Authentication and Partial Message Correction over Adversarial Multiple-Access Channels

Allison Beemer*, Eric Graves†, Joerg Kliewer*, Oliver Kosut‡, Paul Yu†
*Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07103
†Computer and Information Sciences Division, U.S. Army Research Laboratory, Adelphi, MD 20783
‡School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85287

Abstract—**In this paper, we present results on the authentication capacity region for the two-user arbitrarily-varying multiple-access channel. We first consider a standard definition of authentication, in which the receiver may discard both messages if an adversary is detected. For this setting, we show that an extension of the arbitrarily-varying channel condition *overwritability* characterizes the authentication capacity region. We then define γ-correcting authentication, where we require that at least a γ fraction of the users' messages be correctable, even in the presence of an adversary. We give necessary conditions for the γ-correcting authentication capacity region to have nonempty interior, and show that positive rate pairs are achievable over a particular channel that satisfies these conditions.**

I. Introduction

As everyday devices steadily grow more interconnected, the ability to verify the origin of information is increasingly important. Consequently, we study the problem of keyless *authentication* in the presence of an adversary: the receiver must be able to decode in the absence of adversarial action, and is allowed to either decode or declare adversarial interference when the adversary is active. In this paper, we focus on authentication over the arbitrarily-varying multiple-access channel (AV-MAC), an extension of the arbitrarily-varying channel (AVC) [1]. Specifically, a t-user AV-MAC takes as inputs t legitimate user transmissions and an adversarial *state*, which is assumed to be chosen by an adversary who knows the coding scheme, but cannot see the actual user transmissions. The adversary's goal is to trick the receiver into outputting incorrect messages without detecting its interference.

The AVC is the point-to-point version of this scenario, in which there is a single sender and single receiver. The channel condition *overwritability* was shown in [2] to characterize the authentication capacity over the AVC: if an AVC is overwritable, its authentication capacity is equal to zero, and if not, it has authentication capacity equal to the communication capacity of the underlying non-adversarial channel. Other work on authentication in point-to-point settings, with adversaries of varying capabilities and users who may or may not have access to a shared secret key, includes [3]–[11].

The communication capacity region of a two-user AV-MAC, provided the region has nonempty interior, was established by Jahn in [12]. The complete capacity region characterization was subsequently characterized by Gubner [13] and Ahlswede and Cai [14], who together proved that (non)emptiness of the region's interior is determined by a *symmetrizability* condition that is an extension of symmetrizability as defined for an AVC [15]. However, authentication over the two-user AV-MAC has, to the best of our knowledge, not been studied in the literature.

Of relevance to our current work is [16], in which the authors consider authentication over a two-user byzantine MAC, where one of the users may be adversarial. Specifying a byzantine user reduces to the AVC setting considered by [2], but allowing either to be byzantine necessitates an extension to the overwritability condition. Based on this extension, the authors characterize the authentication capacity region. In the current work, we further extend overwritability in order to consider the two-user AV-MAC, where the adversary exists outside of the legitimate setup as a malicious third actor.

We first consider authentication in a manner akin to the definition of [16]: successful authentication occurs if the receiver (1) recovers both messages correctly, or (2) when appropriate, outputs a declaration of interference for one or both users. For this case, we present an extension to overwritability, and show that overwritable AV-MACs have empty authentication capacity region interiors. Furthermore, non-overwritable channels have authentication capacity region equal to the underlying no-adversary communication capacity region: that is, any the rate pair for which reliable *communication* is achievable when the adversary is not acting is also a rate pair for which *authentication* is achievable, whether or not the adversary is active. For channels over which the adversary is capable of disrupting a single transmission but cannot disrupt both transmissions simultaneously, we may wish to recover one message, even if the other must be discarded. For such scenarios, we define *γ-correcting authentication*, and give results on the γ-correcting authentication capacity region.

The paper is organized as follows. Section II introduces the relevant background and notation. Overwritability is extended to the AV-MAC setting, and is used to characterize the authentication capacity region in Section III. In Section IV, we introduce γ-correcting authentication and give results on the

This research was sponsored by the Combat Capabilities Development Command Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-17-2-0183. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Combat Capabilities Development Command Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes not withstanding any copyright notation here on.

978-1-7281-4760-4/20/$31.00 ©2020 IEEE

γ-correcting authentication capacity region. Section V presents a 0.5-correcting authentication coding scheme for a particular channel. Section VI concludes the paper.

II. Preliminaries

Notation: throughout the paper, $[M] := \{1, \ldots, M\}$, and $\|\cdot\|$ denotes the Hamming weight. A random variable will be denoted using a capital letter, with the corresponding alphabet and alphabet elements written with script and lowercase letters, respectively. For example, X is a random variable with alphabet $\mathcal{X}$ such that for all $x \in \mathcal{X}$, $P_X(x)$ is the probability that $X = x$. Vectors will be denoted with boldface, all logarithms will be base 2, and $H(\cdot)$ will denote the entropy function.

We consider authentication over the AV-MAC with two legitimate users, a single receiver, and an outside adversary. We assume that the adversary has full knowledge of the codebooks of the legitimate parties, but no knowledge of the transmissions at any given time. More formally, let $W_{Y|X_1,X_2,S}$ be a discrete memoryless adversarial channel with the sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{S}$, and $\mathcal{Y}$ as the input, state, and output alphabets. For multiple channel uses, we write $W(\mathbf{y} \mid \mathbf{x}_1, \mathbf{x}_2, \mathbf{s})$ to represent the product channel, where the sequence lengths are understood. See Fig. 1 for a depiction. We define an authentication code for this setting as follows.

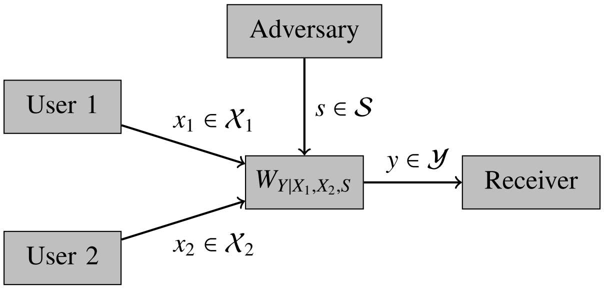

Fig. 1. The two-user AV-MAC.

Definition II.1. An (M_1, M_2, n) *authentication code* for a two-user AV-MAC is given by two encoders f_1 and f_2, and a decoder ϕ:

$$f_1 : [M_1] \to \mathcal{X}_1^n, \quad f_2 : [M_2] \to \mathcal{X}_2^n \tag{1}$$

$$\phi : \mathcal{Y}^n \to ([M_1] \cup \{0\}) \times ([M_2] \cup \{0\}), \tag{2}$$

where an output of "0" in either coordinate indicates adversarial interference.

Notice that this definition may be extended to stochastic encoders, but in this work we will focus on deterministic encoders. In [16], the output of the decoder has been restricted to $([M_1] \times [M_2]) \cup \{(0, 0)\}$. While (2) may be reduced to this type of decoder, allowing for outputs where exactly one coordinate is positive gives the opportunity to decode some information, even if the adversary is active. This will be examined further in Section IV.

Let $\phi^{-1}(A) \subseteq \mathcal{Y}^n$ represent the set of channel outputs which decode to some (i_1, i_2) in the set A under ϕ, and let $\phi^{-1}(A)^c$ be the complement in $\mathcal{Y}^n$ of this set. Let $\mathbf{x}_j(i) := f_j(i)$ denote the length-n encoding of message i by user j. Given transmitted messages i_1 and i_2 and adversarial state $\mathbf{s}$, we define the probability of error for the authentication code (f_1, f_2, ϕ) as:

$$e(i_1, i_2, \mathbf{s}) = \begin{cases} W(\phi^{-1}(\{(i_1, i_2)\})^c \mid \mathbf{x}_1(i_1), \mathbf{x}_2(i_2), \mathbf{s}) & \mathbf{s} = \mathbf{s}_0 \\ W(\phi^{-1}(\{(\hat{i}_1, \hat{i}_2) : \hat{i}_j \in \{0, i_j\}\})^c \mid \mathbf{x}_1(i_1), \mathbf{x}_2(i_2), \mathbf{s}) & \mathbf{s} \neq \mathbf{s}_0, \end{cases} \tag{3}$$

where $\mathbf{s} = \mathbf{s}_0$ denotes that the no-adversary state sequence. We assume that each message pair in $[M_1] \times [M_2]$ is transmitted with equal probability, so that the average probability of error for a given adversarial choice of $\mathbf{s}$ is given by

$$e(\mathbf{s}) = \frac{1}{M_1 M_2} \sum_{(i_1, i_2)} e(i_1, i_2, \mathbf{s}). \tag{4}$$

We then say that a rate pair (R_1, R_2) is *achievable* if there exists a sequence of $(2^{R_1 n}, 2^{R_2 n}, n)$ authentication codes such that $\max_{\mathbf{s}} e(\mathbf{s}) \to 0$ as $n \to \infty$. Notice that $\max_{\mathbf{s}} e(\mathbf{s})$ is the highest average error probability the adversary can hope for, achieved by choosing $\mathbf{s}$ optimally. The *authentication capacity region*, $\mathscr{C}_{\text{auth}}$, is the closure of the set of achievable rate pairs. Let $\mathscr{C}$ denote the capacity region in the no-adversary setting (i.e., $\mathbf{s} = \mathbf{s}_0$).

As mentioned above, an extension of the AVC *symmetrizability* condition fully characterizes when the two-user AV-MAC has empty interior [13], [14]. Recall that an AVC $W_{Y|X,S}$ is *symmetrizable* if there exists a distribution $P_{S|X}$ such that for all x, x', y, $\sum_s P_{S|X}(s|x')W(y|x, s) = \sum_s P_{S|X}(s|x)W(y|x', s)$ [15]. Subsequently, symmetrizability for a two-user AV-MAC is defined as follows.

Definition II.2. [13] A two-user AV-MAC $W_{Y|X_1,X_2,S}$ is $X_1{\times}X_2$-*symmetrizable* if there exists $P := P_{S|X_1,X_2}$ such that for all x_1, x_2, x_1', x_2', y,

$$\sum_s P(s \mid x_1', x_2')W(y|x_1, x_2, s) = \sum_s P(s \mid x_1, x_2)W(y|x_1', x_2', s).$$

The channel is (i) X_1-*symmetrizable* or (ii) X_2-*symmetrizable* if there exists $P := P_{S|X_1}$ or $P_{S|X_2}$, respectively, such that for all x_1, x_2, x_1', x_2', y,

$$\text{(i)} \quad \sum_s P(s \mid x_1')W(y|x_1, x_2, s) = \sum_s P(s \mid x_1)W(y|x_1', x_2, s), \quad \text{or}$$

$$\text{(ii)} \quad \sum_s P(s \mid x_2')W(y|x_1, x_2, s) = \sum_s P(s \mid x_2)W(y|x_1, x_2', s).$$

Example II.3. *Consider the channel with $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{S} = \{0, 1\}$ such that the channel output is the real-valued sum of the input values. We then have $\mathcal{Y} = \{0, 1, 2, 3\}$. Now, $s = 0$ is the no-adversary state, and an output of "3" is immediate indication that an adversary is present. This channel is not $X_1 \times X_2$-symmetrizable. It is, however, both X_1- and X_2-symmetrizable. In other words, the adversary can imitate at most one of the legitimate users at a time.*

In Section III, we will introduce an overwritability condition as an extension of the overwritability condition of [2]. An AVC $W_{Y|X,S}$ is *overwritable* if there exists a distribution $P_{S|X}$ such that for all x, x', y, $\sum_s P_{S|X}(s|x')W(y|x,s) = W(y|x', s_0)$, where s_0 denotes the no-adversary state. This condition is analogous to symmetrizability, but for authentication capacity rather than communication capacity.

III. Authentication over AV-MACs

In this section, we give results on the authentication capacity region for the two-user AV-MAC. Similar to the way in which Definition II.2 is an extension of AVC symmetrizability, we give an extension of overwritability for the two-user AV-MAC.

Definition III.1. A two-user AV-MAC $W_{Y|X_1,X_2,S}$ is $X_1 \times X_2$*-overwritable* if there exists $P_{S|X_1,X_2}$ such that for all x_1, x_2, x_1', x_2', y,

$$\sum_s P_{S|X_1,X_2}(s \mid x_1', x_2')W(y|x_1, x_2, s) = W(y|x_1', x_2', s_0).$$

The channel is (i) X_1*-overwritable* or (ii) X_2*-overwritable* if there exists $P_{S|X_1}$ or $P_{S|X_2}$, respectively, such that for all x_1, x_2, x_1', x_2', y,

$$\text{(i)} \quad \sum_s P_{S|X_1}(s \mid x_1')W(y|x_1, x_2, s) = W(y|x_1', x_2, s_0), \quad \text{or}$$

$$\text{(ii)} \quad \sum_s P_{S|X_2}(s \mid x_2')W(y|x_1, x_2, s) = W(y|x_1, x_2', s_0).$$

Example III.2. *Recall the channel considered in Example II.3; this channel is not overwritable in any sense.*

Example III.3. *Let $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$, $\mathcal{S} = \{s_0, 0, 1\}$, and $\mathcal{Y} = \{0, 1, 2\}$. Let $W_{Y|X_1X_2S}$ be such that $Y = X_1 + X_2$ if $S = s_0$, and $Y = X_1 + S$ otherwise, where "+" denotes real addition. This channel is clearly X_2-overwritable, but is not X_1- nor $X_1 \times X_2$-overwritable.*

As in the point-to-point case, each of the above three overwritability conditions implies the corresponding symmetrizability condition in Definition II.2.

Proposition III.4. *If a channel is $X_1 \times X_2$-overwritable (resp., X_1- or X_2-overwritable), then it is trivially $X_1 \times X_2$-symmetrizable (resp., X_1- or X_2-symmetrizable), in the sense that there exists a distribution $P_{S|X_1,X_2}$ (resp., $P_{S|X_1}$ or $P_{S|X_2}$) giving symmetrizability that is independent of X_1 and X_2.*

Proof. We show that this holds for the $X_1 \times X_2$ case; the other two cases may be shown similarly. Suppose that $W_{Y|X_1,X_2,S}$ is $X_1 \times X_2$-overwritable. Then, there exists $P := P_{S|X_1,X_2}$ such that for all x_1, x_2, x_1', x_2', y,

$$\sum_s P(s \mid x_1', x_2')W(y \mid x_1, x_2, s) = W(y \mid x_1', x_2', s_0).$$

For any choice of $s, \tilde{x}_1, \tilde{x}_2$, define the distribution

$$\tilde{P}_{S|X_1,X_2}(s \mid \tilde{x}_1, \tilde{x}_2) := \frac{1}{|\mathcal{X}_1| \cdot |\mathcal{X}_2|} \sum_{x_1', x_2'} P(s \mid x_1', x_2').$$

Notice that $\tilde{P}_{S|X_1,X_2}$ is independent of X_1 and X_2. Thus, $\tilde{P}_{S|X_1,X_2}$ reduces to a distribution on S; we denote this distribution by $\tilde{P}_S$. For any choice of $x_1, x_2, \tilde{x}_1, \tilde{x}_2, y$,

$$\sum_s \tilde{P}_S(s)W(y \mid x_1, x_2, s) =$$

$$\frac{1}{|\mathcal{X}_1| \cdot |\mathcal{X}_2|} \sum_{x_1',x_2'} \sum_s P(s \mid x_1', x_2')W(y \mid x_1, x_2, s) \quad (5)$$

$$= \frac{1}{|\mathcal{X}_1| \cdot |\mathcal{X}_2|} \sum_{x_1',x_2'} W(y \mid x_1', x_2', s_0) \quad (6)$$

$$= \frac{1}{|\mathcal{X}_1| \cdot |\mathcal{X}_2|} \sum_{x_1',x_2'} \sum_s P(s \mid x_1', x_2')W(y \mid \tilde{x}_1, \tilde{x}_2, s) \quad (7)$$

$$= \sum_s \tilde{P}_S(s)W(y|\tilde{x}_1, \tilde{x}_2, s). \quad (8)$$

Thus, $W_{Y|X_1,X_2,S}$ is trivially $X_1 \times X_2$-symmetrizable. □

However, the converse of Proposition III.4 does not hold, as demonstrated by the following example.

Example III.5. *Consider the channel with $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{S} = \{0, 1\}$ such that the channel output is the modulo 2 sum of the input values. Here, $s = 0$ is the no-adversary state. This channel is not X_1-, X_2-, nor $X_1 \times X_2$-overwritable, but is symmetrizable in every sense.*

We next show that if overwritability in any sense holds, the interior of the authentication capacity region is empty: specifically, at least one of R_1 or R_2 must be zero.

Lemma III.6. *For any two-user AV-MAC, $\mathscr{C}_{auth} \subseteq \mathscr{C}$. If a two-user AV-MAC is X_1-, X_2-, or $X_1 \times X_2$-overwritable, then $\mathscr{C}_{auth}$ has empty interior.*

Proof. Since any coding scheme that achieves authentication must achieve reliable communication in the no-adversary case, any rate pair that is achievable for authentication must also be achievable for communication with no adversary. This proves the first claim.

Next, consider a two-user AV-MAC that is $X_1 \times X_2$-overwritable, and let $P := P_{S|X_1X_2}$ be the guaranteed adversarial distribution. Consider a sequence of (M_1, M_2, n) codes, with $M_1 := 2^{R_1 n}$, $M_2 := 2^{R_2 n}$, $R_1, R_2 \geq 0$. Let $\mathbf{x}_{i_j} := f_j(i_j)$ for $j \in \{1, 2\}$ and $i_j \in [M_j]$, and let $A := \{(j_1, j_2), (j_1, 0), (0, j_2), (0, 0)\}$. Then, $\max_{\mathbf{s}} e(\mathbf{s})$ is bounded below by

$$\max_{\mathbf{s}} e(\mathbf{s}) \geq \sum_{\mathbf{s}} \left(\frac{1}{M_1 M_2} \sum_{(i_1,i_2)} P(\mathbf{s} \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}) \right) e(\mathbf{s}) \quad (9)$$

$$= \sum_{\mathbf{s}} \frac{1}{(M_1 M_2)^2} \sum_{(i_1,i_2),(j_1,j_2)} P(\mathbf{s} \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}) e(j_1, j_2, \mathbf{s}) \quad (10)$$

$$\geq \frac{1}{(M_1 M_2)^2} \sum_{(i_1,i_2),(j_1,j_2),\mathbf{s}} P(\mathbf{s} \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}) W(\phi^{-1}(A)^c \mid \mathbf{x}_{j_1}, \mathbf{x}_{j_2}, \mathbf{s}) \quad (11)$$

$$= \frac{1}{(M_1 M_2)^2} \sum_{(i_1,i_2),(j_1,j_2)} W(\phi^{-1}(A)^c \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}, \mathbf{s}_0) \quad (12)$$

$$\geq \frac{1}{(M_1M_2)^2} \sum_{\substack{(i_1,i_2)\\(j_1,j_2)\neq(i_1,i_2)}} W(\phi^{-1}(\{(i_1,i_2)\}) \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}, \mathbf{s}_0) \tag{13}$$

$$\geq \frac{1}{M_1M_2} \sum_{(j_1,j_2)\neq(i_1,i_2)} (1 - e(\mathbf{s}_0)) \tag{14}$$

$$\geq \frac{M_1M_2 - 1}{M_1M_2} (1 - e(\mathbf{s}_0)) \tag{15}$$

where (12) follows by $X_1 \times X_2$-overwritability. Noting that $\max_{\mathbf{s}} e(\mathbf{s}) \geq e(\mathbf{s}_0)$,

$$\max_{\mathbf{s}} e(\mathbf{s}) \geq \frac{M_1M_2 - 1}{2M_1M_2 - 1},$$

which, for any positive R_1 or R_2, converges to 0.5 as $n \to \infty$. Thus, (R_1, R_2) is not an achievable rate pair for any $(R_1, R_2) \neq (0, 0)$, and we conclude that $\mathscr{C}_{\text{auth}}$ has empty interior.

By analogous arguments, we may show that if $W_{Y|X_1X_2S}$ is X_1-overwritable (resp., X_2-overwritable), (R_1, R_2) is not an achievable rate pair for any $R_1 > 0$ (resp., $R_2 > 0$). In either case, we again conclude that $\mathscr{C}_{\text{auth}}$ has empty interior.

□

Theorem III.7. *Suppose a channel $W_{Y|X_1X_2S}$ is not $X_1 \times X_2$-, X_1-, nor X_2-overwritable. Then, $\mathscr{C}_{auth} = \mathscr{C}$.*

The converse follows easily by Lemma III.6. Achievability is accomplished by the same code construction presented in [16] for achievability over a two-user byzantine MAC (see Appendix E of [17]), with some arguments adjusted for the change in setting. Their construction is roughly as follows: first, the two users transmit their messages using a high-rate-pair coding scheme for the underlying non-adversarial two-user MAC. Subsequently, each user in turn sends a short tag that validates its previously-transmitted message, while the other user transmits a constant symbol. Because the channel is not X_1-, X_2-, nor $X_1 \times X_2$-overwritable, each of the tags can be transmitted with vanishing authentication error probability, and can be used to reliably validate the messages.

Remark III.8. *Consider a channel that is not overwritable in any sense, but is symmetrizable in every sense (e.g. Example III.5). In this case, the communication error probability is bounded away from zero. However, authentication allows the users to obtain useful information in spite of this: when the adversary is active, the receiver at worst correctly identifies its presence without outputting a message pair estimate. On the other hand, if the adversary is not actively tampering with a transmission, the receiver can reliably decode.*

IV. γ-correcting Authentication

As mentioned in Section II, previous work has deemed the decoder successful if $(\hat{i}_1, \hat{i}_2) = (i_1, i_2)$, or, if $\mathbf{s} \neq \mathbf{s}_0$, $(\hat{i}_1, \hat{i}_2) = (0, 0)$. Our definition of the authentication decoder, however, allows for partial decoding of the message pair in the presence of an adversary. Thus, the decoder has the opportunity to recover a message from one user, even if the adversary is present and interference must be declared for the other user. For certain channels, we are able to achieve positive rate pairs while requiring this stricter form of authentication. To this end, we define γ-correcting authentication codes. We present the general definition below, recalling that our present focus is on the two-user case (i.e., $t = 2$).

Definition IV.1. Let $\gamma \in (0, 1)$. We say that an $(M_1, \ldots, M_t, n)$ authentication code for a t-user AV-MAC is *γ-correcting* if, with high probability in n, we can correct at least a γ fraction of the t messages.

We revise Equation (3) slightly to account for this new restriction in the two-user case: for fixed $i_1, i_2, \mathbf{s}$, we define

$$e_\gamma(i_1, i_2, \mathbf{s}) = \begin{cases} W(\phi^{-1}(\{(i_1, i_2)\})^c \mid \mathbf{x}_1(i_1), \mathbf{x}_2(i_2), \mathbf{s}) & \mathbf{s} = \mathbf{s}_0 \\ W(\phi^{-1}(A)^c \mid \mathbf{x}_1(i_1), \mathbf{x}_2(i_2), \mathbf{s}) & \mathbf{s} \neq \mathbf{s}_0, \end{cases} \tag{16}$$

where $A := \{(\hat{i}_1, \hat{i}_2) : \hat{i}_j \in \{0, i_j\}, \ \|(\hat{i}_1, \hat{i}_2)\| \geq \gamma \cdot 2\}$. We then define $e_\gamma(\mathbf{s})$ to be the average over all message pairs of $e_\gamma(i_1, i_2, \mathbf{s})$. In the case of a two-user AV-MAC, $0 < \gamma \leq 0.5$ requires that at least one user be corrected, and $\gamma > 0.5$ gives the reliable communication problem (i.e. both messages must be corrected regardless of adversarial interference). An authentication code is γ-correcting if $e_\gamma(\mathbf{s}) \to 0$ as $n \to \infty$. We define the *γ-correcting authentication capacity region* as the closure of the set of all positive achievable rate pairs (i.e. $R_1, R_2 > 0$), and denote it by $\mathscr{C}_{\text{auth},\gamma}$.

Lemma IV.2. *$\mathscr{C}_{auth,\gamma} \subseteq \mathscr{C}_{auth}$ for all $\gamma \in (0, 1)$.*

Proof. Let $\gamma \in (0, 1)$ and fix an authentication code that is γ-correcting. For any $i_1, i_2, \mathbf{s}$, $e_\gamma(i_1, i_2, \mathbf{s}) \geq e(i_1, i_2, \mathbf{s})$. Thus, $\max_{\mathbf{s}} e_\gamma(\mathbf{s}) \to 0$ implies that $\max_{\mathbf{s}} e(\mathbf{s}) \to 0$, and the code is also an authentication code in the sense of Section III. We conclude that if a rate pair is achievable for γ-correcting authentication, it is also achievable for authentication. □

Theorem IV.3. *Let $\gamma \in (0, 1)$. If a $W_{Y|X_1X_2S}$ is $X_1 \times X_2$-symmetrizable, then $\mathscr{C}_{auth,\gamma}$ has empty interior.*

Proof. Suppose $W_{Y|X_1X_2S}$ is $X_1 \times X_2$-symmetrizable, let $\gamma \in (0, 1)$ and let $P := P_{S|X_1X_2}$ be the guaranteed adversarial distribution. Consider a sequence of (M_1, M_2, n) codes, with $M_1 := 2^{R_1 n}$, $M_2 := 2^{R_2 n}$, $R_1, R_2 \geq 0$. Let $\mathbf{x}_{i_j} := f_j(i_j)$ for $j \in \{1, 2\}$, $i_j \in [M_j]$, and let $A := \{(j_1, j_2), (j_1, 0), (0, j_2)\}$, and $B := \{(i_1, i_2), (i_1, 0), (0, i_2)\}$. Then, $\max_{\mathbf{s}} e_\gamma(\mathbf{s})$ is bounded below by

$$\geq \sum_{\mathbf{s}} \left(\frac{1}{M_1M_2} \sum_{(i_1,i_2)} P(\mathbf{s} \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}) \right) e_\gamma(\mathbf{s}) \tag{17}$$

$$= \frac{1}{(M_1M_2)^2} \sum_{(i_1,i_2),(j_1,j_2),\mathbf{s}} P(\mathbf{s} \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}) e_\gamma(j_1, j_2, \mathbf{s}) \tag{18}$$

$$\geq \frac{1}{(M_1M_2)^2} \sum_{(i_1,i_2),(j_1,j_2),\mathbf{s}} P(\mathbf{s} \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}) W(\phi^{-1}(A)^c \mid \mathbf{x}_{j_1}, \mathbf{x}_{j_2}, \mathbf{s}) \tag{19}$$

$$= \frac{1}{(M_1M_2)^2} \sum_{(i_1,i_2),(j_1,j_2),\mathbf{s}} P(\mathbf{s} \mid \mathbf{x}_{j_1}, \mathbf{x}_{j_2}) W(\phi^{-1}(A)^c \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}, \mathbf{s}) \tag{20}$$

$$\geq \frac{1}{(M_1M_2)^2} \sum_{(i_1,i_2),\mathbf{s},j_1\neq i_1,j_2\neq i_2} P(\mathbf{s} \mid \mathbf{x}_{j_1}, \mathbf{x}_{j_2}) W(\phi^{-1}(B) \mid \mathbf{x}_{i_1}, \mathbf{x}_{i_2}, \mathbf{s}) \tag{21}$$

$$\geq \frac{1}{(M_1M_2)^2} \sum_{\substack{(i_1,i_2),\mathbf{s}\\ j_1\neq i_1,j_2\neq i_2}} P(\mathbf{s} \mid \mathbf{x}_{j_1}, \mathbf{x}_{j_2}) \left(1 - e_\gamma(i_1, i_2, \mathbf{s})\right) \tag{22}$$

$$= \frac{1}{M_1M_2} \sum_{j_1\neq i_1,j_2\neq i_2} \sum_{\mathbf{s}} P(\mathbf{s} \mid \mathbf{x}_{j_1}, \mathbf{x}_{j_2}) \left(1 - e_\gamma(\mathbf{s})\right) \tag{23}$$

$$\geq \frac{(M_1-1)(M_2-1)}{M_1M_2} \left(1 - \max_{\mathbf{s}} e_\gamma(\mathbf{s})\right) \tag{24}$$

where (20) follows by symmetrizability. Then,

$$\max_{s} e_\gamma(\mathbf{s}) \geq \frac{(M_1-1)(M_2-1)}{(M_1-1)(M_2-1) + M_1M_2}.$$

If both R_1 and R_2 are strictly greater than 0, the right side converges to 0.5 as $n \to \infty$. Thus, it must be the case that at least one of R_1 or R_2 is equal to zero, resulting in $\mathscr{C}_{\text{auth},\gamma}$ having empty interior. □

It is possible that a channel is not overwritable in any sense, but is $X_1 \times X_2$-symmetrizable; in this case, $\mathscr{C}_{\text{auth},\gamma}$ has empty interior, even while $\mathscr{C}_{\text{auth}} = \mathscr{C}$ may have nonempty interior.

V. Construction for the Real Addition Binary AV-MAC

If $W_{Y|X_1X_2S}$ is not overwritable, and is not $X_1 \times X_2$-symmetrizable, it is possible that $\mathscr{C}_{\text{auth},\gamma}$ has nonempty interior, even if the channel is X_1- or X_2-symmetrizable. The channel presented in Example II.3 falls into this category; in this section, we present a construction for γ-correcting authentication over this channel.

A. A Small 0.5-correcting Authentication Code

We first present a $(2, 2, 3)$ 0.5-correcting authentication code for transmission over the channel detailed in Example II.3, which outputs the real-valued sum of binary user inputs and the adversarial state. Recall that this channel is not overwritable in any sense, and is not $X_1 \times X_2$-symmetrizable, but is both X_1- and X_2-symmetrizable. Let the codebooks for users 1 and 2 be $\{011, 100\}$, and $\{010, 101\}$, respectively. If the adversary is not present, the possible channel outputs are in $\{021, 112, 110, 201\}$. It is straightforward to see that an active adversary (i.e. an adversary whose state is not 000) will always be detected, and so regular authentication can be achieved with zero error probability.

In fact, this choice of codebooks also forms a 0.5-correcting authentication code. Fig. 2 gives all possible channel outputs, resulting from any pair of inputs and any binary state sequence. Notice that there are four distinct outputs that correspond to multiple possible input/state sequences. In each case, the adversary's strategy is to choose $\mathbf{s}$ to be a valid codeword in one of the users' codebooks. While this ambiguity negates the possibility of completely correcting these four sequences, one user's message can still be corrected with perfect accuracy in every case. Specifically, with outputs of 122 and 211, we can guarantee that $\mathbf{x}_1 = 011$ and 100, respectively. For outputs of 121 and 212, $\mathbf{x}_2 = 010$ and 101, respectively. There is a unique triple of legitimate inputs and state sequence for every other output, allowing for perfect recovery of both $\mathbf{x}_1$ and $\mathbf{x}_2$.

$\mathbf{s} \setminus \mathbf{x}_1 + \mathbf{x}_2$	011+010	011+101	100+010	100+101
000	021	112	110	201
001	022	113	111	202
010	031	122	120	211
011	032	123	121	212
100	121	212	210	301
101	122	213	211	302
110	131	222	220	311
111	132	223	221	312

Fig. 2. The possible channel outputs for all possible input pairs and choices of adversarial state in Section V-A. Outputs arising in multiple ways are shaded.

Clearly, the above construction does not give asymptotic results. However, we can use this small code as a building block to construct a positive rate pair sequence of codes.

B. Extending the Block Length

To extend the scheme of Section V-A to longer block lengths, we add an outer code. For a binary message of length R_1n (resp., R_2n) for User 1 (resp., User 2), first encode the message using a $(2^{R_1n}, n)$ (resp., $(2^{R_2n}, n)$) outer code designed for error correction over the following AVC: the alphabet of the legitimate user is $\mathcal{X} = \{0, 1\}$, and the adversary's alphabet is $\mathcal{S} = \{s_0, 0, 1\}$. For a user input of x and state symbol s, outputs are determined as follows:

$$y = \begin{cases} x & \text{if} \quad s \in \{s_0, x\} \\ \varepsilon & \text{else,} \end{cases} \tag{25}$$

where ε denotes an erasure. The adversary is power-constrained so that it may choose at most $\lfloor n/2 \rfloor$ coordinates to be from $\{0, 1\}$; the remainder must equal s_0. The capacity of this channel is positive (see Appendix A), and so codes of positive rate exist for error correction over this channel. If the message sets of Users 1 and 2 are the same size, the same outer code may be used for each. Next, each bit of the $(2^{R_1n}, n)$ (resp., $(2^{R_2n}, n)$) code is encoded using the appropriate codebook of the $(2, 2, 3)$ 0.5-correcting authentication code for the two-user AV-MAC presented in Section V-A.

Decoding is as follows: first, each 3-bit block of the received sequence is decoded as described in Section V-A. For each block, we may guarantee that at least one of the users is correctable. If the other user's message is not correctable, its output in that coordinate is set to ε. The resulting output of this first stage of decoding is one length-n codeword for each user, each with some number of bits erased. For each 3-bit block, the adversary's choice of state determines which user is targeted (see our discussion in Section V-A); the adversary must split its time between the two users, so at least one user has been targeted in at most half of its coordinates.

Without loss of generality, suppose User 1 is targeted in at most as many positions as is User 2. As a worst-case scenario, we assume that the adversary has targeted half of the bits of User 1's codeword. The effective channel is then the AVC described above and detailed in Appendix A. Since our $(2^{R_1 n}, n)$ code was designed for this channel, we successfully decode with high probability.

In all, this construction gives a $(2^{R_1 n}, 2^{R_2 n}, 3n)$ 0.5-correcting authentication code for the real-addition binary-input two-user AV-MAC. In other words, the rate pair $(R_1/3, R_2/3)$ is achievable for any rates R_1 and R_2 that are achievable over the erasure AVC described above (see Appendix A). Consequently, we have shown that the rate pair $(0.25, 0.25)$ is achievable over this two-user AV-MAC.

VI. Conclusions

In this paper, we gave authentication capacity results for the two-user AV-MAC. For a classical definition of authentication, we showed that the authentication capacity region is characterized by an extension of the AVC channel condition overwritability. We then introduced the concept of γ-correcting authentication, and showed that $\mathscr{C}_{\text{auth},\gamma} \subseteq \mathscr{C}_{\text{auth}}$, and that $\mathscr{C}_{\text{auth},\gamma}$ has empty interior when the channel is $X_1 \times X_2$-symmetrizable. Finally, we showed that positive γ-correcting authentication rate pairs are achievable when the AV-MAC satisfies certain conditions. Ongoing work includes extending our results to the t-user AV-MAC, and the development of computationally efficient constructions for γ-correcting authentication.

References

[1] D. Blackwell, L. Breiman, and A. Thomasian, "The capacities of certain channel classes under random coding," *The Annals of Mathematical Statistics*, vol. 31, no. 3, pp. 558–567, 1960.

[2] O. Kosut and J. Kliewer, "Authentication capacity of adversarial channels," in *IEEE Inf. Theory Workshop (ITW)*. IEEE, 2018, pp. 1–5.

[3] G. J. Simmons, "Authentication theory/coding theory," in *Workshop on the Theory and App. of Cryptographic Techniques*. Springer, 1984, pp. 411–431.

[4] U. Maurer, "Information-theoretically secure secret-key agreement by NOT authenticated public discussion," in *Int'l Conf. on the Theory and App.s of Cryptographic Techniques*. Springer, 1997, pp. 209–225.

[5] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Trans. on Inf. Theory*, vol. 55, no. 2, pp. 906–916, 2009.

[6] E. Graves, P. Yu, and P. Spasojevic, "Keyless authentication in the presence of a simultaneously transmitting adversary," in *IEEE Inf. Theory Workshop (ITW)*. IEEE, 2016, pp. 201–205.

[7] O. Gungor and C. E. Koksal, "On the basic limits of RF-fingerprint-based authentication," *IEEE Trans. on Inf. Theory*, vol. 62, no. 8, pp. 4523–4543, 2016.

[8] J. Perazzone, E. Graves, P. Yu, and R. Blum, "Inner bound for the capacity region of noisy channels with an authentication requirement," in *IEEE Int'l Symp. on Inf. Theory (ISIT)*. IEEE, 2018, pp. 126–130.

[9] A. Beemer, O. Kosut, J. Kliewer, E. Graves, and P. Yu, "Structured coding for authentication in the presence of a malicious adversary," in *IEEE Int'l Symp. on Inf. Theory (ISIT)*. IEEE, 2019, pp. 617–621.

[10] E. Graves, J. Perazzone, P. Yu, and R. Blum, "Secret key authentication capacity region, part II: typical authentication rate," *arXiv preprint arXiv:2001.01667*, 2020.

[11] A. Beemer, E. Graves, J. Kliewer, O. Kosut, and P. Yu, "Authentication against a myopic adversary," *arXiv preprint arXiv:2001.03593*, 2020.

[12] J.-H. Jahn, "Coding of arbitrarily varying multiuser channels," *IEEE Trans. on Inf. Theory*, vol. 27, no. 2, pp. 212–226, 1981.

[13] J. A. Gubner, "On the deterministic-code capacity of the multiple-access arbitrarily varying channel," *IEEE Trans. on Inf. Theory*, vol. 36, no. 2, pp. 262–275, 1990.

[14] R. Ahlswede and N. Cai, "Arbitrarily varying multiple-access channels. I. Ericson's symmetrizability is adequate, Gubner's conjecture is true," *IEEE Trans. on Inf. Theory*, vol. 45, no. 2, pp. 742–749, 1999.

[15] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Trans. on Inf. Theory*, vol. 34, no. 2, pp. 181–193, March 1988.

[16] N. Sangwan, M. Bakshi, B. K. Dey, and V. M. Prabhakaran, "Multiple access channels with adversarial users," in *IEEE Int'l Symp. on Inf. Theory (ISIT)*, 2019, pp. 435–439.

[17] N. Sangwan, M. Bakshi, B. K. Dey, and V. M. Prabhakaran, "Byzantine multiple access," *arXiv preprint arXiv:1904.11925*, 2019.

Appendix A

Consider the AVC described in Section V-B. For $\mathbf{s} \in \mathcal{S}^n$, define $\ell(\mathbf{s}) = \frac{1}{n}\sum_{i=1}^{n} \ell(s_i)$, where $\ell(s) = 0$ if $s = s_0$, and $\ell(s) = 1$ otherwise. The stipulation that the adversary may choose at most $\lfloor n/2 \rfloor$ coordinates of its sequence to be in $\{0, 1\}$ is equivalent to the state constraint $\ell(\mathbf{s}) \leq \Lambda$, where $\Lambda = 0.5$. There are no constraints on the input sequence. Note that our AVC is only symmetrizable using the following choice of $P_{S|X}$:

$$P_{S|X}(s \mid x) = \begin{cases} 1 & \text{if} \quad s = x \\ 0 & \text{else.} \end{cases} \tag{26}$$

Let

$$\Lambda_0(P_X) := \min_{P_{S|X} \in \mathcal{P}} \sum_{x \in \mathcal{X}} \sum_{s \in \mathcal{S}} P_X(x) P_{S|X}(s \mid x) \ell(s),$$

where $\mathcal{P}$ denotes the set of all distributions $P_{S|X}$ satisfying the symmetrizability condition. In our case, $\mathcal{P}$ consists only of the distribution in (26). It is straightforward to see that $\Lambda_0(P_X) = 1$ for any distribution P_X on the input symbols, and thus that $\Lambda < \Lambda_0(P_X)$ for any distribution P_X. So, by Theorem 3 of [15], the capacity of the state-constrained AVC is given by

$$C(\Lambda) = \max_{P_X} I(P_X, \Lambda) := \max_{P_X} \min_{Y : P_{XSY} \in C_0(\Lambda)} I(X; Y) \tag{27}$$

where C_0 is the set of joint distributions $P_{XSY}(x, s, y) = P_X(x) P_S(s) W(y \mid x, s)$, and $C_0(\Lambda)$ denotes those such that $\mathbb{E}[\ell(S)] \leq \Lambda$. Observe that $P_{XSY} \in C_0$ if and only if X and S are independent, and

$$Y = \begin{cases} X & \text{if} \quad S = X, s_0 \\ \varepsilon & \text{else.} \end{cases} \tag{28}$$

Letting $P_X(1) = p$, $P_S(0) = q_0$, $P_S(1) = q_1$, we have

$$C(\Lambda) = \max_{p \in (0,1)} \min_{q_0 + q_1 \leq 0.5} I(X; Y) \tag{29}$$

where

$$\begin{aligned} I(X; Y) &= H(Y) - H(Y \mid X) && (30) \\ &= (1-p)(1-q_1)\log_2 \frac{1}{1-p} + p(1-q_0)\log_2 \frac{1}{p} && (31) \\ &\quad + (1-p) q_1 \log_2 \frac{q_1}{(1-p)q_1 + p q_0} && (32) \\ &\quad + p q_0 \log_2 \frac{q_0}{(1-p)q_1 + p q_0}. && (33) \end{aligned}$$

We conclude that $C(\Lambda) = 0.75$, where the capacity is achieved at $p = 0.5$, $q_0 = q_1 = 0.25$.