Inner Bound for the Capacity Region of Noisy Channels with an Authentication Requirement

Jake Perazzone
Lehigh University
Bethlehem, PA 18015
jbp215@lehigh.edu

Eric Graves and Paul Yu
US Army Research Lab
Adelphi, MD 20783
ericsgraves@gmail.com, paul.l.yu.civ@mail.mil

Rick Blum
Lehigh University
Bethlehem, PA 18015
rb0f@lehigh.edu

***Abstract*—The rate regions of many variations of the standard and wire-tap channels have been thoroughly explored. Secrecy capacity characterizes the loss of rate required to ensure that the adversary gains no information about the transmissions. Authentication does not have a standard metric, despite being an important counterpart to secrecy. While some results have taken an information-theoretic approach to the problem of authentication coding, the full rate region and accompanying trade-offs have yet to be characterized. In this paper, we provide an inner bound of achievable rates with an average authentication and reliability constraint. The bound is established by combining and analyzing two existing authentication schemes for both noisy and noiseless channels. We find that our coding scheme improves upon existing schemes.**

I. Introduction

Authentication, or the ability to verify the identity of the sender of received transmissions, is crucial in secure communications. It is especially important in the wireless channel where malicious parties have easy access to all nodes and can attempt to intercept messages and impersonate legitimate senders. While cryptographic authentication methods are very practical, they are limited to computational complexity as the basis for security. The first information theoretic analysis of authentication was done by Simmons [1] for the noiseless channel in which it was shown that an opponent's attack success probability is lower bounded by $2^{-n\kappa/2}$ when the legitimate parties share a key of length $n\kappa$.

Similar to coding for secrecy in the wire-tap channel, an authentication constraint can be added to a channel code. In [2], Maurer likened authentication to a binary hypothesis test for whether a received message is authentic versus inauthentic. Naturally then, an authentication code would have a decoder that groups certain observations as authentic and others as inauthentic in addition to mapping to possible codewords. A larger authentic set would allow for an increase in rate since fewer observations would be thrown out as inauthentic, but would allow an adversary to more easily send messages that would be falsely authenticated. It is because of this that the additional constraint on the code should lead to a trade-off between rate and authentication capabilities in our inner bound.

This material is based upon work partially supported by the U. S. Army Research Laboratory and the U. S. Army Research Office under grant numbers W911NF-17-1-0331 and W911NF-17-2-0013 and by the National Science Foundation under grants ECCS-1744129 and CNS-1702555.

In [3], Lai et. al. presented a code for noisy channels with authentication capabilities and concluded that if the main channel is not less noisy than the adversary, it is possible to limit the attack success probability to $2^{-n\kappa}$ with a shared key K of length $n\kappa$. Although it was shown that the communication rate is unaffected if $n\kappa$ is small, their analysis is only concerned with cases where $n\kappa$ is a constant independent of n. Gungor and Koksal [4] explored a more general problem and presented an inner bound on the achievable rate with error and erasure exponents for impersonation and substitution attacks both with and without a shared key. We consider the model of [3], while not requiring a constant $n\kappa$ and determine an inner bound that improves upon Gungor and Koksal's coding scheme. Of interest is that the coding scheme can be decomposed into two separate coding schemes, one for source authentication and one for channel authentication. A direct proof is given for the region while the converse is left for future work. If the converse were true, it would prove that authentication under the operational requirements is a limited resource, and that this resource and the message rate must linearly share the channel's capacity.

Our contributions are as follows. First, for all DM-ASC$(t, q, 1)$, a substitution channel, defined in Section II-B, we give an inner bound on the trade-off between the rate r, the key rate κ, and the average type I error exponent α, when the average probability of message error, ϵ, must go to zero with block length n going to infinity. The average type I error exponent is a measure of authentication ability and is defined in Section II-C. It should be noted that this measure of authentication subsumes both the "impostor" and "substitution" attack. Our inner bound is characterized in terms of (in principal) computable information theoretic measures in the form of an inner bound. The derived region subsumes the results of Lai et. al. [3] in which only an asymptotically vanishing key rate is considered. The inner bound is also a strict improvement over the bounds found in Gungor and Koksal [4]. Our scheme benefits from higher communication rates and less key leakage.

Due to space limitations the proofs can be found in [5].

978-1-5386-4780-6/18/$31.00©2018 IEEE

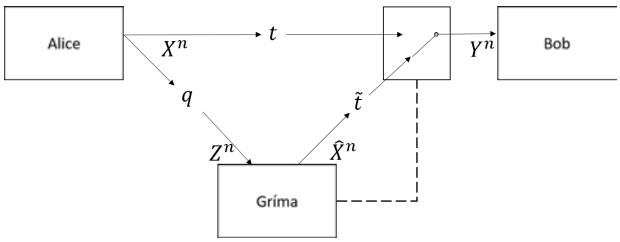

Fig. 1: Channel Model

II. Notation, Model, and Metrics

A. Notation

Random variables and their realizations will be denoted by uppercase and lowercase letters, respectively. The support set of a random variable and other sets are denoted by a calligraphic font. An n-length sequence of random variables, realizations, or sets will be denoted by superscript n. So, X^n is a n-length sequence of random variables which may take on values $x^n \in \mathcal{X}^n$. The probability $X = x$ is denoted $\Pr(X = x)$, or $p_X(x)$, and even $p(x)$ when clear. The probability of a set is written as $p_X(\mathcal{A}) = \sum_{x\in\mathcal{A}} p(x)$, assuming $\mathcal{A} \subseteq \mathcal{X}$ where the set will often be omitted from the summation notation when it is clear, i.e., $\sum_x$. The set of all probability distributions on a certain set, say $\mathcal{X}$, is denoted by $\mathcal{P}(\mathcal{X})$. Similarly, the set of probability distributions of $\mathcal{Y}$ conditioned on $\mathcal{X}$ is denoted as $\mathcal{P}(\mathcal{Y}|\mathcal{X})$. The set $\mathcal{P}(\mathcal{Y} \gg \mathcal{X})$ represents a special subset of $\mathcal{P}(\mathcal{Y}|\mathcal{X})$, where if $v \in \mathcal{P}(\mathcal{Y} \gg \mathcal{X})$ for any $y \in \mathcal{Y}$, there exists at most one $x \in \mathcal{X}$ such that $v(y|x) > 0$. Note, for random variables X, Y, Z, if $p_{Y|X} \in \mathcal{P}(\mathcal{Y} \gg \mathcal{X})$, then $X,\ Y,\ Z$ form a Markov chain, $X \multimap Y \multimap Z$. A superscript of $\otimes n$ will denote the n-fold product distribution of v.

The use of O will refer to the Bachmann-Landau notation. When there is a range of possible values for O, we will use $\doteq$ to denote it. Throughout the paper, the order will only be dependent on continuous functions of the cardinalities of the support sets.

B. Model

Our authentication model consists of three parties. Alice, a legitimate transmitter, wishes to authenticate her communications with Bob, a legitimate receiver, over a discrete memoryless channel in the presence of Gríma, a malicious adversary. Gríma has the ability to intercept Alice's message and send his own to Bob via a noiseless channel. His goal is to have Bob accept his messages as if they were from Alice. To aid in authentication, Alice and Bob share a secret key K which is distributed uniformly over $\mathcal{K} := \{1, \ldots, 2^{n\kappa}\}$.

When Alice wishes to communicate, she jointly encodes a message M, distributed uniformly over $\mathcal{M} := \{1, \ldots, 2^{nr}\}$, and the key K, as codeword X^n. The distribution of X^n is defined by the encoder $f \in \mathcal{P}(\mathcal{X}^n|\mathcal{M}, \mathcal{K})$, where $\mathcal{P}(\mathcal{X}^n|\mathcal{M}, \mathcal{K})$ is the set of all probability distributions over $\mathcal{X}^n$ conditioned on $\mathcal{M} \times \mathcal{K}$. Alice then transmits X^n to both Bob and Gríma. The three parties are connected via a *discrete memoryless-adversarial substitution channel* (DM-ASC) which consists of three discrete memoryless channels, $(t, q, \tilde{t})$, and a Gríma-controlled switch. The triple represents the channels from Alice to Bob, Alice to Gríma, and Gríma to Bob, respectively, while the switch controls Bob's observations.

Note that for simplicity, we use the triple $(t, q, \tilde{t})$ instead of the formal septuple $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \tilde{\mathcal{X}}, t, q, \tilde{t})$, assuming that these values specify $\mathcal{X},\ \mathcal{Y},\ \mathcal{Z},\ \tilde{\mathcal{X}}$ by their non-zero indices. Furthermore, we will assume for the remainder that $\mathcal{X},\ \mathcal{Y},\ \mathcal{Z},\ \tilde{\mathcal{X}}$ are all discrete and finite. The channel is depicted in Figure 1.

When the switch is open, Bob will receive Alice's transmission over t. In other words, $Y^n|X^n$ will be distributed according to $t^{\otimes n}(y^n|x^n) := \prod_{i=1}^n t(y_i|x_i)$ where $t \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$. When the switch is closed, Gríma first obtains $Z^n|X^n$, then determines $\hat{X}^n$ and transmits to Bob. We only consider $(t, q, 1)$ in which the channel from Gríma to Bob is noiseless, i.e. $\tilde{\mathcal{X}} = \mathcal{Y}$, as in [3], [4]. Thus, $Y^n|X^n$ will be distributed according to

$$\sum_{z^n} \psi(y^n|z^n) q^{\otimes n}(z^n|x^n),$$

where $q \in \mathcal{P}(\mathcal{Z}|\mathcal{X})$, and $\psi \in \mathcal{P}(\mathcal{Y}^n|\mathcal{Z}^n)$. Gríma is free to choose any attack strategy, ψ, including ones modeled after the standard impersonation and substitution attacks. Regardless of the switch's position, Bob receives Y^n and either makes an estimate of the message, M^*, or declares an intrusion, !, which is determined by a decoder $\varphi \in \mathcal{P}(\mathcal{M} \cup \{!\}\,|\mathcal{Y}^n, \mathcal{K})$.

C. Performance Metrics

Before presenting the performance metrics, we define an authentication code.

Definition 1. *A* code *is any pair* (f, φ)*, where* $f \in \mathcal{P}(\mathcal{X}^n|\mathcal{M}, \mathcal{K})$ *and* $\varphi \in \mathcal{P}(\mathcal{M} \cup \{!\}\,|\mathcal{Y}^n, \mathcal{K})$*. The* rate *of* (f, φ) *is* $n^{-1} \log_2 |\mathcal{M}|$*, the* block-length *of* (f, φ) *is* n*, and the* key requirement *of* (f, φ) *is* $n^{-1} \log_2 |\mathcal{K}|$.

The performance of the code is measured in two ways, reliability and type I error. Reliability is measured by the average probability of error over all keys and messages at Bob, that is

$$\varepsilon_{f,\varphi} := |\mathcal{K}|^{-1} |\mathcal{M}|^{-1} \sum_{m,k} \varepsilon_{f,\varphi}(m, k) < \epsilon, \tag{1}$$

where $\epsilon \in (0, 1)$ is a chosen constraint and

$$\varepsilon_{f,\varphi}(m, k) := 1 - \sum_{x^n, y^n} \varphi(m|y^n, k) t^{\otimes n}(y^n|x^n) f(x^n|m, k). \tag{2}$$

Type I error refers to the fact that authenticating is equivalent to a binary hypothesis test where the null hypothesis is an intrusion and the alternate hypothesis is authenticity. Therefore, a good code limits the average type I error by

$$\omega_{f,\varphi} := \max_{\psi \in \mathcal{P}(\mathcal{Y}^n|\mathcal{Z}^n)} E_{Z^n,M,K} \left[\omega_{f,\varphi}(\psi, z^n, m, k)\right] \leq 2^{-na}, \tag{3}$$

where

$$\omega_{f,\varphi}(\psi, z^n, m, k) := \sum_{y^n} \psi(y^n|z^n)\varphi(\mathcal{M} - \{m\}\,|y^n, k). \quad (4)$$

Definition 2. *A code (f, φ) is called an* $(r, \alpha, \kappa, \epsilon, n)$-average authentication *(AA) code for DM-ASC$(t, q, 1)$ if the block-length is n, the rate at least r, the key requirement at most κ, it is reliable in that $\varepsilon_{f,\varphi} < \epsilon$ and it satisfies the average authenticity requirement:*

$$\omega_{f,\varphi} < 2^{-n\alpha}. \quad (5)$$

Our study aims to determine what types of codes are possible in the following sense.

Definition 3. *A triple (a, b, c) is said to be* achievable *for the DM-ASC $(t, q, 1)$ if there exist a sequence of $\{(r_i, \alpha_i, \kappa_i, \epsilon_i, i)\}_{i=1}^{\infty}$-AA codes (f_i, φ_i) such that*

$$\lim_{i\to\infty} |(r_i, \alpha_i, \kappa_i, \epsilon_i, i) - (a, b, c, 0, i)|_2 \to 0.$$

The average authentication region *(AAR) is then*

$$\mathcal{C}_A(t, q, 1) := \{(a, b, c) : (a, b, c) \text{ is achievable for DM-ASC}(t, q, 1)\}. \quad (6)$$

III. Background

Before presenting the inner bound for the average authentication region, we review existing schemes. First, we review Lai's [3] strategy and frame it in terms of information metrics for ease of comparison. Next, we examine Simmons' [1] strategy for the noiseless channel and transform Gungor and Koksal's [4] inner bound into our terms.

A. Lai's Strategy

In [3], Lai et. al. propose essentially using a code designed for a wire-tapper channel, and sending the key as part of the message. The specific code they proposed is optimal for their limited scenario (key requirement $\to 0$), but in light of the forthcoming discussion, it is not optimal in ours.

Recognizing that the essence of the construction is to transmit two independent messages (the message itself and the key), with one subject to a secrecy constraint, the most logical coding scheme is a special class of codes for the *discrete memoryless broadcast channel with confidential communications (t,q,)* (DM-BCC(t, q)). While we are the first to notice and use this specific construction for the purpose of authentication, we refer to this as Lai's strategy. Before continuing we discuss the DM-BCC.

The achievable rate region of the DM-BCC was first derived by Csiszár and Körner in [6] and later refined in [7, Chapter 17]. In said model, there exist three messages that Alice wishes to send, a common message, $m_0 \in \mathcal{M}_0 := \{1, \ldots, 2^{nr_0}\}$, that is to be decoded by both Bob and Gríma, a private message, $m_s \in \mathcal{M}_s := \{1, \ldots, 2^{nr_s}\}$, that is to be decoded by Bob and kept secret from Gríma, and finally a message, $m_1 \in \mathcal{M}_1 := \{1, \ldots, 2^{nr_1}\}$, to be decoded by only Bob, but without a secrecy constraint. Secrecy in this context is indicated by

$$\mathsf{I}(p_{Z^n|M_s}, p_{M_s}) \le \epsilon_n,$$

where $\epsilon_n \to 0$ as $n \to \infty$. Meaning that the information gained about M_s from Gríma's observations asymptotically vanishes. All messages have reliability constraints for their intended recipients. The three messages are jointly coded as X^n and sent through the channel where Bob observes $Y^n|X^n$, which is distributed as $t^{\otimes n}(y^n|x^n)$ while Gríma observes, $Z^n|X^n$, distributed as $q^{\otimes n}(z^n|x^n)$.

The triple (r_0, r_s, r_1) is achievable for the DM-BCC(t, q) if

$$\begin{aligned} r_0 + r_s + r_1 &\le \mathsf{I}(t\rho, \sigma|\tau) + \min\left(\mathsf{I}(t\rho\sigma, \tau), \mathsf{I}(q\rho\sigma, \tau)\right) \\ r_s &\le \mathsf{I}(t\rho, \sigma|\tau) - \mathsf{I}(q\rho, \sigma|\tau) \\ r_0 &\le \min\left(\mathsf{I}(t\rho\sigma, \tau), \mathsf{I}(q\rho\sigma, \tau)\right), \end{aligned}$$

for some $\rho \in \mathcal{P}(\mathcal{X}|\mathcal{U})$, $\sigma \in \mathcal{P}(\mathcal{U} \gg \mathcal{W})$ and $\tau \in \mathcal{P}(\mathcal{W})$, and sets $\mathcal{U}$ and $\mathcal{W}$ such that $|\mathcal{U}| = (|\mathcal{X}| + 1)(|\mathcal{X}| + 3)$ and $|\mathcal{W}| = |\mathcal{X}|+3$. It can be seen here that secrecy is only possible when the channel from Alice to Gríma's is not less noisy than the channel from Alice to Bob.

Lai's strategy attains authentication capabilities by implementing the coding scheme for the DM-BCC(t, q) in which Alice's message is sent as M_1 and the key is sent as M_s while $M_0 = \emptyset$. If message rates are chosen within the achievable region above, Bob will decode the message reliably, satisfying the reliability constraint of an authentication code. Additionally, since the key is also reliably decoded and each y^n corresponds to only one k, he can declare authenticity when $\hat{k} = k$. The security constraint on $M_s = K$ reduces the information about the key that is leaked to Gríma; the analysis of our work will determine the degree of effectiveness.

As stated before, non-zero rates are only possible when t is less noisy than q, i.e. when $\mathsf{I}(t\rho, \sigma|\tau) > \mathsf{I}(q\rho, \sigma|\tau)$. To solve this issue, we return to Simmons' strategy for the noiseless case.

B. Simmon's Strategy

Simmons' authentication scheme [1] for noiseless channels breaks down the problem into protecting against two different attacks, i.e., an impostor formerly referred to as "impersonation" attack and a substitution attack. The attacks differ in that in the former, Gríma attacks without first observing one of Alice's transmissions, while in the latter, Gríma does. In the strategy, the code is created by independently and randomly choosing $|\mathcal{K}| = 2^{n\kappa}$ not necessarily unique subsets of $\mathcal{M}$, each denoted as $\mathcal{M}(k) \subset \mathcal{M}$. The size of each subset is $|\mathcal{M}(k)| = 2^{-n\kappa/2}|\mathcal{M}|$ where each element $m \in \mathcal{M}(k)$ corresponds to a single message $\tilde{m} \in \tilde{\mathcal{M}} := \left\{1, \ldots, |\mathcal{M}|\, 2^{-n\kappa/2}\right\}$. Then, to communicate $\tilde{m}$, Alice sends the associated m from the subset indexed by their shared key, k. Bob authenticates a message when the observed m is an element of the correct $\mathcal{M}(k)$. The rate of communication in this scheme is $n^{-1}\log_2\left|\tilde{\mathcal{M}}\right| = n^{-1}\log_2|\mathcal{M}| - \kappa/2$.

Since an observed m can be contained in multiple $\mathcal{M}(k)$, Gríma will be unable to immediately infer which key was used for authentication. In order to launch a successful substitution attack, Gríma must choose an $m' \neq m$ that is contained in the same $\mathcal{M}(k)$, however on average there is only $|\mathcal{K}|\left(|\mathcal{M}(k)|\,/\,|\mathcal{M}|\right)^2 = 1$ subset that contains both m and m'. Therefore, he must essentially guess the correct key to fool Bob which happens with probability $2^{-n\kappa/2}$ since there are, on average, $|\mathcal{K}|\left(|\mathcal{M}(k)|\,/\,|\mathcal{M}|\right) = 2^{n\kappa/2}$ subsets that contain m. In terms of an achievable rate region, this scheme can achieve the triple $(n^{-1}\log_2|\mathcal{M}| - \kappa/2, \kappa/2, \kappa)$. Simmons' strategy, together with Lai's strategy, forms the basis for our code.

C. Gungor and Koksal's Bounds

Inner bounds for the average achievability region of a DM-ASC$(t, q, \tilde{t})$, have been established by Gungor and Koksal [4]. Specifically, their scheme splits Alice and Bob's shared key into two smaller keys, one for authentication (á la Lai's strategy) and one for secrecy. These two keys are then used as the dimensions in a two dimensional dimensional binning process, where the codeword corresponding to the triple of messages and keys is chosen independently. The independent choice over the secrecy key, though, leaks extraneous information since there is no need to differentiate between secrecy keys at the legitimate receiver.

In any case, the set of all achievable (r, α, κ) derived from their scheme is a subset of

$$(r, \alpha, \kappa) \in \bigcup_{\tilde{\kappa}\in\mathbb{R}_+} \mathcal{R}_G(\tilde{\kappa}) \tag{7}$$

where $\mathcal{R}_G(\tilde{\kappa})$

$$:= \left\{ r, \alpha, \kappa : \begin{array}{rl} r + \kappa & \leq \mathsf{I}(t\rho, \tau) + \tilde{\kappa} \\ \alpha - \kappa & \leq -\tilde{\kappa} \\ \alpha & \leq \min_{\nu\in\mathcal{P}(\mathcal{Z}|\mathcal{U})} \mathsf{L}_G(\nu, q\rho, t\rho, \tilde{\kappa}, \tau) \end{array} \right\} \tag{8}$$

and $\mathsf{L}_G(\nu, q\rho, t\rho, \tilde{\kappa}, \tau) = \mathsf{D}(\nu||q\rho|\tau) + |\tilde{\kappa} + \mathsf{I}(t\rho, \tau) - \mathsf{I}(\nu, \tau)|^+$. A proof of this can be found in [5, Appendix A].

IV. Authentication Capacity Region

We now present our main theorems and the inner bound of the average authentication region. First, we present the minor contribution of characterizing the inner bound of the authentication region using Lai's strategy.

Theorem 4.

$$\left\{ (r, \alpha, \kappa) : \begin{array}{rl} r + \alpha & \leq \mathsf{I}(t\rho, \sigma\tau) \\ \alpha & \leq \min_{\nu\in\mathcal{P}(\mathcal{Z}|\mathcal{U})} \mathsf{L}(\nu; t\rho, q\rho, \sigma, \tau) \\ \alpha & \leq \mathsf{I}(t\rho, \sigma|\tau) \\ \alpha - \kappa & \leq 0 \end{array} \right\} \subset \mathcal{C}_A(t, q, 1), \tag{9}$$

where $\mathsf{L}(\nu; t\rho, q\rho, \sigma, \tau) := \mathsf{D}(\nu||q\rho|\sigma\tau) + |\mathsf{I}(t\rho, \sigma|\tau) - \mathsf{I}(\nu, \sigma|\tau) + |\mathsf{I}(t\rho\sigma, \tau) - \mathsf{I}(\nu\sigma, \tau)|^+|^+$, *for all* $\rho \in \mathcal{P}(\mathcal{X}|\mathcal{U})$, $\sigma \in \mathcal{P}(\mathcal{U} \gg \mathcal{W})$, *and* $\tau \in \mathcal{P}(\mathcal{W})$ *where* $|\mathcal{U}|$ *and* $|\mathcal{W}|$ *are finite.*

Proof: See [5, Appendix C], along with the supporting code construction, message error analysis and type I error analysis in [5, Appendix F]. ∎

The type I error capabilities are limited by the capacity of the wire-tap channel and if the secrecy capacity is 0, then no authentication is possible. We now extend Simmons' strategy and although it will only be applied to the triples from Theorem 4, the associated code construction makes no such assumption on the genesis of the original code.

Theorem 5. *If* $(r, \alpha, \kappa) \in \mathcal{C}_A$ *then* $(r-\beta, \alpha+\beta, \kappa+2\beta) \in \mathcal{C}_A$, *for all non-negative* $\beta < r$.

Proof: See [5, Appendix D]. ∎

Now to obtain our inner bound, we combine Theorems 4 and 5.

Theorem 6.

$$\left\{ (r, \alpha, \kappa) : \begin{array}{rl} r + \alpha & \leq \mathsf{I}(t\rho, \sigma\tau) \\ 2\alpha - \kappa & \leq \min_{\nu\in\mathcal{P}(\mathcal{Z}|\mathcal{U})} \mathsf{L}(\nu; t\rho, q\rho, \sigma, \tau) \\ 2\alpha - \kappa & \leq \mathsf{I}(t\rho, \sigma|\tau) \\ \alpha - \kappa & \leq 0 \end{array} \right\} \subset \mathcal{C}_A(t, q, 1), \tag{10}$$

where $\mathsf{L}(\nu; t\rho, q\rho, \sigma, \tau) := \mathsf{D}(\nu||q\rho|\sigma\tau) + |\mathsf{I}(t\rho, \sigma|\tau) - \mathsf{I}(\nu, \sigma|\tau) + |\mathsf{I}(t\rho\sigma, \tau) - \mathsf{I}(\nu\sigma, \tau)|^+|^+$, *for all distributions* $\rho \in \mathcal{P}(\mathcal{X}|\mathcal{U})$, $\sigma \in \mathcal{P}(\mathcal{U} \gg \mathcal{W})$, *and* $\tau \in \mathcal{P}(\mathcal{W})$ *and* $|\mathcal{U}|$ *and* $|\mathcal{W}|$ *are finite.*

Proof: The proof can be found in [5, Appendix E]. ∎

This inner bound exhibits a trade-offs between rate, type I error, and key requirement in information theoretic terms. It is apparent from the first condition that this scheme requires communication and authentication share the main channel's capacity. As long as $\min_{\nu\in\mathcal{P}(\mathcal{Z}|\mathcal{U})} \mathsf{L}(\nu; t\rho, q\rho, \sigma, \tau)$ is non-zero, an increase in the length of the secret key provides a proportional increase in type I error. Whereas when the condition is zero, an increase in α requires twice the increase in κ as evident in Simmons' scheme.

Our scheme also improves over Gungor and Koksal's inner bound in this respect, since our scheme does not continue to unnecessarily leak information when Gríma's channel is less noisy than Bob's channel. Instead, in such a case, our scheme reverts to that of Simmon's, which is known to be optimal.

V. Examples

To demonstrate that our inner bound outperforms Gungor and Koksal's inner, we provide a few examples and analyses. While it is easy to see that our inner bound (10) is larger than Lai's (9) due to the addition of $2\alpha - \kappa$, we will provide an explicit example to show that (10) also improves upon Gungor's inner bound (8). For clarity, we will examine the case where t and q are binary symmetric channels (BSC) with transition probabilities λ_t and λ_q respectively.

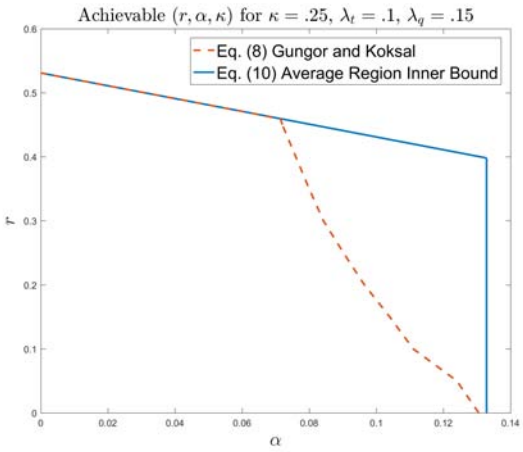

Fig. 2: AAR outperforms Gungor's inner bound when α is large.

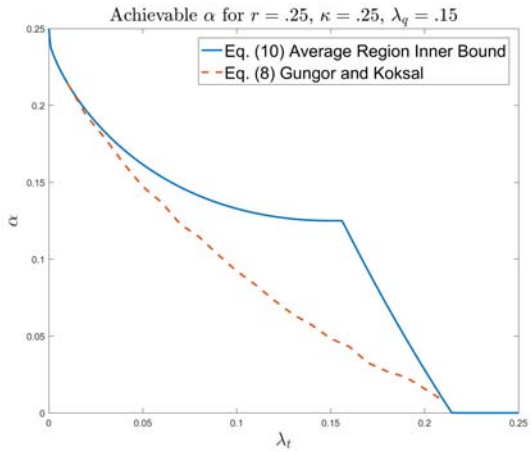

Fig. 3: Given an r and κ pair, AAR achieves a greater range of α for a constant adversarial channel (λ_t is the transition probability of channel t).

In a BSC, (10) simplifies to

$$\begin{aligned} r + \alpha &< \mathsf{I}(t, \sigma\tau) \\ 2\alpha - \kappa &< \min_{\nu \in \mathcal{P}(\mathcal{Z}|\mathcal{X})} \mathsf{L}^*(\nu; t, q, \sigma, \tau) \\ 2\alpha - \kappa &\leq \mathsf{I}(t, \sigma|\tau) \\ \alpha - \kappa &\leq 0, \end{aligned}$$

where σ is now a distribution on X given W and $\mathsf{L}^*(\nu; t, q, \sigma, \tau) = \mathsf{D}(\nu||q|\sigma\tau) + |\mathsf{I}(t, \sigma|\tau) - \mathsf{I}(\nu, \sigma|\tau) + |\mathsf{I}(t\sigma, \tau) - \mathsf{I}(\nu\sigma, \tau)|^+|^+$. Meanwhile, (8) simplifies to

$$\mathcal{R}_G(\tilde{\kappa}) := \left\{ r, \alpha, \kappa : \begin{array}{r} r + \kappa \leq \mathsf{I}(t, \tau) + \tilde{\kappa} \\ \alpha - \kappa \leq -\tilde{\kappa} \\ \alpha \leq \min_{\nu \in \mathcal{P}(\mathcal{Y}|\mathcal{X})} \mathsf{L}_G(\nu, q, t, \tilde{\kappa}, \tau) \end{array} \right\}, \tag{11}$$

where $\mathsf{L}_G(\nu, q, t, \tilde{\kappa}, \tau) = \mathsf{D}(\nu||q|\tau) + |\tilde{\kappa} + \mathsf{I}(t, \tau) - \mathsf{I}(\nu, \tau)|^+$. In the interest of space, we will leave a more complete analysis in [5] and only present numerical examples here.

A. BSC Examples

First, we consider a case when the main channel is less noisy than Gríma's channel, where in specific $\lambda_t = .1$ and $\lambda_q = .15$. The trade off between the rate and the authentication, given a fixed key rate, for both (10) and (8) is plotted in Figure 2. Note the equivalence of the two regions for small α. As α increases, though, (10) becomes strictly larger than (8). While (10) obtains a constant value for $r + \alpha$, which is equal to the capacity of t, approximately .531, (8) struggles due to the inefficiency of their coding scheme. This aligns with intuition, as (10) uses the channel capacity for authenticity until the secrecy capacity is exhausted, and then switches to Simmons' scheme to further the authentication exponent.

Next, in Figure 3 the rate, key requirement, and adversarial channel are held constant while the maximum possible α achievable via (10) and (8) is computed for a range of main channel transition probabilities, λ_t. Both schemes have a dramatic performance decrease when the main channel becomes worse than the adversarial channel. Still (10) is generally larger than (8) for many possible main channels. It should be noted the point where $\alpha = 0$ is exactly the point where the capacity of the channel equals .25, in other words both schemes are using all of the channels capacity simply to provide reliable communications.

REFERENCES

[1] G. J. Simmons, "Authentication theory/coding theory." in *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, 1984, pp. 411–431.

[2] U. Maurer, "Authentication theory and hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1350–1356, July 2000.

[3] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE transactions on information theory*, vol. 55, no. 2, pp. 906–916, 2009.

[4] O. Gungor and C. E. Koksal, "On the basic limits of rf-fingerprint-based authentication," *IEEE transactions on information theory*, vol. 62, no. 8, pp. 4523–4543, 2016.

[5] J. Perazzone, E. Graves, and P. Yu, "Inner bound of the capacity region of noisy channels with an authentication requirement," *arXiv preprint arXiv:1801.03920*, 2018.

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[7] ——, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011. [Online]. Available: http://books.google.com/books?id=2gsLkQlb8JAC