Secure Integrated Sensing and Communication Under Correlated Rayleigh Fading

Martin Mittelbach[1], Rafael F. Schaefer[1], Matthieu Bloch[2], Aylin Yener[3], and Onur Günlü[4]
[1]Chair of Information Theory and Machine Learning, TU Dresden, {martin.mittelbach, rafael.schaefer}@tu-dresden.de
[2]School of Electrical and Computer Engineering, Georgia Institute of Technology, matthieu.bloch@ece.gatech.edu
[3]Department of Electrical and Computer Engineering, The Ohio State University, yener@ece.osu.edu
[4]Information Theory and Security Laboratory, Linköping University, onur.gunlu@liu.se

***Abstract*—We consider a secure integrated sensing and communication (ISAC) scenario, in which a signal is transmitted through a state-dependent wiretap channel with one legitimate receiver with which the transmitter communicates and one honest-but-curious target that the transmitter wants to sense. The secure ISAC channel is modeled as two state-dependent fast-fading channels with correlated Rayleigh fading coefficients and independent additive Gaussian noise components. Delayed channel outputs are fed back to the transmitter to improve the communication performance and to estimate the channel state sequence. We establish and illustrate an achievable secrecy-distortion region for degraded secure ISAC channels under correlated Rayleigh fading. We also evaluate the inner bound for a large set of parameters to derive practical design insights for secure ISAC methods. The presented results include in particular parameter ranges for which the secrecy capacity of a classical wiretap channel setup is surpassed and for which the channel capacity is approached.**

I. Introduction

Integrating the digital and physical world, envisioned for future communication systems, requires a network to react to changes in real-time through sensing and communication [1]. An insightful example is a millimeter wave (mmWave) integrated sensing and communication (ISAC) system that aims to sense a target by estimating relevant channel parameters to fine-tune the communication scheme [2], [3].

There have recently been multiple information-theoretic studies of ISAC that extend previous results, such as [4]–[6]. Focusing on vehicular radar applications for mmWave systems, an information-theoretic model is proposed in [7] for ISAC. In this model, encoded messages are sent over a state dependent channel with generalized feedback such that the state is only known at the receiver and the feedback is used to improve communication and to estimate the channel state. The rate-distortion region is characterized for independent and identically distributed (i.i.d.) channel states and memoryless ISAC channels with strictly causal channel output feedback. Subsequent works include extensions to multiple access channels [8], broadcast channels [7], two-way channels [9], and transmitter actions [10].

Since a single modality is used to both communicate with a legitimate receiver and detect a target, the sensing signal may carry sensitive information about the message communicated, which may then is leaked to a curious target. Since the signal power at the sensed target impacts both the secrecy and sensing performance, there exists a tradeoff between the two [2], [11]–[13]. This tradeoff is characterized in [11] for degraded and reversely-degraded ISAC channels, when the transmitter aims to reliably communicate with the legitimate receiver by using the ISAC channel, estimate the channel state by using the channel output feedback, and keep the message hidden from the target that acts as an eavesdropper. The results in [11] show that it is possible to surpass the secrecy capacity by using the channel output feedback for secure ISAC applications, which is in line with the insights from wiretap channel with feedback results, such as in [14]–[19].

In this work, we establish an achievable rate region for stochastically-degraded secure ISAC channels under bivariate Rayleigh fading by using a Gaussian channel input. Since closed form expressions for this rate region remain elusive, we derive integral expressions from the involved differential entropies, which are amenable to simplified and stable numerical evaluations. Based on the evaluation results, insights are presented including, in particular, parameter ranges for which secure-ISAC rates greater than the secrecy capacity can be achieved and for which the channel capacity is approached. Moreover, we provide accurate approximations, which allow easy-to-compute numerical evaluations.

II. System Model and Problem Definition

We consider the secure ISAC model depicted in Fig. 1, which includes one transmitter, one legitimate receiver, one state estimator, and an eavesdropper (Eve). The transmitter wants to transmit a uniformly distributed message M from the finite message set $\mathcal{M}$ through a fast fading additive Gaussian noise (AGN) secure ISAC channel, in which i.i.d. fading channel coefficients (S_1^n, S_2^n) are causally estimated by the receiver and eavesdropper, respectively. The fading coefficients $(S_{1,i}, S_{2,i})$ with non-negative real-valued alphabet $\mathcal{S}_1 \times \mathcal{S}_2$ are correlated according to a known joint probability density function (pdf) f_{S_1,S_2}, but their realizations are not known by the transmitter. For discussions about how to extend the results to include complex fading channel coefficients and complex noise components, see [20, Section V-A].

Given M, the transmitter generates the channel inputs X^n by using encoding functions $\mathsf{Enc}_i(\cdot)$ such that $X_i = \mathsf{Enc}_i(M, Z^{i-1})$ for all $i = [1 : n]$, where Z^{i-1} is the

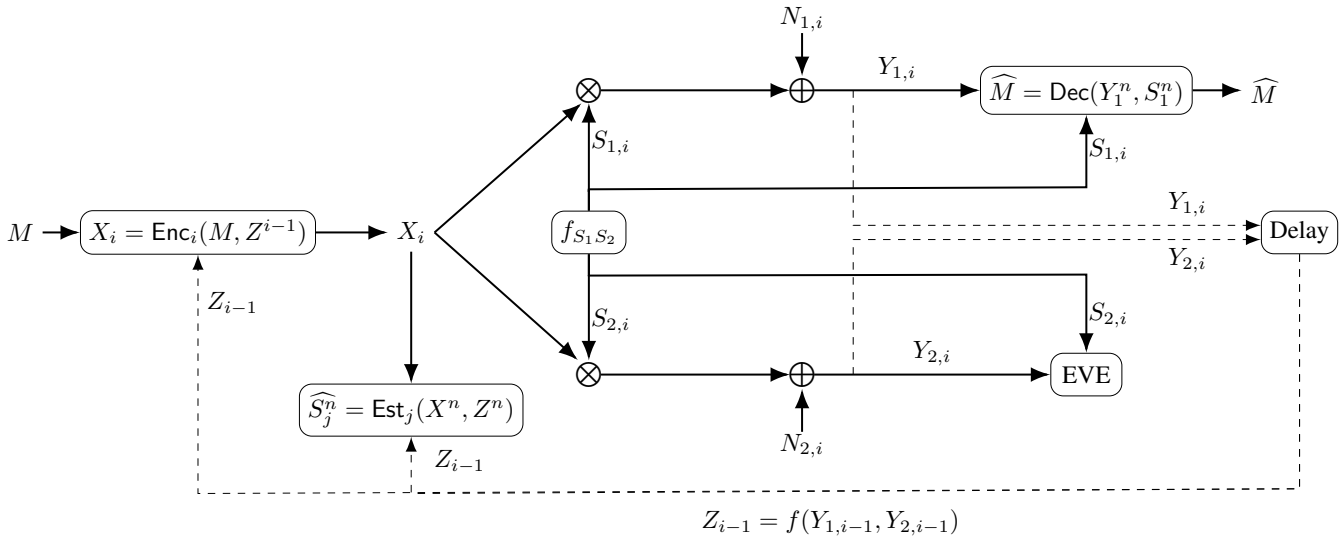

Fig. 1. Secure ISAC model for $i = [1:n]$ and $j = 1, 2$, for which the message M should be kept secret from the eavesdropper. We impose an average transmit power constraint on the channel input symbols X_i and assume independent AGN components $N_{1,i}$ and $N_{2,i}$. We principally consider perfect channel output feedback with unit symbol time delay, i.e., $Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1})$ such that the function $f(\cdot,\cdot)$ is the identity function.

delayed channel output feedback. We impose an average power constraint on the subsequent transmitted symbols, i.e., we have

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}[X_i^2] \le P \tag{1}$$

for all messages M, where $\mathbb{E}[\cdot]$ denotes expectation. The channel output for the legitimate receiver at time i is

$$Y_{1,i} = S_{1,i}X_i + N_{1,i} \tag{2}$$

where $N_{1,i}$ are i.i.d. Gaussian distributed with zero mean, variance $\sigma_{N_1}^2$, and independent of $(S_{1,i}, S_{2,i}, X_i)$. The legitimate receiver observes the sequences (Y_1^n, S_1^n) and estimates the transmitted message as $\widehat{M} = \mathsf{Dec}(Y_1^n, S_1^n)$, where $\mathsf{Dec}(\cdot)$ is a decoding function. Similarly, the channel output for the eavesdropper at time i is

$$Y_{2,i} = S_{2,i}X_i + N_{2,i} \tag{3}$$

where $N_{2,i}$ are i.i.d. Gaussian distributed with zero mean, variance $\sigma_{N_2}^2$, and independent of $(S_{1,i}, S_{2,i}, X_i, N_{1,i})$. The transmitted message M should be kept secret from the eavesdropper that observes (Y_2^n, S_2^n). Finally, the state estimator observes both the channel output feedback

$$Z_{i-1} = f(Y_{1,i-1}, Y_{2,i-1}) \tag{4}$$

and the codeword symbol X_i to estimate the fading channel coefficients (S_1^n, S_2^n) as $\widehat{S_j^n} = \mathsf{Est}_j(X^n, Z^n)$ for $j = 1, 2$, where $\mathsf{Est}_j(\cdot,\cdot)$ is an estimation function with range $\mathcal{S}_j^n$.

For simplicity, we assume the deterministic processing function $f(\cdot,\cdot)$ is the identity function, so the channel output feedback is perfect, i.e., we have noiseless channel output feedback $Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1})$. This simplification allows us to obtain fundamental insights into the optimal coding schemes and helps tackle the noisy feedback scenario, which is generally challenging; see, e.g., achievability results for wiretap channels with generalized output feedback in [19]. Note that the achievability proofs for wiretap channels generally require a local randomness source at the encoder, which is true also for the results given below. The randomness can be provided, e.g., by using hardware-intrinsic security primitives [21]. We next define the secrecy-distortion region for the secure correlated fast-fading ISAC problem.

Definition 1: A secrecy-distortion tuple (R, D_1, D_2) is *achievable* for the secure correlated fast-fading ISAC problem if, for any $\epsilon > 0$, there exist $n \ge 1$, one encoder-decoder pair, and two state estimators $\mathsf{Est}_j(X^n, Y_j^n) = \widehat{S_j^n}$, $j = 1, 2$ such that

$$\Pr[M \ne \widehat{M}] \le \epsilon \qquad \text{(reliability)} \tag{5}$$

$$\frac{1}{n}\log|\mathcal{M}| \ge R - \epsilon \qquad \text{(message rate)} \tag{6}$$

$$\frac{1}{n}I(M; Y_2^n, S_2^n) \le \epsilon \qquad \text{(weak secrecy)} \tag{7}$$

$$\mathbb{E}\big[d_j(S_j^n, \widehat{S_j^n})\big] \le D_j + \epsilon \quad \text{for } j = 1, 2 \qquad \text{(distortions)} \tag{8}$$

where $d_j(s^n, \widehat{s^n}) = \frac{1}{n}\sum_{i=1}^{n} d_j(s_i, \widehat{s}_i)$ for $j = 1, 2$ are averaged per-letter distortion metrics.

The secrecy-distortion region $\mathcal{R}_{\text{S-ISAC}}$ is the closure of the set of all achievable tuples for the secure correlated fast-fading ISAC problem under perfect channel output feedback. $\Diamond$

Since the transmitted message is independent of the channel state, the secrecy condition in (7) is equivalent to the inequality $I(M; Y_2^n | S_2^n) \le n\epsilon$. Furthermore, there are ISAC models, such as in [22], that consider a practical application, in which only a part of the channel parameters are relevant for the transmitter. By not imposing the estimation of the exact channel state at the transmitter via adapting (8), one can extend our results for such practical settings.

III. Correlated-Fading AGN ISAC Channel Secrecy-Distortion Regions

A. Secrecy-Distortion Region

We first define physically- and stochastically-degraded ISAC channels; see also [7], [11].

Definition 2: An ISAC channel is *physically-degraded* if X and (Y_2, S_2) are conditionally independent given (Y_1, S_1). Moreover, an ISAC channel is *stochastically-degraded* if the joint probability distribution of (X, Y_1, S_1, Y_2, S_2) can be preserved by using a marginal probability distribution of (X, Y_1, S_1) such that the corresponding ISAC channel is physically-degraded. $\lozenge$

We next state the secrecy-distortion region given in [11] for physically-degraded secure ISAC channels under strong secrecy, i.e., $I(M; Y_2^n, S_2^n) \leq \epsilon$, for discrete-alphabet random variables and state estimators of the form $\mathsf{Est}_j(X^n, Y_1^n, Y_2^n) = \widehat{S_j^n}$. We then evaluate the entropy terms in the given rate region to characterize the secrecy-distortion regions for the secure ISAC channels considered in this work.

Theorem 1 ([11, Theorem 1]): For physically-degraded ISAC channels, the secrecy-distortion region is the union w. r. t. all probability distributions P_X of the rate-distortion tuples (R, D_1, D_2) satisfying

$$D_j \geq \mathbb{E}[d_j(S_j, \widehat{S}_j))] \qquad \text{for } j = 1, 2 \tag{9}$$

$$R \leq \min \Big\{ \big(H(Y_1, S_1 | Y_2, S_2) - H(S_1 | Y_1, Y_2, S_2, X) \big), \; I(X; Y_1 | S_1) \Big\} \tag{10}$$

$$\mathsf{Est}_j(x, y_1, y_2) = \underset{\tilde{s} \in \widehat{\mathcal{S}}_j}{\operatorname{argmin}} \sum_{s_j \in \mathcal{S}_j} P_{S_j | X Y_1 Y_2}(s_j | x, y_1, y_2) \; d_j(s_j, \tilde{s}). \tag{11}$$

The measures in the secrecy-distortion region in Theorem 1 remain valid for correlated-fading channels with independent AGN components, as depicted in Fig. 1, for the following reasons: (i) any achievability proof for strong secrecy also follows under weak secrecy, and by replacing δ_n in [11, Eq. (72)] with $n\delta_n$, one can obtain the matching converse for weak secrecy; (ii) the outer bound applies to arbitrary random variables and does not assume any degradedness; (iii) there is a discretization procedure to generalize the achievability proof to well-behaved continuous-alphabet random variables, such as the considered fading and noise distributions [23, Remark 3.8]; (iv) one can show that changing the estimator form does not change the entropy terms in the rate region, although achieved distortion levels might change since the estimators given in (11) should be also adapted. Moreover, the state estimators considered in Definition 1 make the measures in Theorem 1 valid also for stochastically-degraded channels, which follows because the constraints (5)–(8) in Definition 1 only depend on the marginal probability distributions of (X, Y_1, S_1) and (X, Y_2, S_2). This extension is important, as the practical secure ISAC model considered in this work is not physically-degraded.

We next consider the secrecy-distortion region for stochastically-degraded ISAC channels for the secure ISAC model given in Fig. 1 and focus on the secrecy rate. In what follows expectations with subscripts of random variables indicate that we first calculate the argument of the expectation for fixed realization of the subscript and afterwards calculate the expectation w. r. t. the distribution of the subscript. Using [12, Proposition 1], we have following result.

Corollary 1: The secrecy-distortion region for the secure ISAC model depicted in Fig. 1 is the union w. r. t. all pdfs f_X of the rate-distortion tuples (R, D_1, D_2) satisfying

$$R \leq \min \Big\{ \mathbb{E}_{S_1, S_2}\big[h(S_1 X + N_1 | S_2 X + N_2)\big] - h(N_1) \tag{12a}$$

$$+ \; \mathbb{E}_X\big[h(S_1 X + N_1 | S_2)\big], \tag{12b}$$

$$\mathbb{E}_{S_1}\big[h(S_1 X + N_1)\big] - h(N_1) \Big\} \tag{12c}$$

such that (9) is satisfied for a given distortion metric by using estimators of the form $\mathsf{Est}_j(X^n, Y_1^n, Y_2^n) = \widehat{S_j^n}$.

Denote the complementary cumulative distribution function of a real-valued random variable U as $\bar{F}_U(u) = \Pr[U \geq u]$. We provide a sufficient but not necessary condition to generate a stochastically-degraded secure ISAC channel based on the stochastic ordering of the channel outputs Y_1 and Y_2.

Proposition 1: The secure ISAC channel in (2) and (3) is stochastically-degraded if $S_1^2/\sigma_{N_1}^2$ is *stochastically larger* than $S_2^2/\sigma_{N_2}^2$, i.e., if we have, for all $s \geq 0$,

$$\bar{F}_{S_1^2}\left(\frac{s}{\sigma_{N_1}^2}\right) \geq \bar{F}_{S_2^2}\left(\frac{s}{\sigma_{N_2}^2}\right). \tag{13}$$

The proof of Proposition 1 follows from [20, Lemma 3] after appropriate changes to account for the noise variances. For necessity discussions see [24, Lemmas 1–4].

We next specify the correlated fast-fading distribution, for which we characterize an achievable secrecy-distortion region, when the secure ISAC channel is stochastically-degraded.

B. Bivariate Rayleigh Fading

Suppose the fading random variables (S_1, S_2) are distributed according to a bivariate Rayleigh fading distribution with pdf

$$f_{S_1, S_2}(s_1, s_2) = \frac{4 s_1 s_2}{\sigma_{S_1}^2 \sigma_{S_2}^2 (1 - \rho^2)} \exp\left(- \frac{1}{1 - \rho^2} \left(\frac{s_1^2}{\sigma_{S_1}^2} + \frac{s_2^2}{\sigma_{S_2}^2} \right) \right) \times I_0\left(\frac{2}{1 - \rho^2} \sqrt{\rho^2 \frac{s_1^2}{\sigma_{S_1}^2} \frac{s_2^2}{\sigma_{S_2}^2}} \right), \quad s_1, s_2 \geq 0 \tag{14}$$

where $I_0(x) = \frac{1}{\pi} \int_0^\pi e^{x \cos(\phi)} \mathrm{d}\phi$ denotes the zeroth-order modified Bessel function of the first kind [25, 10.25.2, 10.32.1]. The parameters $\sigma_{S_1}^2$ and $\sigma_{S_2}^2$ in (14) are

$$\sigma_{S_1}^2 = \mathbb{E}\big[S_1^2\big], \qquad \sigma_{S_2}^2 = \mathbb{E}\big[S_2^2\big] \tag{15}$$

denoting (with a slight abuse of common notation) the second moments of S_1 and S_2. Furthermore, ρ^2, for $0 \leq \rho^2 < 1$, denotes the power correlation coefficient, i.e., we have

$$\operatorname{cor}(S_1^2, S_2^2) = \rho^2 \tag{16}$$

which is the Pearson correlation coefficient between S_1^2 and S_2^2. For later reference, we provide the marginal pdfs f_{S_1} and f_{S_2} of S_1 and S_2

$$f_{S_1}(s_1) = \frac{2\,s_1}{\sigma_{S_1}^2} \exp\Big(- \frac{s_1^2}{\sigma_{S_1}^2}\Big), \quad s_1 \geq 0, \tag{17}$$

$$f_{S_2}(s_2) = \frac{2s_2}{\sigma_{S_2}^2} \exp\Big(- \frac{s_2^2}{\sigma_{S_2}^2}\Big), \quad s_2 \geq 0 \tag{18}$$

as well as further moments

$$\mathbb{E}\big[S_1\big] = \sqrt{\frac{\pi}{4}\sigma_{S_1}^2}, \quad \mathbb{E}\big[S_2\big] = \sqrt{\frac{\pi}{4}\sigma_{S_2}^2},$$

$$\operatorname{var}\big[S_1\big] = \Big(1 - \frac{\pi}{4}\Big)\sigma_{S_1}^2, \quad \operatorname{var}\big[S_2\big] = \Big(1 - \frac{\pi}{4}\Big)\sigma_{S_2}^2, \tag{19}$$

$$\operatorname{cov}\big[S_1, S_2\big] = \sigma_{S_1}\sigma_{S_2}\left(E\Big(\sqrt{\rho^2}\Big) - \frac{1}{2}\big(1-\rho^2\big)K\Big(\sqrt{\rho^2}\Big) - \frac{\pi}{4}\right) \tag{20}$$

where $\operatorname{cov}[\cdot,\cdot]$ and $\operatorname{var}[\cdot]$ denote (co)variance and

$$K(z) = \int_0^{\frac{\pi}{2}} \big(1 - z^2\sin^2(t)\big)^{-\frac{1}{2}}\,\mathrm{d}t \tag{21}$$

$$E(z) = \int_0^{\frac{\pi}{2}} \big(1 - z^2\sin^2(t)\big)^{\frac{1}{2}}\,\mathrm{d}t \tag{22}$$

are the complete elliptic integrals of the first and second kind [25, 19.2.4, 19.2.5, 19.2.8]. Moreover, with the marginals (17) and (18) and basic transformations we obtain the complementary cumulative distribution functions of S_1^2 and S_2^2 as

$$\bar{F}_{S_1^2}(s_1) = \exp\left(-\frac{s_1}{\sigma_{S_1}^2}\right), \quad s_1 \geq 0,$$

$$\bar{F}_{S_2^2}(s_2) = \exp\left(-\frac{s_2}{\sigma_{S_2}^2}\right), \quad s_2 \geq 0.$$

Therefore, for the bivariate Rayleigh distribution, the condition (13) on stochastic degradedness is equivalent to

$$\frac{\sigma_{N_2}^2}{\sigma_{N_1}^2} \;\leq\; \frac{\sigma_{S_1}^2}{\sigma_{S_2}^2}. \tag{23}$$

IV. Achievable Rates for Gaussian Input

Given (12), the main goal is to find the maximum of its right-hand side w. r. t. the distribution P_X of the random variable X. However, this is a difficult optimization problem, so we provide instead an achievable rate for a Gaussian input X. Subsequently, we evaluate (12a)–(12c) for X being a zero-mean Gaussian random variable with positive variance P, where X is independent of (S_1, S_2, N_1, N_2).

A. Evaluation of Eq. (12a)

Proposition 2: Under the assumptions above, we have

$$\begin{aligned}\mathbb{E}_{S_1,S_2}\big[h(S_1X + N_1|S_2X + N_2)\big] - h(N_1)\\ = \frac{1}{2}\int_0^\infty \log_2(1+s) f_S(s)\,\mathrm{d}s\end{aligned} \tag{24}$$

where

$$\begin{aligned}f_S(s) = \sigma_1^2\sigma_2^2 \exp\left(\frac{\sigma_2^2}{2P(1-\rho^2)}\right)\exp\Big(-\frac{\sigma_1^2 s + \sqrt{A(s)}}{2P(1-\rho^2)}\Big)\\ \times\left(\frac{1}{2P\sqrt{A(s)}} + \frac{\sigma_1^2 s + \sigma_2^2}{2PA(s)} + (1-\rho^2)\frac{\sigma_1^2 s + \sigma_2^2}{A(s)^{\frac{3}{2}}}\right)\end{aligned} \tag{25}$$

with

$$A(s) = (\sigma_1^2 s)^2 + (2 - 4\rho^2)\sigma_1^2\sigma_2^2 s + (\sigma_2^2)^2, \tag{26}$$

$$\sigma_1^2 = \frac{\sigma_{N_1}^2}{\sigma_{S_1}^2}, \quad \sigma_2^2 = \frac{\sigma_{N_2}^2}{\sigma_{S_2}^2}. \tag{27}$$

The derivation of Proposition 2 is given in Appendix A. The representation in Proposition 2 as a one-dimensional integral is particularly convenient for numerical evaluations and is used in Section V.

B. Evaluation of Eq. (12b)

First, we rewrite (12b) as

$$\mathbb{E}_X\big[h(S_1X + N_1|S_2)\big] = \mathbb{E}_X\big[h(S_1X + N_1, S_2)\big] - h(S_2).$$

Using the marginal pdf (18) of S_2, we obtain

$$\begin{aligned}h(S_2) &= -\int_0^\infty f_{S_2}(s_2)\log_2\big(f_{S_2}(s_2)\big)\,\mathrm{d}s_2\\ &= -2\log_2\left(\frac{2}{\sigma_{S_2}}\right)\int_0^\infty u\exp\big(-u^2\big)\,\mathrm{d}u\\ &\quad - 2\int_0^\infty u\exp\big(-u^2\big)\log_2(u)\,\mathrm{d}u\\ &\quad + \frac{2}{\ln(2)}\int_0^\infty u^3\exp\big(-u^2\big)\,\mathrm{d}u\\ &= \frac{1}{\ln(2)}\left(1 + \frac{\gamma}{2}\right) + \frac{1}{2}\log_2\left(\frac{\sigma_{S_2}^2}{4}\right)\end{aligned} \tag{28}$$

using the substitution $u = s_2/\sigma_{S_1}$ and the integral relations $\int_0^\infty u\exp(-u^2)\,\mathrm{d}u = \int_0^\infty u^3\exp(-u^2)\,\mathrm{d}u = 1/2$ and $\int_0^\infty u\exp(-u^2)\ln(u)\,\mathrm{d}u = -\gamma/4$, where $\gamma = 0.577216\ldots$ denotes Euler's constant [25, 5.2.3].

The evaluation of $\mathbb{E}_X\big[h(S_1X + N_1, S_2)\big]$ requires the following calculations. Let $Y_1(x) = xS_1 + N_1$. Then the joint pdf of $\big(Y_1(x), S_2\big)$ is given for $x > 0$ by the convolution integral

$$f_{Y_1(x),S_2}(y_1, s_2) = \int_0^\infty \frac{1}{x} f_{S_1,S_2}\left(\frac{t}{x}, s_2\right) f_{N_1}(y_1 - t)\mathrm{d}t \tag{29}$$

for $-\infty < y_1 < \infty$ and $s_2 \geq 0$. Furthermore, we have

$$\begin{aligned}&h(xS_1 + N_1, S_2) =\\ &-\int_{y_1=-\infty}^{\infty}\int_{s_2=0}^{\infty} f_{Y_1(x),S_2}(y_1, s_2)\log_2\Big(f_{Y_1(x),S_2}(y_1, s_2)\Big)\,\mathrm{d}y_1\mathrm{d}s_2.\end{aligned} \tag{30}$$

Due to symmetry, we obtain

$$\begin{aligned}&\mathbb{E}_X\big[h(S_1X + N_1, S_2)\big]\\ &\qquad = 2\int_0^\infty h(xS_1 + N_1, S_2) f_X(x)\,\mathrm{d}x.\end{aligned} \tag{31}$$

As we can evaluate the convolution integral in (29) numerically, we rely on numerical calculations also for (30) and (31).

An upper bound of $\mathbb{E}_X\big[h(S_1X+N_1|S_2)\big]$, for which the numerical evaluation is much easier is the following.

Proposition 3: Under the assumptions above, we have

$$\begin{aligned}&\mathbb{E}_X\big[h(S_1X+N_1|S_2)\big]\\&\le\frac{1}{2}\log_2\left(2(\pi\mathrm{e})^2\sigma_{S_1}^2\tilde{c}\,P\right)+\frac{\pi}{2\ln(2)}\operatorname{erfi}\left(\sqrt{\frac{\tilde{\sigma}_1^2}{2\,\tilde{c}\,P}}\right)+1\\&\quad-\frac{1}{\ln(2)}\left(\frac{\tilde{\sigma}_1^2}{2\,\tilde{c}\,P}\,{}_2F_2\big(1,1;\tfrac{3}{2},2;\frac{\tilde{\sigma}_1^2}{2\,\tilde{c}\,P}\big)+1+\gamma\right)\end{aligned}\tag{32}$$

with the parameters

$$\tilde{\sigma}_1^2=\left(1-\frac{\pi}{4}\right)\frac{\sigma_{N_1}^2}{\sigma_{S_1}^2},\quad \tilde{c}=\left(1-\frac{\pi}{4}\right)^2\left(1-\operatorname{cor}(S_1,S_2)^2\right)\tag{33}$$

where

$$\operatorname{cor}[S_1,S_2]=\frac{\operatorname{cov}[S_1,S_2]}{\sqrt{\operatorname{var}[S_1]\operatorname{var}[S_2]}}\tag{34}$$

$$=\left(1-\frac{\pi}{4}\right)^{-1}\left(E\left(\sqrt{\rho^2}\right)-\frac{1}{2}\big(1-\rho^2\big)K\left(\sqrt{\rho^2}\right)-\frac{\pi}{4}\right)\tag{35}$$

with $K(\cdot)$ and $E(\cdot)$ the elliptic integrals given in (21) and (22), respectively. Moreover, $\operatorname{erfi}(y)=-\imath\operatorname{erf}(\imath y)=-\frac{2\imath}{\sqrt{\pi}}\int_0^{\imath y}\exp\big(-t^2\big)\,\mathrm{d}t$ denotes the imaginary error function [25, 7.2.1] and ${}_pF_q(a_1,\ldots,a_p;b_1,\ldots,b_q;z)$ denotes the generalized hypergeometric function [25, 16.2.1].

The proof of Proposition 3 is given in Appendix B.

C. Evaluation of Eq. (12c)

Proposition 4: Under the assumptions above, we have

$$\begin{aligned}&\mathbb{E}_{S_1}\big[h(S_1X+N_1)\big]-h(N_1)\\&\qquad=-\frac{1}{2\ln(2)}\exp\left(\frac{1}{P}\right)\operatorname{Ei}\left(\frac{1}{P}\right),\end{aligned}\tag{36}$$

where $\operatorname{Ei}(z)=-\int_{-z}^{\infty}\frac{\exp(-t)}{t}\,\mathrm{d}t$ denotes the exponential integral function [25, 6.2.5].

The derivation of Proposition 4 is given in Appendix C.

V. Numerical Results and Discussions

We next evaluate the results of Section IV numerically for interesting parameter regimes. To simplify notation, we denote the sum of (12a) and (12b) by R_α and the sum of (12a) and the upper bound (32) of (12b) by $R_{\alpha,\mathrm{ub}}$, respectively. Furthermore, we denote (12c) by R_β. With this notation, we have for the achievable rate in Section IV

$$R\le\min\big\{R_\alpha,R_\beta\big\}\le\min\big\{R_{\alpha,\mathrm{ub}},R_\beta\big\}.\tag{37}$$

Based on the representation in (24)–(26) as one-dimensional integral, we numerically evaluate (12a) with MATHEMATICA. Similarly, the upper bound in (32) is numerically evaluated, and the same applies to (12c) using (36). However, the numerical evaluation of (12b) is more involved. First, we numerically calculate the convolution integral in (29) on a sufficiently-dense grid for the variables y_1 and s_2. Then, we numerically calculate the differential entropy $h(xS_1+N_1,S_2)$ using (30) based on an interpolated version of the density $f_{Y_1(x),S_2}(y_1,s_2)$. Repeating these calculations for a sufficiently-dense set of values x, we numerically calculate $\mathbb{E}_X\big[h(S_1X+N_1,S_2)\big]$ using (31) and an interpolated version of the function $x\mapsto h(xS_1+N_1,S_2)$. Combining with (28), we finally obtain (12b).

$\rho^2\in\{0.01,0.50,0.90\}$	
$\sigma_{N_1}^2=1$	$\sigma_{N_2}^2\in\{0.10,0.50\}$
$\sigma_{S_1}^2\in\{0.10,0.50,1.00\}$	$\sigma_{S_2}^2\in\big\{\sigma_{S_1}^2/\sigma_{N_2}^2\,,\,\sigma_{S_1}^2/10\sigma_{N_2}^2\big\}$

TABLE I
PARAMETER SETS FOR NUMERICAL CALCULATIONS

We consider the case of a stochastically-degraded secure ISAC channel, i. e., we assume the chosen parameter values satisfy inequality (23). Moreover, we assume that $\sigma_{N_1}^2>\sigma_{N_2}^2$, which is the interesting regime where the corresponding wiretap channel does not allow secure communication. Table I summarizes parameter sets satisfying these conditions for which we subsequently present and discuss numerical results.

In Figs. 2–4, given in Appendix D, we illustrate the results for R_α, $R_{\alpha,\mathrm{ub}}$, and R_β as a function of the transmit power P for different values of the power correlation coefficient ρ^2. For the matrix of subfigures in each figure, the parameter $\sigma_{S_1}^2$ is modified from top to bottom and the parameter $\sigma_{N_2}^2$ from left to right, respectively, whereas $\sigma_{N_1}^2=1$ is fixed. The parameter $\sigma_{S_2}^2$ is modified within a subfigure.

Our conclusions for a degraded secure ISAC channel with correlated Rayleigh fading for the parameter ranges given in Table I are discussed next.

From (36), we observe that R_β is only a function of the transmit power P such that the curves of R_β are the same in all diagrams. From (24)–(26), we observe that (12a) as a summand of R_α and $R_{\alpha,\mathrm{ub}}$ is a function of ρ^2, P, and the parameter ratios $\sigma_{N_1}^2/\sigma_{S_1}^2$ and $\sigma_{N_2}^2/\sigma_{S_2}^2$. Similarly, the upper bound (32) as a summand of $R_{\alpha,\mathrm{ub}}$, is a function of ρ^2, P, $\sigma_{S_1}^2$, and $\sigma_{N_1}^2$ and it does not depend on $\sigma_{S_2}^2$ and $\sigma_{N_2}^2$. Although not explicit from the derived equations, the numerical results also show that (12b) as a summand of R_α does not depend on $\sigma_{S_2}^2$ and $\sigma_{N_2}^2$. Therefore, the curves of R_α and $R_{\alpha,\mathrm{ub}}$ in Figs. 2–4 within one subfigure and between two subfigures in the same row differ only due to the summand (12a).

The results show that $R_{\alpha,\mathrm{ub}}$ and R_α curves behave highly similarly with a small constant gap. Thus, for most of the parameter constellations the much-easier-to-calculate $R_{\alpha,\mathrm{ub}}$, instead of R_α, can be used to interpret the results.

Furthermore, we observe the following monotonicities: R_α increases for increasing parameters $\sigma_{S_1}^2$ or $\sigma_{N_2}^2$ and for decreasing parameters $\sigma_{S_2}^2$ or ρ^2. The interesting regime where the channel capacity is approached is when R_β determines the right-hand side of (12). The range for the power P where R_β determines (12), increases with increasing $\sigma_{S_1}^2$ or $\sigma_{N_2}^2$ and decreasing $\sigma_{S_2}^2$ or ρ^2. For low correlation ρ^2, this range stretches over all considered power values for almost

all parameter constellations, whereas for highly correlated fading coefficients it shrinks to low power values. Thus, in the low power regime channel capacity is always approached irrespective of the values of the remaining parameters.

ACKNOWLEDGMENT

This work has been supported by the German Federal Ministry of Education and Research (BMBF) through the research hub *6G-life* under grant 16KISK001K, the German Research Foundation (DFG) as part of Germany's Excellence Strategy – EXC 2050/1 - Project ID 390696704 - Cluster of Excellence *CeTI*, the U.S. National Science Foundation (NSF) under grants CCF 1955401 and 2148400, the U.S. Department of Transportation under grant 69A3552348327 for the CARMEN+ University Transportation Center, the ZENITH Research and Leadership Career Development Fund, and the ELLIIT funding endowed by the Swedish government.

REFERENCES

[1] T. Wild, V. Braun, and H. Viswanathan, "Joint design of communication and sensing for beyond 5G and 6G systems," *IEEE Access*, vol. 9, pp. 30 845–30 857, Feb. 2021.

[2] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Towards multi-functional 6G wireless networks: Integrating sensing, communication and security," July 2021, [Online]. Available: arxiv.org/abs/2107.07735.

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

[4] W. Zhang, S. Vedantam, and U. Mitra, "Joint transmission and state estimation: A constrained channel coding approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 7084–7095, Oct. 2011.

[5] H. Wymeersch *et al.*, "Integration of communication and sensing in 6G: A joint industrial and academic perspective," in *IEEE Annu. Int. Symp. Pers., Indoor Mobile Radio Commun.*, Helsinki, Finland, Sep. 2021, pp. 1–7.

[6] S. Buzzi, C. D'Andrea, and M. Lops, "Using Massive MIMO arrays for joint communication and sensing," in *Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, Nov. 2019, pp. 5–9.

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

[8] M. Kobayashi, H. Hamad, G. Kramer, and G. Caire, "Joint state sensing and communication over memoryless multiple access channels," in *IEEE Int. Symp. Inf. Theory*, Paris, France, July 2019, pp. 270–274.

[9] M. Ahmadipour and M. Wigger, "An information-theoretic approach to collaborative integrated sensing and communication for two-transmitter systems," *IEEE J. Sel. Areas Inf. Theory*, vol. 4, pp. 112–127, June 2023.

[10] T. Welling, O. Günlü, and A. Yener, "Transmitter actions for secure integrated sensing and communication," in *IEEE Int. Symp. Inf. Theory*, Athens, Greece, July 2024, to appear.

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

[12] O. Günlü, M. Bloch, R. F. Schaefer, and A. Yener, "Secure integrated sensing and communication for binary input additive white Gaussian noise channels," in *IEEE Int. Symp. Joint Commun. & Sensing*, Seefeld, Austria, Mar. 2023, pp. 1–6.

[13] M. Ahmadipour, M. Wigger, and S. Shamai, "Integrated communication and receiver sensing with security constraints on message and state," in *IEEE Int. Symp. Inf. Theory*, Taipei, Taiwan, June 2023, pp. 2738–2743.

[14] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," *Electron. Notes Discrete Math.*, vol. 21, pp. 155–159, Aug. 2005.

[15] A. Cohen and A. Cohen, "Wiretap channel with causal state information and secure rate-limited feedback," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1192–1203, Mar. 2016.

[16] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "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.

[17] B. Dai, A. J. H. Vinck, Y. Luo, and Z. Zhuang, "Capacity region of non-degraded wiretap channel with noiseless feedback," in *IEEE Int. Symp. Inf. Theory*, Cambridge, MA, July 2012, pp. 244–248.

[18] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8115–8130, Dec. 2013.

[19] G. Bassi, P. Piantanida, and S. Shamai, "The wiretap channel with generalized feedback: Secure communication and key generation," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2213–2233, Apr. 2019.

[20] D. Tse and R. Yates, "Fading broadcast channels with state information at the receivers," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3453–3471, June 2012.

[21] O. Günlü and R. F. Schaefer, "An optimality summary: Secret key agreement with physical unclonable functions," *Entropy*, vol. 23, no. 1, p. 16, 2020.

[22] Y. Liu, M. Li, A. Liu, J. Lu, R. Du, and T. X. Han, "Generalized modeling and fundamental limits for multiple-access integrated sensing and communication systems," May 2022, [Online]. Available: arxiv.org/abs/2205.05328.

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

[24] P.-H. Lin and E. Jorswieck, "On the fast fading Gaussian wiretap channel with statistical channel state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 46–58, Jan. 2016.

[25] F. W. J. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, Eds., *NIST Handbook of Mathematical Functions*. Cambridge, UK: Cambridge University Press, 2010.

[26] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*, 4th ed. Boston, MA, US: McGraw-Hill, 2002.

[27] A. P. Prudnikov, Y. A. Brychov, and O. I. Marichev, *Integrals and Series, Volume 2: Special Functions*. New York, NY, USA: Gordon and Breach Science, 1986.

[28] ——, *Integrals and Series, Volume 1: Elementary Functions*. New York, NY, USA: Gordon and Breach, 1986.

APPENDIX A
PROOF OF PROPOSITION 2

Proof: Let us fix $S_1 = s_1$ and $S_2 = s_2$ for some $s_1, s_2 \geq 0$. Then $(s_1X + N_1, s_2X + N_2)$ is jointly Gaussian with zero mean and covariance matrix

$$\begin{pmatrix} s_1^2P + \sigma_{N_1}^2 & s_1s_2P \\ s_1s_2P & s_2^2P + \sigma_{N_2}^2 \end{pmatrix}$$

since X, N_1, and N_2 are independent Gaussian random variables with positive variances P, $\sigma_{N_1}^2$, and $\sigma_{N_2}^2$. For the conditional differential entropy $h\big(s_1X + N_1|s_2X + N_2\big)$, we therefore obtain

$$\begin{aligned} &h\big(s_1X + N_1 \,|\, s_2X + N_2\big) \\ &\quad = h\big(s_1X + N_1, s_2X + N_2\big) - h\big(s_2X + N_2\big) \\ &\quad = \frac{1}{2}\log_2\left(2\pi\mathrm{e}\sigma_{N_1}^2\right) + \frac{1}{2}\log_2\left(1 + \frac{s_1^2/\sigma_{N_1}^2}{s_2^2/\sigma_{N_2}^2 + 1/P}\right). \end{aligned} \tag{38}$$

Using (38), we can write

$$\begin{aligned} &\mathbb{E}_{S_1,S_2}\big[h(S_1X + N_1|S_2X + N_2)\big] \\ &\qquad = h(N_1) + \frac{1}{2}\,\mathbb{E}_S\big[\log_2\big(1 + S\big)\big] \end{aligned}$$

where the random variable S is given by

$$S = \frac{T_1}{T_2 + 1/P}$$

with $(T_1, T_2) = \big(S_1^2/\sigma_{N_1}^2, S_2^2/\sigma_{N_2}^2\big)$. Since S is a ratio of random variables, the pdf f_S of S has the following integral representation [26, Eq. 6.60]

$$f_S(s) = \int_{1/P}^{\infty} u f_{T_1,T_2}\big(s \cdot u, u - 1/P\big)\,\mathrm{d}u, \quad s \geq 0 \tag{39}$$

where f_{T_1,T_2} is the joint pdf of (T_1, T_2) given by

$$f_{T_1,T_2}(t_1,t_2) = \frac{\sigma_1^2\sigma_2^2}{(1-\rho^2)} \exp\bigg(-\frac{1}{1-\rho^2}\Big(\sigma_1^2 t_1 + \sigma_2^2 t_2\Big)\bigg) \times I_0\bigg(\frac{2}{1-\rho^2}\sqrt{\rho^2\,\sigma_1^2 t_1\,\sigma_2^2 t_2}\bigg), \quad t_1, t_2 \geq 0 \tag{40}$$

where σ_1^2 and σ_2^2 are as specified in (27).

We substitute $\tilde{u} = (u - 1/P)$ in (39), plug it in (40), and then subsitute $v = \sqrt{\tilde{u}(\tilde{u} + 1/P)}$ to obtain

$$f_S(s) = \frac{\sigma_1^2\sigma_2^2}{1-\rho^2} \exp\bigg(\frac{\sigma_2^2}{2P(1-\rho^2)}\bigg) \exp\bigg(-\frac{\sigma_1^2 s}{2P(1-\rho^2)}\bigg) \times \int_0^{\infty} \bigg[\frac{\theta v}{\sqrt{v^2+\theta^2}} + v\bigg] \exp\Big(-\alpha\sqrt{v^2+\theta^2}\Big) I_0\big(\beta v\big)\,\mathrm{d}v$$

where

$$\alpha = \frac{\sigma_1^2 s + \sigma_2^2}{1-\rho^2}, \quad \beta = 2\frac{\sqrt{\rho^2\sigma_1^2\sigma_2^2\, s}}{1-\rho^2}, \quad \theta = \frac{1}{2P}.$$

Using this representation, we can directly apply [27, Sec. 2.5.6.10] and [27, Sec. 2.5.6.13]. After collecting terms we finally obtain the form of the density f_S given in (25), which completes the proof. ∎

Appendix B
Proof of Proposition 3

Proof: Fix $X = x$ for some $x \in \mathbb{R}$. Then, the differential entropy $h\big(xS_1 + N_1, S_2\big)$ is bounded by

$$h\big(xS_1 + N_1, S_2\big) \leq \frac{1}{2}\log_2\bigg((2\pi\mathrm{e})^2\Big(\mathrm{var}\big[xS_1 + N_1\big]\mathrm{var}\big[S_2\big] - \big(\mathrm{cov}\big[xS_1 + N_1, S_2\big)\big]^2\Big)\bigg)$$

as a result of the differential entropy maximizing property of the Gaussian distribution with a given covariance matrix. Since S_1, S_2, and N_1 are independent, we have

$$\begin{aligned}\mathrm{var}\big[xS_1 + N_1\big] &= x^2\mathrm{var}[S_1] + \mathrm{var}[N_1],\\ \mathrm{cov}\big[xS_1 + N_1, S_2\big] &= x\,\mathrm{cov}\big[S_1, S_2\big].\end{aligned}$$

With the variance $\mathrm{var}[S_1]$ and covariance $\mathrm{cov}\big[S_1, S_2\big]$ given in (19) and (20), we obtain

$$h\big(xS_1 + N_1, S_2\big) \leq a + \frac{1}{2}\log_2\big(\tilde{c}\,x^2 + \tilde{\sigma}_1^2\big)$$

where $\tilde{c}$ and $\tilde{\sigma}_1^2$ are as defined in (33) and

$$a = \frac{1}{2}\log_2\big((2\pi\mathrm{e})^2\sigma_{S_1}^2\sigma_{S_2}^2\big).$$

Due to the monotonicity of the integral and symmetry properties, we have

$$\begin{aligned}&\mathbb{E}_X\big[h(S_1X + N_1|S_2)\big]\\ &\quad= \mathbb{E}_X\big[h(S_1X + N_1, S_2)\big] - h(S_2)\\ &\quad\leq 2\int_0^{\infty}\bigg(a + \frac{1}{2}\log_2\big(\tilde{c}\,x^2 + \tilde{\sigma}_1^2\big)\bigg) f_X(x)\,\mathrm{d}x - h(S_2).\end{aligned}$$

To evaluate the integral, we use the substitution $u = x^2$, the correspondence [28, 2.6.23.4][1], and the identities $\mathrm{erfi}(y) = -\imath\,\mathrm{erf}(\imath y)$ and $\frac{\sqrt{\pi}}{2\,z}\mathrm{erf}(z) = {}_1F_1\big(\frac{1}{2}; \frac{3}{2}; -z^2\big)$ [25, 13.6.7]. Using the expression of the differential entropy $h(S_2)$ given in (28) yields the bound for $\mathbb{E}_X\big[h(S_1X + N_1|S_2)\big]$ given in Proposition 3. ∎

Appendix C
Proof of Proposition 4

Proof: Fix $S_1 = s_1$ for some $s_1 \geq 0$. Then, $s_1X + N_1$ is a Gaussian random variable with zero mean and variance $s_1^2P + \sigma_{N_1}^2$ since X and N_1 are independent Gaussian random variables with positive variances P and $\sigma_{N_1}^2$. For the differential entropy $h\big(s_1X + N_1\big)$, we obtain

$$h\big(s_1X + N_1\big) = \frac{1}{2}\log_2\big(2\pi\mathrm{e}\sigma_{N_1}^2P\big) + \frac{1}{2}\log_2\bigg(\frac{s_1^2}{\sigma_{N_1}^2} + \frac{1}{P}\bigg). \tag{41}$$

Using (41), we can write

$$\begin{aligned}&\mathbb{E}_{S_1}\big[h(S_1X + N_1)\big]\\ &\quad= h(N_1) + \frac{1}{2}\log_2\big(P\big) + \frac{1}{2}\,\mathbb{E}_{T_1}\big[\log_2\big(T_1 + 1/P\big)\big]\end{aligned}$$

where $T_1 = S_1^2/\sigma_{N_1}^2$. With the marginal pdf (17) of the random variable S_1 and basic density transformation, we obtain the pdf

$$f_{T_1}(t_1) = \exp(-t_1), \quad t_1 \geq 0$$

of the random variable T_1 such that we have

$$\begin{aligned}&\mathbb{E}_{T_1}\big[\log_2\big(T_1 + 1/P\big)\big]\\ &\quad= \int_0^{\infty}\log_2\big(t_1 + 1/P\big)\exp(-t_1)\,\mathrm{d}t_1\\ &\quad= -\log_2(P) - \frac{1}{\ln(2)}\exp\bigg(\frac{1}{P}\bigg)\mathrm{Ei}\bigg(-\frac{1}{P}\bigg).\end{aligned}$$

The integral is solved using the substitution $u = (t_1 + 1/P)$ and integration by parts. Collecting the terms yields (36). ∎

Appendix D
Figures for Numerical Results

See Figs. 2-4 below.

[1] Please note that in [28, 2.6.23.4] the sign before ${}_2F_2(\cdot;\cdot;\cdot)$ is incorrect.

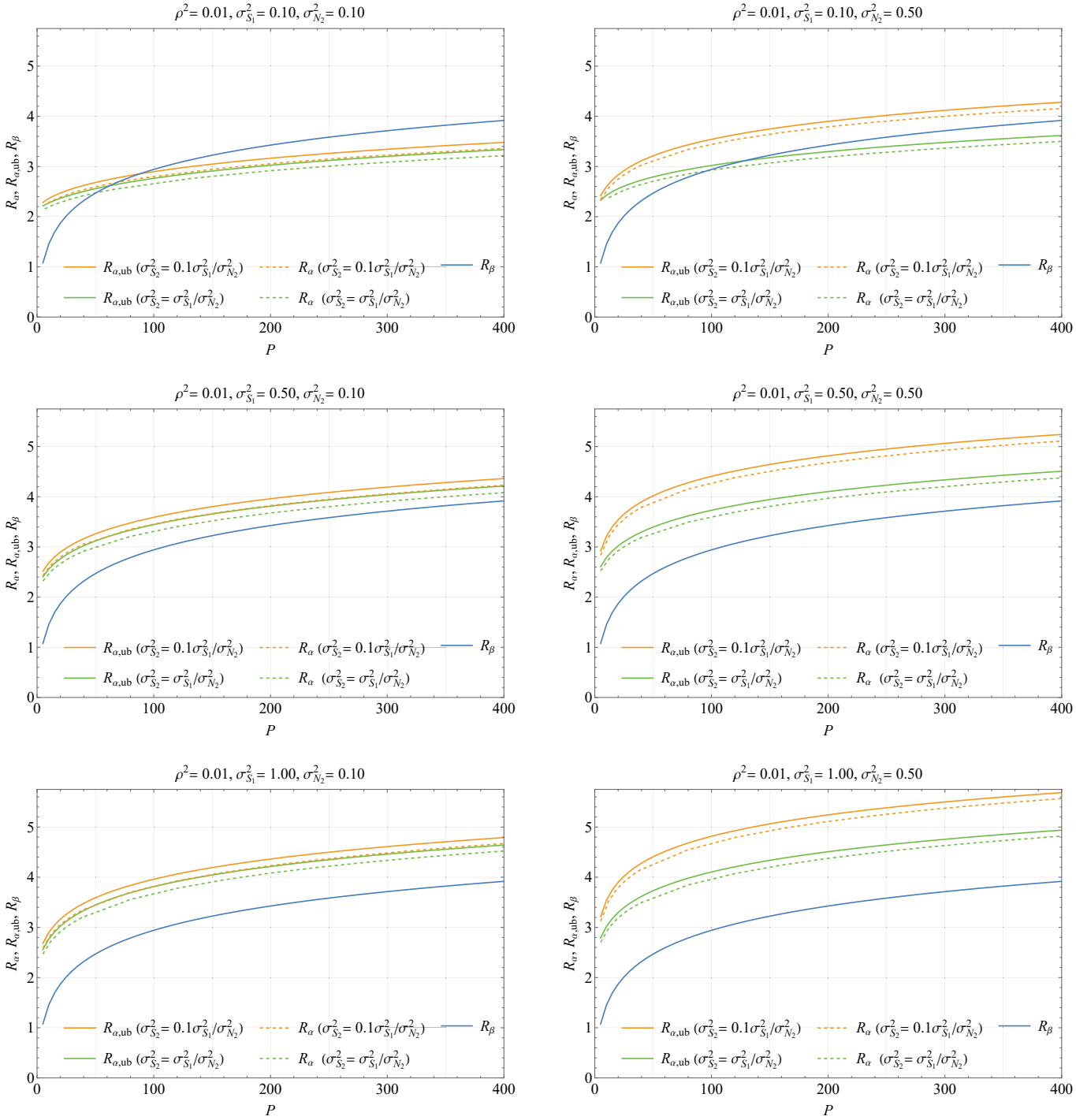

Fig. 2. $R_\alpha, R_{\alpha,\mathrm{ub}},$ and R_β for power correlation coefficient $\rho^2 = 0.01$.

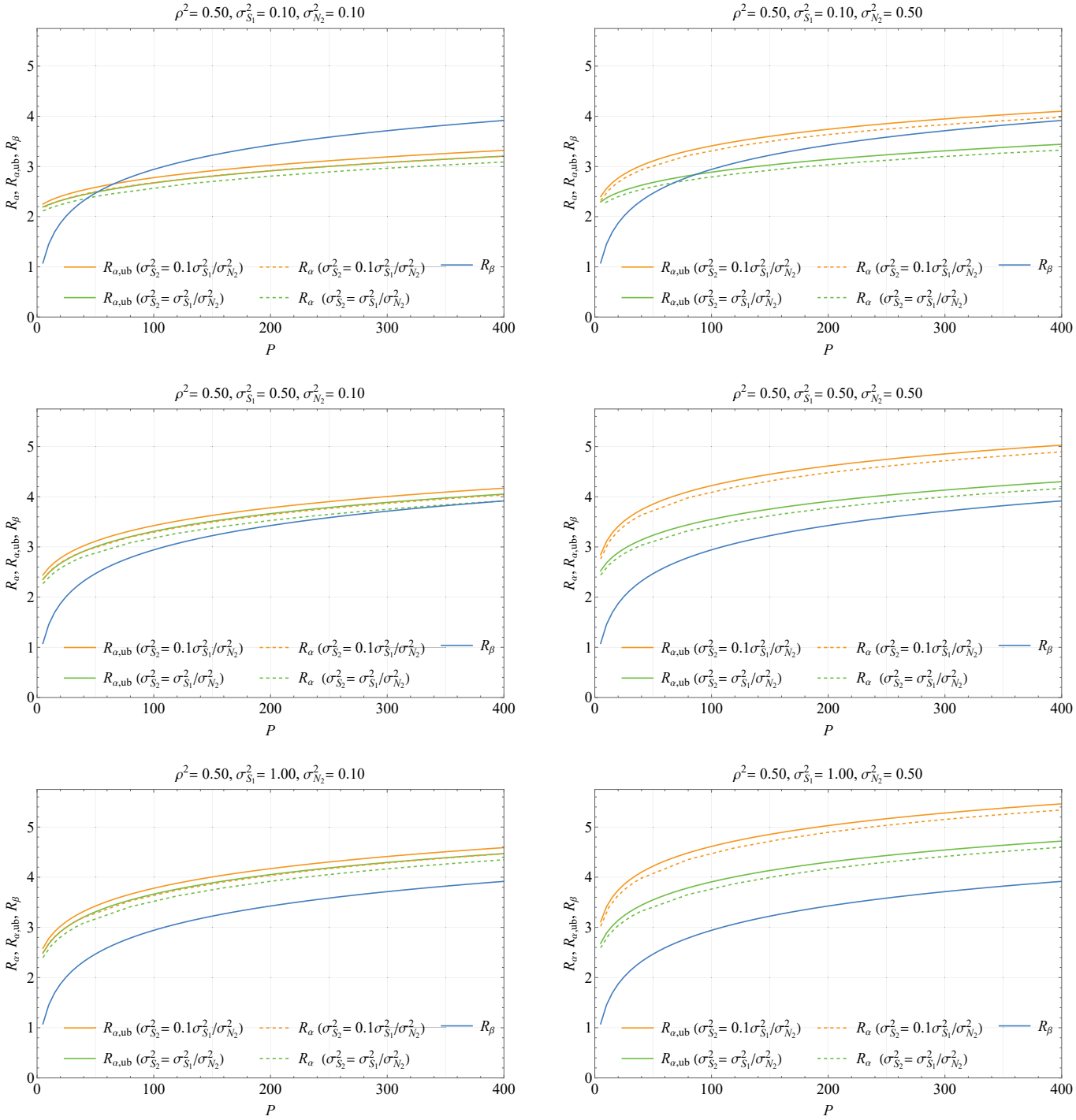

Fig. 3. $R_\alpha, R_{\alpha,\mathrm{ub}},$ and R_β for power correlation coefficient $\rho^2 = 0.50$.

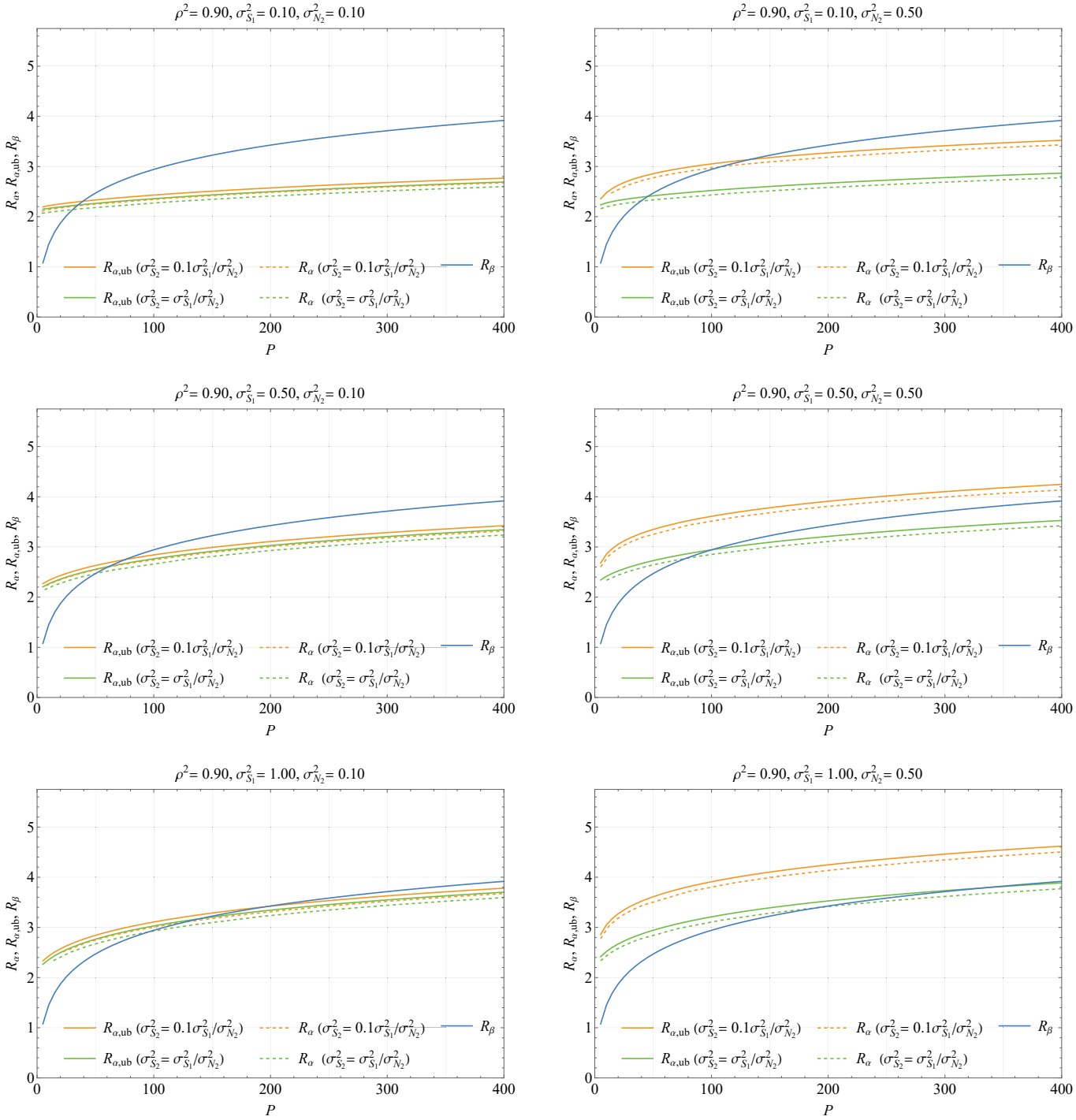

Fig. 4. $R_\alpha, R_{\alpha,\mathrm{ub}},$ and R_β for power correlation coefficient $\rho^2 = 0.90$.