Full-Duplex vs. Half-Duplex Secret-Key Generation

Hendrik Vogt, Aydin Sezgin
Ruhr-Universität Bochum, Germany
{hendrik.vogt, aydin.sezgin}@rub.de

Abstract—Secret-key agreement from reciprocal wireless channels has been considered a valuable supplement for security at the physical-layer (PHYSEC). On the one hand, full-duplex (FD) communication is regarded as one of the key technologies in future 5G systems. On the other hand, the success of 5G depends, among other things, on the ability to allow for secure communication. However, most key agreement models are based on half-duplex (HD) setups. Therefore, in this work, we propose representations of key generation models in both HD and FD modes. We analyze the performance of FD vs. HD modes by utilizing the key-communication function of secret-key agreement. It turns out that, for the application of key agreement, the FD approach enables advantages over the conventional HD setups. In particular, we derive a condition that guarantees improved performance of FD over HD mode in the high SNR regime.

I. INTRODUCTION

The emerging deployment of devices with wireless connectivity in large numbers — commonly denoted as the Internet of Things (IoT) — has attracted significant attention in research community. The communication between the nodes can be partitioned into two types, i.e., full-duplex (FD) and half-duplex (HD). In FD, also known as two-way communication, nodes can simultaneously transmit and receive information on the same frequency band. From practical viewpoint, a number of works (see [1], for instance), have proposed functional FD prototypes. Due to the close proximity of transmitter and receiver antennas, simultaneous transmission and reception of information emanates a key issue of self-interference (SI). Characterization and cancellation of SI is one of the main issue in the practical implementation of FD systems [2].

In key agreement systems, a node Alice encrypts the message with the help of a secret key and broadcasts it over the network. The second legitimate node, Bob, knows the secret key and can easily decode the confidential message, while the eavesdropper Eve cannot. From information-theoretic viewpoint, Ahlswede et al. [3] study the problem of secret key agreement in bi-directional systems. They coined the notion of a source-type model, where all users observe information from jointly random sources. Alice and Bob utilize these sources in order to distill an advantage over Eve. More specifically, these models require some amount of public communication by Alice and Bob, since it is shown to be beneficial in terms of an advantage. The maximum rate at which secret keys can be generated is called as secret-key capacity.

This work was funded by the Federal Ministry of Education and Research (BMBF) of the Federal Republic of Germany (Förderkennzeichen 16 KIS 0030, Prophylaxe). The authors alone are responsible for the content of the paper.

The source-type model by [3] has gained much attention in the research community and is extended to study a number of channels, namely, rate-limited public communication for Gaussian sources [4], and Gaussian vector sources [5].

In practice, the main challenge is how to distribute these keys securely. In general, the channel state between two legitimate nodes, i.e., Alice-to-Bob and Bob-to-Alice is known to be largely reciprocal, while the channel from both legitimate nodes to Eves is not necessarily the same. Thus, Alice and Bob can utilize the advantage of common information to distill a secret key which can be used to secure information. The model that we study in this work consists of two phases, namely probing of the channel state and subsequently, Alice performs a single, one-way public communication to Bob under a transmission rate constraint. This is sometimes referred to as one-shot key reconciliation. It is interesting to note that, for this setup, the secret-key capacity is known [6]. The key ingredients in this work are the HD and FD representations of the aforementioned model. We believe that in practical implementation of such systems, it is important to understand the trade-off between HD and FD mode for secret-key agreement systems. We establish a condition under which the FD mode outperforms the HD mode in high signal-to-noise ratio (SNR) regimes. To the best of our knowledge, no work in existing literature has focused on the secret-key generation problem from reciprocal wireless channel viewpoint under rate-constraint public communication with FD capabilities.

The paper is structured as follows. In Section II the system models of both HD and FD modes are introduced. Section III defines the secret-key rate, more specifically, the key-communication function, necessary for evaluation of system performance. In section IV the main contributions are derived and discussed. Finally, section V concludes this paper by summarizing its contribution.

We will use following notation throughout this work. All vectors are denoted by small bold-face letters \( \mathbf{x} \), and matrices by capital bold-face letters \( \mathbf{A} \). The operators \( \exp \) and \( \ln \) denote the exponent and logarithm with respect to base \( e \), while \( \exp_2 \) and \( \log_2 \) are used for base 2.

II. SYSTEM MODEL

The system model is depicted in Fig. 1. We assume that the legitimate nodes Alice and Bob and the passive eavesdropper Eve have one antenna each. All channels comply with a real-valued flat-fading model. Furthermore, the channel \( h_{ab} \) of direction Alice-to-Bob is not fully correlated to the reverse channel \( h_{ba} \).
We assume that the channel process behaves in a block-fading fashion, i.e., during one coherence block the channel coefficients remain constant and change to independent fading fashion, i.e. during one coherence block the channel observations are i.i.d. source observations. As mentioned before, due to the imposed channel rate constraint, the transmission of a signal from Alice-to-Bob cannot achieve the capacity of a fast-fading channel. Therefore, Alice utilizes the remaining $(1 - \beta)n$ coherence blocks to send a public message to Bob by communication rate $R_p$. Since the channel demands a rate constraint, Alice and Bob need to quantize their observations. As mentioned before, due to the imposed channel rate constraint, the transmission of a signal from Alice-to-Bob is done in the spirit of Wyner-Ziv coding. We assume that Bob has only imperfect CSI available. Subsequently, the communication cannot achieve the capacity of a fast-fading channel with perfect CSI \cite{6}, but rather a lower bound on it. The channel state variable is given by

\begin{equation}
\hat{h}_{ab} = \hat{h}_{ab} + \hat{h}_{ab},
\end{equation}

where $\hat{h}_{ab}$ is the part of the channel state that Bob estimates and uses as side information, and $\hat{h}_{ab} \sim \mathcal{N}(0, \sigma^2_{\text{mmse}})$ is the estimation error.

1) HD mode

The channel input-output relationship from Alice-to-Bob is given by

\begin{equation}
y_c = h_{ab}x_c + n_c,
\end{equation}

where $x_c \sim \mathcal{N}(0, \text{snr})$ independent of $h_{ab}$, and $n_c \sim \mathcal{N}(0, 1)$ is independent noise. Similarly as in the estimation phase, Bob
obtains a noisy version of the channel state from probing, depicted in eq. (15).

2) **FD mode**

As previously noted, in FD mode the communication terminals are harmed by self-interference, and thus Bob receives

\[ y_c = h_{ab}x_c + \alpha \sqrt{\text{snr}} \cdot n_{lc} + n_c, \] (5)

where \( x_c \sim \mathcal{N}(0, \text{snr}) \), \( n_{lc} \sim \mathcal{N}(0, 1) \) is the residual noise after interference cancellation and \( n_c \sim \mathcal{N}(0, 1) \) is independent noise. Furthermore, Bob obtains imperfect channel knowledge from probing like in the estimation phase, depicted in eq. (2b).

**C. Key generation**

Following the estimation and communication phase, Alice computes a secret key from her observations \( x^{sn} \), Bob obtains a key from the public message and the observations \( y^{sn} \), while Eve tries to reconstruct the key from observations \( z^{sn} \) and the public message. The performance is measured by the probability of error and both strong uniformity and secrecy [8], where \( R_{sk} \) denotes the secret-key rate satisfying the aforementioned conditions.

**Definition 1.** The secret-key rate with respect to a certain public communication rate, is denoted by the key-communication function \( R_{sk} \) \( (R_p) \).

### III. COMPUTATION OF RATES

In this section, we derive the rates that serve as metric for performance evaluation.

**A. Communication rates**

We now provide the description to compute the communication rate expression for both HD and FD modes.

1) **HD mode**

Following [9], the communication rate per block between Alice-to-Bob channel is given by

\[ I(x_c; y_c | \hat{h}_{ab}) = h(x_c) - h(x_c | y_c, \hat{h}_{ab}). \] (6)

Furthermore, Bob performs LMMSE estimation of the channel state from probing. By using (1b), the estimation error yields

\[ \hat{\sigma}_{\text{mmse}}^2 = 1 - \frac{E[h_{ab}^2]}{E[y^2]} = \frac{1}{1 + \text{snr}}. \] (7)

Subsequently, from (6) by skipping the details exhibited in [9], we get

\[ I(x_c; y_c | \hat{h}_{ab}) \geq \frac{1}{2} \log_2 \left( 1 + \frac{\text{snr}(1 + \text{snr})}{1 + 2 \text{snr}} \right). \] (8)

The achievable communication rate is given by averaging (8) over all possible realizations of \( \hat{h}_{ab} \) and is given by

\[ R_p^{(HD)} = \frac{(1 - \beta)}{4} E_{\hat{h}_{ab}} \left[ \log_2 \left( 1 + \frac{\text{snr}(1 + \text{snr})}{1 + 2 \text{snr}} \right) \right]. \] (9)

In what follows, we provide an upper bound on the communication rate of (9). Recall from (3) that the estimated channel state has a distribution \( \hat{h}_{ab} \sim \mathcal{N}(0, \sigma_{\text{mmse}}^2) \). Let

\[ c_{\text{HD}} := \frac{\text{snr}(1 + \text{snr})}{1 + 2 \text{snr}}, \]

then we can write (9) as

\[ R_p^{(HD)} \leq \frac{1 - \beta}{4} E_{\hat{h}_{ab}} \left[ \log_2 \left( 1 + c_{\text{HD}} \hat{h}_{ab}^2 \right) \right] \leq \frac{1}{4} \left( 1 - \beta \right) \log_2 \left( 1 + \text{snr} \frac{\sigma_{\text{mmse}}^2 + \alpha^2}{1 + 2 \text{snr}} \right) = (10, (10)) \]

where \((a)\) follows by Jensen’s inequality since \( \log_2 (1 + \text{snr}) \) is a concave function, and \((b)\) follows from (7).

2) **FD mode**

By following the similar reasoning like in HD mode, we have

\[ I(x_c; y_c | \hat{h}_{ab}) \geq \frac{1}{2} \log_2 \left( 1 + \frac{\text{snr}}{1 + (\sigma_{\text{mmse}}^2 + \alpha^2) \text{snr}} \right). \] (11)

Bob experiences self-interference when estimating \( \hat{h}_{ab} \) from channel probing like in (2b), so the error from LMMSE estimation is

\[ \sigma_{\text{mmse}}^2 = \frac{1 + \alpha^2 \text{snr}}{1 + \text{snr}(1 + \alpha^2)}. \] (12)

In contrast to HD mode, neither Bob nor Alice need to split frequency or time resources for transmission or reception, so they are able to support twice the rate compared to the HD case [10]. Subsequently, the supported communication rate is

\[ R_p^{(FD)} = \frac{(1 - \beta)}{2} E_{\hat{h}_{ab}} \left[ \log_2 \left( 1 + \frac{\text{snr}}{1 + (\sigma_{\text{mmse}}^2 + \alpha^2) \text{snr}} \right) \right]. \] (13)

We derive a lower bound on (13). The idea is following the line of (11). First, a shorter form

\[ c_{\text{FD}} := \frac{\text{snr}(1 + \text{snr}(1 + \alpha^2))}{1 + 2 \text{snr} + \alpha \text{snr}(1 + \text{snr})}, \] (14)

is introduced, as a consequence, we have

\[ R_p^{(FD)} = \frac{1 - \beta}{2} E_{\hat{h}_{ab}} \left[ \log_2 \left( 1 + c_{\text{FD}} \hat{h}_{ab}^2 \right) \right] \quad (a) \leq \frac{1}{2} \log_2 \left( 1 + c_{\text{FD}} \exp \left( \ln \hat{h}_{ab}^2 \right) \right) \]

\[ \geq \frac{1}{2} \log_2 \left( 1 + c_{\text{FD}} \exp \left( E_{\hat{h}_{ab}} \left[ \ln \hat{h}_{ab}^2 \right] \right) \right), \] (15)
where \((a)\) utilizes the fact that \(\log_2(1 + ce^x)\) is a convex function. Moreover, using a shorter notation \(\sigma_h^2 = 1 - \sigma_{nm}^2\), the expectation yields
\[
E_{hab}\left[ \ln \hat{h}_{ab} \right] = \frac{1}{\sqrt{2 \pi \sigma_h^2}} \int_{\mathbb{R}} x^2 \exp \left( -\frac{x^2}{2 \sigma_h^2} \right) dx \\
= \ln \frac{\sigma_h^2}{\hat{h}^2} + \frac{1}{\sqrt{2 \pi}} \int_{\mathbb{R}} y^2 \exp \left( -\frac{y^2}{2} \right) dy \\
= \ln \sigma_h^2 + \Psi(0.5) + \ln 2 \\
= \ln \frac{\sigma_h^2}{2} - \gamma. \tag{16}
\]
where \((a)\) holds due to the substitution \(x = \sigma_h y\), \((b)\) is true because the integral can be solved in closed form \([12]\) including the Digamma function \(\Psi(x)\), and in \((c)\) we have the Euler-Mascheroni constant \(\gamma = 0.57721\ldots\). Continuing from \([15]\) while using \([16]\), we have
\[
R_p^{(FD)} \geq \frac{1 - \beta}{2} \log_2 \left( 1 + \alpha_{FD} \frac{\sigma_h^2}{2} e^{-\gamma} \right) \\
= \frac{1 - \beta}{2} \log_2 \left( 1 + \alpha_{FD} \frac{\sigma_h^2}{2} \right) - \frac{1}{2} \log_2 \left( 1 + 2 \sigma_{nm}^2 + \alpha^2 \sigma_{nm}^2 (1 + \alpha_{FD}) \right) \tag{17}
\]
where \((a)\) is due to \([14]\) and
\[
\sigma_h^2 = 1 - \sigma_{nm}^2 = \frac{\sigma_{nm}^2}{1 + \alpha \sigma_{nm}^2 + \sigma_{nm}^2}.
\]

B. Secret-key rates

We now provide the secret-key rate for Gaussian sources with rate-limited public communication.

**Proposition 1.** Let Alice, Bob and Eve observe a zero-mean Gaussian multiple vector source \((x, \hat{y}, \hat{z})\) in the form
\[
\hat{y} = bx + w_y \tag{18a} \\
\hat{z} = ex + w_z, \tag{18b}
\]
where \(b \in \mathbb{R}^{N_y}, e \in \mathbb{R}^{N_z}, x \sim \mathcal{N}(0, \sigma_x^2), w_y \sim \mathcal{N}(0, I_{N_y})\) and \(w_z \sim \mathcal{N}(0, I_{N_z})\). Furthermore, let \(\beta\) be the fraction of total number of observations available at each node. Then, the rate region \((R_{sk}, R_p)\) is the union of all achievable rate pairs satisfying
\[
R_p \geq \frac{1 - \beta}{2} \log_2 \frac{\sigma_x^2}{\sigma_{zx}^2} - \frac{1 - \beta}{2} \log_2 \left( \frac{bb^T \sigma_x^2 + I}{bb^T \sigma_{zx}^2 + I} \right), \tag{19a}
\]
\[
R_{sk} \leq \frac{1 - \beta}{2} \log_2 \left( \frac{bb^T \sigma_x^2 + I}{bb^T \sigma_{zx}^2 + I} \right) - \frac{1}{2} \log_2 \left( \frac{ee^T \sigma_x^2 + I}{ee^T \sigma_{zx}^2 + I} \right), \tag{19b}
\]
for some \(\sigma_x^2 \geq \sigma_{zx}^2 > 0\), where \(\sigma_{zx}^2\) denotes the conditional covariance of \(x\) given a (Gaussian) random variable \(u\).

**Proof:** The proof of \([19]\) follows along similar lines as in \([5]\) Section V and is omitted for brevity.

We are going to apply the result of \([19]\) to our one system model of section \([3]\) i.e., for \((1)\) and \((2)\). Therefore, we need the following proposition.

**Proposition 2.** For specific non-singular matrices \(A_y \in \mathbb{R}^{N_y \times N_y}, A_z \in \mathbb{R}^{N_z \times N_z}\), the achievable rate region \((R_{sk}, R_p)\) defined for \((18a)\) and \((18b)\), also holds for \((1)\) and \((2)\), respectively.

**Proof:** The computation of the achievable rate region in \([19]\) for model \((18)\) depends on joint probability distributions only through marginal \((x, y)\) and \((x, z)\) \([4]\) Appendix C. Let \(\hat{y}\) and \(\hat{z}\) be the Gaussian random variables with the same second-order moments as \(y\) and \(z\), respectively, and the same joint statistics with \(x\). In what follows, we elaborate the connection of \(\hat{z}\) and \(z\) only. Similar arguments can be used to straightforwardly show the relationship between \(\hat{y}\) and \(y\) and is omitted. Let
\[
\hat{z} := A_z \hat{z} = A_z e x + A_z w_z, \tag{20}
\]
where \(A_z \in \mathbb{R}^{N_z \times N_z}\) non-singular. Since \(A_z\) is invertible, the transformation \(A_z \hat{z}\) provides a sufficient statistic. Therefore, any mutual information regarding \(\hat{z}\) yields the same result as for \(\hat{z}\). Subsequently, we need the same joint and second-order marginal statistics of \(z\) and \(\hat{z}\):
\[
\sigma_{zz} := E[zz] = E[\hat{z} \hat{z}] = A_z \sigma_z^2 A_z^T, \tag{21}
\]
\[
\Sigma_z := E[\hat{z} \hat{z}^T] = E[zz^T] = A_z \sigma_z^2 A_z^T + A_z A_z^T \tag{22}
\]
As a consequence, by using \([22]\), we have
\[
A_z A_z^T = \Sigma_z - \sigma_{zz} \sigma_{zz}^{-1} \sigma_{xz}^2 = : \Sigma_z | x. \tag{23}
\]
We find the squared norms of the parameter vectors \(b\) and \(e\). We show the derivation of \(||e||^2\) here only, since it follows analogously for \(||b||^2\). Starting with \([21]\), the squared norm of the parameter vector can be evaluated:
\[
||e||^2 = \sigma_{xx}^{-1} \sigma_{xx}^{-1} \sigma_{xx}^{-1} \sigma_{xx}^{-1} \sigma_{xx}^{-1} = \frac{\sigma_{xx}^{-1} \sigma_{xx}^{-1} \sigma_{xx}^{-1} \sigma_{xx}^{-1} \sigma_{xx}^{-1}}{\sigma_{xx}^{-1}}, \tag{24}
\]
where \((a)\) follows from \([23]\) and \((b)\) is due to the Woodbury matrix identity. One can follow the same steps in order to obtain the analogous expression of
\[
||b||^2 = \sigma_{yy}^{-1} \sigma_{yy}^{-1} \sigma_{yy}^{-1} \sigma_{yy}^{-1} \sigma_{yy}^{-1} = \frac{\sigma_{yy}^{-1} \sigma_{yy}^{-1} \sigma_{yy}^{-1} \sigma_{yy}^{-1} \sigma_{yy}^{-1}}{\sigma_{yy}^{-1}}. \tag{25}
\]
C. Key-communication function

The following proposition provides the concrete relation of the secret key rate as a function of public communication rate.

**Proposition 3.** The key-communication function is given by

\[ R_{sk}(R_p) = \frac{1 - \exp(-2R_p \beta/\beta) \sigma_z^2}{2 \log_2 (1 + \sigma_z^2)} \|b\|^2 + \|e\|^2 \]  

(26)

**Proof:** First, we pick the minimum possible \( R_p \) by taking equality in (19a). We apply Sylvester’s determinant formula \[13\] to

\[ \left| bb^T \right| = 1 + \sigma_z^2 \|b\|^2. \]

Subsequently, from (19a), we get

\[ \sigma_z^2 = \exp(2R_p \beta/\beta) (1 + \sigma_z^2 \|e\|^2) - \sigma_z^2 \|b\|^2. \]

(27)

Finally, by plugging (27) into (19b) and using Sylvester’s formula, we get (26).

Immediately from utilizing the preceding result, we can deduce the following property.

**Property 1.** The key-communication function \( R_{sk}(R_p) \) is positive if and only if \( R_p > 0 \) and \( \|b\|^2 > \|e\|^2 \) hold.

**Proof:** Let \( R_{sk}(R_p) > 0 \). This implies that, the numerator in (26) inside the log function must be larger than the denominator. This holds if

\[ \exp(2R_p \beta/\beta) (1 + \sigma_z^2 \|e\|^2) < \|b\|^2 - \|e\|^2. \]

The exponential term is always smaller or equal to one due to the non-negative communication rate, therefore the inequality can only be fulfilled if \( \|b\|^2 > \|e\|^2 \) and \( R_p > 0 \) hold. Conversely, assuming the conditions are satisfied, then one can strictly lower bound (26) by removing the exponential term, which in turn yields \( R_{sk}(R_p) > 0 \).

We are going to derive representations of the key-communication function for both HD and FD modes.

1) HD mode

The key-communication function of (26) is denoted by \( R_{sk}^{(HD)}(R_p) \) with the specific parameters

\[ \|b_z^{(HD)}\|^2 := \sigma_z^2 \|b\|^2, \quad \|e_z^{(HD)}\|^2 := \sigma_z^2 \|e\|^2, \]

where \( \sigma_z^2, \|b\|^2, \|e\|^2 \) are derived from (24) and (25) based on (1). The details of the computation are omitted.

Moreover, we apply the upper bound of (10) to the HD communication rate. This leads to an upper bound on the key-communication function (26), defined by \( R_{sk}^{(HD)} \) in the following.

2) FD mode

In this case, the key-communication function is described by \( R_{sk}^{(FD)} \) with parameters

\[ \|b_z^{(FD)}\|^2 := \sigma_z^2 \|b\|^2, \quad \|e_z^{(FD)}\|^2 := \sigma_z^2 \|e\|^2, \]

where \( \sigma_z^2, \|b\|^2, \|e\|^2 \) are derived from (24) and (25) based on (2). We apply the lower bound of the FD communication rate (17), which results in a lower bound on the key-communication function of (26), given by \( R_{sk}^{(FD)} \).

**Remark 1.** The particular choice of bounds has the merit that any actual improvement of FD over HD mode can only be better than or at least equal to the difference \( R_{sk}^{(FD)} - R_{sk}^{(HD)}. \)

IV. RESULTS

In this section, we present results by comparing performance of HD and FD approaches. We analyze the following metric:

**Definition 2.** The FD over HD improvement ratio and its lower bound is given for \( R_{sk}^{(FD)} \neq 0 \) and \( R_{sk}^{(FD)} \geq R_{sk}^{(HD)} \) by

\[ \eta := \frac{R_{sk}^{(FD)} - R_{sk}^{(HD)} - R_{sk}^{(HD)}}{R_{sk}^{(FD)}} \]  

(28)

Figure 3 depicts an example of secret-key rates and improvement ratios, both in their exact and bounded versions. Apparently the bounded approximations get closer to the exact values for higher SNR. Furthermore, we examine the case for arbitrarily high SNR at both the legitimate nodes and the eavesdropper. Subsequently, the independent noise in (1) and (2) is neglected. Furthermore, for convenience, we assume that the eavesdropper experiences symmetric statistics of the observations, i.e., \( \rho_{ba} = \rho_{be} \). In order to satisfy positive definiteness of \( \Sigma_z, \Sigma_{x|x}, \Sigma_y \) and \( \Sigma_{y|x} \), we have to restrict \( 2 \rho_{ae} - 1 < \rho_e < 1, \rho_{ba} \neq 1 \) and \( \delta^2 \rho_{ba} \neq 1 \). By omitting some details, we have

\[ \|b_z^{(HD)}\|^2 = \frac{\delta^2 \rho_{ba}}{1 - \delta^2 - \rho_{ba}}, \quad \|e_z^{(HD)}\|^2 = \frac{2 \rho_{ae}}{1 + \rho_e - 2 \rho_{ae}}, \]

\[ \|b_z^{(FD)}\|^2 = \frac{\rho_{ba}}{(1 + \alpha^2) - \rho_{ba}}, \quad \|e_z^{(FD)}\|^2 = \frac{2 \rho_{ae}}{(1 + \alpha^2)(1 + \rho_e) - 2 \rho_{ae}}. \]

We consider the upper bound on key-communication function \( R_{sk}^{(HD)} \) in HD mode and the lower bound \( R_{sk}^{(FD)} \) in FD mode.

**Remark 2.** The communication rate in HD case is arbitrarily high, since a noiseless channel supports unlimited capacity. Subsequently, the exponential term of (26) vanishes. However, in FD mode, the channel is still noisy due to the SI, which scales with SNR. For convenience, we define a short form of the exponential term of (26) in FD mode by

\[ r_{\beta}(\alpha) := \lim_{\delta \to \infty} \exp(- \frac{2}{\beta} R_{sk}^{(FD)}) \]

\[ = (1 + \frac{1}{2\alpha^2} e^{-\gamma})^{-(\delta - 1)}. \]

(29)

Next, we provide a proposition which shows under what conditions FD performs better than HD.
Proposition 4. A sufficient condition for $\eta > 0$ in the high SNR regime is given if the following relations are satisfied:

$$\rho_{ba} > 2\rho_{ac} > 1 + \alpha^2 > 0,$$

(30)

$$\delta^2 \leq \frac{1 - r_\beta(\alpha)}{(1 + \alpha^2)^2 - \rho_{ba} r_\beta(\alpha)}.$$  

(31)

Proof: In order to obtain a positive secret-key rate, we furthermore need to fulfill Property [1] therefore we have condition (30).

For the inequality (31), we note that the relation $\|e_x^{(HD)}\|^2 \geq \|e_x^{(FD)}\|^2$ is always satisfied for any $\alpha \geq 0$, thus the denominator of (26) in HD mode is always larger or equal to that in FD mode. Next, we assure that the numerator of (26) is always larger in FD mode. Subsequently, we assume the condition

$$\|b_x^{(FD)}\|^2 - \|b_x^{(HD)}\|^2 > r_\beta(\alpha) \left( \|b_x^{(FD)}\|^2 - \|e_x^{(FD)}\|^2 \right).$$

(32)

The RHS of inequality (32) can be upper bounded as follows:

$$r_\beta(\alpha) \left( 1 + \alpha^2 \right) \rho_{ba}^2 \left( 1 + \rho_e \right) - 2\rho_{ac}^2 \left( 1 + \alpha^2 \right)$$

$$\leq \theta \rho_{ba}^2 \left( 1 + \rho_e \right) - 2\rho_{ac}^2 \left( 1 + \alpha^2 \right)$$

$$\leq r_\beta(\alpha) \rho_{ba}^2,$$

(33)

where in (a) the denominator is decreased by multiplying $(1 + \alpha^2)$ to the subtrahend. Finally, in (b), the numerator is increased by removing $(1 + \alpha^2)$ from the subtrahend. By assuming $\rho_{ba}^2 > 0$, which is actually covered by (30), condition (31) directly follows. □

The above proposition shows an interesting property. The condition (31) directly follows. Therefore, Alice and Bob might decide on the preferred mode based on their own knowledge only, i.e., the relative strength of self-interference $\alpha$, channel reciprocity $\rho_{ba} \delta$ or the trade-off $\beta$ between estimation and communication phase. In addition, it turns out that the conditions (30) and (31) are quite mild, hence we expect that in many practical situations there is an improvement of FD over HD mode. Especially, this holds for the following:

Corollary 1. In case of perfect self-interference cancellation, $R_{sk}^{(FD)} > R_{sk}^{(HD)}$ always holds for any $\delta^2 < 1$.

Proof: Without self-interference, we have $\alpha = 0$, and therefore public communication rate is unlimited even in the FD case. Consequently, it is sufficient having $\|b_x^{(FD)}\|^2 > \|b_x^{(HD)}\|^2$, which is the case if $\delta^2 < 1$. □

V. CONCLUSION

In this work, we compare secret-key generation from reciprocal wireless channels for nodes with half-duplex (HD) or full-duplex (FD) capabilities. We have partitioned system models into both cases that capture the channel probing part as well as the public communication overhead required for key reconciliation. In addition, the key-communication function and a metric for comparison of HD and FD modes are formulated. We have analyzed the performance of FD mode over HD in the high SNR regime in particular. The results show an improvement in secret-key rate in FD over HD mode. Therefore, for a system designer, a key agreement protocol running in FD mode is a considerable option in order to improve the performance.

References

[1] A. K. Khandani, “Two-way (true full-duplex) wireless,” in 13th Canadian Workshop on Information Theory (CWIT), IEEE, 2013, pp. 33–38.
[2] D. Korpi, T. Riihonen, V. Syrjala, L. Anttila, M. Valkama, and R. Wichman, “Full-Duplex Transceiver System Calculations: Analysis of ADC and Linearity Challenges,” IEEE Transactions on Wireless Communications, vol. 13, no. 7, pp. 3821–3836, July 2014.
[3] R. Ahsiswede and I. Csiszar, “Common randomness in information theory and cryptography, i. secret sharing,” IEEE Transactions on Information Theory, vol. 39, no. 4, pp. 1121–1132, 1993.
[4] S. Watanabe and Y. Oohama, “Secret key agreement from correlated Gaussian sources by rate limited public communication,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 93, no. 11, pp. 1976–1983, 2010.
[5] ——, “Secret key agreement from vector Gaussian sources by rate limited public communication,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 541–550, 2011.
[6] R. Chou and M. Bloch, “Separation of Reliability and Secrecy in Rate-Limited Secret-Key Generation,” IEEE Transactions on Information Theory, vol. 60, no. 8, pp. 4941–4957, Aug 2014.
[7] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

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

[9] M. Medard, “The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channel,” *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 933–946, 2000.

[10] E. Ahmed, A. M. Eltawil, and A. Sabharwal, “Rate gain region and design tradeoffs for full-duplex wireless communications,” *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3556–3565, 2013.

[11] O. Oyman, R. U. Nabar, H. Bolcskei, and A. J. Paulraj, “Tight lower bounds on the ergodic capacity of Rayleigh fading MIMO channels,” in *IEEE Global Telecommunications Conference (GLOBECOM)*, vol. 2. IEEE, 2002, pp. 1172–1176.

[12] P. M. Lee, *Bayesian statistics: an introduction*. John Wiley & Sons, 2012.

[13] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge University press, 2012.