Secret Key Generation via Pulse-Coupled Synchronization

Hessam Mahdavifar, *Member, IEEE*, and Najme Ebrahimi, *Member, IEEE*

Abstract—A novel framework for sharing common randomness and generating secret keys in wireless networks is considered. In particular, a network of users equipped with pulse oscillators (POs) and coupling mechanisms in between is considered. Such mechanisms exist in synchronized biological and natural systems, and have been exploited to provide synchronization in distributed networks. We show that naturally-existing initial random phase differences between the POs in the network can be utilized to provide *almost identical* common randomness to the users. This randomness is extracted from the synchronization time in the network. Bounds on the entropy of such randomness are derived for a two-user system and a conjecture is made for a general n-user system. Then, a three-terminal scenario is considered including two legitimate users and a passive eavesdropper, referred to as Eve. Since in a practical setting Eve receives pulses with propagation delays, she can not identify the exact synchronization time. A simplified model is then considered for Eve's receiver and then a bound on the rate of secret key generation is derived. Also, it is shown, under certain conditions, that the proposed protocol is resilient to an active jammer equipped with a similar pulse generation mechanism.

I. Introduction

Physical layer security methods provide an alternative to conventional encryption schemes in order to ensure security in wireless networks [1]. Alternatively, they can be deployed to exchange secret keys between the nodes in order to complement the higher layer encryption schemes. The fundamental works of [2], [3] established the use of common randomness for secret key generation. An important question is then how to generate common randomness at the nodes in order to utilize such protocols in wireless networks. To this end, properties of wireless links, such as channel gain and delay are shown to provide a great source for the common randomness, which have recently received significant attention [4].

There are several challenges, however, to standardize channel-based secret key generation protocols. A common assumption in such protocols is the channel reciprocity between the legitimate parties [5], [6]. This would require a perfect synchronization to avoid phase and frequency mismatch between the wireless nodes which is often hard to ensure in distributed networks [7]. Furthermore, if the nodes are static, then with no channel variations the amount of secret key bits that can be generated will be limited. To resolve this, induced randomness can be introduced in wireless nodes to increase the rate of secret key generation [8]. However, in general, such channel-based secret key generation protocols require an extra level of key reconciliation over the public channel to ensure

H. Mahdavifar and N. Ebrahimi are with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109 (email: hessam@umich.edu and najme@umich.edu).

the generated keys match at both ends. This would require an entire standardization of channel coding and modulation for this purpose which would make a barrier in deploying such methods in practice.

We recently proposed a novel approach to implementation of physical layer security by exploiting coupling dynamics in the network [9]. Such coupling dynamics are already being used for synchronization in wireless networks. In particular, we suggested to use coupled oscillators to implement the proposed approach in radio-frequency (RF) front end [9]. It is well-known that a network of RF coupled oscillators converges within nanoseconds to a steady-state condition provided that initial free-running frequencies are within a certain *locking range* [10], [11]. However, such coupling dynamics, such as electromagnetic coupling, are often limited to short distance ranges for this specific application.

In this paper, we propose to exploit synchronization mechanisms based on pulse-coupled oscillators in order to securely generate random keys in distributed networks. The proposed methods do not require extra processing, e.g., the shared randomness is almost identical at the nodes, and extra hardware to generate randomness. They also do not require channel randomness and consequently, assumptions on channel reciprocity. The naturally-existing random phase differences between the wireless nodes, prior to synchronization, would serve as the source of common randomness. It is shown, under a simplified model for the eavesdropper, that a positive-rate secret key can always be guaranteed. Furthermore, the resilience of the proposed protocol to certain jamming attacks is discussed.

The rest of this paper is organized as follows. In Section II some background on pulse-coupled oscillators and secret key generation is provided. In Section III the system model is formulated. In Section IV bounds on the entropy of shared common randomness are derived. In Section V secret key generation rate in the presence of Eve is characterized. Resilience of the proposed protocols to jamming attacks is discussed in Section VI. Finally, the paper is concluded in Section VII.

II. Preliminaries

A. Pulse coupled oscillators

A pulse oscillator (PO) is characterized using a state variable x which increases monotonically toward a normalized threshold of $x = 1$. In the model considered in [12], x evolves as $x = f(\phi)$, where ϕ is the normalized time that increases from 0 to 1. Also, $f(0) = 0$ and $f(1) = 1$. The PO transmits a pulse, which can be ideally considered as a delta function with width 0, once its state x reaches 1. Then ϕ is reset to 0. The function f is assumed to be concave down and strictly increasing, i.e.,

$f' > 0$ and $f'' < 0$ over $[0, 1]$. Also, we assume that f is semi-diffrentiable at 0 and 1, and hence f' is bounded over $[0, 1]$. An example of x in an electrical system is the charge of a capacitor in a resistor-capacitor (RC) circuit as a function of time. This matches with the Peskin model [13], which considers $f(\phi) = c(1 - e^{-\gamma\phi})$, where c, γ are constants.

Networks of coupled POs naturally exist in synchronized biological and natural systems [12], [13], and have been exploited to provide synchronization in distributed wireless networks [7]. Such a network is modeled as follows. Suppose that each node in the network is equipped with an identical PO. Let $\epsilon \in (0, 1)$ be a fixed parameter. When a node V receives a pulse from one of its neighbors, denoted by U, in the network, its dynamic changes as follows. If the current state of V, x_V, is at least $1 - \epsilon$, then it is changed to $x_V = 1$ and a pulse is transmitted by V right away. This implies that U and V are synchronized. Otherwise, when $x_V < 1 - \epsilon$, the state of V is changed to $x_V + \epsilon$, i.e., its phase ϕ is changed to $\phi' = f^{-1}(f(\phi) + \epsilon)$. This can be thought as applying an extra charge of ϵ to V's capacitor upon arrival of an external pulse. For simplicity, suppose that the network is fully connected, in which case when two nodes become synchronized, they stay synchronized moving forward. It is proved in [12] that, for any n, network synchronization occurs in a fully connected network of n identical POs, i.e., all the nodes synchronize to each other, except for a measure-zero set of initial phases $(\phi_1, \phi_2, \ldots, \phi_n)$, where ϕ_i is the initial phase of the i-th PO.

B. Secret key generation

Secret key generation protocols aim at securely establishing random keys between legitimate parties using common randomness. In this paper, we mostly focus on a case involving two legitimate parties Alice and Bob together with a passive Eve. In particular, a three-terminal source-type model is considered. Such model, in general, can be described as follows. Let $X \in \mathcal{X}$, $Y \in \mathcal{Y}$, and $Z \in \mathcal{Z}$ denote Alice's, Bob's, and Eve's observations, respectively, where $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are the corresponding alphabets. Following the convention, let capital letters denote the random variables and small letters denote their instances. In the considered source-type model, X, Y, Z are distributed according to a joint probability distribution $p_{X,Y,Z}$. The goal for Alice and Bob is to agree on a shared secret key K, based on their observations X and Y using an arbitrary number of communication rounds over a public channel with unlimited capacity. Such process is tightly related to Slepian-Wolf compression. The connection is useful for designing the so-called *key reconciliation* stage of secret key generation protocols using cosets of practical error-correcting codes. The security of K is measured in an information-theoretic sense given Eve's observation Z and all the public interactions between Alice and Bob. The two-user secret key capacity, denoted by $\mathcal{S}(X; Y|Z)$, is bounded as follows [3, Theorem 2 and 3]:

$$\max\{I(X; Y) - I(X; Z), I(Y; X) - I(Y; Z)\} \leqslant \mathcal{S}(X; Y|Z)$$
$$\leqslant \min\{I(X; Y), I(X; Y|Z)\}. \tag{1}$$

Such results were later extended to multiple-terminal scenarios [14]. Furthermore, an exact characterization was derived for a case in which only one round of communication occurs from Alice to Bob [2, Theorem 2].

III. SYSTEM MODEL

Consider a fully connected network where the network nodes are equipped with identical POs. Suppose that each PO starts with a random phase that is uniformly distributed over $[0, 1]$. Then the POs enter a dynamic system as described in Section II-A. Each node counts the number of pulses its PO transmits till network synchronization occurs. The network synchronization can be identified by individual nodes once no external pulses are received between two consecutive pulses. Each node saves this number as the common randomness. The following lemma shows that all the nodes observe the same number, up to a difference of 1. Let m_i denote the number of pulses that the node V_i, for $i = 1, 2, \ldots, n$, has transmitted so far at a given time.

Lemma 1: For any i, j, we have $|m_i - m_j| \leqslant 1$.

Proof: The proof is by noting that before V_i and V_j become synchronized, it is not possible that V_i transmits two consecutive pulses without V_j transmitting any pulse in between. In fact once V_i sends a pulse, we have $\phi_i = 0$, while $\phi_j > 0$. Now, since $f^{-1}(f(\phi) + \epsilon)$ is a strictly increasing function, we have $\phi_j > \phi_i$ which holds when pulses external to V_i and V_j arrive as well. This holds till $\phi_j = 1$, in which case V_j sends a pulse before V_i sends the next one. ∎

The lemma implies that the number of pulses that each PO counts till network synchronization occurs can serve as a source of *almost* noise-free common randomness.

Let us refer to a time-interval during which each of the POs send one pulse as a *full cycle*. Then time is split into non-overlapping and consecutive *full cycles*. Note that since the time between two consecutive pulses by each of the POs keep changing, we can not define a *full cycle* as a fixed time interval. Due to delays in propagation of pulses, an external user/eavesdropper can not exactly identify when synchronization occurs. Under propagation delays, and assuming the delays between POs is less than half the time unit, the synchronization still occurs for $n = 2$ [15], and under certain conditions for general n [15] and also for locally connected networks [16]. To this end, a certain *refractory period* ρ is defined and a PO does not update its state for ρ seconds right after it sends a pulse.

Motivated by practical considerations of propagation delays we describe Eve's observation as follows. During each *full cycle*, Eve receives n delayed pulses from the n POs. Then she can process the timings between received pulses, compare them with her estimates of propagation delays with each of the nodes, and also compare the timings with previous *full cycles*. Taking all these information into account to model Eve's receiver is not an easy task. Instead, we consider s simplified binary symmetric channel-type model for Eve as follows. Let a binary random variable S indicates whether all nodes are synchronized in the current *full cycle* or not, e.g., if synchronization occurs/has occurred, then $S = 1$ and otherwise, $S = 0$. Then Eve observes $Z = S$ with probability $1 - p$, and $Z = 1 - S$ with probability

p, for some $p \in (0, \frac{1}{2})$. Also, we consider a memoryless model, in which Eve's observation noise $Z \oplus S$ is independent across different *full cycles*.

Most of prior work on physical layer security involves a *passive* eavesdropper. In our proposed framework, an active eavesdropper may try to act as a legitimate node of the network by deploying similar pulse-coupling mechanisms in order to detect the synchronization time which will be used for key generation. However, such a malicious act can be detected by other nodes assuming they know the total number of nodes in the network. In this paper, we do not formulate such active eavesdropping methods and leave it for future work. There may exist, however, another type of adversary interested in *jamming* the proposed protocol by randomly/selectively sending pulses into the network in order to prevent synchronization. We model this scenario by assuming that the jammer has the same pulse generation mechanism as other nodes in the network, i.e., it can send at most one pulse during each *full cycle*. Also, suppose that legitimate nodes can not distinguish between pulses sent by other legitimate nodes and the jammer. We will show that synchronization may not occur and provide an upper bound on the probability of such event in Section VI.

IV. ENTROPY OF SHARED RANDOMNESS VIA PULSE-COUPLED SYNCHRONIZATION

Let M denote the random variable that represents the total number of pulses before synchronization. In order to simplify the formulation, we take the maximum of the counted pulses by POs as the shared randomness M, knowing that each of the POs has counted either M or $M-1$ pulses. At the end of this section, we discuss how such inconsistency can be resolved.

Let $\{p_i\}_{i=1}^{\infty}$ denote the probability distribution of M, where $p_i = Pr\{M = i\}$. The goal is to upper bound and lower bound p_i's in order to provide bounds on the entropy of M.

We consider only two nodes. For two oscillators, we show that, roughly speaking, the probability distribution of the number of pulses before synchronization occurs behave like a discretized exponential distribution.

Similar to [12], let

$$h(\tau) \stackrel{\text{def}}{=} f^{-1}(\epsilon + f(1-\tau)), \ R(\tau) \stackrel{\text{def}}{=} h(h(\tau)). \quad (2)$$

Let $\delta = 1 - f^{-1}(1 - \epsilon)$. Then the domain of h is $(\delta, 1)$ and the domain of R is $(\delta, h^{-1}(\delta))$.

Let $\phi, \phi + \tau$ denote the initial phases of the two POs, where $0 < \phi < \phi + \tau < 1$. If $\tau \leqslant \delta$, i.e., $f(1 - \tau) \geqslant 1 - \epsilon$, then the two POs synchronize after the next pulse. Otherwise, the phase difference, after the first pulse is sent, become $h(\tau)$, where $h(.)$ is defined in (2). Hence, $R(\tau)$ is the phase difference after the *full cycle*. Then it is shown in [12, Proposition 2.2.] that R has a fixed point τ^* that is a repeller, i.e., for $\tau < \tau^*$, $R(\tau) < \tau$, and for $\tau > \tau^*$, $R(\tau) > \tau$. Furthermore, it is shown in [12, Lemma 2.1] that $h' < -1$ and $R' > 1$ over their domains. Since f' is bounded over $[0, 1]$, it can be shown that, $\sup |h'| < \infty$, $\inf R' > 1$, and $\sup R' < \infty$ over their domains. Then let

$$\lambda_0 \stackrel{\text{def}}{=} 1/|\sup h'|, \ \lambda_1 \stackrel{\text{def}}{=} 1/\sup R', \ \lambda_2 \stackrel{\text{def}}{=} 1/\inf R', \quad (3)$$

where $0 < \lambda_1 < \lambda_2 < 1$, and $\lambda_0 > 1$ by [12, Lemma 2.1]. Let also τ^* denote the fixed point of R.

Lemma 2: There exists an increasing sequence of $\{\tau_i\}_{i=1}^{\infty}$ and a decreasing sequence of $\{\tau_i'\}_{i=1}^{\infty}$ such that

- (i) $\lim_{i \to \infty} \tau_i = \lim_{i \to \infty} \tau_i' = \tau^*$.
- (ii) For initial phase difference $\tau \in [\tau_i, \tau_{i+1}] \cup [\tau_{i+1}', \tau_i']$, we have $M = i$.

Proof: Let $\tau_0 = 0$, $\tau_0' = 1$, $\tau_1 = \delta$, $\tau_1' = h^{-1}(\delta)$, where $\delta = 1 - f^{-1}(1 - \epsilon)$. Then for $i \geqslant 1$, let $\tau_{i+1} = R^{-1}(\tau_i)$ and $\tau_{i+1}' = R^{-1}(\tau_i')$. To prove the first condition, note that τ^* is also a fixed point for R^{-1}. Also, since R is a repeller, R^{-1} is a contraction mapping. Hence, (i) follows. The proof of the second part is by induction on i. Note that if the initial phase diffrence τ is in $[0, \delta]$, then synchronization occurs after the first pulse is sent. Hence, $M = 1$. If $\tau \in [h^{-1}(\delta), 1]$, then after the first pulse the phase difference becomes $h(\tau) \in [0, \delta]$. Hence, synchronization occurs after each of the POs send one pulse and again, $M = 1$. Now, suppose that $\tau \in [\tau_i, \tau_{i+1}] \cup [\tau_{i+1}', \tau_i']$, where $i > 0$. After a *full cycle* the phase difference becomes $R(\tau)$ which belongs to $[\tau_{i-1}, \tau_i] \cup [\tau_i', \tau_{i-1}']$, and the proof follows by induction hypothesis. ∎

Let

$$a_i = \tau_i - \tau_{i-1}, \ b_i = \tau_{i-1}' - \tau_i', \quad (4)$$

for any $i \geqslant 1$, where $\{\tau_i\}$ and $\{\tau_i'\}$ are as introduced in the proof of Lemma 2. Then we have the following corollary.

Corollary 3: Assuming that the initial phase difference is uniform we have $p_i = a_i + b_i$, where $p_i = Pr\{M = i\}$.

Lemma 4: For any $i \geqslant 2$, $\lambda_1 p_{i-1} \leqslant p_i \leqslant \lambda_2 p_{i-1}$, where λ_1, λ_2 are defined in (3).

Proof: Let $\tau = \tau_i$, for some $i \geqslant 2$, where $\{\tau_i\}$ is defined in the proof of Lemma 2. Then we have

$$a_i = \tau - R(\tau), a_{i-1} = R(\tau) - R(R(\tau)),$$

where $\{a_i\}$ is defined in (4). Since R is a continuous and differentiable function, then by the mean value theorem, there exists $c \in [\tau, R(\tau)]$ such that

$$R'(c) = \frac{R(R(\tau)) - R(\tau)}{R(\tau) - \tau} = \frac{a_{i-1}}{a_i}.$$

Then by definition of λ_1, λ_2 in (3) we have

$$\lambda_1 \leqslant \frac{a_i}{a_{i-1}} \leqslant \lambda_2.$$

The same argument can be applied to b_i's and then the lemma follows by Corollary 3. ∎

Note that Lemma 4 implies that the distribution of M resembles a discretized exponential distribution, i.e., p_i decays exponentially fast as i grows. In particular, it is shown in the next proposition that M has a bounded entropy. It is assumed that $p_1 < 1/e \approx 0.37$. If p_1, and possibly p_2, are greater than $1/e$, then we can exclude them, apply the following proposition to the rest of p_i's, and add the terms corresponding to p_1 and p_2 in $H(M)$ as constants.

Proposition 5: In the two-user pulse coupling system, we have

$$\frac{g(c)}{1 - \lambda_1} + \frac{cg(\lambda_1)}{(1 - \lambda_1)^2} \leqslant H(M) \leqslant \frac{g(c)}{1 - \lambda_2} + \frac{cg(\lambda_2)}{(1 - \lambda_2)^2},$$

where $g(x) = -x \log x$, λ_1, λ_2 are defined in (3), and $c = p_1 = 1 + \delta - h^{-1}(\delta)$.

Proof: By Lemma 4 we have $p_1\lambda_1^{i-1} \leqslant p_i \leqslant p_1\lambda_2^{i-1}$. Then the proof follows by the definition of entropy function $H(.)$ and noting that $g(x) = -x\log x$ is increasing for $x \leqslant 1/e$. ∎

Remark 1. We conjecture that in a general set-up consisting of n POs, $H(M) = O(\log n)$. More specifically, we believe it can be shown that after $O(n)$ *full cycles* the POs are split into $O(1)$ clusters, each consisting of synchronized POs. Then one can only analyze the entropy of shared randomness involving a constant number of POs and use the bound on the entropy of sum of two random variables to prove the conjecture.

Remark 2. In order to resolve the possible difference of 1 between counted pulses by the two users, a simple key reconciliation method can be deployed as follows. Users will exchange their observations modular 3. Then if there is a difference, the user with smaller observation increments it by 1 which would make it an error-free common randomness. In general, if we want to recover from a larger difference, up to a certain d, between observations, e.g., due to an initial phase difference of more than one unit of time, the same procedure can be deployed. In that case, users exchange their observation modular $2d + 1$ using which reconciliation can be done.

V. SECRET KEY RATE

A three-terminal model, as described in Section II-B, is considered. The common randomness M between Alice and Bob is generated according to the process discussed in Section IV with a slight modification as follows. In order to avoid long waiting times, Alice and Bob set a fixed threshold $\tilde{m}$. They continue to send pulses until each of them sends $\tilde{m}$ pulses, regardless of whether synchronization has occurred or not, at which point they stop the current *session*. Then they may start a new *session* with new initial random phases, e.g., by simply reseting their POs, and the same process will be repeated. If synchronization has occurred at some point during the *session*, then the common randomness M is the number of pulses till that point. Otherwise, $M = \tilde{m}$. In other words, the probability distribution $(p_1, p_2, \dots)$, characterized in Corollary 3, is truncated as follows. For $i = 1, 2, \dots, \tilde{m} - 1$, $Pr\{M = i\} = p_i$, and $Pr\{M = \tilde{m}\} = \sum_{i=\tilde{m}}^{\infty} p_i$. Also, for $i > \tilde{m}$, $Pr\{M = i\} = 0$. Furthermore, we assume that the common randomness M is identical at Alice and Bob, i.e., $X = Y = M$, and $\mathscr{X} = \mathscr{Y} = \{1, 2, \dots, \tilde{m}\}$.

Remark 3. In order to recover from possible differences between Alice's and Bob's observations a procedure, as discussed in Remark 2, can be deployed. Since $M \bmod (2d+1)$ is then revealed to Eve, Alice and Bob take $\lfloor M/(2d+1) \rfloor$ as the common randomness. The bounds provided in this section can be also modified to reflect this extra step, however, we keep assuming M as the common randomness to simplify derivations.

Eve's observation Z, according to the model described in Section II-A, is as follows. Let $S = \{S_i\}_{i=1}^{\tilde{m}}$ denote the synchronization indicator sequence, where S_i is the indicator of synchronization in the i-th *full cycle*, as defined in Section III, for $i = 1, 2, \dots, \tilde{m}$. Note that if $M = m$, then we have $S_i = 0$, for $1 \leqslant i < m$, and $S_i = 1$, for $m \leqslant i \leqslant \tilde{m}$. Then

$Z = (Z_1, Z_2, \dots, Z_{\tilde{m}})$, where $Z_i = S_i \oplus Q_i$, and Q_i's are i.i.d. with $\text{Ber}(p)$, where p is the model parameter described in Section III.

In general, when $X = Y = M$ in the three-terminal model, the lower and upper bounds in (1) match. Hence, the secret key capacity, which can be denoted by $\mathcal{S}(M|Z)$, is given as follows:

$$\mathcal{S}(M|Z) = H(M) - I(M; Z) = H(M|Z). \tag{5}$$

Since the complexity of the exact computation of $H(M|Z)$ is exponential in terms of $\tilde{m}$, we provide a lower bound on $\mathcal{S}(M|Z)$ in terms of the parameters of the coupling system as well as Eve's parameter p. The lower bound shows that the secret key rate $\mathcal{S}(M|Z)$ is strictly positive regardless of the choice for $\tilde{m}$. The following lemma is useful to derive such a bound.

Lemma 6: For any $m_1, m_2 \in \{1, 2, \dots, \tilde{m}\}$ we have

$$\frac{Pr\{Z|M = m_1\}}{Pr\{Z|M = m_2\}} \geqslant \left(\frac{p}{1-p}\right)^{|m_1 - m_2|},$$

for any instance of Z.

Proof: Let $\{s_{i,j}\}_{i=1}^{\tilde{m}}$ denote the synchronization indicator sequences for m_j, $j = 1, 2$. Also, note that

$$Pr\{Z|M = m_j\} = \Pi_{i=1}^{\tilde{m}} Pr\{Z_i|S_i = s_{i,j}\}.$$

This together with noting that $\{s_{i,1}\}$ and $\{s_{i,2}\}$ differ in exactly $|m_1 - m_2|$ positions, and the assumption on the noise $Q_i = Z_i \oplus S_i$ (i.i.d. with $\text{Ber}(p)$) complete the proof. ∎

Proposition 7: For the considered three-terminal model with common shared randomness M the secret key rate $\mathcal{S}(M|Z)$ is lower bounded as

$$\mathcal{S}(M|Z) \geqslant \log\min\{\frac{1}{1-\delta_1}, 1 + (1-\lambda_2)\delta_2\frac{1-\delta_2^{\tilde{m}}}{1-\delta_2}\}, \tag{6}$$

where $\delta_1 = \lambda_1 p/(1-p)$, $\delta_2 = \lambda_2^{-1} p/(1-p)$, and λ_1, λ_2 are defined in (3).

Proof: For any $m_0 \in \{1, 2, \dots, \tilde{m}\}$, using the Bayes' rule and the law of total probability we have

$$Pr\{M = m_0|Z\} = \frac{Pr\{Z|M = m_0\}Pr\{M = m_0\}}{\sum_{m=1}^{\tilde{m}} Pr\{Z|M = m\}Pr\{M = m\}}. \tag{7}$$

By plugging the bounds from Lemma 6 and Lemma 4 in (7), for $m_0 \in \{1, 2, \dots, \tilde{m} - 1\}$ we have

$$Pr\{M = m_0|Z\} \leqslant 1/\sum_{i=0}^{\infty} \lambda_1^i (p/1-p)^i = 1 - \delta_1, \tag{8}$$

for any instance of Z. And, similarly, for $\tilde{m}$ we have

$$Pr\{M = \tilde{m}|Z\} \leqslant 1/\left(1 + \sum_{i=1}^{\tilde{m}-1} \lambda_2^{-i}(p/1-p)^i(1-\lambda_2)\right)$$
$$= 1/\left(1 + (1-\lambda_2)\delta_2\frac{1-\delta_2^{\tilde{m}}}{1-\delta_2}\right), \tag{9}$$

where we again used bounds from Lemma 6 and Lemma 4 in (7) while noting that $Pr\{M = \tilde{m}\} = \sum_{i=\tilde{m}}^{\infty} p_i$.

As stated in (5), $\mathcal{S}(M|Z) = H(M|Z)$. Note that for any two random variables M, Z, we have

$$H(M|Z) \geqslant -\log\max_{m,z} Pr\{M = m|Z = z\}.$$

This together with bounds in (8) and (9) complete the proof. ∎

Remark 4. Note that the second term over which minimization of (6) takes place is increasing with $\tilde{m}$. Therefore, the lower bound provided in Proposition 7 is non-decreasing with $\tilde{m}$. Hence, the secret key rate, in terms of bits/session, is strictly positive regardless of $\tilde{m}$ and is actually bounded away from 0 as $\tilde{m} \to \infty$. Also, there is a certain threshold such that increasing $\tilde{m}$ beyond that threshold does not improve the lower bound of (6). It would be interesting to see if the actual secret key rate $\mathcal{S}(M|Z)$ exhibits the same behavior.

Remark 5. Here, we do not discuss a coding method for Alice and Bob to extract a secure key K from M in an information-theoretic sense, i.e., $I(K; Z)$ being small. In particular, since $H(M)$ is bounded, as shown in Section IV, there is no asymptotic behavior for such information-theoretic arguments. One has to consider several *sessions* between Alice and Bob and then apply standard key extraction techniques, e.g., using polar codes [17], to a sequence of shared symbols M_j's. Alternatively, an *ad-hoc* solution is also possible by simply applying a linear transform, e.g. a polarization matrix [18], to the sequence $\{S_i\}_{i=1}^{\tilde{m}}$ in one session. Although S_i's are not independent, an argument similar to [19, Proposition 3] can be used to show that compression of M and also extracting a secure K can be done to some extent (Again, no concrete results can be made here as there is no asymptotic behavior). Such solutions are low complex and can be locally and identically performed by Alice and Bob without any need for further communication. The details are left for future work.

VI. RESILIENCE AGAINST JAMMING ATTACKS

Consider a two-user scenario where legitimate users want to establish synchronization and to extract a common randomness, as discussed in Section IV. Suppose that there is a jammer present in the network equipped with a similar PO, as modeled in Section III.

Let λ_0 be as defined in (3). This parameter is frequently used throughout this section. Let τ denote the phase difference between the two POs at the beginning of a *full cycle*. If there is no jammer, then the phase difference becomes $R(\tau)$ at the end of the *full cycle*, as discussed in Section IV. In the presence of a jammer, the dynamic may change as will be described in the following lemma. Note that in the remaining of this section we discard specifying the domains of h and R and assume the following: if $\tau > 1$, then $h(\tau)$ is replaced by 0; if $\tau > h^{-1}(\delta)$, then $R(\delta)$ is replaced by 1; if $\tau < \delta$, then $h(\tau)$ is replaced by 1 and $R(\tau)$ is replaced by 0, where δ is defined in Section IV as $\delta = 1 - f^{-1}(1 - \epsilon)$.

Lemma 8: Let τ, τ' denote the phase differences at the beginning and at the end of a *full cycle*. Then

$$\tau' \in \left[h\left(\lambda_0 h(\tau)\right), \max\{R(\lambda_0 \tau), \lambda_0 R(\tau)\} \right],$$

where h, R, and λ_0 are defined in (2), and (3), respectively.

Proof: There are three possible scenarios for the arrival time of jammer's pulse during one *full cycle* in terms of how many pulses, either 0, 1, or 2 pulses, have been sent in that cycle. Consider the first case where jammer's pulse arrives at a time t before any of the two POs send a pulse. Let $\phi, \phi + \tau$

denote the phases of the two POs at time t. Then the phases change to $h(1 - \phi)$, $h(1 - \phi - \tau)$ right after t (Note that h is a decreasing function with $h' < -1$). Since h is a continuous and differentiable function, then by the mean value theorem, there exists $c \in [\phi, \phi + \tau]$ such that

$$1 < \frac{h(1 - \phi - \tau) - h(1 - \phi)}{\tau} = -h'(1 - c) \leqslant \lambda_0.$$

Hence, the phase difference τ is scaled by at most a factor of $\lambda_0 > 0$. Since $R = h(h(.))$ is an increasing function, the phase τ' at the end of *full cycle* is at most $h\left(h(\lambda_0 \tau)\right) = R(\lambda_0 \tau)$. Similarly, if t is after both users have sent a pulse, then τ' is at most $\lambda_0 h\left(h(\tau)\right) = \lambda_0 R(\tau)$. And if t is after one of the users has sent a pulse, then τ' is actually reduced and lower bounded by $h\left(\lambda_0 h(\tau)\right)$. This completes the proof. ∎

Let $R_\lambda(\tau) \stackrel{\text{def}}{=} h\left(\lambda h(\tau)\right)$. Then we have the following lemma.

Lemma 9: There exists at most one fixed point for each of the functions $R_\lambda(\tau)$, $\lambda R(\tau)$, and $R(\lambda \tau)$, for any $\lambda > 1$. Furthermore, if $R(\lambda \delta) < \delta$, then $R_\lambda(\tau)$, $\lambda R(\tau)$, and $R(\lambda \tau)$ have exactly one fixed point.

Proof: Since $R' > 1$ and $h' < -1$ over their domains, the derivatives of $R_\lambda(\tau)$, $\lambda R(\tau)$, and $R(\lambda \tau)$ are also greater than 1 over their domains. Hence, the first part follows. Now, let $F(\tau) = R(\lambda \tau) - \tau$. Note that the domain of R is $(\delta, h^{-1}(\delta))$ and it can be observed that $F(h^{-1}(\delta)) > 0$. Now, if $R(\lambda \delta) < \delta$ (equivalent to $F(\delta) < 0$) and since $F' > 0$, then there exists exactly one root for F which becomes a fixed point for $\lambda R(\tau)$. Since F is an increasing function, then $F(\delta/\lambda) < F(\delta) < 0$ or equivalently $\lambda R(\delta) < \delta$. Therefore, $\lambda R(\delta)$ has a unique fixed point using the same argument. Also, note that $R_\lambda(\delta) < \delta$ and it can be observed that $R_\lambda(h^{-1}(\delta)) > h^{-1}(\delta)$ is equivalent to $R(\lambda \delta) < \delta$ since h is a decreasing function. Hence, $R_\lambda(\delta)$ has a unique fixed point using the same argument. ∎

Corollary 10: Suppose that $R(\lambda \delta) < \delta$ and let τ_λ^* denote the fixed point for $R(\lambda \tau)$. Then $\lambda \tau_\lambda^*$ is the fixed point for $\lambda R(\tau)$ and $h^{-1}(\tau_\lambda^*)$ is the fixed point for $R_\lambda(\tau)$.

The following proposition is the main result of this section which shows that synchronization always occurs, under certain conditions, in the presence of jamming attacks.

Proposition 11: If $R(\lambda_0 \delta) < \delta$, where λ_0 is defined in (3), then there exists a $\tau^* \in (\delta, h^{-1}(\delta))$ such that for any initial phase difference τ with $\tau \notin (\tau^*, h^{-1}(\tau^*))$, synchronization always occurs in the presence of the jamming attack.

Proof: Let τ^* denote the fixed point of $R(\lambda_0 \tau)$, which exists by Lemma 9. Then for any λ, where $1 < \lambda < \lambda_0$, the fixed points of $R_\lambda(\tau)$, $\lambda R(\tau)$, and $R(\lambda \tau)$ belong to $(\tau^*, h^{-1}(\tau^*))$. Furthermore, since the derivatives of $R_\lambda(\tau)$, $\lambda R(\tau)$, and $R(\lambda \tau)$ are also greater than 1, they are repeller functions. In particular, for $\tau > h^{-1}(\tau^*)$, we have $R_\lambda(\tau) > \tau$, and for $\tau < \tau^*$, we have $\max\{R(\lambda_0 \tau), \lambda_0 R(\tau)\} < \tau$. The proposition follows by this together with Lemma 8. ∎

The result of Proposition 11 can be also interpreted as follows. Assuming that $R(\lambda_0 \delta) < \delta$ holds, then synchronization occurs with probability at least $1 - h^{-1}(\tau^*) + \tau^*$, where τ^* is the fixed point of $R(\lambda_0 \tau)$. Then the results of Section IV and Section V can be extended to cases where a jammer is also present. In fact, we expect that these results will be scaled by a constant factor as the probability of synchronization and

perhaps a modification of the parameters of the distribution of shared randomness is also needed.

VII. CONCLUSION

In this paper, motivated by practical limitations of secret key generation protocols, we proposed to exploit readily available synchronization mechanisms in wireless networks, in particular pulse-coupled synchronization, for sharing common randomness between legitimate parties. The initial random phases of the POs deployed by the parties serve as the source of common randomness. Bounds on the entropy of such randomness, which is almost identically observed by the users, are derived for a two-user system. Furthermore, a three-terminal scenario is considered including two legitimate parties and a passive Eve. Eve's receiver is modeled and then a bound on the secret key rate is derived. Also, it is shown that, under certain conditions, the proposed protocol is resilient to active jamming with similar pulse generation mechanism.

There are several directions for future work. It is interesting to generalize the result of Section IV to networks with more than two users and, in particular, to check the validity the conjecture discussed in Remark 1. In a more abstract setup and assuming a central user, this relates to the problem of distributed secret sharing in multi-user scenarios [20]. The eavesdropper's model, described in Section III and investigated in Section V, can be extended to take into account memory, imperfectness of pulses, synchronization error, etc. The model for the jamming attack, discussed in Section VI, can be also extended to consider more general attacks such as a fixed-power interference, sending higher frequency pulses, etc. Furthermore, implementing the proposed system in front-end antennas, e.g., using setups similar to [21], is another interesting future direction.

REFERENCES

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

[2] 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.

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE transactions on information theory*, vol. 39, no. 3, pp. 733–742, 1993.

[4] 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.

[5] 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.

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

[7] 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.

[8] N. Aldaghri and H. Mahdavifar, "Fast secret key generation in static environments using induced randomness," *Proceedings of IEEE Globcom*, Abu Dhabi, UAE, Dec 2018.

[9] N. Ebrahimi, H. Mahdavifar, and E. Afshari, "A novel approach to secure communication in physical layer via coupled dynamical systems," *Proceedings of IEEE Globcom*, Abu Dhabi, UAE, Dec 2018.

[10] 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.

[11] 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.

[12] R. E. Mirollo and S. H. Strogatz, "Synchronization of pulse-coupled biological oscillators," *SIAM Journal on Applied Mathematics*, vol. 50, no. 6, pp. 1645–1662, 1990.

[13] C. S. Peskin, "Mathematical aspects of heart physiology," *Courant Inst. Math*, pp. 268–278, 1975.

[14] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[15] U. Ernst, K. Pawelzik, and T. Geisel, "Synchronization induced by temporal delays in pulse-coupled oscillators," *Physical review letters*, vol. 74, no. 9, p. 1570, 1995.

[16] L. Ferrari, A. Scaglione, R. Gentz, and Y.-W. P. Hong, "Convergence results on pulse coupled oscillator protocols in locally connected networks," *IEEE/ACM Trans. on Networking*, vol. 25, no. 2, pp. 1004–1019, 2017.

[17] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.

[18] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[19] 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.

[20] M. Soleymani and H. Mahdavifar, "Distributed multi-user secret sharing," *arXiv preprint arXiv:1801.04384*, 2018.

[21] N. Ebrahimi, B. Yektakhah, K. Sarabandi, H.-S. Kim, D. D. Wentzloff, and D. Blaauw, "A novel physical layer security technique using master-slave full duplex communication," *Proceedings of IEEE/MTT-S International Microwave Symposium (IMS)*, Boston, MA, June 2019.