Strong Converse for a Degraded Wiretap Channel via Active Hypothesis Testing

Masahito Hayashi* Himanshu Tyagi† Shun Watanabe‡

***Abstract*—We establish an upper bound on the rate of codes for a wiretap channel with public feedback for a fixed probability of error and secrecy parameter. As a corollary, we obtain a strong converse for the capacity of a degraded wiretap channel with public feedback. Our converse proof is based on a reduction of active hypothesis testing for discriminating between two channels to coding for wiretap channel with feedback.**

I. Introduction

We consider secure message transmission over a wiretap channel $W : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ with noiseless, public feedback. For each transmission $x \in \mathcal{X}$ over W, the receiver observes a random output $Y \in \mathcal{Y}$ and an eavesdropper observes a correlated side-information $Z \in \mathcal{Z}$, with probability $W(Y, Z|x)$. Furthermore, the receiver can send a feedback to the transmitter over a noiseless channel. However, the feedback channel is public and any communication sent over it is available to the eavesdropper. The transmitter seeks to send a message M to the receiver without revealing it to the eavesdropper. For a given probability of error ϵ and a given secrecy parameter δ, what is the maximum possible rate $C_{\epsilon,\delta}$ of a transmitted message?

For a degraded wiretap channel W with no feedback, the wiretap capacity $C = \inf_{\epsilon,\delta} C_{\epsilon,\delta}$ was established in the seminal work of Wyner [19] where it was shown that

$$C = \max_{\mathrm{P}_X} I\left(X \wedge Y \mid Z\right).$$

The capacity of a general wiretap channel was established in [3]. Extensions to wiretap channels with general statistics were considered in [4]. The model with feedback considered here was introduced in [8] where it was noted that the availability of a noiseless feedback can enable positive rates of transmission over a wiretap channel with zero capacity (see, also, [10]). However, the wiretap capacity with feedback remains unknown in general; $\max_{\mathrm{P}_X} I\left(X \wedge Y \mid Z\right)$ constitutes an upper bound on it.

In this paper, we establish a *strong version* of this bound and show that for $\epsilon + \delta < 1$

$$C_{\epsilon,\delta} \le \max_{\mathrm{P}_X} I\left(X \wedge Y \mid Z\right),$$

thereby characterizing $C_{\epsilon,\delta}$ for all $0 < \epsilon, \delta < 1$ for a degraded wiretap channel. A partial strong converse for a degraded wiretap channel was established in [11] for a restricted range of ϵ, δ. Another strong converse for a degraded wiretap channel for the case when $\delta \to 0$ was established, concurrently to this work, in [15]. In this work, we show a strong converse for all values of ϵ and δ.

Our proof relies on a slight modification of a recent reduction of hypothesis testing to secret key agreement shown in [17], [18]. Specifically, we show that a wiretap channel code yields an active hypothesis test for distinguishing between two channels [6]. Consequently, the rate of a wiretap code is bounded above by the rate of the optimum exponent of the probability of error of type II for discriminating a channel W from another channel V such that $V(y, z|x) = V_2(z|x)V_1(y|z)$, given that the probability of error of type I is less than $\epsilon + \delta$. This gives an upper bound on the length of a wiretap code, which leads to the strong converse upon using the characterization of the optimal exponent for channel discrimination derived in [6]. This approach is along the lines of *meta-converse* of [13], where a reduction of hypothesis testing to channel coding was used to establish a finite-blocklength converse for the channel coding problem (see, also, [12] and [5, Section 4.6]).

Our main result is given in the next section. Section III and IV contains a review of relevant results in binary hypothesis testing and secret key agreement, respectively. The final section contains a proof of our main result.

II. Main result

We describe a generalization of the classic wiretap channel coding problem [19], [3] that was considered in [8], [10], [1], where, in addition to transmitting over the wiretap channel, the terminals can communicate using a noiseless, public feedback channel from the receiver to the transmitter.

A wiretap code for a discrete[1] memoryless wiretap channel $W : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ with feedback consists of (possibly randomized) encoder mappings $e_t : \{1, ..., N\} \times \mathcal{F}^t \to \mathcal{X}$, $1 \le t \le n$, feedback mappings $f_t : \mathcal{Y}^t \to \mathcal{F}$, $0 \le t \le n-1$, and a decoder $d : \mathcal{Y}^n \to \{1, ..., N\}$. For a random message $M \sim \mathtt{unif}\{1, ..., N\}$, the protocol begins with a feedback F_0 from the receiver at $t = 0$. Subsequently, at each time instance $1 \le t \le n-1$ the transmitter sends $X_t = e_t(M, F^{t-1})$ and the channel outputs (Y_t, Z_t)

*The Graduate School of Mathematics, Nagoya University, Japan, and The Centre for Quantum Technologies, National University of Singapore, Singapore. Email:masahito@math.nagoya-u.ac.jp

†Information Theory and Applications (ITA) Center, University of California, San Diego, La Jolla, CA 92093, USA. Email: htyagi@eng.ucsd.edu

‡Department of Information Science and Intelligent Systems, University of Tokushima, Tokushima 770-8506, Japan, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA. Email: shunwata@is.tokushima-u.ac.jp

[1]The restriction to discrete alphabet is cosmetic. Our results apply to channels with continuous alphabet. In particular, our strong converse holds for the Gaussian wiretap channel [9].

with probability $W(Y_t, Z_t|X_t)$. The receiver observes Y_t and sends feedback $F_t = f_t(Y^t)$, and the eavesdropper observes Z_t. The protocol stops with a final transmission $X_n = e_n(M, F^{n-1})$ over the channel and the subsequent decoding $\hat{M} = d(Y^n)$ by the receiver. We denote by $\mathbf{F}$ the overall feedback communication $F_0, ..., F_{n-1}$.

The mappings $(\{e_t\}_{t=1}^n, \{f_t\}_{t=0}^{n-1}, d)$ constitute an (N, n, ϵ, δ) wiretap code if

$$\mathrm{P}\left(M \neq \hat{M}\right) \leq \epsilon,$$

and

$$\|\mathrm{P}_{MZ^n\mathbf{F}} - \mathrm{P}_M \times \mathrm{P}_{Z^n\mathbf{F}}\|_1 \leq \delta,$$

where $\|\mathrm{P} - \mathrm{Q}\|_1$ denotes the variation distance between P and Q given by

$$\|\mathrm{P} - \mathrm{Q}\|_1 = \frac{1}{2}\sum_x |\mathrm{P}(x) - \mathrm{Q}(x)|.$$

A rate $R > 0$ is (ϵ, δ)-achievable if there exists an $(\lfloor 2^{nR} \rfloor, n, \epsilon, \delta)$ wiretap code for all n sufficiently large. The (ϵ, δ)-*wiretap capacity* $C_{\epsilon,\delta}$ is the supremum of all (ϵ, δ)-achievable rates.

Our main result in an upper bound on $C_{\epsilon,\delta}$

Theorem 1. *For $0 \leq \epsilon, \delta$ with $\epsilon + \delta < 1$, the (ϵ, δ)-wiretap capacity is bounded above as*

$$C_{\epsilon,\delta} \leq \max_{\mathrm{P}_X} I\left(X \wedge Y \mid Z\right).$$

For the special case of a degraded wiretap channel W with $W(y, z|x) = W_1(y|x)W_2(z|y)$, Theorem 1 yields a *strong converse* for wiretap capacity.

Corollary 2. *For a degraded wiretap channel W,*

$$C_{\epsilon,\delta} = \begin{cases} \max_{\mathrm{P}_X} I\left(X \wedge Y \mid Z\right), & 0 < \epsilon < 1 - \delta, \\ \max_{\mathrm{P}_X} I\left(X \wedge Y\right), & 1 - \delta \leq \epsilon < 1. \end{cases}$$

Proof. For $0 < \epsilon < 1 - \delta$, the result is an immediate corollary of Theorem 1 and [19][2]. For $1 - \delta \leq \epsilon < 1$, the converse follows from the strong converse for the capacity of a DMC with feedback (*cf.* [14]). Moving to the proof of achievability, it suffices to restrict to $\epsilon + \delta = 1$. For this case, achievability follows by randomizing between an $(\epsilon_n, 1)$ wiretap code, $\epsilon_n \to 0$ as $n \to \infty$, and a $(1, 0)$ wiretap code – the randomizing bit is communicated as the public feedback F_0 by the receiver[3] □

As a preparation for the proof of Theorem 1 given in Section V, we review some results in hypothesis testing and secret key agreement in the next two sections.

III. Hypothesis testing

Consider a simple binary hypothesis testing problem with null hypothesis P and alternative hypothesis Q, where P and Q are distributions on the same alphabet $\mathcal{X}$. Upon observing a value $x \in \mathcal{X}$, the observer needs to decide if the value was generated by the distribution P or the distribution Q. To this end, the observer applies a stochastic test T, which is a conditional distribution on $\{0, 1\}$ given an observation $x \in \mathcal{X}$. When $x \in \mathcal{X}$ is observed, the test T chooses the null hypothesis with probability $\mathrm{T}(0|x)$ and the alternative hypothesis with probability $T(1|x) = 1 - T(0|x)$. For $0 \leq \epsilon < 1$, denote by $\beta_\epsilon(\mathrm{P}, \mathrm{Q})$ the infimum of the probability of error of type II given that the probability of error of type I is less than ϵ, i.e.,

$$\beta_\epsilon(\mathrm{P}, \mathrm{Q}) := \inf_{\mathrm{T}\,:\,\mathrm{P}[\mathrm{T}] \geq 1-\epsilon} \mathrm{Q}[\mathrm{T}],$$

where

$$\begin{aligned} \mathrm{P}[\mathrm{T}] &= \sum_x \mathrm{P}(x)\mathrm{T}(0|x), \\ \mathrm{Q}[\mathrm{T}] &= \sum_x \mathrm{Q}(x)\mathrm{T}(0|x). \end{aligned}$$

The following result credited to Stein characterizes the optimum exponent of $\beta_\epsilon(\mathrm{P}^n, \mathrm{Q}^n)$ where $\mathrm{P}^n = \mathrm{P} \times ... \times \mathrm{P}$ and $\mathrm{Q}^n = \mathrm{Q} \times ... \times \mathrm{Q}$.

Lemma 3. (*cf.* [7, Theorem 3.3]) *For every $0 < \epsilon < 1$, we have*

$$\lim_{n\to\infty} -\frac{1}{n}\log \beta_\epsilon(\mathrm{P}^n, \mathrm{Q}^n) = D(\mathrm{P}\|\mathrm{Q}),$$

where $D(\mathrm{P}\|\mathrm{Q})$ is the Kullback-Leibler divergence given by

$$D(\mathrm{P}\|\mathrm{Q}) = \sum_{x\in\mathcal{X}} \mathrm{P}(x)\log\frac{\mathrm{P}(x)}{\mathrm{Q}(x)},$$

with the convention $0\log(0/0) = 0$.

Next, we review a problem of active hypothesis testing where the distribution at each instance is determined by a prior action. Specifically, given two DMCs $W : \mathcal{X} \to \mathcal{Y}$ and $V : \mathcal{X} \to \mathcal{Y}$, we seek to design a transmission-feedback scheme such that by observing the channel inputs, channel outputs, and feedback we can determine if the underlying channel is W or V. Formally, an n-length active hypothesis test consist of (possibly randomized) encoder mappings $e_t : \mathcal{F}^t \to \mathcal{X}$, $1 \leq t \leq n$, feedback mappings $f_t : \mathcal{Y}^t \to \mathcal{F}$, $0 \leq t \leq n-1$, and a conditional distribution T on $\{0, 1\}$ given $X^n, Y^n, \mathbf{F}$. On observing $X^n, Y^n, \mathbf{F}$, we detect the null hypothesis W with probability $T(0|X^n, Y^n, \mathbf{F})$ and alternative hypothesis V with probability $T(1|X^n, Y^n, \mathbf{F})$. Analogous to $\beta_\epsilon(\mathrm{P}, \mathrm{Q})$, the quantity $\beta_\epsilon(W, V, n)$, for $0 \leq \epsilon < 1$, is the infimum of the probability of error of type II over all n length active hypothesis tests for null hypothesis W and alternative hypothesis V such that the probability of error of type I is no more than ϵ.

The following analogue of Stein's lemma for active hypothesis testing was established in [6] (see, also, [14]).

[2]While the secrecy criterion in [19] is different from variational secrecy required here, the achievability result for the latter follows from the results in [2], [4].

[3]Alternatively, the sender can transmit the randomizing bit over the wiretap channel with neglible rate loss.

Theorem 4 ([6])**.** *For $0 < \epsilon < 1$,*

$$\lim_n -\frac{1}{n}\log \beta_\epsilon(W,V,n) = \max_{\mathrm{P}_X} D\big(W\|V \mid \mathrm{P}_X\big) = \max_x D\big(W_x\|V_x\big),$$

where W_x and V_x, respectively, denote the xth row of W and V.

Remarkably, the exponent above is achieved without any feedback, *i.e.*, while feedback is available, it does not help to improve the asymptotic exponent of $\beta_\epsilon(W,V,n)$.

IV. Secret key agreement

In this section, we review two party secret key (SK) agreement where parties observing random variables X and Y communicate interactively over a public channel to agree on a SK that is concealed from an eavesdropper with access to the communication and a side-information Z.

Formally, the parties communicate using an interactive communication $\mathbf{F} = F_1, ..., F_r$ where $F_1 = F_1(X), F_2 = F_2(Y, F_1), F_3 = F_3(X, F^2)$, $F_4 = F_4(Y, F^3)$ and so on. A random variable $K = K(X, \mathbf{F})$ constitutes an (ϵ, δ)-SK if there exists $\hat{K} = \hat{K}(Y, \mathbf{F})$ such that

$$\mathrm{P}\left(K \neq \hat{K}\right) \leq \epsilon,$$

and

$$\|\mathrm{P}_{KZ\mathbf{F}} - \mathrm{P}_{\mathtt{unif}} \times \mathrm{P}_{Z\mathbf{F}}\|_1 \leq \delta.$$

The following upper bound on the number of values k taken by an (ϵ, δ)-SK K was shown in [17], [18]:

$$\log k \leq -\log \beta_{\epsilon+\delta+\eta}(\mathrm{P}_{XYZ}, \mathrm{Q}_{XYZ}) + 2\log\frac{1}{\eta},$$

for all $0 < \eta < 1 - \epsilon - \delta$, and all $\mathrm{Q}_{XYZ} = \mathrm{Q}_{X|Z}\mathrm{Q}_{Y|Z}\mathrm{Q}_Z$. Underlying the proof of this bound is an intermediate reduction argument in [17, Lemma 1] that relates SK agreement to hypothesis testing. We recall this result below.

Theorem 5 ([17], [18])**.** *For $0 \leq \epsilon, \delta, \epsilon + \delta < 1$, let random variables $K, \hat{K}$, and Z be such that $\mathrm{P}\left(K \neq \hat{K}\right) \leq \epsilon$ and*

$$\|\mathrm{P}_{KZ} - \mathrm{P}_{\mathtt{unif}} \times \mathrm{P}_Z\|_1 \leq \delta,$$

where $\mathrm{P}_{\mathtt{unif}}$ denotes a uniform distribution on k values. Then, for every $0 < \eta < 1 - \epsilon - \delta$ and every $\mathrm{Q}_{K\hat{K}Z} = \mathrm{Q}_{K|Z}\mathrm{Q}_{\hat{K}|Z}\mathrm{Q}_Z$,

$$\log k \leq -\log \beta_{\epsilon+\delta+\eta}(\mathrm{P}_{K\hat{K}Z}, \mathrm{Q}_{K\hat{K}Z}) + 2\log\frac{1}{\eta}.$$

V. Proof of main result

We present a converse result that applies for every fixed n and is asymptotically tight, giving the strong converse result of Theorem 1.

Theorem 6. *For $0 \leq \epsilon, \delta, \epsilon + \delta < 1$, given an (N, n, ϵ, δ)-wiretap code, we have*

$$\log N \leq -\log \beta_{\epsilon+\delta+\eta}(W, V, n) + 2\log\frac{1}{\eta},$$

for all $0 < \eta < 1 - \epsilon - \delta$ and all channels $V : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ such that $V(y, z|x) = V_2(z|x)V_1(y|z)$.

Proof of Theorem 1. Theorem 1 follows form Theorems 6 and 4 upon noting that for $W(y, z|x) = W_2(z|x)W_1(y|z, x)$

$$\begin{aligned}
&\min_V \max_{\mathrm{P}_X} D\big(W\|V \mid \mathrm{P}_X\big) \\
&= \min_{V_1} \max_{\mathrm{P}_X} D\big(W_1\|V_1 \mid \mathrm{P}_X W_2\big) \\
&= \max_{\mathrm{P}_X} \min_{V_1} D\big(W_1\|V_1 \mid \mathrm{P}_X W_2\big) \\
&= \max_{\mathrm{P}_X} D\big(\mathrm{P}_{Y|ZX}\|\mathrm{P}_{Y|Z} \mid \mathrm{P}_{ZX}\big) \\
&= \max_{\mathrm{P}_X} I\left(X \wedge Y \mid Z\right),
\end{aligned}$$

where P_{XYZ} is given by $\mathrm{P}_X W$. □

We need the following result to prove Theorem 6.

Lemma 7. *For a wiretap channel $V : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ such that $V(y, z|x) = V_2(z|x)V_1(y|z)$, a random message M, and a wiretap code, let $\hat{M} = d(Y^n)$ and $\mathbf{F}$ be the corresponding feedback. Then, the induced distribution $\mathrm{Q}_{M\hat{M}Z^n\mathbf{F}}$ satisfies factorization condition*

$$\mathrm{Q}_{M\hat{M}|Z^n\mathbf{F}} = \mathrm{Q}_{M|Z^n\mathbf{F}} \times \mathrm{Q}_{\hat{M}|Z^n\mathbf{F}}.$$

Proof of Lemma 7. Denote by U_x and U_y, respectively, the local randomness at the transmitter and the receiver, and by F^t the feedback $(F_0, ..., F^t)$. Thus, the encoder mapping e_t is a (deterministic) function of (M, U_x, F^{t-1}) and the feedback mapping f_t is a (deterministic) function of (Y^t, U_y). The proof entails a repeated application of the fact that conditionally independent random variables remain so when conditioned additionally on an interactive communication (cf. [16]) and is completed by induction. Specifically, note first that $\mathrm{Q}_{MU_xU_y|F_0} = \mathrm{Q}_{MU_x|F_0}\mathrm{Q}_{U_y|F_0}$ since (M, U_x) and U_y are independent and F_0 is an interactive communication. Under the induction hypothesis

$$\begin{aligned}
&\mathrm{Q}_{MU_xX^{t-1}U_yY^{t-1}|Z^{t-1}F^{t-1}} \\
&\quad = \mathrm{Q}_{MU_xX^{t-1}|Z^{t-1}F^{t-1}}\mathrm{Q}_{U_yY^{t-1}|Z^{t-1}F^{t-1}},
\end{aligned}$$

we get

$$\begin{aligned}
&I\left(M, U_x, X^t \wedge U_y, Y^t \mid Z^t, F^{t-1}\right) \\
&= I\left(M, U_x, X^t \wedge U_y, Y^{t-1} \mid Z^t, F^{t-1}\right) \\
&\leq I\left(M, U_x, X^t \wedge U_y, Y^{t-1} \mid Z^{t-1}, F^{t-1}\right) \\
&= I\left(M, U_x, X^{t-1} \wedge U_y, Y^{t-1} \mid Z^{t-1}, F^{t-1}\right) \\
&= 0,
\end{aligned}$$

where the first equality and inequality follow since Y_t and Z_t, respectively, are outputs of V_1 for input Z_t and V_2 for input X_t, and the second equality holds since $X_t = e_t(M, U_x, F^{t-1})$, which completes the proof. □

Proof of Theorem 6. Given an (N, n, ϵ, δ) wiretap code, a message $M \sim \mathtt{unif}\{1, ..., N\}$ and its decoded value $\hat{M} = d(Y^n)$ satisfy the conditions for Theorem 5 with $K = M, \hat{K} = \hat{M}$, and $Z = (Z^n, \mathbf{F})$. Letting $\mathrm{Q}_{M\hat{M}Z^n\mathbf{F}}$ be the distribution on $(M, \hat{M}, Z^n, \mathbf{F})$ when the underlying channel is V, by Lemma 7 and Theorem 5 we get

$$\log N \leq -\log \beta_{\epsilon+\delta+\eta}(\mathrm{P}_{M\hat{M}Z^n\mathbf{F}}, \mathrm{Q}_{M\hat{M}Z^n\mathbf{F}}) + 2\log \frac{1}{\eta}.$$

Note that a test for the simple binary hypothesis testing problem for $\mathrm{P}_{M\hat{M}Z^n\mathbf{F}}$ and $\mathrm{Q}_{M\hat{M}Z^n\mathbf{F}}$ along with the wiretap code constitutes an active hypothesis test for W and V. Therefore,

$$\begin{aligned} &-\log \beta_{\epsilon+\delta+\eta}(\mathrm{P}_{M\hat{M}Z^n\mathbf{F}}, \mathrm{Q}_{M\hat{M}Z^n\mathbf{F}}) \\ &\quad \leq -\log \beta_{\epsilon+\delta+\eta}(W, V, n), \end{aligned}$$

which completes the proof. □

Acknowledgements

MH is partially supported by a MEXT Grant-in-Aid for Scientific Research (A) No. 23246071. MH is also partially supported by the National Institute of Information and Communication Technology (NICT), Japan. The Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part i: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[2] I. Csiszár, "Almost independence and secrecy capacity," *Prob. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.

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

[4] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, April 2006.

[5] ——, *Quantum Information: An Introduction*. Springer, 2006.

[6] ——, "Discrimination of two channels by adaptive methods and its application to quantum system," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3807–3820, Aug 2009.

[7] S. Kullback, *Information Theory and Statistics*. Dover Publications, 1968.

[8] S. Leung-Yan-Cheong, "Multi-user and wiretap channels including feedback," *Ph. D. Dissertation, Stanford University*, 1976.

[9] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[10] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[11] C. Morgan and A. Winter, ""pretty strong" converse for the quantum capacity of degradable channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 317–333, Jan 2014.

[12] H. Nagaoka, "Strong converse theorems in quantum information theory," in *ERATO Workshop on Quantum Information Science 2001,Univ. Tokyo, Tokyo, Japan, September 68*, 2001, p. 33.

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

[14] Y. Polyanskiy and S. Verdú, "Arimoto channel coding converse and Rényi divergence," *Proc. Conference on Communication, Control, and Computing (Allerton)*, pp. 1327–1333, 2010.

[15] V. Y. F. Tan and M. R. Bloch, "Information spectrum approach to strong converse theorems for degraded wiretap channels," *arXiv:1406.6758*, 2014.

[16] H. Tyagi and P. Narayan, "How many queries will resolve common randomness?" *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5363–5378, September 2013.

[17] H. Tyagi and S. Watanabe, "A bound for multiparty secret key agreement and implications for a problem of secure computing," in *Proc. EUROCRYPT*, 2014, pp. 369–386.

[18] ——, "Converses for secret key agreement and secure computing," *CoRR*, vol. abs/1404.5715, 2014.

[19] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.