possible distributions yields the capacity region. ■

*Theorem 4:* Suppose that Eve has full knowledge of the coupling coefficients $A_{1,2}, A_{2,1}$. Then

$$C_{s,\mathcal{D}} = \{(R_1, R_2) : R_1 \leqslant \max_{p_{\Omega_1}} H(\Omega_1|\Omega_1 + N_1),$$
$$R_2 \leqslant \max_{p_{\Omega_2}} H(\Omega_2|\Omega_2 + N_2)\},$$

where the maximizations are over all the possible distributions $p_{\Omega_1}(\omega_1)$ and $p_{\Omega_2}(\omega_2)$ over their locking range, $N_i \sim \mathcal{N}(0, \sigma_{n_i})$, and $\sigma_{n_1} = \sigma_n\alpha_1 A_{1,2}$, $\sigma_{n_2} = \sigma_n\alpha_2 A_{2,1}$.

*Proof:* Since the initial phases $\varphi_1, \varphi_2$ do not affect the outputs at the two end nodes, by Corollary 2 the input-output relation of the two-way wiretap channel is reduced to

$$X_1 = Y_2 = \Omega_1, \quad X_2 = Y_1 = \Omega_2.$$

Also, by (12) and the assumption that Eve has full knowledge about $A_{1,2}, A_{2,1}$, Eve's observation $Z$ can be written in terms of $\Omega_1$ and $\Omega_2$ as

$$Z = (\Omega_1, \Omega_2) + (-\alpha_1 A_{1,2} N_y, \alpha_2 A_{2,1} N_y) \stackrel{\text{def}}{=} (Z_1, Z_2),$$

where $N_y \sim \mathcal{N}(0, \sigma^2)$. Given that $\Omega_1$ and $\Omega_2$ are independent and the particular form of output $Z$, the two-way wiretap channel essentially is split into two one-way wiretap channels for each direction. Then, for instance for the one-way wiretap channel with input and output $\Omega_1$ and Eve's observation $Z_1$, the secrecy capacity $C_{s,1}$ is derived by (8) as

$$C_{s,1} = \max_{p_{\Omega_1}}\big(H(\Omega_1) - I(\Omega_1; Z_1)\big) = \max_{p_{\Omega_1}} H(\Omega_1|Z_1),$$

which completes the proof. ■

The fundamental property of the proposed protocol that enables secure communication is that Eve is not part of the coupled network and hence, her receiver is not synchronized with $\mathcal{V}_1$ and $\mathcal{V}_2$. Therefore, on one hand, Eve has noisy observations about $\Delta\varphi$. On the other hand, Alice and Bob have perfect observation of $\Delta\varphi$ as they are synchronized and form a feedback loop in steady state. These properties of the coupled dynamical system are exploited in the proofs of Theorem 3 and Theorem 4. In particular, these results imply that regardless of Eve's physical location and how strong her receiver is the achievable rates are positive, i.e., secure communication is possible.

## IV. Secret Key Generation via Coupled Oscillators: RF System Design and Simulation

In this section, we aim at putting the proposed protocol into a setting consisting of RF local oscillators that is applicable to IoT networks. In IoT networks, it is often the case that a power-constrained IoT device communicates with a central node in order to convey some potentially sensitive information to the network. In such scenarios, as described in Section, II-B, the IoT device is a slave node and the central node is a master node in a master-slave coupled system. Then the dynamics of the master node does not change regardless of initial conditions of the slave node and hence, the two-way wiretap channel model discussed in Section III reduces to a one-way wiretap channel

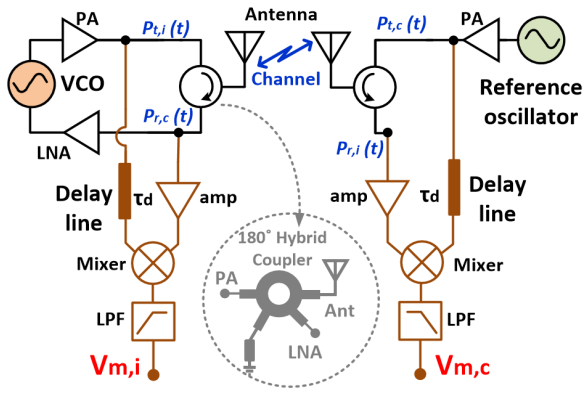


Fig. 2: The proposed secure wireless network with the protocols completely employs at the RF front-end.

model. In this case, the slave node aims at communicating securely with the master node. In fact, we have $R_2 = 0$ in Theorem 3 and Theorem 4, and $R_1$ serves a the secrecy rate of the wiretap channel.

In general, a secure communication, as proposed in Section III, requires estimation of several parameters of the wireless channel, such as the channel gain. Such estimations should be done in the back-end of the physical layer. The focus of this section is only on the RF front-end in order to show that the concept of security via coupled dynamical systems is feasible in practice. Therefore, we limit our attention to an easier task, that is to securely share a random sequence, that can serve as a secret key for encryption/decryption protocols, between the master and the slave node. The actual implementation of keyless physical layer security requires an entire design of the physical layer processing unit, including the front-end RF antennas as well as back-end processing unit including channel estimations, encoding, e.g., using nested polar codes proposed in [16], and decoding, and is left for future work. It is worth noting that generating a shared random key in physical layer only using the RF front-end antennas and without any back-end processing is by itself a new contribution of this paper and to the best of our knowledge is the first such protocol.

### A. RF system design

We propose to use a master-slave system design that exploits wireless coupled oscillator synchronization technique, as discussed in Section II-B, to provide a frequency-locked network. The proposed architectureis shown in Fig. 2. The initial free-running frequency drift between the slave and the master node, i.e., $\omega_i - \omega_c$, provides a coupling phase shift $\Delta\varphi$ between them once the slave node locks its frequency to the carrier frequency $\omega_c$ in steady state, as stated in (6). This coupling phase shift will be detected by mixing the received signal and delayed transmitted signal at each of the nodes using our proposed architecture. Note that the protocol is stated only for one session and can be performed repeatedly in order to produce a sequence of random bits.

In order to enable both nodes to measure $\Delta\varphi$ variation, the mixer at each node compares the transmitted and received signals. The mixer output voltage is denoted by $V_{m,i}$ and $V_{m,c}$ for the salve and the master node, respectively, in Fig. 2. The transmitted signal from the master node, denoted by $P_{t,c}(t)$, can be expressed as:

$$P_{t,c}(t) = |P_c| \, cos(\omega_c t + \varphi_c), \tag{13}$$

where $|P_c|$ and $\varphi_c$ are the magnitude and phase of transmitted signal and are assumed to be constant during each session. The received signal $P_{r,c}(t)$ is expressed by

$$P_{r,c}(t) = G_{ch} \, |P_c| \, cos(\omega_c t + \varphi_c - \varphi_{ch}), \tag{14}$$

where $G_{ch}$ and $\varphi_{ch}$ are the path loss and phase shift associated to the channel, respectively. The received signal at the slave node will be amplified by a low-noise amplifier (LNA) and creates a unidirectional injection path to the slave's LO. At the steady state, if the injection power is strong enough, the frequency drift of $\Delta\omega$ provides phase shift between two nodes as expressed in (6). The signal that the slave node transmits to the master is then

$$P_{t,i}(t) = |P_i| \, cos(\omega_c t + \varphi_c - \varphi_{ch} + \Delta\varphi), \tag{15}$$

where $|P_i|$ is the steady state amplitude of the slave node's signal transmitted to the master node. The received signal at the master node from the slave node is then

$$P_{r,i}(t) = G_{ch} \, |P_i| \, cos(\omega_c t + \varphi_c - 2\varphi_{ch} + \Delta\varphi). \tag{16}$$

Since there is a wave propagation delay of $\tau_d = d_{1,2}/c$, where $d_{1,2}$ is the distance between the two nodes, between the transmitting and receiving signals, a delay block of $\tau_d$ is needed at each node before the transmitted signal is mixed with the received signal. This delay is realized during an initial handshake and provides phase shift equivalent to the propagation phase shift delay $\varphi_{ch}$. The mixer's output signal at the master node, $V_{m,c}$, and the slave node, $V_{m,i}$ are the results of passing $P_{t,c}(t - \tau_d) \times P_{r,i}(t)$ and $P_{r,c}(t) \times P_{t,i}(t - \tau_d)$, respectively, through a low-pass filter (LPF) to get the DC voltage as

$$V_{m,c} = V_{m,i} = \frac{G_{ch}|P_i| \, |P_c|}{2} \, cos(\Delta\varphi - \varphi_{ch}) \tag{17}$$

Note that if the two nodes are not frequency-synchronized, the frequency-drift $\Delta\omega$ appears as a tone at the mixer's output and both nodes will understand. In our protocol, $V_{m,c}$ and $V_{m,i}$ given by (17) serve as the common source of randomness. The slave node randomly changes the frequency drift in each session resulting in randomly selected $\Delta\varphi$ using the coupling mechanism. This ensures uncorrelated random bits, after quantization, which is used to generate the secret key.

### B. Eavsdropper's model and security

In this subsection, we discuss the security of the proposed system in the previous section in the presence of an eavesdropper Eve. Then simulation results are provided assuming a standard RF receiver for Eve.

In physical layer security settings, the eavesdropper is often assumed to be passive only listening to the communication. However, in our proposed system, even if Eve can transmit power, she can only synchronize her RF system with the master node. If she tries to synchronize her receiver with the slave node to get partial information about $\Delta\varphi$, the dynamics of the slave's receiver changes and such malicious activities can be detected. In Fig. 3, a standard RF front-end receiver for Eve is considered which can be used for synchronization with the master node and receiving the transmitted signals by the master-slave network.

The received signal by Eve, denoted by$P_{r,e}(t)$, is the spatial summation of the received signals from the slave node, denoted

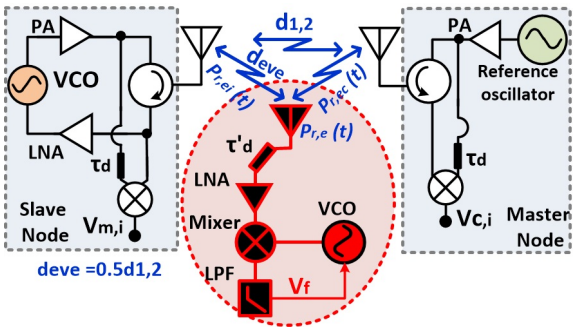


Fig. 3: The eavesdropper front-end protocol.

by $P_{r,ei}(t)$, and the master node, denoted by $P_{r,ec}(t)$. The frequency and phase of $P_{r,e}(t)$ is locked to the network. Then we have $P_{r,e}(t) = P_{r,ec}(t) + P_{r,ei}(t)$. By (15) and (13) this can be written in the complex domain as

$$P_{r,e}(t) = e^{j\omega_c t+\varphi_c+\varphi_{sl}}(h_c + h_i e^{j(\Delta\varphi-\varphi_{ch})}), \qquad (18)$$

where $h_c = G_{sl}|P_c|$ and $h_i = G_{sl}|P_i|$ are the received power magnitude by Eve from the master and the slave node, respectively, and $G_{sl}$ is the path loss in Eve's direction with propagation phase shift of $\varphi_{sl}$ assumed to be the same for both the master-slave nodes for simplicity. The phase $\Delta\varphi-\varphi_{ch}$ contains the randomness that the slave is sending to the master.

For power-constrained IoT devices, such as the slave node here, the $G_{sl}|P_i|$ term is negligible compared to the dominant term $(G_{sl}|P_c|)$. This implies that the variations in the received power by Eve, i.e., $P_{r,e}(t)$, is negligible, as $\Delta\varphi$ changes, thereby making the shared random sequence secure to her. Note that standard features of wireless channel for physical layer secret key generation, such as the gain and phase of the channel between the legitimate parties being random and unknown to Eve [6], are already included in the shared randomness in our protocol (17). On top of these features, our proposed protocol has the aforementioned additional factor that enables highly secure key generation.

### C. Simulation results in ADS

The proposed secret key generation protocol in RF front-end shown in Fig. 2 is simulated in ADS. The distance between the two nodes is assumed to be 10 m, which is suitable for indoor IoT applications. The propagation path loss for this setting is below 50 dB. The carrier frequency is set at 24 GHz, where a high efficient coupled oscillator can be implemented for an optimum design in terms of power consumption, bandwidth and locking range trade-off [14].

The average range of saturated output power of power amplifier (PA) at this frequency is 20 dBm with 25% efficiency [19]. Also, the low noise amplifier at this frequency range has an average gain of 10 dB with 5 dB noise figure. The master node PA has saturated output power around 20 dBm while the PA at slave node gets saturated around the lower output power 10 dBm for saving power consumption. In addition, the low noise amplifier (LNA) of master node, as shown in Fig. 2 has 10 dB gain while the LNA of slave node has 5 dB gain. The LO of slave node uses an LC oscillator architecture with 20% tuning range at 24 GHz. The frequency of the LO is tuned using digital-controlled switched capacitors for phase shift generation, $\Delta\varphi$, and the shared random sequence. An absolute maximum achievable phase shift $\Delta\varphi_{max}$ for an LC oscillator is $90^0$, [14]. For the key generation, for example for generating

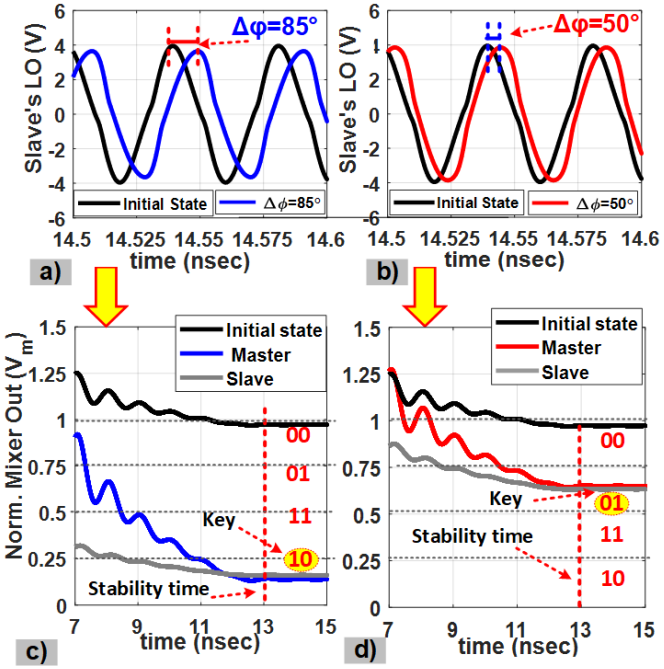


Fig. 4: Simulation results for the bits generation for the proposed front-end, a) transient results of the slave's LO for generating bits 10 of $\Delta\varphi = 85^0$, b) transient results for generating bits 01 of $\Delta\varphi = 50^0$ c) the normalized generated output voltage of the mixer at master and slave nodes for bits 10 and $\Delta\varphi = 85^0$, d) the normalized output voltage for bits 01 and $\Delta\varphi = 50^0$.

2-bits per synchronization frame, the phase shift range is quantized into four ranges. The quantization boundaries are set at $0, \text{arc cos}(3/4), \text{arc cos}(1/2), \text{arc cos}(1/4), 90^o$ and then using Gray mapping two bits, e.g., 00, 01, 11, and 10, are assigned to each range. The phase shift $\Delta\varphi$ is also reflected at the mixer's output voltages, $V_{m,c}, V_{m,i}$, as expressed in (17). For example, the phase shift, $\Delta\varphi$, in the range of $[0, \text{arc cos}(3/4)]$ is mapped to to mixer's output voltage in the range of $V_m/V_{m,max} \in [0.75, 1]$. The result for two cases of key generation, $\Delta\varphi = 85^0$ and $\Delta\varphi = 50^0$, are illustrated in Fig. 4 and are compared with the initial state to demonstrate the phase shift $\Delta\varphi$. Hence, Fig. 4 a) and b) show the transient simulation of the LO of the slave node under two phase shift locking conditions of $\Delta\varphi = 85^0$ and $\Delta\varphi = 50^0$. This corresponds to shared secret bits of 10 and 01, respectively. Note that each generated phase shift is compared with the same initial condition. The associated normalized $V_{m,i}$ of the initial phase shift falls in the range of $[0.75, 1]$. In Fig. 4 c) it is shown that the generated phase shift of $\Delta\varphi = 85^0$ results in the normalized output voltage of the slave's mixer, $V_{m,i}/V_{m,max}$, being in the range of $[0, 0.25]$, which corresponds to shared bits of 10. It is also shown that the mixer's output voltage at the master node falls in the same range and therefore, the master node obtains the same desired bit sequence of 10. The result for the generated secret bits of 01, corresponding to phase shift $\Delta\varphi = 50^0$ is also shown in Fig. 4 d). It confirms that the normalized mixer's output voltages, $V_{m,c}$ and $V_{m,i}$, at both slave and master node falls into the same region of $[0.5, 0.75]$.

The reliability of the generated key is another important factor in a secure system. In general, phase noise of oscillators in the system can adversely affect the system reliability. In

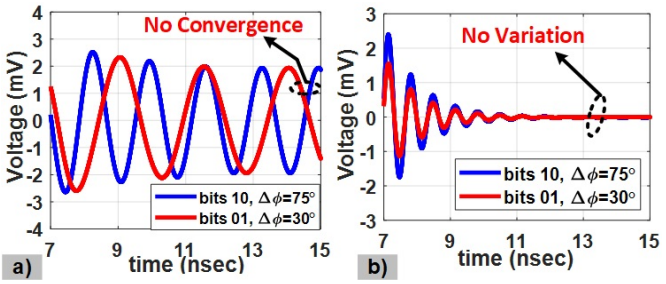


Fig. 5: The generated output voltage at eavesdropper end, a) while the eavesdropper is not synchronized to the network. b) while the LO's of eavesdropper is able to be frequency locked to network, for two case of bits generations, $\Delta\varphi = 50^0$ and $\Delta\varphi = 85^0$.

our simulations, oscillators are ideal with a single tone power spectral density and hence, they do not encounter phase noise. This results in a perfect 100% reliability of the system, i.e., the slave node and the master node get the same random sequence 100% of the time according to (17). In a practical scenario, the integrated phase noise power in this range of frequency is typically a number between $1^o$ and $5^o$ [14]. For instance, consider a typical phase noise of $4^o$, i.e., phase noise $\sim \mathcal{N}(0, \sigma^2)$, where $\sigma = 4$. Then the probability of bit mismatch between the master node and the slave node is roughly $2\times10^{-3}$.

The security of the system is also tested in the RF front-end for Eve, such as the slave LO architecture as shown in Fig. 3. Her mixer's output voltage is then shown in Fig. 5 a) and b) for unlocked and locked conditions, respectively. As shown in Fig. 5 a), the output voltage of the mixer does not converge and oscillates at the frequency equal to the frequency drift between $\omega_c$ and initial free-running frequency of Eve's LO. Fig. 5 b) shows the mixer's output of Eve under frequency locking condition. In this case, it can not identify the phase variation $\Delta\varphi$ between the master node and the slave node. It can be observed that a constant phase is observed over time by Eve, regardless of what secret bits are being shared. In other words, Eve experiences the same conditions as in Theorem 3, although for a different reason that the master node's power dominates the slave node's power. In other words, Eve is not able to follow the phase shift trend happening between the master node and the slave node. The simulation result confirms the security of the proposed system.

## V. Conclusion and Future Work

In this paper, we proposed a new framework for secure communication and secret key generation in physical layer by means of networks of coupled dynamical systems. Secure messages or secret random keys are exchanged between users through the relation of initial conditions and steady-state conditions in local dynamical system. From a information-theoretic point of view, the proposed system is modeled as a two-way wiretap channel and secrecy capacity regions are derived. Furthermore, an RF front-end system is proposed to realize this model in a wireless setting by means of local coupled oscillators. In particular, a unidirectional master-slave coupling architecture is simulated using ADS Keysight simulator and simulation results are provided.

There are several directions for future research. The information-theoretic model of the coupled network is only studied for the two-user case. A natural question is then whether the proposed model can be extended to multi-user cases such as multiple-access channels, broadcast channels etc, or new analytical methods need to be developed to this end. Furthermore, the capacity results are derived only in extreme cases and an interesting problem is to derive them under more general assumptions. Another research direction is to implement the proposed RF system design in a chipset and to see how the proposed protocol perform in a practical wireless setting. Furthermore, an in-depth study of LO phase noise will potentially lead to new analytical tools to predict the reliability of the proposed protocol.

## References


[1] Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 and UIA2; Document 2: SNOW 3G specification, 3GPP Specification 35.216.

[2] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklós, and Z. Turányi, "Design aspects of network assisted device-to-device communications," *IEEE Communications Magazine*, vol. 50, no. 3, 2012.

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[4] A. D. Wyner, "The wire-tap channel," *The bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[6] 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.

[7] 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*. ACM, 2008, pp. 128–139.

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

[9] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 1125–1133.

[10] R. Mudumbai, G. Barriac, and U. Madhow, "On the feasibility of distributed beamforming in wireless networks," *IEEE Transactions on Wireless communications*, vol. 6, no. 5, 2007.

[11] O. Simeone, U. Spagnolini, Y. Bar-Ness, and S. H. Strogatz, "Distributed synchronization in wireless networks," *IEEE Signal Processing Magazine*, vol. 25, no. 5, 2008.

[12] N. Ebrahimi and J. Buckwalter, "Robustness of injection-locked oscillators to cmos process tolerances," in *International Conference on Applications in Nonlinear Dynamics*. Springer, 2016, pp. 245–263.

[13] Y. Kuramoto, *Chemical oscillations, waves, and turbulence*. Springer Science & Business Media, 2012, vol. 19.

[14] N. Ebrahimi, P.-Y. Wu, M. Bagheri, and J. F. Buckwalter, "A 71–86-ghz phased array transceiver using wideband injection-locked oscillator phase shifters," *IEEE Transactions on Microwave Theory and Techniques*, vol. 65, no. 2, pp. 346–361, 2017.

[15] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[16] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[17] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[18] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of lorenz-based chaotic circuits with applications to communications," *IEEE Transactions on circuits and systems II: Analog and digital signal processing*, vol. 40, no. 10, pp. 626–633, 1993.

[19] A. Komijani, A. Natarajan, and A. Hajimiri, "A 24-ghz,+ 14.5-dbm fully integrated power amplifier in 0.18-/spl mu/m cmos," *IEEE Journal of Solid-State Circuits*, vol. 40, no. 9, pp. 1901–1908, 2005.

[20] H.-C. Chang, X. Cao, U. K. Mishra, and R. A. York, "Phase noise in coupled oscillators: Theory and experiment," *IEEE Transactions on Microwave Theory and Techniques*, vol. 45, no. 5, pp. 604–615, 1997.