

Testing Against Independence with An Eavesdropper

Sara Faour*, Mustapha Hamad*, Mireille Sarkiss**, and Michèle Wigger*

*LTCI, Telecom Paris, IP Paris, sara.faour@ip-paris.fr, mustapha.hamad7@gmail.com, michele.wigger@telecom-paris.fr

**SAMOVAR, Telecom SudParis, IP Paris, mireille.sarkiss@telecom-sudparis.eu

We study a distributed binary hypothesis testing (HT) problem with communication and security constraints, involving three parties: a remote sensor called Alice, a legitimate decision center called Bob, and an eavesdropper called Eve, all having their own source observations. In this system, Alice conveys a rate- R description of her observations to Bob, and Bob performs a binary hypothesis test on the joint distribution underlying his and Alice's observations. The goal of Alice and Bob is to maximize the exponential decay of Bob's miss-detection (type-II error) probability under two constraints: Bob's false-alarm (type-I error) probability has to stay below a given threshold and Eve's uncertainty (equivocation) about Alice's observations should stay above a given security threshold even when Eve learns Alice's message. For the special case of testing against independence, we characterize the largest possible type-II error exponent under the described type-I error probability and security constraints.

Index Terms—Distributed hypothesis testing, error exponents, security constraints, side information.

I. INTRODUCTION

IN future ultra-massive type communications, billions of IoT devices and sensors will be connected and cooperate together to detect, measure, and monitor environmental phenomena and events in distributed monitoring and alert systems. The different events can be considered as different hypotheses and are assumed to determine the joint probability distribution underlying the data observed at the various nodes. We focus on binary hypothesis testing where we have two possible events: a normal situation, called *null hypothesis* \mathcal{H}_0 , and an alert situation, called *alternative hypothesis* \mathcal{H}_1 . In this case, there are two types of errors. Type-I error refers to the event that the decision center decides on \mathcal{H}_0 while the true hypothesis is \mathcal{H}_1 . Type-II error refers to the event that the decision center decides on \mathcal{H}_1 while the true hypothesis is \mathcal{H}_0 .

We consider in this paper *distributed hypothesis testing (DHT)* with a single sensor Alice and a single decision center Bob, each observing an independently and identically distributed (i.i.d.) source sequence, where the two sequences are jointly drawn according to the known probability mass function P_{XY} under hypothesis \mathcal{H}_0 and according to the product of the marginals $P_X P_Y$ under \mathcal{H}_1 . Information-theorists refer to this setup as *testing against independence*. Alice can send a rate- R message to Bob describing her observations and aiming to help Bob in deciding on the true hypothesis. The focus here is on the Stein exponent, i.e., on the largest possible exponential decay for Bob's type-II error probability under the requirement that his type-I error probability stays below a given threshold $\epsilon \in (0, 1)$. This largest possible type-II error exponent in this setup was determined by Ahlswede and

Csiszár [1] and does not depend on the value of ϵ . In this paper, we consider an extension of the Ahlswede-Csiszár result to a setup including an additional eavesdropper Eve that observes a local i.i.d. source sequence, intercepts Alice's message to Bob M , and wishes to learn about Alice's source sequence X^n . In this extended setup, Alice is required to choose her message in a way that Eve's equivocation about the source X^n stays above pre-determined thresholds given the two hypothesis.

Hypothesis testing has also been considered under other security constraints. In particular, the works in [2]–[7] focused on ensuring data privacy in various forms. For instance, [5] considered a model where a sensor has to pre-randomize its data before using it on the distributed hypothesis testing problem. In [2], not the sensor's data but only a related information has to be kept private from the decision center, either in an average distortion or equivocation sense. The work in [7] allowed for interactive communication and applied a privacy constraint inspired by the cryptography literature.

The secrecy scenario with an external eavesdropper that we study in the present paper, was already treated in [8] and in [9] for the more general scenario of testing against conditional independence. As we show, in the special case of testing against independence, the type-II error exponents proposed in [8], [9] are optimal in the limit of vanishing type-I error probabilities $\epsilon \rightarrow 0$ but are generally suboptimal for fixed $\epsilon > 0$. For general $\epsilon > 0$, the optimal exponent is achieved by using the scheme in [8], [9] with probability $(1 - \epsilon)$ and using a degenerate scheme with probability ϵ . In this degenerate scheme, Alice sends a dummy zero-message, and upon receiving this message, Bob declares the alternative hypothesis \mathcal{H}_1 . The converse is shown through a change-of-measure argument and by proving asymptotic Markov chains, similar to the converse proofs in [10], [11], see also [12]. In this paper, we however need extra non-trivial steps for the converse bounds on the equivocation under the two hypotheses.

Notation: We follow standard notations. In particular, we denote by $o(1)$ any function that tends to 0 as $n \rightarrow \infty$. Also, we denote by $\mathcal{T}_\mu^{(n)}(P_{XY})$ the strongly typical set defined in [1], and we abbreviate $\mathcal{T}_{n^{-1/3}}^{(n)}(P_{XY})$ simply by $\mathcal{T}^{(n)}(P_{XY})$. We further abbreviate *probability mass function* by *pmf*. When the pmf is not clear from the context, we write $H_P(\cdot)$ and $I_P(\cdot; \cdot)$ to indicate that entropy and mutual information are meant with respect to P_{XY} .

II. PROBLEM SETUP AND MAIN RESULT

Consider the DHT setup illustrated in Figure 1 involving the three terminals Alice, Bob, and Eve. Depending on the binary

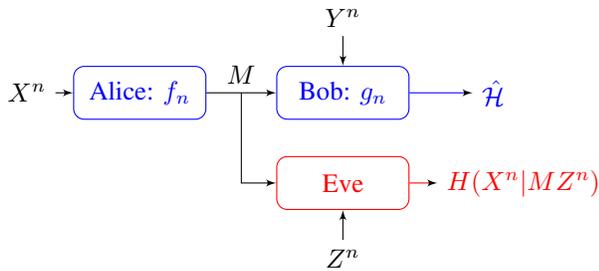


Fig. 1: DHT with communication and security constraints.

hypothesis \mathcal{H}_0 or \mathcal{H}_1 , the observations at the three terminals obey the following joint distribution

$$\text{under } \mathcal{H}_0: (X^n, Y^n, Z^n) \sim P_{XYZ}^{\otimes n} \quad (1)$$

$$\text{under } \mathcal{H}_1: (X^n, Y^n, Z^n) \sim Q_{XYZ}^{\otimes n}, \quad (2)$$

where $Q_{XYZ} = P_X P_Y P_{Z|XY}$.

Alice observes the independent and identically distributed (i.i.d.) length- n sequence X^n and sends $M = f_n(X^n)$ for some randomized encoding function of the form $f_n: \mathcal{X}^n \rightarrow \mathcal{M}$ and message space $\mathcal{M} \triangleq \{1, \dots, \lceil 2^{nR} \rceil\}$, where $R > 0$ is the maximum allowed rate of transmission. Given its own observation Y^n and after observing message M , Bob guesses the true hypothesis as $\hat{\mathcal{H}} = g_n(M, Y^n)$ using a decision rule of the form $\mathcal{M} \times \mathcal{Y}^n \rightarrow \{\mathcal{H}_0, \mathcal{H}_1\}$. Bob's type-I and type-II error probabilities are then given by

$$\alpha_n(f_n, g_n) := \mathbb{P}(\hat{\mathcal{H}} = \mathcal{H}_1 | \mathcal{H}_0) \quad (3)$$

$$\beta_n(f_n, g_n) := \mathbb{P}(\hat{\mathcal{H}} = \mathcal{H}_0 | \mathcal{H}_1). \quad (4)$$

Definition 1: Given $\epsilon > 0$, a tuple $(R, \theta, \Delta_0, \Delta_1)$ is achievable, if there exists a sequence of encoding and decoding functions $\{(f_n, g_n)\}_n$ satisfying

$$\overline{\lim}_{n \rightarrow \infty} \alpha_n(f_n, g_n) \leq \epsilon \quad (5a)$$

$$\underline{\lim}_{n \rightarrow \infty} -\frac{1}{n} \log \beta_n(f_n, g_n) \geq \theta \quad (5b)$$

$$\underline{\lim}_{n \rightarrow \infty} \frac{1}{n} H(X^n | M, Z^n, \mathcal{H}_j) \geq \Delta_j, \quad j \in \{0, 1\}. \quad (5c)$$

Theorem 1: For $\epsilon \in (0, 1)$, the quadruple $(R, \theta, \Delta_0, \Delta_1)$ is achievable if, and only if, there exists a conditional pmf $P_{U|X}$ so that

$$R \geq I_P(U; X), \quad (6)$$

$$\theta \leq I_P(U; Y), \quad (7)$$

$$\Delta_0 \leq (1 - \epsilon)H_P(X|UZ) + \epsilon H_P(X|Z), \quad (8)$$

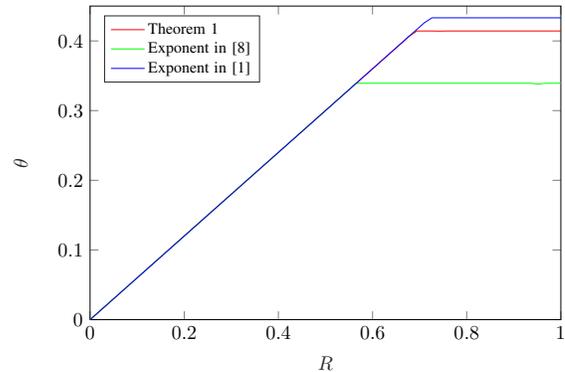
$$\Delta_1 \leq (1 - \epsilon)H_Q(X|UZ) + \epsilon H_Q(X|Z), \quad (9)$$

where indices P and Q refer to the joint pmfs

$$P_{UXYZ} = P_{U|X} P_{XYZ} \quad (10)$$

$$Q_{UXYZ} = P_{U|X} P_X P_Y P_{Z|XY}. \quad (11)$$

Remark 1: In the limit $\epsilon \rightarrow 0$ and for $\Delta_1 \geq H_Q(X|Z)$, the fundamental rate-exponent-equivocations region in Theorem 1 recovers the regions presented in [8], [9], which only considered an equivocation constraint under the null hypothesis \mathcal{H}_0 .

Fig. 2: Type-II error exponent θ in function of R .

For a general positive $\epsilon > 0$, the fundamental rate-exponent-equivocations region in Theorem 1 however is larger, unless Δ_0 is sufficiently small.

We evaluate Theorem 1 for a specific example.

Example 1: Consider a binary source X , and assume that Y and Z are obtained by passing X through a binary erasure channel (BEC) and a binary symmetric channel (BSC), respectively. Source and channel parameters are given by

$$P_X(0) = 1 - P_X(1) = 0.8, \quad (12)$$

$$P_{Y|X}(e|x) = 0.4, \quad (13)$$

$$P_{Z|X}(1-x|x) = 0.2, \quad (14)$$

$$Q_{Z|X}(1-x|x) = 0.3. \quad (15)$$

We also fixed $\Delta_0 = \Delta_1 = 0.13$ and $\epsilon = 0.2$. For this example, the equivocation constraint under \mathcal{H}_1 is always less stringent than under \mathcal{H}_0 .

Figure 2 shows the largest exponent θ for which the quadruple $(R, \theta, \Delta_0, \Delta_1)$ is achievable according to Theorem 1, and compares it to the exponent proposed in [8] and the largest exponent achievable without any security constraints [1]. For small rates R , all three exponents coincide and the equivocation constraints under both hypotheses seem inactive. For larger rates R , the optimal exponent in Theorem 1 dominates the sub-optimal exponent in [8] because $\epsilon > 0$. For even larger rates R , the security constraints become stringent the exponent in Theorem 1 is below the Ahlswede-Csiszár exponent in [1].

III. OPTIMAL CODING SCHEME

Choose a conditional pmf $P_{U|X}$ so that

$$R > I_P(U; X) \quad (16)$$

where we defined the joint pmf

$$P_{UXYZ} = P_{U|X} P_{XYZ}. \quad (17)$$

Codebook generation: Independently generate $\lceil 2^{nR} \rceil$ sequences $u^n(1), \dots, u^n(\lceil 2^{nR} \rceil)$ by picking each entry of each sequence i.i.d. according to P_U . Denote the realization of the set of codewords \mathcal{C} .

Encoder Alice: Fix a small value $\mu > 0$. Alice behaves in a randomized way, described by a Bernoulli- $(1 - \epsilon)$ random

variable Ξ and the likelihood encoder corresponding to the chosen codebook \mathcal{C} [13], [14]

$$P_{M'|X^n}^{\text{LE},\mathcal{C}}(m|x^n) = \frac{P_{X|U}^{\otimes n}(x^n|u^n(m))}{\sum_{m \in \{1, \dots, \lceil 2^{nR} \rceil\}} P_{X|U}^{\otimes n}(x^n|u^n(m))} \quad (18)$$

If $\Xi = 0$, then Alice sends $M = 0$. Otherwise, for $X^n = x^n$, it picks $M' \in \{1, \dots, \lceil 2^{nR} \rceil\}$ according to the conditional distribution $P_{M'|X^n}^{\text{LE},\mathcal{C}}(\cdot|x^n)$. If the pair $(u^n(M'), x^n) \in \mathcal{T}^{(n)}(P_{UX})$, then Alice sends $M = M'$ and otherwise she sends $M = 0$.

Decoder Bob: Assume $Y^n = y^n$ and $M = m$. Bob declares $\hat{H} = \mathcal{H}_0$ if $m \neq 0$ and $(u^n(m), y^n) \in \mathcal{T}_{2\mu}^{(n)}(P_{UY})$. Else it declares $\hat{H} = \mathcal{H}_1$.

Sketch of Analysis: Given $\Xi = 0$, the analysis is simple. Trivially, the type-II error probability equals 0 and the type-II error probability equals 1. Moreover, equivocations under the two hypotheses are $H_P(X|Z)$ and $H_Q(X|Z)$.

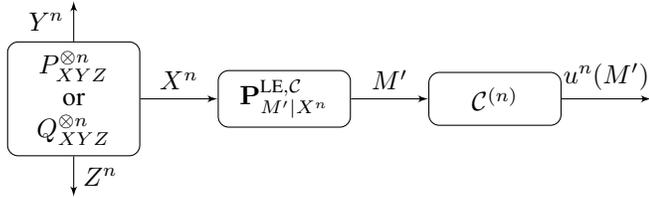


Fig. 3: Encoding

Given $\Xi = 1$, the analysis is similar to [2] and based on the soft covering lemma in [14]. The likelihood encoding system is depicted in Figure 3. Since $R > I(U; X)$, the pair $(u^n(M'), X^n)$ is jointly typical under both hypotheses with a probability (when averaged over the random code construction) tending exponentially fast to 1 as $n \rightarrow \infty$. One can thus restrict the analysis to this assumption. Moreover, since $R > I(U; X)$, by the generalized soft-covering lemma in [14], on average over the random code construction the joint pmf induced by the real system in Figure 3 is close to the pmf induced by the idealized system in Figure 4.

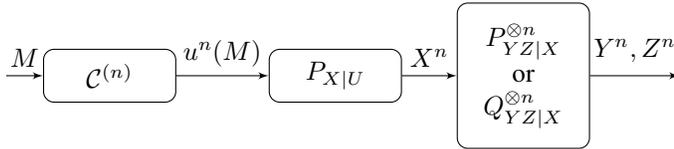


Fig. 4: Idealized distribution.

By standard arguments, it can be concluded that on the idealized system and when $u^n(M) \in \mathcal{T}^{(n)}(P_U)$, then the type-II error probability exponent is equal to $\theta = I(U; Y)$. The type-I error probability tends to 0 as $n \rightarrow \infty$ simply by the weak law of large numbers. Equivocation on the *idealized system* under \mathcal{H}_0 is bounded as follows:

$$\frac{1}{n} H(X^n | U^n(M) Z^n) = \frac{1}{n} \sum_{i=1}^n H(X_i | u_i(M) Z_i) \quad (19)$$

$$= H_P(X|UZ) + o(1), \quad (20)$$

where the first equality holds by the memorylessness of the channels and the second equality because $P_{U_i(M)}$ tends to

P_U as $n \rightarrow \infty$ as mentioned above. Combining all these observations concludes the proof.

IV. CONVERSE PROOF TO THEOREM 1

Fix an achievable exponent $\theta < \theta_\epsilon^*(R)$ and a sequence of (random) encoding and decision functions so that (5) are satisfied. Further fix a blocklength $n > 0$ and let M and \hat{H} be the message and the guess produced by the chosen encoding and decision functions for this given blocklength.

Define the set

$$\mathcal{D}_n \triangleq \left\{ (x^n, y^n) \in \mathcal{T}_{n^{-1/3}}^{(n)}(P_{XY}) : g_n(f_n(x^n), y^n) = \mathcal{H}_0 \right\} \quad (21)$$

By the constraint on the type-I error probability and since by [15, Lemma 2.12]

$$P_{XY}^{\otimes n} \left(\mathcal{T}_{n^{-1/3}}^{(n)}(P_{XY}) \right) \geq 1 - \frac{|\mathcal{X}||\mathcal{Y}|}{4n^{1/3}}, \quad (22)$$

we obtain by the basic laws of probability

$$\Lambda_n := P_{XY}^{\otimes n}(\mathcal{D}_n) \geq 1 - \epsilon - \frac{|\mathcal{X}||\mathcal{Y}|}{4n^{1/3}}. \quad (23)$$

Let $(\tilde{X}^n, \tilde{Y}^n)$ be the restriction of the pair (X^n, Y^n) to \mathcal{D}_n , $\tilde{M} = f_n(\tilde{X}^n)$ the new message, and \tilde{Z}^n the output of the discrete memoryless channel (DMC) $P_{Z|XY}$ for input sequences $(\tilde{X}^n, \tilde{Y}^n)$. Under \mathcal{H}_0 , the probability distribution of the quadruple $(M, \tilde{X}^n, \tilde{Y}^n, \tilde{Z}^n)$ is

$$P_{M\tilde{X}^n\tilde{Y}^n\tilde{Z}^n}(m, x^n, y^n, z^n) \triangleq P_{XY}^{\otimes n}(x^n, y^n) \cdot \frac{\mathbb{1}\{(x^n, y^n) \in \mathcal{D}_n\}}{\Lambda_n} \Pr[f_n(x^n) = m]. \quad (24)$$

Let T be uniform over $\{1, \dots, n\}$ independent of all other random variables.

Lemma 1: For the distribution in (24), the following limits hold as $n \rightarrow \infty$:

$$P_{\tilde{X}^T \tilde{Y}^T} \rightarrow P_{XY} \quad (25)$$

$$\left| \frac{1}{n} H(\tilde{X}^n \tilde{Y}^n) - H(\tilde{X}^T \tilde{Y}^T) \right| \rightarrow 0 \quad (26)$$

$$\left| \frac{1}{n} H(\tilde{Y}^n) - H(\tilde{Y}^T) \right| \rightarrow 0 \quad (27)$$

$$\left| \frac{1}{n} H(\tilde{X}^n | \tilde{Y}^n) - H(\tilde{X}^T | \tilde{Y}^T) \right| \rightarrow 0. \quad (28)$$

Proof: See Appendix A. ■

We bound the rate, the type-II error exponent and the equivocation based on Lemma 1.

Rate: Throughout the following paragraphs, all quantities are calculated according to the pmf in (24) or the pmf P_{XYZ} , and we shall not mention this explicitly. For the rate we have:

$$R \geq \frac{1}{n} H(\tilde{M}) = \frac{1}{n} I(\tilde{M}; \tilde{X}^n \tilde{Y}^n) \quad (29)$$

$$= \frac{1}{n} H(\tilde{X}^n \tilde{Y}^n) - \frac{1}{n} H(\tilde{X}^n \tilde{Y}^n | \tilde{M}) \quad (30)$$

$$= H(\tilde{X}^T \tilde{Y}^T) + o(1) - \frac{1}{n} \sum_{t=1}^n H(\tilde{X}_t \tilde{Y}_t | \tilde{X}^{t-1} \tilde{Y}^{t-1} \tilde{M}) \quad (31)$$

$$= H(\tilde{X}^T \tilde{Y}^T) + o(1) - H(\tilde{X}^T \tilde{Y}^T | \tilde{X}^{T-1} \tilde{Y}^{T-1} \tilde{M} T) \quad (32)$$

$$= I(\tilde{X}_T \tilde{Y}_T; \tilde{X}^{T-1} \tilde{Y}^{T-1} \tilde{M} T) + o(1) \quad (33)$$

$$\geq I(\tilde{X}_T; U) + o(1), \quad (34)$$

where we defined $U \triangleq (\tilde{X}^{T-1}, \tilde{Y}^{T-1}, \tilde{M}, T)$.

To bound the error exponent, define $\tilde{\mathcal{H}} \triangleq g_n(\tilde{M}, \tilde{Y}^n)$ and notice inequality

$$D(P_{\tilde{Y}^n \tilde{M}} \| P_{\tilde{Y}^n} P_{\tilde{M}}) \stackrel{(a)}{\geq} D(P_{\tilde{Y}^n \tilde{M}}(\tilde{\mathcal{H}}) \| P_{\tilde{Y}^n} P_{\tilde{M}}(\tilde{\mathcal{H}})) \quad (35)$$

$$\stackrel{(b)}{=} 1 \cdot \log \frac{1}{P_{\tilde{Y}^n \tilde{M}}(\tilde{\mathcal{H}} = 0)}, \quad (36)$$

where (a) holds by the data-processing inequality and (b) holds by the definition of divergence and because $\tilde{\mathcal{H}} = 0$ with probability 1.

Type-II error exponent: We have:

$$\beta_n = -\frac{1}{n} \log P_{\tilde{Y}^n} P_{\tilde{M}}(\hat{\mathcal{H}} = 0) \quad (37)$$

$$\stackrel{(c)}{\leq} -\frac{1}{n} \log P_{\tilde{Y}^n} P_{\tilde{M}}(\tilde{\mathcal{H}} = 0) - \frac{2}{n} \log \Lambda_n \quad (38)$$

$$\stackrel{(d)}{\leq} \frac{1}{n} D(P_{\tilde{Y}^n \tilde{M}} \| P_{\tilde{Y}^n} P_{\tilde{M}}) + o(1) \quad (39)$$

$$= \frac{1}{n} I(\tilde{M}; \tilde{Y}^n) + o(1) \quad (40)$$

$$\leq \frac{1}{n} H(\tilde{Y}^n) - \frac{1}{n} \sum_{t=1}^n H(\tilde{Y}_t | \tilde{M} \tilde{X}^{t-1} \tilde{Y}^{t-1}) + o(1) \quad (41)$$

$$\stackrel{(e)}{\leq} H(\tilde{Y}_T) + o(1) - H(\tilde{Y}_T | U) \quad (42)$$

$$= I(\tilde{Y}_T; U) + o(1), \quad (43)$$

where (c) holds because

$$P_{\tilde{Y}^n}(y) \leq \frac{P_{Y^n}(y^n)}{\Lambda_n} \quad \text{and} \quad P_{\tilde{M}}(m) \leq \frac{P_M(m)}{\Lambda_n}; \quad (44)$$

(d) holds by (23) and (36); and (e) holds by (27).

Equivocation under \mathcal{H}_0 : We define $E \triangleq \mathbb{1}\{(X^n, Y^n) \in \mathcal{D}_n\}$ and note:

$$\begin{aligned} & \frac{1}{n} H(X^n | M Z^n) \\ & \stackrel{(f)}{=} \frac{1}{n} \sum_{t=1}^n H(X_t | X^{t-1} Y^{t-1} M Z^n) \end{aligned} \quad (45)$$

$$\begin{aligned} & = \frac{1}{n} \sum_{t=1}^n H(X_t | X^{t-1} Y^{t-1} M Z^n E) \\ & \quad + \frac{1}{n} \sum_{t=1}^n I(E; X_t | X^{t-1} Y^{t-1} M Z^n) \end{aligned} \quad (46)$$

$$\begin{aligned} & \leq \frac{1}{n} \sum_{t=1}^n H(X_t | X^{t-1} Y^{t-1} M Z^n E) \\ & \quad + \frac{1}{n} \sum_{t=1}^n I(E; X_t, Y_t | X^{t-1} Y^{t-1} M Z^n) \end{aligned} \quad (47)$$

$$\begin{aligned} & \stackrel{(g)}{\leq} \frac{1}{n} \sum_{t=1}^n H(\tilde{X}_t | \tilde{X}^{t-1} \tilde{Y}^{t-1} \tilde{M} \tilde{Z}^n) \Pr[E = 1] \\ & \quad + \frac{1}{n} \sum_{t=1}^n H(X_t | Z_t, E = 0) \Pr[E = 0] \\ & \quad + \frac{1}{n} I(E; X^n Y^n | M Z^n) \end{aligned} \quad (48)$$

$$\begin{aligned} & \leq H(\tilde{X}_T | U \tilde{Z}_T) \Pr[E = 1] \\ & \quad + H(X_T | Z_T, E = 0) \Pr[E = 0] + \frac{1}{n} \end{aligned} \quad (49)$$

where (f) holds by the Markov chain $X_t \rightarrow (M, X^{t-1}, Z^n) \rightarrow Y^{t-1}$; and (g) because event $E = 1$ corresponds to the change of measure in (28) and because conditioning can only reduce entropy.

Define $F = 1$ as the indicator function

$$F = \mathbb{1}\{(X^n, Z^n) \in \mathcal{T}^{(n)}(P_{XZ})\}. \quad (50)$$

Similarly to the proof of (25), one can show that

$$P_{X_T Z_T | E=0, F=1} \rightarrow P_{XZ}, \quad (51)$$

and thus by continuity of the entropy functional

$$H(\tilde{X}_T | \tilde{Z}_T, E = 0, F = 1) \rightarrow H(X | Z). \quad (52)$$

Since $H(\tilde{X}_T | \tilde{Z}_T, E = 0, F = 0)$ is bounded by $\log |\mathcal{X}|$ and

$$\Pr[F = 0, E = 0] \leq \Pr[F = 0] = o(1), \quad (53)$$

we conclude that

$$H(\tilde{X}_T | \tilde{Z}_T, E = 0) \Pr[E = 0] \leq H(X | Z) \Pr[E = 0] + o(1), \quad (54)$$

which combined with (49) yields

$$\begin{aligned} \frac{1}{n} H(X^n | M Z^n) & \leq H(\tilde{X}_T | U \tilde{Z}_T) \Pr[E = 1] \\ & \quad + H(X | Z) \Pr[E = 0] + o(1). \end{aligned} \quad (55)$$

For sufficiently large values of the blocklength n , the conditional entropy $H(\tilde{X}_T | U \tilde{Z}_T)$ is smaller than $H(X | Z)$ because $P_{\tilde{X}_T \tilde{Z}_T} \rightarrow P_{XZ}$, and thus (23) and (55) yields:

$$\begin{aligned} \frac{1}{n} H(X^n | M Z^n) & \leq H(\tilde{X}_T | U \tilde{Z}_T) \left(1 - \epsilon - \frac{|\mathcal{X}||\mathcal{Y}|}{4n^{1/3}}\right) \\ & \quad + H(X | Z) \left(\epsilon + \frac{|\mathcal{X}||\mathcal{Y}|}{4n^{1/3}}\right) + o(1). \end{aligned} \quad (56)$$

Equivocation under \mathcal{H}_1 : The proof is similar as under \mathcal{H}_0 , but requires adding new random variables $Y'^n = (Y'_1, \dots, Y'_n)$ obtained by passing X^n through the DMC $P_{Y|X}$. We restrict the tuples (X^n, Y'^n, Z^n, M) to tuples so that $(X^n, Y'^n) \in \mathcal{D}_n$ as introduced in (21). Then the joint pmf under \mathcal{H}_1 of the restricted tuple $(\bar{X}^n, \bar{Y}'^n, \bar{Z}^n, \bar{M})$ is

$$\begin{aligned} & Q_{\bar{M} \bar{X}^n \bar{Y}'^n \bar{Z}^n}(m, x^n, y'^n, z^n) \\ & \triangleq P_{XY}^{\otimes n}(x^n, y'^n) \cdot \frac{\mathbb{1}\{(x^n, y'^n) \in \mathcal{D}_n\}}{\Lambda_n} \\ & \quad \cdot Q_{Z|X}(z^n | x^n) P_{M|X^n}(m | x^n), \end{aligned} \quad (57)$$

where $Q_{Z|X}(z|x) = \sum_y P_Y(y) P_{Z|XY}(z|x, y)$.

Following the same steps as leading to (56), but where P_{XZ} is replaced by $Q_{XZ} = P_X Q_{Z|X}$, the sequence Y^n by Y'^n , and the restricted tuple $(\bar{M}, \bar{X}^n, \bar{Y}'^n, \bar{Z}^n)$ by $(\bar{M}, \bar{X}^n, \bar{Y}'^n, \bar{Z}^n)$, we obtain an equivocation bound under \mathcal{H}_1 :

$$\begin{aligned} \frac{1}{n} H_Q(X^n | M Z^n) & \leq H(\bar{X}_T | \bar{U} \bar{Z}_T) \left(1 - \epsilon - \frac{|\mathcal{X}||\mathcal{Y}|}{4n^{1/3}}\right) \\ & \quad + H_Q(X | Z) \left(\epsilon + \frac{|\mathcal{X}||\mathcal{Y}|}{4n^{1/3}}\right) + o(1). \end{aligned} \quad (58)$$

Note that (\tilde{U}, \tilde{X}) have same pmf as (U, \tilde{X}) defined previously, and \tilde{Z}_T is obtained by passing \tilde{X} through the DMC $Q_{Z|X}$.

Concluding the proof: Before being able to conclude the proof, we notice the following set of inequalities (where again all pmfs are with respect to the pmf in (24)):

$$0 = \frac{1}{n} I(\tilde{M}; \tilde{Y}^n | \tilde{X}^n) \quad (59)$$

$$= \frac{1}{n} H(\tilde{Y}^n | \tilde{X}^n) - \frac{1}{n} H(\tilde{Y}^n | \tilde{X}^n \tilde{M}) \quad (60)$$

$$= H(\tilde{Y}_T | \tilde{X}_T) + o(1) - \frac{1}{n} \sum_{t=1}^n H(\tilde{Y}_t | \tilde{X}^n \tilde{Y}^{t-1} \tilde{M}) \quad (61)$$

$$\geq H(\tilde{Y}_T | \tilde{X}_T) + o(1) - H(\tilde{Y}_T | \tilde{X}_T \tilde{X}^{T-1} \tilde{Y}^{T-1} \tilde{M} T) \quad (62)$$

$$= I(\tilde{Y}_T; U | \tilde{X}_T) + o(1). \quad (63)$$

Thus,

$$\lim_{n \rightarrow \infty} I(\tilde{Y}_T; U | \tilde{X}_T) = 0. \quad (64)$$

The proof is then concluded by combining (34), (43), (56), and (58) with limit (64) and taking $n \rightarrow \infty$. Details are as follows. By Carathéodory's theorem, and because $P_{\tilde{X}_T \tilde{U}} = P_{\tilde{X}_T \tilde{U}}$, we can conclude that the existence of a random variable \tilde{U}_n over an alphabet of size $|\mathcal{X}| + 3$ and so that

$$R \geq I_P(U_n; \tilde{X}_T) + o(1) \quad (65)$$

$$- \frac{1}{n} \log \beta_n \leq I_P(U_n; \tilde{Y}_T) + o(1) \quad (66)$$

$$\liminf_{n \rightarrow \infty} H_P(X^n | M, Z^n) \leq H(\tilde{X}_T | U_n, \tilde{Z}_T) \quad (67)$$

$$\liminf_{n \rightarrow \infty} H_Q(X^n | M, Z^n) \leq H(\tilde{X}_T | U_n, \tilde{Z}'_T), \quad (68)$$

where \tilde{Z}'_T is obtained by passing \tilde{X}_T through the DMC $Q_{Z|X}$.

Considering a subsequence of blocklengths $\{n_i\}_{i=1}^{\infty}$ for which the joint pmf $P_{\tilde{X}_T \tilde{Y}_T U_n}$ converges, we conclude the existence of joint pmfs P_{XYZU} and Q_{XYUZ} with the properties desired in Theorem 1. This concludes the proof of the converse.

V. CONCLUSION

We have studied the problem of distributed hypothesis testing against independence over a rate-limited noiseless channel with both communication and security constraints. We have characterized the largest possible type-II error exponent at the legitimate receiver under constraints on the legitimate receiver's type-I error probability and the equivocations measured at an eavesdropper. In the limit of vanishing type-I error probability the results recover the previous result in [8]. This previous result is however disproved when positive type-I error probabilities are allowed.

An interesting future research direction is to extend our results to a scenario with variable-length coding, when the expected rate but not the maximum rate is constrained.

APPENDIX A PROOF OF LEMMA 1

To prove (25), notice that

$$P_{\tilde{X}_T \tilde{Y}_T}(x, y) = \frac{1}{n} \sum_{t=1}^n P_{\tilde{X}_t \tilde{Y}_t}(x, y) \quad (69)$$

$$= \mathbb{E} \left[\frac{1}{n} \sum_{t=1}^n \mathbb{1}\{\tilde{X}_t = x, \tilde{Y}_t = y\} \right] \quad (70)$$

$$= \mathbb{E}[\pi_{\tilde{X}_n \tilde{Y}_n}(x, y)]. \quad (71)$$

Since by the definition of the typical set,

$$|\pi_{\tilde{X}_n \tilde{Y}_n}(x, y) - P_{XY}(x, y)| \leq n^{-1/3}, \quad (72)$$

we conclude that as $n \rightarrow \infty$ the probability $P_{\tilde{X}_T \tilde{Y}_T}(x, y)$ tends to $P_{XY}(x, y)$.

To prove (26), notice first that

$$\begin{aligned} & \frac{1}{n} H(\tilde{X}^n \tilde{Y}^n) + \frac{1}{n} D(P_{\tilde{X}^n \tilde{Y}^n} \| P_{XY}^{\otimes n}) \\ &= -\frac{1}{n} \sum_{(x^n, y^n) \in \mathcal{D}_n} P_{\tilde{X}^n \tilde{Y}^n}(x^n, y^n) \log P_{XY}^{\otimes n}(x^n, y^n) \end{aligned} \quad (73)$$

$$= -\frac{1}{n} \sum_{t=1}^n \sum_{(x^n, y^n) \in \mathcal{D}_n} P_{\tilde{X}^n \tilde{Y}^n}(x^n, y^n) \log P_{XY}(x_t, y_t) \quad (74)$$

$$= -\frac{1}{n} \sum_{t=1}^n \sum_{(x, y) \in \mathcal{X} \times \mathcal{Y}} P_{\tilde{X}_t \tilde{Y}_t}(x, y) \log P_{XY}(x, y) \quad (75)$$

$$= - \sum_{(x, y) \in \mathcal{X} \times \mathcal{Y}} P_{\tilde{X}_T \tilde{Y}_T}(x, y) \log P_{XY}(x, y) \quad (76)$$

$$= H(\tilde{X}_T \tilde{Y}_T) + D(P_{\tilde{X}_T \tilde{Y}_T} \| P_{XY}). \quad (77)$$

Combined with the following two limits (78) and (79), this establishes (26). The first relevant limit is

$$D(P_{\tilde{X}_T \tilde{Y}_T} \| P_{XY}) \rightarrow 0, \quad (78)$$

which holds by (25) and because $P_{\tilde{X}_T \tilde{Y}_T}(x, y) = 0$ whenever $P_{XY}(x, y) = 0$. The second limit is:

$$\frac{1}{n} D(P_{\tilde{X}^n \tilde{Y}^n} \| P_{XY}^{\otimes n}) \rightarrow 0, \quad (79)$$

and holds because $\frac{1}{n} \log \Lambda_n \rightarrow 0$ and by the following set of inequalities:

$$\begin{aligned} 0 &\leq \frac{1}{n} D(P_{\tilde{X}^n \tilde{Y}^n} \| P_{XY}^{\otimes n}) \\ &= \frac{1}{n} \sum_{(x^n, y^n) \in \mathcal{D}_n} P_{\tilde{X}^n \tilde{Y}^n}(x^n, y^n) \log \frac{P_{\tilde{X}^n \tilde{Y}^n}(x^n, y^n)}{P_{XY}^{\otimes n}(x^n, y^n)} \end{aligned} \quad (80)$$

$$= -\frac{1}{n} \sum_{(x^n, y^n) \in \mathcal{D}_n} P_{\tilde{X}^n \tilde{Y}^n}(x^n, y^n) \log \Lambda_n \quad (81)$$

$$= -\frac{1}{n} \log \Lambda_n. \quad (82)$$

To prove (27), notice that by the same arguments as we concluded (77), we also have

$$\frac{1}{n} H(\tilde{Y}^n) + \frac{1}{n} D(P_{\tilde{Y}^n} \| P_Y^{\otimes n}) = H(\tilde{Y}_T) + D(P_{\tilde{Y}_T} \| P_Y). \quad (83)$$

Moreover, (78) and (79) imply

$$\frac{1}{n} D(P_{\tilde{Y}^n} \| P_Y^{\otimes n}) \rightarrow 0 \quad (84)$$

$$D(P_{\tilde{Y}_T} \| P_Y) \rightarrow 0, \quad (85)$$

which combined with (83) imply (27).

The last limit (28) follows by the chain rule and limits (26) and (27). This concludes the proof.

REFERENCES

- [1] R. Ahlswede and I. Csiszár, "Hypothesis testing with communication constraints," *IEEE Transactions on Information Theory*, vol. 32, no. 4, pp. 533–542, 1986.
- [2] S. Sreekumar, A. Cohen, and D. Gündüz, "Privacy-aware distributed hypothesis testing," *Entropy*, vol. 22, no. 6, 2020. [Online]. Available: <https://www.mdpi.com/1099-4300/22/6/665>
- [3] J. Liao, L. Sankar, V. Y. F. Tan, and F. du Pin Calmon, "Hypothesis testing under mutual information privacy constraints in the high privacy regime," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1058–1071, 2018.
- [4] R. Tandon, L. Sankar, and H. V. Poor, "Discriminatory lossy source coding: Side information privacy," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5665–5677, 2013.
- [5] S. B. Amor, A. Gilani, S. Salehkalaibar, and V. Y. F. Tan, "Distributed hypothesis testing with privacy constraints," in *2018 International Symposium on Information Theory and Its Applications (ISITA)*, 2018, pp. 742–746.
- [6] Z. Li, T. J. Oechtering, and D. Gündüz, "Privacy against a hypothesis testing adversary," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1567–1581, 2019.
- [7] V. Narayanan, M. Mishra, and V. M. Prabhakaran, "Private two-terminal hypothesis testing," in *2020 IEEE International Symposium on Information Theory (ISIT)*, 2020, pp. 1001–1006.
- [8] M. Mhanna and P. Piantanida, "On secure distributed hypothesis testing," in *2015 IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 1605–1609.
- [9] S. Sreekumar and D. Gündüz, "Testing against conditional independence under security constraints," in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 181–185.
- [10] M. Hamad, M. Wigger, and M. Sarkiss, "Multi-hop network with multiple decision centers under expected-rate constraints," 2022. [Online]. Available: <https://arxiv.org/abs/2208.14243>
- [11] —, "Strong converses using change of measure and asymptotic markov chains," in *In Proc. of IEEE 2022 ITW*. Bombay, India: arXiv, Nov. 2022. [Online]. Available: <https://arxiv.org/abs/2205.08910>
- [12] H. Tyagi and S. Watanabe, "Strong converse using change of measure arguments," *IEEE Transactions on Information Theory*, vol. 66, no. 2, pp. 689–703, 2020.
- [13] E. C. Song, P. Cuff, and H. V. Poor, "The likelihood encoder for lossy source compression," in *2014 IEEE International Symposium on Information Theory*, 2014, pp. 2042–2046.
- [14] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7584–7605, 2014.
- [15] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011.