Testing Against Conditional Independence Under Security Constraints

Sreejith Sreekumar and Deniz Gündüz
Imperial College London, UK
Email: {s.sreekumar15, d.gunduz}@imperial.ac.uk

***Abstract*—A distributed binary hypothesis testing problem involving three parties, a remote node, called the observer, a legitimate decoder, called the detector, and an adversary, is studied. The remote node observes a discrete memoryless source, and communicates its observations over a rate-limited noiseless public channel to the detector, which tests for the conditional independence of its own observations from that of the remote node, conditioned on some additional side information. The adversary, in addition to observing the public message, has access to its own correlated side-information. Considering the type 2 error exponent for a given type 1 error probability constraint as the performance measure for the hypothesis test at the detector, and equivocation of the source at the adversary as the secrecy measure, a single-letter characterization of the *rate-error exponent-equivocation trade-off* is established. Additionally, for a general distortion measure, imposing the average distortion at the adversary as the measure of secrecy achieved, an inner bound on the trade-off between the rate, error exponent and average distortion is obtained. This bound is shown to be tight under the less noisy condition on the adversary's side information.**

I. Introduction

In a distributed learning system, the performance of the learning algorithm depends critically on the communication between the agents involved. Typically, agents provide information about their data to a remote decision maker in return for some utility based on the quality of the decisions taken. On the other hand, security of the underlying data is becoming more and more important due to the ever increasing capabilities of data-mining and machine learning algorithms. An adversary having access to the information shared over the common link can make inferences about the underlying sensitive user data.

In distributed learning applications the goal is typically to learn the joint probability distribution of the data available at different locations, or nodes in the system. Usually, there is some prior knowledge about the joint distribution, for example, that it belongs to a certain set of known probability distributions. In such a scenario, the detector, which tries to infer the joint distribution, uses a hypothesis test to decide on the joint distribution of the data based on its own observations and the data that it receives from other nodes. Often the inter-node communication happens over a channel, e.g., over a wireless link, that is vulnerable to external third party attacks. In addition to the data available over the public channel, the eavesdropper may have access to additional correlated data that further risks data security. While communicating data more accurately to the detector achieves better utility in general, it also risks data security, as the same communication is also observed by the adversary. Therefore, there is an inherent trade-off between the utility of the provided data, i.e., the detector's performance and the security against adversaries.

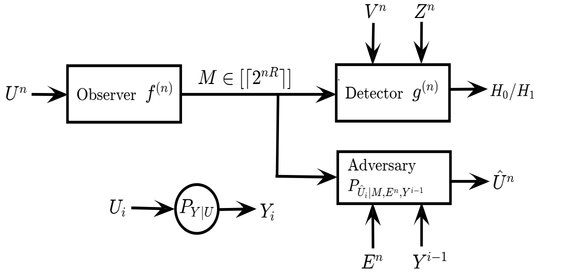

Fig. 1: HT in the presence of an adversary.

In this paper, we study the problem of distributed hypothesis testing (HT) under a secrecy constraint imposed due to the presence of an unintended receiver. We study a special case of the general hypothesis testing problem known as the testing against conditional independence (TACI) problem, in which the detector tests whether its own observation is conditionally independent of the data at a remote observer, conditioned on an additional side-information available at the decision maker. Distributed hypothesis testing from an information theoretic perspective has been studied extensively in the past, although many open problems remain. Testing against independence, e.g., no side-information Z, is studied in [1] and [2], where the best achievable type 2 error exponent (T2EE) is established, in addition to other fundamental results for the general hypothesis testing problem. The TACI is first studied in [3], where the optimality of a random binning based encoding scheme is shown. Various multi-terminal scenarios have been studied in [4] and [5]. Recently, the optimal T2EE for TACI over a noisy channel is established in [6]. The information theoretic framework for analyzing secrecy is first introduced in the seminal paper of Shannon [7]. Equivocation as a measure of secrecy first appears in [8] and has been used extensively in the literature to quantify the amount of information leakage to the adversary in various communication and compression settings (see [9], [10], [11] and references therein). A more general rate-distortion approach to secrecy is first explored in the work of Yamamoto for the case of a noiseless channel with rate constraint R, where, in addition to a distortion constraint D at the legitimate receiver, a minimum distortion requirement Δ is enforced at the adversary [12].

In this paper, we study TACI in the presence of an adversary, considering the availability of distinct side information sequences available at the legitimate receiver and the adversary. Our contributions are as follows: i) With equivocation as the metric of secrecy, we establish a tight single-letter characterization of the rate-error exponent-equivocation trade-off (R, κ, Ω), where κ is the type 2 error exponent and Ω is the equivocation enforced at the adversary; ii) when average distortion Δ is the metric of secrecy for an arbitrary additive distortion measure, we obtain a single-letter inner bound on the set of achievable (R, κ, Δ) tuples; and iii) this inner bound is shown to match with a trivial outer bound under the so-called *less noisy* condition, thus establishing the optimal trade-off.

A. Notations

We denote random variables (r.v.'s) and their realizations by upper and lower case letters (e.g., X and x), respectively. Sets are denoted by calligraphic letters, e.g., the alphabet of r.v. X is denoted by $\mathcal{X}$. The sequence $X_1, \ldots, X_n$ is denoted by X^n. $\mathbb{1}(\cdot)$ and $[a]^+$, $a \in \mathbb{R}$ denotes the indicator function and $\max(a, 0)$, respectively. $X - Y - Z$ denotes a Markov chain between r.v.'s X, Y and Z. Notation $\xrightarrow{(n)}$ denotes asymptotic limit with respect to n, e.g., $a_n \xrightarrow{(n)} 0$ means the sequence a_n tends to zero asymptotically with n. $\mathbb{P}(\mathcal{E})$ denotes the probability of the event $\mathcal{E}$. For positive real m, we define $[m] \triangleq \{1, \ldots, \lceil m \rceil\}$. For set $\mathcal{A}$, we denote its complement by $\mathcal{A}^c$. The values of radius of the typical set appearing in the proofs below such as δ, δ', δ'' etc. are chosen such that the probability of the coding error events decay exponentially. The details are omitted here due to space constraints.

II. Problem formulation

Consider the HT setup in the presence of an adversary, illustrated in Fig. 1. The observer observes the memoryless source sequence U^n, and using the encoding function $f^{(n)}: \mathcal{U}^n \to [2^{nR}]$, sends the message index $M \triangleq f^{(n)}(U^n)$ to the detector over an error-free public channel, which is also observed by the adversary. In addition, the adversary also observes an i.i.d. side information E^n (correlated with U^n) and has causal access[1] to samples Y^{i-1} for estimating $\hat{U}_i$, where Y^n is the output of a discrete memoryless channel $P_{Y|U}$ with input U^n. Given its own independent and identically distributed (i.i.d.) observation V^n and side-information Z^n, the detector performs TACI with null hypothesis $H_0 : P_{UVZEY}$ and alternate hypothesis $H_1 : Q_{UVZEY} = P_{UEYZ}P_{V|Z}$ on the joint distribution of U, V, Z, E and Y. The adversary is interested in the reconstruction $\hat{U}^n$, such that the average distortion between U^n and $\hat{U}^n$ is minimized for a given single-letter distortion metric $d(\cdot, \cdot)$. To summarize, our system model comprises of:

- i.i.d. samples $(U^n, V^n, Z^n, E^n, Y^n)$ generated according to $P^n_{UVZEY} = \prod_{i=1}^n P_{UVZEY}$ under hypothesis H_0, and according to $Q^n_{UVZEY} = \prod_{i=1}^n Q_{UVZEY}$ under hypothesis H_1.
- Stochastic encoder $f^{(n)}: \mathcal{U}^n \to [2^{nR}]$, $M \triangleq f^{(n)}(U^n)$.
- Decoder $g^{(n)} : [2^{nR}] \times \mathcal{Z}^n \times \mathcal{V}^n \to \{0, 1\}$, where 0 and 1 indicate H_0 and H_1, respectively.
- Adversary decoding functions $\{P_{\hat{U}_i|M,E^n,Y^{i-1}}\}_{i=1}^n$.
- Bounded additive distortion metric at the adversary $d : \mathcal{U} \times \hat{\mathcal{U}} \to [0, D_m]$ with multi-letter distortion defined as

$$d(u^n, \hat{u}^n) \triangleq \frac{1}{n} \sum_{i=1}^n d(u_i, \hat{u}_i). \tag{1}$$

Let $\mathcal{A} \subseteq [2^{nR}] \times \mathcal{Z}^n \times \mathcal{V}^n$ and $\mathcal{A}^c$ denote the acceptance region for H_0 and H_1, respectively. The detector is then given by $g^{(n)}(m, z^n, v^n) = \mathbb{1}\left((m, z^n, v^n) \in \mathcal{A}^c\right)$. Let $\bar{\alpha}\left(f^{(n)}, g^{(n)}\right) \triangleq P_{MZ^nV^n}(\mathcal{A}^c)$ and $\bar{\beta}\left(f^{(n)}, g^{(n)}\right) \triangleq P_{MZ^n} \times P_{V^n|Z^n}(\mathcal{A})$ denote the type 1 and type 2 error probabilities for $\left(f^{(n)}, g^{(n)}\right)$ pair, respectively. For a given type 1 error probability constraint ϵ, we define the minimum type 2 error probability over all possible decoders as

$$\beta\left(f^{(n)}, \epsilon\right) \triangleq \inf_{g^{(n)}} \bar{\beta}\left(f^{(n)},\ g^{(n)}\right), \tag{2}$$

such that $\bar{\alpha}\left(f^{(n)},\ g^{(n)}\right) \leq \epsilon$.

Definition 1. *For a given type 1 error probability constraint ϵ, a rate-error exponent-distortion tuple (R, κ, Δ) is* achievable*, if there exists a sequence of encoding and decoding functions $f^{(n)}: \mathcal{U} \to [2^{nR}]$ and $g^{(n)} : [2^{nR}] \times \mathcal{Z}^n \times \mathcal{V}^n \to \{0, 1\}$ such that*

$$\limsup_{n\to\infty} \frac{\log\left(\beta(f^{(n)}, \epsilon)\right)}{n} \leq -\kappa, \text{ and} \tag{3}$$

$$\mathbb{E}\left[d\left(U^n, \hat{U}^n\right)\right] \geq \Delta. \tag{4}$$

The rate-error exponent-distortion region $\mathcal{R}^*(\epsilon)$ is the closure of the set of all achievable (R, κ, Δ) tuples for a given ϵ.

Remark 2. *It is well known that the equivocation constraint can be obtained as a special case of the more general distortion constraint considered above, using* log-loss *as the distortion measure, and assuming that the source is causally disclosed to the adversary [13]. Setting $Y^n = U^n$, and taking $d(u, \hat{u}) = -\log(\hat{u}(u))$, where $\hat{u}(\cdot)$ is a probability distribution on $\mathcal{U}$, results in a constraint of the form*

$$\frac{1}{n} H(U^n|M, E^n) \geq \Omega, \tag{5}$$

in (4)*, where Ω is the equivocation constraint.*

In this paper, we focus on the single-letter characterization of the region $\mathcal{R}^*(\epsilon)$, as the type 1 error probability tends to zero, i.e., $\lim_{\epsilon\to 0} \mathcal{R}^*(\epsilon)$, which we denote by $\mathcal{R}^*$. Similarly to [1], it can be shown using Stein's lemma that,

$$\lim_{\epsilon\to 0} \lim_{n\to\infty} \sup_{f^{(n)}} \frac{-\log\left(\beta\left(f^{(n)}, \epsilon\right)\right)}{n} = \theta(R), \tag{6}$$

$$\text{where } \theta(R) \triangleq \sup_n \sup_{f^{(n)}} \frac{1}{n} I(M; V^n|Z^n),$$

[1] This assumption known as *causal disclosure* results in a generic system model, where secrecy achieved at the adversary is measured using a single-letter distortion metric, of which equivocation is a special case. For more details, see [13].

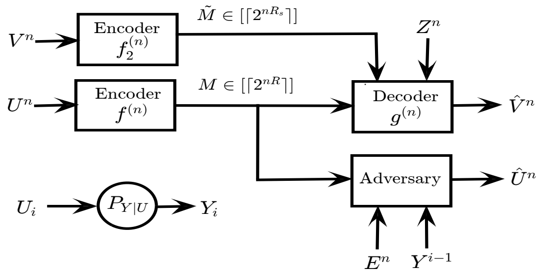

Fig. 2: Equivalent source-coding problem in the presence of a helper and an adversary.

$$\text{s.t } (V^n, Z^n, E^n, Y^n) - U^n - M,\ M \in [2^{nR}]. \tag{7}$$

The n-letter characterization of $\mathcal{R}^*$ is thus given by

$$\kappa \leq \frac{1}{n} I(M; V^n | Z^n), \tag{8}$$

such that (7) and (4) are satisfied. Noting that $I(M; V^n|Z^n) = nH(V|Z) - H(V^n|Z^n, M)$, the problem of characterizing $\mathcal{R}^*$ is equivalent to that of the set of all (R, R_s, Δ) tuples satisfying

$$R_s \geq \frac{1}{n} H(V^n | M, Z^n), \tag{9}$$

such that (7) and (4) are satisfied. Eqn. (9) is the $n-$letter characterization of the lossless source coding problem with a helper and an adversary as depicted in Fig. 2. In this equivalent problem, the helper communicates its observation U^n to the legitimate receiver through a noiseless public channel with rate constraint R, while the main encoder transmits over a private link of rate R_s a compressed version of its observation of the source V^n, which is to be reconstructed losslessly by the legitimate decoder, while ensuring that (4), the average distortion constraint at the adversary, is also satisfied. Let $\mathcal{R}_s^*$ denote the closure of all achievable (R, R_s, Δ) pairs. Then, the following equivalence holds.

$$(R, \kappa, \Delta) \in \mathcal{R}^* \Leftrightarrow (R, H(V|Z) - \kappa, \Delta) \in \mathcal{R}_s^*. \tag{10}$$

In the next section, we obtain a single-letter inner bound on $\mathcal{R}^*$ via a bound on $\mathcal{R}_s^*$ by exploiting the equivalence in (10). The proof of this bound, which is omitted here due to space constraint, relies on the *soft-covering lemma* and properties of total variation [13], [14]. For the special case of equivocation as the measure of secrecy, we obtain a single-letter characterization of the complete $(R.\kappa, \Omega)$ trade-off.

III. Main Results

The main results of the paper and the sketches of their proofs are presented in this section. We first state the result for the special case of equivocation[2] as a measure of secrecy at the adversary. Although the equivocation is a special case of the distortion based framework introduced above, we provide a separate proof here as the inner bound for $\mathcal{R}^*$ obtained below for an arbitrary distortion measure is not tight when specialized to the case of log-loss distortion measure and $Y^n = U^n$.

Theorem 3. *For $d(u, \hat{u}) = -\log(\hat{u}(u))$, where $\hat{u}(\cdot)$ is a probability distribution on $\mathcal{U}$, and $Y^n = U^n$, $(R, \kappa, \Omega) \in \mathcal{R}^*$ if and only if there exist auxiliary r.v.'s W_1 and W_2, such that*

$$R \geq I(W_2; U|Z) \tag{11}$$

$$\kappa \leq I(W_2; V|Z) \tag{12}$$

$$\Omega \leq H(U|W_2, Z) + I(U; Z|W_1) - I(U; E|W_1) \tag{13}$$

for some joint distribution $P_U P_{W_2|U} P_{W_1|W_2} P_{ZEV|U}$.

Proof: We first obtain a characterization for $\mathcal{R}_s^*$, and the proof follows from the equivalence in (10). We show that $(R, R_s, \Omega) \in \mathcal{R}_s^*$ if and only if there exists auxiliary r.v.'s W_1 and W_2, such that

$$R \geq I(W_2; U|Z) \tag{14}$$

$$R_s \geq H(V|W_2, Z) \tag{15}$$

$$\Omega \leq H(U|W_2, Z) + I(U; Z|W_1) - I(U; E|W_1) \tag{16}$$

for some joint distribution $P_U P_{W_2|U} P_{W_1|W_2} P_{ZEV|U}$.

Achievability: We generate a codebook similarly to [16]. First, fix a joint distribution $P_{UVEZY} P_{W_2|U} P_{W_1|W_2}$ satisfying (14)-(16). .

Codebook of the encoder of source U^n: Fix non-negative numbers R_1, R_1', R_2, R_2'. Generate codewords $W_1^n(m_1, m_1')$, $m_1 \in [2^{nR_1}]$, $m_1' \in [2^{nR_1'}]$ drawn independently according to distribution $\prod_{i=1}^n P_{W_1}$. Denote this codebook by $\mathcal{C}_{w_1}^n$. For each (m_1, m_1'), generate codewords $W_2^n(m_1, m_1', m_2, m_2')$, $m_2 \in [2^{nR_2}]$, $m_2' \in [2^{nR_2'}]$ independently drawn according to distribution $\prod_{i=1}^n P_{W_2|W_1}(w_{2i}|W_{1i}(m_1, m_1'))$. Denote this codebook by $\mathcal{C}_{w_2}^n$. Denote the two codebooks $\mathcal{C}_{w_1}^n$ and $\mathcal{C}_{w_2}^n$ together by $\mathcal{C}_u^n$. The codebook $\mathcal{C}_u^n$ is known to all the parties including the adversary.

Codebook of the encoder of source V^n: This codebook is generated by performing uniform random binning on the V^n sequences, i.e., an index $\tilde{M}$ is assigned to each v^n sequence uniformly at random from the set $[2^{nR_s}]$, $R_s \geq 0$. We denote this assignment by $f_2^{(n)}(V^n) = \tilde{M}$.

Encoding: The encoder of source U^n uses joint-typicality encoding, i.e., it first looks for (M_1, M_1', M_2, M_2') such that $(U^n, W_1^n(M_1, M_1'), W_2^n(M_1, M_1', M_2, M_2')) \in T_{[UW_1W_2]_\delta}^n$, $\delta > 0$, where T_δ^n denotes the $\delta-$ typical set as defined in [17]. If successful, the indices $M = (M_1, M_2)$ are transmitted; otherwise, it transmits a pair of indices chosen uniformly at random from the set $[2^{nR_1}] \times [2^{nR_2}]$. The indices (M_1', M_2') are not transmitted, but are intended to be recovered by the legitimate decoder using its side information Z^n. The encoder of source V^n sends the bin-index $\tilde{M}$ via its channel.

Decoding: The legitimate decoder first checks for the unique indices $(\hat{M}_1', \hat{M}_2')$ such that $(W_1^n(M_1, \hat{M}_1'), W_2^n(M_1, \hat{M}_1', M_2, \hat{M}_2'), Z^n) \in T_{[W_1W_2Z]_{\delta'}}^n$, $\delta' > 0$. If successful, it then checks for a unique sequence

[2] After the submission of our paper, we became aware of [15] which characterizes the optimal-error exponent-equivocation region for testing against independence, i.e., $Z = \emptyset$.

$\tilde{V}^n$ in bin $\tilde{M}$ such that $(\tilde{V}^n, W_2^n(M_1, \hat{M}_1', M_2, \hat{M}_2'), Z^n) \in T^n_{[VW_2Z]_{\delta''}}$, $\delta'' > 0$. If this is also successful, it sets the estimate as $\hat{V}^n = \tilde{V}^n$; otherwise, a random sequence from set $\mathcal{V}^n$ is chosen as the estimate.

Analysis of probability of error: The following events may result in an error at the encoder or decoder.

$$\mathcal{E}_{EE} = \left\{ \begin{array}{l} (U^n, W_1^n(m_1, m_1'), W_2^n(m_1, m_1', m_2, m_2')) \notin T^n_{\delta}, \\ \forall\ m_1, m_1', m_2, m_2' \end{array} \right\}$$

$$\mathcal{E}_{D1} = \left\{ \begin{array}{l} \exists\ (\hat{M}_1', \hat{M}_2') \neq (M_1', M_2'),\ \text{s.t.} \\ (W_1^n(M_1, \hat{M}_1'), W_2^n(M_1, \hat{M}_1', M_2, \hat{M}_2'), Z^n) \in T^n_{\delta'} \end{array} \right\}$$

$$\mathcal{E}_{D2} = \left\{ (V^n, W_2^n(M_1, \hat{M}_1', M_2, \hat{M}_2'), Z^n) \notin T^n_{\delta''} \right\}$$

$$\mathcal{E}_{D3} = \left\{ \begin{array}{l} \exists\ \tilde{V}^n \neq V^n, f(\tilde{V}^n) = f(V^n)\ \text{s.t.} \\ (\tilde{V}^n, W_2^n(M_1, \hat{M}_1', M_2, \hat{M}_2'), Z^n) \in T^n_{\delta''} \end{array} \right\}$$

We analyze the probability of error $\mathbb{P}(\mathcal{E}) \triangleq \mathbb{P}(V \neq \hat{V})$ averaged over the random codebook $\mathcal{C}_U^n$ and random bin-assignment. By the union bound,

$$\begin{aligned} \mathbb{P}(\mathcal{E}) \leq \mathbb{P}(\mathcal{E}_{EE}) + \mathbb{P}(\mathcal{E}_{EE}^c \cap \mathcal{E}_{D1}) + \mathbb{P}(\mathcal{E}_{EE}^c \cap \mathcal{E}_{D1}^c \cap \mathcal{E}_{D2}) \\ + \mathbb{P}(\mathcal{E}_{EE}^c \cap \mathcal{E}_{D1}^c \cap \mathcal{E}_{D2}^c \cap \mathcal{E}_{D3}). \end{aligned}$$

By the covering lemma [18], $\mathbb{P}(\mathcal{E}_{EE}) \xrightarrow{(n)} 0$, provided that $I(U;W_1) < R_1 + R_1'$ and $I(U;W_2|W_1) < R_2 + R_2'$. Similarly, by the packing lemma [18], $\mathbb{P}(\mathcal{E}_{EE}^c \cap \mathcal{E}_{D1}) \xrightarrow{(n)} 0$ provided $R_1' < I(W_1;Z)$ and $R_2' < I(W_2;Z|W_1)$. By the Markov lemma [18], $\mathbb{P}(\mathcal{E}_{EE}^c \cap \mathcal{E}_{D1}^c \cap \mathcal{E}_{D2}) \xrightarrow{(n)} 0$. Finally, using standard arguments, it can be shown that $\mathbb{P}(\mathcal{E}_{EE}^c \cap \mathcal{E}_{D1}^c \cap \mathcal{E}_{D2}^c \cap \mathcal{E}_{D3}) \xrightarrow{(n)} 0$ if $R_s > H(V|W_2, Z)$. The lower bound on the equivocation follows similarly to the analysis in [16]. Thus, by the standard random coding arguments, if (14)-(16) hold (with strict inequality), there exists a deterministic codebook such that $\mathbb{P}(\mathcal{E})$ tends to zero asymptotically, and the distortion constraint at the adversary is satisfied. Using the equivalence in (10), this completes the proof of the achievability of (R, κ, Ω) satisfying (11)-(13) since $\mathcal{R}^*$ and $\mathcal{R}_s^*$ are closed sets by definition.

Converse: The converses for (11) and (13) follow similarly to [16]. Define auxiliary r.v.'s $W_1 \triangleq (W_{1Q}, Q)$ and $W_2 \triangleq (W_{2Q}, Q)$, where $W_{1i} \triangleq (M, Z_{i+1}^n, E^{i-1})$ and $W_{2i} \triangleq (M, U^{i-1}, Z^{i-1}, Z_{i+1}^n, E^{i-1})$, $i \in [n]$, and Q is a r.v. independent of all the other r.v.'s and uniformly distributed over $[n]$. Then, for any $\epsilon' > 0$ and sufficiently large n, we have

$$\begin{aligned} & n(R + \epsilon') \geq H(M) = I(M; U^n, Z^n, E^n) \\ & \geq I(M; U^n, E^n|Z^n) = \textstyle\sum_{i=1}^n I(M; U_i, E_i|U^{i-1}, E^{i-1}, Z^n) \\ & = \textstyle\sum_{i=1}^n I(M, U^{i-1}, Z^{i-1}, Z_{i+1}^n, E^{i-1}; U_i, E_i|Z_i) \qquad (17) \\ & \qquad \geq \textstyle\sum_{i=1}^n I(W_{2i}; U_i|Z_i) = nI(W_2; U|Z). \qquad (18) \end{aligned}$$

Here, (17) follows since the sequences (U^n, Z^n, E^n) are memoryless. Next, the equivocation of source U^n at the adversary can be bounded as follows.

$$\begin{aligned} & H(U^n|E^n, M) && (19) \\ & = H(U^n|M, Z^n) + I(U^n; Z^n|M) - I(U^n; E^n|M) \\ & = H(U^n|M, Z^n) + I(U^n; Z^n) - I(M; Z^n) \\ & \quad - I(U^n; E^n) + I(M; E^n) && (20) \\ & = \textstyle\sum_{i=1}^n [H(U_i|M, U^{i-1}, Z^n) + I(U_i; Z_i) - I(M, Z_{i+1}^n; Z_i) \\ & \qquad\qquad - I(U_i; E_i) + I(M, E^{i-1}; E_i)] \\ & \quad + \sum_{i=1}^n [I(E_i; Z_{i+1}^n|M, E^{i-1}) - I(Z_i; E^{i-1}|M, Z_{i+1}^n)] && (21) \\ & = \textstyle\sum_{i=1}^n \big[H(U_i|M, U^{i-1}, Z^n, E^{i-1}) + I(U_i; Z_i) - I(U_i; E_i) \\ & \quad + I(E_i; M, Z_{i+1}^n, E^{i-1}) - I(Z_i; M, Z_{i+1}^n, E^{i-1})\big] && (22) \\ & = \textstyle\sum_{i=1}^n H(U_i|W_{2i}, Z_i) + I(U_i; Z_i) - I(U_i; E_i) \\ & \quad + I(E_i; W_{1i}) - I(Z_i; W_{1i}) \\ & = n[H(U|W_2, Z) + I(U; Z|W_1) - I(U; E|W_1)]. && (23) \end{aligned}$$

Here, (20) and (22) follow from the Markov chain relations $(E^n, Z^n) - U^n - M$ and $U_i - (M, U^{i-1}, Z^n) - E^{i-1}$, respectively, while (21) is obtained using the Csiszar-Körner inequality [9].

Finally, we prove the bound on R_s. First, note that

$$\begin{aligned} & n(R_s + \epsilon') \geq H(\tilde{M}|M, Z^n) \\ & = H(\tilde{M}|M, Z^n) + H(V^n|\tilde{M}, M, Z^n) - H(V^n|\tilde{M}, M, Z^n) \\ & \geq H(\tilde{M}, V^n|Z^n, M) - \epsilon_n && (24) \end{aligned}$$

where $\epsilon_n \xrightarrow{(n)} 0$. Eqn. (24) follows from Fano's inequality. Defining $\epsilon'' \triangleq \epsilon' + \frac{\epsilon_n}{n}$, from (24) we get

$$\begin{aligned} & n(R_s + \epsilon'') \geq H(V^n|M, Z^n) + H(\tilde{M}|V^n, Z^n, M) \\ & \geq H(V^n|M, Z^n) \geq \textstyle\sum_{i=1}^n H(V_i|V^{i-1}, M, Z^n, U^{i-1}) \\ & = \textstyle\sum_{i=1}^n H(V_i|M, Z^n, U^{i-1}) && (25) \\ & \geq \sum_{i=1}^n H(V_i|M, Z^n, U^{i-1}, E^{i-1}) = n \sum_{i=1}^n \frac{1}{n} H(V_i|Z_i, W_{2i}) \\ & = nH(V_Q|Z_Q, W_{2Q}, Q) = nH(V|Z, W_2) && (26) \end{aligned}$$

where (25) follows since $V^{i-1} - (M, U^{i-1}, Z^n) - V_i^n$ form a Markov chain. Eqns. (18), (23) and (26), along with the fact that $\mathcal{R}_s^*$ is closed complete the proof of the converse via the equivalence in (10). ■

Next, we state an achievability result for the more general case when secrecy is measured using an arbitrary distortion measure $d(\cdot,\cdot)$ at the adversary. Due to space constraints, the proof of this theorem is omitted here and will be presented in an extended version of this paper.

Theorem 4. $(R, \kappa, \Delta) \in \mathcal{R}^*$ *if there exist auxiliary r.v.'s* W_1

and W_2, such that

$$R \geq I(W_2;U|Z) \tag{27}$$

$$\kappa \leq I(W_2;V|Z) \tag{28}$$

$$\begin{aligned}\Delta \leq & \min\{\zeta_s,\zeta_p\} \min_{\phi(e)} \mathbb{E}\left[d\left(U,\phi(E)\right)\right] \\ & + [\zeta_s - \zeta_p]^+ \min_{\phi(e,w_1)} \mathbb{E}\left[d\left(U,\phi(E,W_1)\right)\right] \\ & + (1-\zeta_s) \min_{\phi(e,w_2)} \mathbb{E}\left[d\left(U,\phi(E,W_2)\right)\right],\end{aligned} \tag{29}$$

where

$$\zeta_p \triangleq \min\left(\frac{[I(W_1;Z)-I(W_1;E)]^+}{I(W_1;Y|E)},1\right), \tag{30}$$

$$\zeta_s \triangleq \min\left(\frac{[I(W_2;Z|W_1)-I(W_2;E|W_1)]^+}{I(Y;W_2|W_1,E)},1\right), \tag{31}$$

for some distribution $P_U P_{W_2|U} P_{W_1|W_2} P_{ZEVY|U}$.

Remark 5. *It can be shown using standard arguments based on the Fenchel-Eggleston-Carathéodory's theorem that, considering auxiliary r.v.'s W_1 and W_2 such that $|\mathcal{W}_1| \leq |\mathcal{U}|+2$, $|\mathcal{W}_2| \leq (|\mathcal{U}|+2)(|\mathcal{U}|+1)$ and $|\mathcal{W}_1| \leq |\mathcal{U}|+7$, $|\mathcal{W}_2| \leq (|\mathcal{U}|+7)(|\mathcal{U}|+4)$ suffices in Theorem 3 and 4, respectively.*

We also have the following trivial outer-bound for $\mathcal{R}^*$ for the case when Y is constant (with probability 1).

Theorem 6. *$(R,\kappa,\Delta) \in \mathcal{R}^*$ only if there exist auxiliary r.v.'s W_1 and W_2, such that*

$$R \geq I(W_2;U|Z) \tag{32}$$

$$\kappa \leq I(W_2;V|Z) \tag{33}$$

$$\Delta \leq \min_{\phi(e)} \mathbb{E}\left[d\left(U,\phi(E)\right)\right] \tag{34}$$

for some distribution $P_U P_{W_2|U} P_{W_1|W_2} P_{ZEV|U}$.

Proof: The first two conditions follow directly from the converse of the TACI problem considered in [6], when the noisy channel between the source U^n and the detector is replaced by a noiseless channel of rate R. Eqn. (34) follows by noting that the distortion at the adversary cannot be more than that can be obtained by a symbol-by-symbol reconstruction $\hat{U}_i = \phi(E_i)$ using only the side-information E^n (ignoring the message from the observer). ■

Definition 7. *Side information Z is said to be* strictly less noisy *than E if for all r.v.'s S satisfying the Markov condition $S - U - (Z,E)$, we have $I(S;Z) > I(S;E)$ whenever $I(S;E) > 0$.*

Corollary 8. *For strictly less noisy side information Z compared to E at the legitimate decoder, and Y constant, $(R,\kappa,\Delta) \in \mathcal{R}$ if and only if there exist auxiliary r.v.'s W_1 and W_2, such that*

$$R \geq I(W_2;U|Z) \tag{35}$$

$$\kappa \leq I(W_2;V|Z) \tag{36}$$

$$\Delta \leq \min_{\phi(e)} \mathbb{E}\left[d\left(U,\phi(E)\right)\right] \tag{37}$$

for some distribution $P_U P_{W_2|U} P_{W_1|W_2} P_{ZEV|U}$.

Proof: For the strictly less noisy case with constant Y, we note that $I(Z;W_1) > I(E;W_1)$, $I(Z;W_2|W_1) > I(E;W_2|W_1)$, $I(W_1;Y|E) = 0$ and $I(W_2;Y|W_1,E) = 0$. This implies that $\zeta_p = \zeta_s = 1$. Substituting these values into Theorem 4 proves the achievability, while the matching converse follows trivially from Theorem 6. ■

IV. Conclusions

We have studied the TACI problem over a rate-limited noiseless channel in the presence of an adversary. With equivocation as the measure of secrecy, we have established a complete characterization of the rate-exponent-equivocation trade-off. For an arbitrary distortion measure at the adversary as the secrecy criterion, we have provided an inner bound for the rate-exponent-distortion region using a coding scheme that involves superposition coding along with binning. We have then shown this bound to be tight when the side information at the legitimate decoder is less noisy compared to that of the adversary.

References

[1] R. Ahlswede and I. Csiszár, "Hypothesis testing with communication constraints," *IEEE Trans. Inf. Theory*, vol. 32, no. 4, pp. 533–542, Jul. 1986.

[2] T. S. Han, "Hypothesis testing with multiterminal data compression," *IEEE Trans. Inf. Theory*, vol. 33, no. 6, pp. 759–772, Nov. 1987.

[3] M. S. Rahman and A. B. Wagner, "On the optimality of binning for distributed hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 58, no. 10, pp. 6282–6303, Oct. 2012.

[4] M. Wigger and R. Timo, "Testing against independence with multiple decision centers," in *IEEE Int. Conf. on Signal Proc. and Comm.*, Bengaluru, India, Jun. 2016.

[5] W. Zhao and L. Lai, "Distributed testing against independence with multiple terminals," in *52nd Annual Allerton Conference on Communication, Control and Computing*, Monticello (IL), USA, Oct. 2014.

[6] S. Sreekumar and D. Gündüz, "Distributed hypothesis testing over noisy channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Aachen, Germany, Jun. 2017.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[8] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[9] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May. 1978.

[10] R. Tandon, S. Ulukus, and K. Ramchandran, "Secure source coding with a helper," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2178–2187, Apr. 2013.

[11] D. Gündüz, E. Erkip, and H. Poor, "Secure lossless compression with side information," in *IEEE ITW 2008*, Porto, Portugal, May. 2008.

[12] H. Yamamoto, "A rate-distortion problem for a communication system with a secondary decoder to be hindered," *IEEE Trans. Inf. Theory*, vol. 34, no. 4, pp. 835–842, Jul. 1988.

[13] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7584–7605, Dec. 2014.

[14] E. C. Song, P. Cuff, and H. V. Poor, "The likelihood encoder for lossy compression," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1836–1849, Apr. 2016.

[15] M. Mhanna and P. Piantanida, "On secure distributed hypothesis testing," in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, Jun. 2015.

[16] J. Villard and P. Piantanida, "Secure multiterminal source coding with side information at the eavesdropper," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3668–3692, Jun. 2013.

[17] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[18] A. E. Gamal and Y.-H. Kim, *Network Information theory*. Cambridge University Press, 2011.