ICASSP 2024 - 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) | 979-8-3503-4485-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICASSP48485.2024.10448166

NONASYMPTOTIC PERFORMANCE LIMITS OF LOW-LATENCY SECURE INTEGRATED SENSING AND COMMUNICATION SYSTEMS

Onur Günlü[1], *Matthieu Bloch*[2], *Rafael F. Schaefer*[3,4], *and Aylin Yener*[5]

[1]Electrical Engineering Department, Linköping University, Sweden
[2]School of Electrical and Computer Engineering, Georgia Institute of Technology, USA
[3]Chair of Information Theory and Machine Learning, TU Dresden, Germany
[4]BMBF Research Hub 6G-life & Cluster of Excellence CeTI, Dresden, Germany
[5]Department of Electrical and Computer Engineering, The Ohio State University, USA

ABSTRACT

This paper considers an information theoretic model for secure integrated sensing and communication (ISAC) with the goal of establishing fundamental limits in low-latency scenarios. In this secure ISAC model, a message is transmitted through a state-dependent wiretap channel with decoder-side state availability. The model is studied under a strong secrecy constraint when only a part of the transmitted message should be kept secret. First, the secrecy-distortion rate region is established for a degraded channel by treating the model as a special case of a feed-backed secure ISAC model. Finite-length inner bounds are then proved by applying nonasymptotic random binning techniques. Bounds on the rates have a similar form to common finite-length bounds, and the distortion bound follows from a bound for letter-typical sequences.

Index Terms— integrated sensing and communication, joint communication and sensing, physical layer security, coding for security, finite blocklength analysis.

1. INTRODUCTION

The vision for future communication and computation networks includes an integration of the physical and digital worlds by enabling high-resolution and high-accuracy sensing and positioning. This enables an accurate digital representation of the real world, i.e., a digital twin. Such a seamless integration can leverage intelligence to automatically react to changing physical environments [1]. Using high frequencies as well as massive numbers of antennas and wide bandwidth allows one to achieve integrated sensing and communication (ISAC), which improves the performance of each component simultaneously with high energy efficiency and enables new services such as activity recognition [2]. For instance, a mmWave joint communication and radar system in autonomous vehicles can detect a target or estimate the parameters of the channel that are of interest to refine the communication scheme and to make intelligent decisions on demand [3–5].

Motivated by the promises of ISAC, a fundamental information theoretic model for joint communication and radar systems is proposed in [4]. In this model, the communication channel depends on the channel state (determined by the receiver position, grid plan and surroundings, frequency band, etc.) that should be estimated at the transmitter and there is channel output feedback available at the transmitter (obtained via reflections). However, there is a missing constraint in this and other models for ISAC. Since the same waveform and network infrastructure are used for both sensing and communication, ISAC broadcasts in the sensing signal, e.g., via beam sweeping, the information that is aimed only at a set of legitimate receivers to a large area in which there can be attackers. Thus, the joint and broadcast nature of ISAC makes it mandatory to provide security guarantees against active and passive attacks to the network [5, 6]. In this work, we consider a practical secure ISAC model that consists of a wiretap channel [7, 8] with channel states available only at the corresponding receivers, one of which is the sensed target that is interested in the messages transmitted to the legitimate receiver, i.e., the sensed target is the eavesdropper. We also consider channel output feedback available at the transmitter that can be obtained through reflections and are used to estimate the channel states for both receivers. This model is a simplified version of the secure ISAC model in [8, Fig. 1], as the channel output feedback is not used to improve communication performance. Such a model is commonly considered in the literature since, e.g., one would then not need to adapt the encoding operations according to the feedback, so a low-latency constraint can be

This work has been supported by the German Federal Ministry of Education and Research (BMBF) within the national initiative on 6G Communication Systems through the research hub *6G-life* under Grant 16KISK001K as well as within the national initiative for Post-Shannon Communication (NewCom) under Grant 16KIS1004, German Research Foundation (DFG) as part of Germany's Excellence Strategy – EXC 2050/1 - Project ID 390696704 - Cluster of Excellence *"Centre for Tactile Internet with Human-in-the-Loop" (CeTI)*, ZENITH Research and Leadership Career Development Fund, ELLIIT funding endowed by the Swedish government, and the National Science Foundation (NSF) under grants CCF 1955401 and 2148400 as part of the Resilient & Intelligent NextG Systems (RINGS) program.

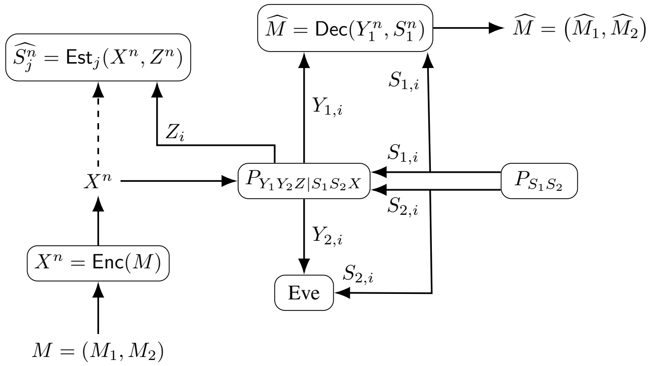

Fig. 1. Practical secure ISAC model under partial secrecy, i.e., only M_2 should be kept secret from Eve, for $j = 1, 2$ and $i = [1 : n]$, where $\mathsf{Enc}(\cdot)$ and $\mathsf{Dec}(\cdot)$ are an encoder-decoder pair and $\mathsf{Est}(\cdot)$ is an estimation function. Assume that M and (S_1^n, S_2^n) are independent. We consider practical secure ISAC with perfect output feedback, i.e., we have $Z_i = (Y_{1,i}, Y_{2,i})$.

satisfied. We establish the rate region for the practical secure ISAC model when the wiretap channel is degraded. We also establish achievable nonasymptotic performance limits by fixing the blocklength to establish a reference point for practical secure ISAC implementations.

2. SYSTEM MODEL

Consider the practical secure ISAC model shown in Fig. 1, which consists of a transmitter, a legitimate receiver, a target that acts as an eavesdropper (Eve), and a state estimator at the transmitter side. Suppose the message $M = (M_1, M_2) \in \mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$ is uniformly distributed, i.e., we have $M \sim P_M^U$, and it is sent through a practical state-dependent memoryless ISAC channel $P_{Y_1Y_2Z|S_1S_2X}$ with independent and identically distributed (i.i.d.) state sequence $(S_1^n, S_2^n) \in \mathcal{S}_1^n \times \mathcal{S}_2^n$ generated according to a known probability distribution $P_{S_1S_2}^n$. The channel inputs X^n are computed from the message M. For all channel uses $i \in [1 : n]$, the legitimate receiver observes $S_{1,i} \in \mathcal{S}_1$ and $Y_{1,i} \in \mathcal{Y}_1$, whereas Eve observes $S_{2,i} \in \mathcal{S}_2$ and $Y_{2,i} \in \mathcal{Y}_2$. The legitimate receiver aims to reliably reconstruct M, whereas Eve aims to learn information about M_2, which is called partial secrecy in [9]. Furthermore, the state estimator at the transmitter side observes the channel inputs X^n and the channel output feedback symbols $Z^n \in \mathcal{Z}^n$ to estimate the state sequence (S_1^n, S_2^n) as $\widehat{S_j^n} = \mathsf{Est}_j(X^n, Z^n) \in \widehat{\mathcal{S}_j}^n$ for $j = 1, 2$. Assume that all symbol sets are finite; see [8] for further motivations for a general secure ISAC model.

The secrecy-distortion region for the practical secure ISAC model is defined next.

Definition 1. Under partial secrecy, a secrecy-distortion tuple (R_1, R_2, D_1, D_2), where $\log|\mathcal{M}_j| = nR_j$ for $j = 1, 2$, is *achievable* if, for any $\delta > 0$, there exist one encoder, one decoder, $n \geq 1$, and two state estimators $\widehat{S_j^n} = \mathsf{Est}_j(X^n, Z^n)$ such that

$$\Pr\left[M \neq \widehat{M}\right] \leq \delta \qquad \text{(reliability)} \qquad (1)$$

$$\mathbb{E}\big[d_j(S_j^n, \widehat{S_j^n})\big] \leq D_j + \delta \quad \text{for } j = 1, 2 \quad \text{(distortions)} \qquad (2)$$

$$I(M_2; Y_2^n | S_2^n) \leq \delta \qquad \text{(strong secrecy)} \qquad (3)$$

where we have per-letter distortion metrics $d_j(s^n, \widehat{s^n}) = \frac{1}{n}\sum_{i=1}^{n} d_j(s_i, \hat{s}_i)$ for $j = 1, 2$ that are bounded by a value $d_{\max}$. The secrecy-distortion region $\mathcal{R}_{\text{PS}}$ is the closure of the set of all achievable tuples under partial secrecy. ♢

We next define degraded practical ISAC channels, for which we illustrate the secrecy-distortion region. We remark that the set of degraded channels includes both stochastically- and physically-degraded channels; see also [4, 8]. To simplify the proofs, we consider $Z_i = (Y_{1,i}, Y_{2,i})$ for the rest of this work.

Definition 2. Define a practical ISAC channel $P_{Y_1Y_2|S_1S_2X}$ as *degraded* if there exists a random variable $\widetilde{Y}_1$ such that we have $\widetilde{Y}_1 | \{S_1 = s_1, X = x\} \sim P_{Y_1|S_1X}(\tilde{y}_1|s_1, x)$ and

$$\begin{aligned} P_{\widetilde{Y}_1Y_2S_1S_2|X} &= P_{\widetilde{Y}_1Y_2|S_1S_2X}P_{S_1S_2} \\ &= P_{S_1}P_{\widetilde{Y}_1|S_1X}P_{Y_2S_2|S_1\widetilde{Y}_1}. \end{aligned} \qquad (4)$$

♢

We next establish the secrecy-distortion region for degraded practical ISAC channels, which is an asymptotic result, i.e., $n \to \infty$. We remark that the constraints in (1)-(3) only depend on the marginal probability distributions of the tuples (X, Y_1, S_1) and (X, Y_2, S_2) if we impose estimators of the form $\mathsf{Est}_j(x, y_j)$ for $j = 1, 2$, i.e., $y_{(3-j)}$ is not used to estimate s_j. Thus, the secrecy-distortion region for the physically-degraded practical ISAC channels is also valid for degraded practical ISAC channels.

Define for any $a \in \mathbb{R}$

$$[a]^+ = \max\{a, 0\}. \qquad (5)$$

Theorem 1. *For a degraded practical ISAC channel, $\mathcal{R}_{\text{PS}}$ is the union over all joint distributions P_{VX} of the rate tuples (R_1, R_2, D_1, D_2) that satisfy*

$$\begin{aligned} &R_2 \leq [I(V; Y_1|S_1) - I(V; Y_2|S_2)]^+ \\ &R_1 + R_2 \leq I(V; Y_1|S_1) \\ &D_j \geq \mathbb{E}[d_j(S_j, \widehat{S}_j))] \qquad \textit{for } j = 1, 2 \end{aligned} \qquad (6)$$

where we have

$$P_{VXY_1Y_2S_1S_2} = P_{V|X}P_XP_{S_1S_2}P_{Y_1Y_2|S_1S_2X}, \qquad (7)$$

and it suffices to use per-letter estimators

$$\mathsf{Est}_j(x, y_j) = \underset{\tilde{s} \in \widehat{\mathcal{S}}_j}{\operatorname{argmin}} \sum_{s_j \in \mathcal{S}_j} P_{S_j|XY_j}(s_j|x, y_j)\, d_j(s_j, \tilde{s}). \quad (8)$$

It also suffices to consider $|V| \leq |\mathcal{X}| + 1$.

Proof Sketch. The converse result follows by generalizing the degraded wiretap channel result in [7]. We next summarize the proof. Suppose for some $n \geq 1$ and $\delta_n > 0$, there exist an encoder, decoder, and state estimators such that (1)-(3) are satisfied for some tuple (R_1, R_2, D_1, D_2). Let

$$\epsilon_n = \frac{H_b(\delta_n)}{n} + \delta_n(R_1 + R_2) \tag{9}$$

where $H_b(\cdot)$ is the binary entropy function, such that $\epsilon_n \to 0$ if $\delta_n \to 0$. Applying Fano's inequality and (1), we obtain

$$H(M_1, M_2|Y_1^n, S_1^n) \overset{(a)}{\leq} H(M_1, M_2|\widehat{M_1}, \widehat{M_2}) \leq n\epsilon_n \tag{10}$$

where (a) allows one to use a randomized decoder. Define $V_i \triangleq (M_1, M_2, Y_1^{i-1}, S_1^{i-1}, Y_{2,i+1}^n, S_{2,i+1}^n)$ such that for all $i \in [1 : n]$ we have the Markov chain $V_i - X_i - (Y_{1,i}, Y_{2,i}, S_{1,i}, S_{2,i})$.

We have

$$\begin{aligned}
&n(R_1 + R_2) \overset{(a)}{\leq} I(M_1, M_2; Y_1^n|S_1^n) + n\epsilon_n \\
&\overset{(b)}{\leq} \sum_{i=1}^n \big[H(Y_{1,i}|S_{1,i}) \\
&\qquad - H(Y_{1,i}|M_1, M_2, Y_1^{i-1}, S_1^i, Y_{2,i+1}^n, S_{2,i+1}^n) + \epsilon_n\big] \\
&= \sum_{i=1}^n \big(I(V_i; Y_{1,i}|S_{1,i}) + \epsilon_n\big)
\end{aligned} \tag{11}$$

where (a) follows by (10) and since (M_1, M_2, S_1^n) are mutually independent and (b) follows because

$$S_{1,i+1}^n - (M_1, M_2, Y_1^{i-1}, S_1^i) - Y_{1,i} \tag{12}$$

forms a Markov chain.

We also obtain

$$\begin{aligned}
&nR_2 \overset{(a)}{\leq} H(M_2|Y_2^n, S_2^n) + \delta_n \\
&= I(M_2; Y_1^n, S_1^n|Y_2^n, S_2^n) + H(M_2|Y_1^n, Y_2^n, S_1^n, S_2^n) + \delta_n \\
&\overset{(b)}{\leq} \sum_{i=1}^n \Big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i}) \\
&\qquad - H(Y_{1,i}, S_{1,i}|Y_1^{i-1}, S_1^{i-1}, Y_{2,i}^n, S_{2,i}^n, M_1, M_2)\Big] \\
&\quad + n\epsilon_n + \delta_n \\
&= \sum_{i=1}^n \Big[I(Y_{1,i}, S_{1,i}; V_i|Y_{2,i}, S_{2,i})\Big] + n\epsilon_n + \delta_n \\
&\overset{(c)}{=} \sum_{i=1}^n \Big[I(Y_{1,i}; V_i|S_{1,i}) - I(Y_{2,i}; V_i|S_{2,i})\Big] + n\epsilon_n + \delta_n
\end{aligned} \tag{13}$$

where (a) follows by (3), (b) follows by (10) and because the practical ISAC channel is degraded so that for all $i \in [1 : n]$

$$(Y_{1,i}, S_{1,i}) - (Y_1^{i-1}, S_1^{i-1}, Y_{2,i}^n, S_{2,i}^n, M_1, M_2) - (Y_2^{i-1}, S_2^{i-1}) \tag{14}$$

forms a Markov chain, and (c) follows because V_i is independent of $(S_{1,i}, S_{2,i})$ for all $i \in [1 : n]$ and because the practical ISAC channel is degraded so that $V_i - (Y_{1,i}, S_{1,i}) - (Y_{2,i}, S_{2,i})$ forms a Markov chain.

Distortion bounds follow by (2) and can be achieved by using the estimators in (8). Furthermore, by introducing a uniformly distributed time-sharing random variable Q that takes values in $[1 : n]$ and is independent of other random variables, and by letting $\delta_n \to 0$, the converse proof follows; see also [4, 8] for similar steps.

Achievability proof follows by applying similar steps as in [8, Section III] using the output statistics of random binning (OSRB) method [10, 11] with a channel prefixing auxiliary random variable V and applying the steps in [12, Section 1.6]; see also [13] by considering the state estimates as a function of the channel input and outputs. Thus, we omit its proof. □

We next provide an achievable finite-length bound for the secrecy-distortion region of the practical ISAC channel.

3. NONASYMPTOTIC LIMITS OF PRACTICAL SECURE ISAC

Nonasymptotic performance limits of the practical secure ISAC model can be characterized by fixing the blocklength n to a finite value in (1)-(3), for which different δ values can be imposed and this allows us to illustrate the effect of each constraint on rates and distortions separately. Thus, we have the following definition for the nonasymptotic rate region of the practical secure ISAC model.

Definition 3. Under partial secrecy and for fixed $\delta_{\text{r}}, \delta_{\text{D}}, \delta_{\text{sec}} > 0$ and $n \geq 1$, a nonasymptotic secrecy-distortion tuple (R_1, R_2, D_1, D_2), where $\log|\mathcal{M}_j| = nR_j$ for $j = 1, 2$, is $(\delta_{\text{r}}, \delta_{\text{D}}, \delta_{\text{sec}}, n)$-*achievable* if there exist one encoder, one decoder, and two per-letter state estimators $\widehat{S}_j = \mathsf{Est}_j(X, Y_j)$ such that

$$\Pr\big[M \neq \widehat{M}\big] \leq \delta_{\text{r}} \tag{15}$$

$$\mathbb{E}\big[d_j(S_j^n, \widehat{S_j^n})\big] \leq D_j + \delta_{\text{D}} \quad \text{for } j = 1, 2 \tag{16}$$

$$||P_{M_2 Y_2^n S_2^n} - P_{M_2}^U P_{S_2}^n P_{Y_2|S_2}^n||_1 \leq \delta_{\text{sec}} \tag{17}$$

where we have the per-letter distortion metrics that are bounded by a value $d_{\max}$. The nonasymptotic secrecy-distortion region $\mathcal{R}_{\text{PS}}(\delta_{\text{r}}, \delta_{\text{D}}, \delta_{\text{sec}}, n)$ is the closure of the set of all $(\delta_{\text{r}}, \delta_{\text{D}}, \delta_{\text{sec}}, n)$-achievable tuples under partial secrecy. ◊

We remark that the nonasymptotic strong secrecy constraint in (17) is an L^1 distance constraint, unlike the asymptotic counterpart in (3) that measures the same security performance by using a conditional mutual information term. Using the L^1 distance as the security metric simplifies our proof since we use the nonasymptotic OSRB method that provides bounds for this metric.

We next provide a $(\delta_{\mathrm{r}}, \delta_{\mathrm{D}}, \delta_{\mathrm{sec}}, n)$-achievable nonasymptotic secrecy-distortion region $\mathcal{R}_{\mathrm{PS}}(\delta_{\mathrm{r}}, \delta_{\mathrm{D}}, \delta_{\mathrm{sec}}, n)$ when the practical ISAC channel is degraded.

Similar to [14], we denote the information density of a probability distribution P_{XYZ} as

$$\imath(X, YZ) = \log \frac{P_{XYZ}(x,y,z)}{P_X(x) P_{YZ}(y,z)} \tag{18}$$

and the channel dispersions for the channels $P_{Y_1|VS_1}$ and $P_{Y_2|VS_2}$, respectively, as

$$V_{Y_1|S_1} = \mathbb{E}_{P_{VY_1S_1}}\big[\mathrm{Var}[\imath(V, Y_1S_1)|V]\big], \tag{19}$$

$$V_{Y_2|S_2} = \mathbb{E}_{P_{VY_2S_2}}\big[\mathrm{Var}[\imath(V, Y_2S_2)|V]\big] \tag{20}$$

where $\mathrm{Var}[\cdot]$ denotes the variance.

Denote the inverse Q-function as $Q^{-1}(\cdot)$ and define

$$\mu_{s\hat{s}} = \min_{(s,\hat{s}) \in \mathrm{supp}(P_{S\widehat{S}})} P_{S\widehat{S}}(s, \hat{s}). \tag{21}$$

Theorem 2. *For a degraded practical ISAC channel, a $(\delta_r, \delta_D, \delta_{sec}, n)$-achievable nonasymptotic secrecy-distortion region under partial secrecy is the union over all joint distributions P_{VX} of the rate tuples (R_1, R_2, D_1, D_2) that satisfy, for any $\theta \in [0,1]$,*

$$\begin{aligned} R_2 \leq \Big[& I(V;Y_1|S_1) - I(V;Y_2|S_2) \\ & - Q^{-1}\bigg(\theta\Big(\delta_r + \mathcal{O}\big(\frac{1}{\sqrt{n}}\big)\Big)\bigg)\sqrt{\frac{V_{Y_1|S_1}}{n}} \\ & - Q^{-1}\bigg((1-\theta)\Big(\delta_{sec} + \mathcal{O}\big(\frac{1}{\sqrt{n}}\big)\Big)\bigg)\sqrt{\frac{V_{Y_2|S_2}}{n}} \\ & + \mathcal{O}\Big(\frac{\log n}{n}\Big)\Big]^+, \end{aligned} \tag{22}$$

$$\begin{aligned} R_1 + R_2 \leq \Big[& I(V;Y_1|S_1) + \mathcal{O}\Big(\frac{\log n}{n}\Big) \\ & - Q^{-1}\bigg(\theta\Big(\delta_r + \mathcal{O}\big(\frac{1}{\sqrt{n}}\big)\Big)\bigg)\sqrt{\frac{V_{Y_1|S_1}}{n}}\Big]^+ \end{aligned} \tag{23}$$

and

$$D_j \geq \mathbb{E}[d_j(S_j, \widehat{S}_j))] - \epsilon_D \qquad \textit{for } j = 1,2 \tag{24}$$

such that

$$\delta_D = \epsilon_D(1 + D_j + \epsilon_D) + 2|\mathcal{S}||\widehat{\mathcal{S}}|e^{-2n\epsilon_D^2 \mu_{s_j \hat{s}_j}^2} d_{max}. \tag{25}$$

We have (7) and use per-letter estimators in (8).

Proof Sketch. The proof mainly follows by applying the achievability proof technique used in [14, Section IV] that includes significant modifications of the nonasymptotic binning methods proposed in [15,16], which also use finite-length techniques of [17,18]; see also [19].

The proof follows by considering i.i.d. random variables $(V^n, X^n, Y_1^n, S_1^n, Y_2^n, S_2^n)$ such that

$$\mathbb{E}[d_j(S_j, \widehat{S}_j))] \leq D_j + \epsilon_D \tag{26}$$

for $j = 1,2$ and some $\epsilon_D \geq 0$ that satisfies (25). Denote the set of ϵ_{D}-letter typical sequences as $T_{\epsilon_{\mathrm{D}}}^n(P_{S\widehat{S}})$ and the error event that the sequences $(S_j^n, \widehat{S_j^n})$ are not ϵ_{D}-letter typical as

$$\mathcal{E} = \{(S_j^n, \widehat{S_j^n}) \notin T_{\epsilon_{\mathrm{D}}}^n(P_{S_j\widehat{S}_j})\}. \tag{27}$$

The equality in (25) is required since we have

$$\begin{aligned} & \mathbb{E}[d_j(S_j^n, \widehat{S_j^n})] \\ & = \Pr[\mathcal{E}]\ \mathbb{E}[d_j(S_j^n, \widehat{S_j^n})|\mathcal{E}] + \Pr[\mathcal{E}^c]\ \mathbb{E}[d_j(S_j^n, \widehat{S_j^n})|\mathcal{E}^c] \\ & \overset{(a)}{\leq} \Pr[\mathcal{E}]\ d_{\mathrm{max}} + \Pr[\mathcal{E}^c]\ (1+\epsilon_{\mathrm{D}})\ \mathbb{E}[d_j(S_j, \widehat{S}_j))] \\ & \overset{(b)}{\leq} 2|\mathcal{S}||\widehat{\mathcal{S}}|e^{-2n\epsilon_{\mathrm{D}}^2 \mu_{s_j\hat{s}_j}^2}\ d_{\mathrm{max}} + (1+\epsilon_{\mathrm{D}})\ (D_j + \epsilon_{\mathrm{D}}) \end{aligned} \tag{28}$$

where (a) follows because the distortion metrics are per-letter with bound d_{max} and from the typical average lemma [20, pp. 26] and (b) follows by (26) and from the bound on the probability of the error event $\mathcal{E}$ given in [21, Eq. (6.34)], which can be applied since per-letter estimators are used.

We first illustrate the existence of nonasymptotic random binning methods that simultaneously satisfy $\Pr\big[M \neq \widehat{M}\big] \leq \theta\delta_{\mathrm{r}}$ and $||P_{M_2Y_2^nS_2^n} - P_{M_2}^U P_{S_2}^n P_{Y_2|S_2}^n||_1 \leq (1-\theta)\delta_{\mathrm{sec}}$ for any $\theta \in [0,1]$. Similar to the OSRB method, we first consider a source coding problem that is operationally dual to our problem, i.e., Protocol A. In this problem, the encoder observes (V^n, X^n) and independently and uniformly assigns three random bin indices $F_v \in [1:2^{n\widetilde{R}}]$, $M_1 = M_{v_1} \in [1:2^{nR_1}]$, and $M_2 = M_{v_2} \in [1:2^{nR_2}]$. As in [15, pp. 3] and [14, Eq. (12)], we consider a mismatch stochastic likelihood coder (SLC) as the decoder, which allows one to bound the expected error probability averaged over the random binning ensemble. To impose (almost) independence constraints, including the strong secrecy constraint, we apply [15, Theorem 1] and to impose reliable sequence reconstruction constraints, we apply [15, Theorem 2], respectively. Thus, we can obtain constraints on the rates $(\widetilde{R}, R_1, R_2)$ by applying Berry-Esseen Theorem such that L^1 distances between the observed and target probability distributions are bounded by a fixed value for Protocol B, an equivalent channel coding problem with extra randomness F. Moreover, we can eliminate the extra randomness F by showing that there exists a fixed realization $F = f$ on which the encoder and decoder can agree publicly, as in [10, 14]. Lastly, by choosing the free parameters as chosen in [14, Eq. (36)], we obtain the results given in (22) and (23). □

We remark that the bounds given in (22) and (23) may be improved by using, e.g., privacy amplification methods, as in [22], analysis of which we leave as future work.

4. REFERENCES

[1] H. Andersson, "Joint communication and sensing in 6G networks," Available at https://www.ericsson.com/en/blog/2021/10/joint-sensing-and-communication-6g. (2023/08/21).

[2] A. Bayesteh et al., "Integrated sensing and communication (isac) - from concept to practice," *Commun. Huawei Research*, pp. 4–25, Sep. 2022.

[3] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security," *IEEE Commun. Mag.*, vol. 60, no. 4, pp. 65–71, Apr. 2022.

[4] M. Ahmadipour, M. Kobayashi, M. Wigger, and G. Caire, "An information-theoretic approach to joint sensing and communication," *IEEE Trans. Inf. Theory*, May 2022, early access.

[5] G. Fettweis et al., "Joint communications & sensing - Common radio-communications and sensor technology," *VDE Positionspapier*, July 2021.

[6] M. Bloch et al., "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

[7] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] O. Günlü, M. R. Bloch, R. F. Schaefer, and A. Yener, "Secure integrated sensing and communication," *IEEE J. Select. Areas Inf. Theory*, vol. 4, pp. 40–53, May 2023.

[9] J. D. D. Mutangana, R. Tandon, Z. Goldfeld, and S. Shamai, "Wiretap channel with latent variable secrecy," in *Proc. of IEEE Int. Symp. Inf. Theory*, Melbourne, Australia, July 2021, pp. 837–842.

[10] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[11] J. M. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7377–7385, Nov. 2011.

[12] M. Bloch, *Lecture Notes in Information-Theoretic Security*, Atlanta, GA: Georgia Inst. Technol., July 2018.

[13] O. Günlü, M. Bloch, and R. F. Schaefer, "Secure multifunction computation with private remote sources," in *IEEE Int. Symp. Inf. Theory*, Melbourne, Australia, July 2021, pp. 1403–1408.

[14] G. Cervia, T. J. Oechtering, and M. Skoglund, "(ϵ, n) fixed-length strong coordination capacity," in *IEEE Inf. Theory Workshop*, Kanazawa, Japan, Oct. 2021, pp. 1–6.

[15] M. H. Yassaee, M. R. Aref, and A. Gohari, "Non-asymptotic output statistics of random binning and its applications," in *IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, July 2013, pp. 1849–1853.

[16] M. H. Yassaee, M. R. Aref, and A. Gohari, "A technique for deriving one-shot achievability results in network information theory," in *IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, July 2013, pp. 1287–1291.

[17] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[18] V. Kostina and S. Verdu, "Fixed-length lossy compression in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3309–3338, June 2012.

[19] V. Y. F. Tan, "Achievable second-order coding rates for the wiretap channel," in *IEEE Int. Conf. Commun. Syst.*, Singapore, Nov. 2012, pp. 65–69.

[20] A. El Gamal and Y.-H. Kim, *Network Information Theory*, Cambridge, U.K.: Cambridge University Press, 2011.

[21] G. Kramer, *Multi-User Information Theory*, Munich, Germany: Techn. Univ. Munich, 2018.

[22] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, July 2019.