Structured Coding for Authentication in the Presence of a Malicious Adversary

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

***Abstract*—Authentication in the presence of a malicious adversary consists of either recovering the legitimate transmission or declaring that the adversary has interfered with the transmission. In this work, we present a structured coding scheme for keyless authentication over a discrete memoryless binary-input, symmetric adversarial channel. Our scheme allows for coding rates up to the non-adversarial capacity of the underlying channel, as well as bounded-complexity decoding.**

I. Introduction

Consider a scenario where users wish to ensure reliable communication over an unsecured channel: in such a setting, the ability to reliably detect the presence of a malicious adversary can be of high value. This problem, known as authentication, is a relaxation of the more general arbitrarily-varying channel (AVC): in both settings, the channel takes as inputs both the legitimate transmission and an adversarial state [1]. The adversary maliciously chooses a state with the goal of causing a decoding error at the receiver. Over the AVC, the receiver then attempts to recover the legitimate transmission in spite of the adversary's interference. A plethora of variations on the AVC appear in the literature, in which the adversary has varying degrees of power and knowledge of the legitimate transmission, and the sender and receiver may or may not have access to a shared key. In the authentication setting, the receiver also succeeds if the presence of adversarial interference is detected. That is, if no adversary is present, the receiver must decode to the intended message correctly; otherwise, the receiver must either decode correctly or detect the adversary. Variations are examined in [2], [3], [4].

The capacity of the AVC was studied in [5], where the authors establish a necessary and sufficient channel condition for positive capacity in the case where the adversary is oblivious to the actual transmission, but has complete knowledge of the codebook. This condition, called *symmetrizability*, indicates channel conditions that allow an adversary to successfully convince the receiver that a different codeword was transmitted. In [6], an analogous (but stronger) condition, *overwritability*, was given for authentication. It was shown that for channels which are not overwritable, the capacity is equal to the non-adversarial capacity of the channel. This result is proven using techniques similar to those used in [5]. In both cases, the transmitter and receiver do not have access to any shared secret key: the adversary is aware of all parts of the coding strategy.

In this paper, we adopt the setting and follow the general structure of the proof in [6], but with significant differences in terms of practical realization. While the former makes use of classical random coding arguments, we aim to demonstrate that there exist structured coding schemes with bounded decoding complexity that may accomplish keyless authentication at rates approaching channel capacity. To the best of our knowledge, such results for structured codes have not yet been presented in the literature. We utilize existing linear codes designed for non-adversarial channels to arrive at a scheme that inherits the rate and error probability of these codes. It is important to note that simply using a linear code designed for the non-adversarial channel will not provide any security against the adversary: such a code has so much structure that the adversary may thwart the legitimate users every time. Thus, we also incorporate the use of short, nonlinear message hashes in our scheme. Algebraic manipulation detection (AMD) codes bear some similarity to our proposed scheme, and are used in [7] to construct codes for additive errors by concatenating with a list-decodable linear code. It is important to note that the authors of [7] focus on error correction, and that their model includes a power-constrained adversary but no channel noise on top of adversarial interference, as ours will.

We restrict our focus to discrete memoryless channels (DMCs) for which the input and state alphabets are binary and for which the corresponding non-adversarial channel is symmetric [8]. These channels are simple enough to capture the basic features of our approach, and will provide guidance for extensions to more general channels.

The remainder of the paper is organized as follows. In Section II, we introduce relevant notation and background.We present our main results in Section III, and Section IV concludes the paper.

II. Preliminaries

We consider authentication when there is a legitimate sender and receiver, as well as an active adversary who induces some

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.

978-1-5386-9291-2/19/$31.00 ©2019 IEEE

channel state at each transmission. More formally, let $W_{Y|X,S}$ be a discrete adversarial channel, with the finite sets $\mathcal{X}, \mathcal{S}$, and $\mathcal{Y}$ as the input, state, and output alphabets, respectively. Let $\mathbb{F}_2$ denote the field of order two. In this paper, we will consider the case where $\mathcal{X} = \mathcal{S} = \mathbb{F}_2$, and the output of the channel depends only on the sum of the input and state in $\mathbb{F}_2$: $W_{Y|X+S}$. Additionally, we will assume $W_{Y|X+0}$ is a non-trivial binary-input DMC that is *symmetric* as defined in [8]; roughly, such channels may be decomposed into a set of binary symmetric channels (BSCs) and a binary erasure channel (BEC). More specifically, a binary-input channel is symmetric if there exists a bijection $\pi : \mathcal{Y} \to \mathcal{Y}$ such that (1) $\pi = \pi^{-1}$, and (2) $W(y \mid 0) = W(\pi(y) \mid 1)$ for all $y \in \mathcal{Y}$. The BSC and the BEC themselves are examples of such a channel.

In this paper, any decoder $\mathcal{D}$ of a binary linear code C of length n is assumed to have the symmetry property that $\mathbf{y} \in \mathcal{D}^{-1}(\mathbf{c})$ where $\mathbf{y} \in \mathcal{Y}^n$, $\mathbf{c} \in C$ if and only if for all $\mathbf{c}' \in C$, $\mathbf{y}' \in \mathcal{D}^{-1}(\mathbf{c}+\mathbf{c}')$, where $y'_i = y_i$ if $c'_i = 0$, and $y'_i = \pi(y_i)$ if $c'_i = 1$. Notice that some channel outputs may belong to multiple decoder preimages if they contain erasure symbols. For such output words, we stipulate that the probability the word decodes to each potential codeword is uniform. This decoder property holds for a large class of decoders for transmission over symmetric channels. For example, for low-density parity-check (LDPC) codes and message passing decoders, these symmetry conditions on the channel and decoders may be compared with those of [9]; for polar codes, see [10].

For a length-n sequence, we define

$$W^n(\mathbf{y} \mid \mathbf{x} + \mathbf{s}) = \prod_{i=1}^{n} W(y_i \mid x_i + s_i).$$

With a slight abuse of notation, we will write $W(\mathbf{y} \mid \mathbf{x}+\mathbf{s})$ when the sequence lengths are understood. Let $s_0 := 0 \in \mathbb{F}_2$ and the corresponding state sequence $\mathbf{s}_0 := \mathbf{0} \in \mathbb{F}_2^n$ represent the no-adversary state: i.e. $W_{Y|X}$ is a non-adversarial channel. Then, an *authentication code* for this channel is an encoder/decoder pair:

$$\begin{aligned} f &: \{1, 2, \ldots, M\} \to \mathbb{F}_2^n \\ \phi &: \mathcal{Y}^n \to \{0, 1, 2, \ldots, M\}, \end{aligned}$$

where an output of “0” from ϕ indicates a declaration of adversarial interference. The decoder ϕ is successful if either the output message is equal to the input message, or, if $\mathbf{s} \neq \mathbf{s}_0$, the output is equal to 0. In other words, the decoder either successfully detects adversarial interference, or it decodes to the legitimate message.

Let $\phi^{-1}(A) \subseteq \mathcal{Y}^n$ represent the set of channel outputs which decode to some $i \in A$ under ϕ, and let $\phi^{-1}(A)^c$ be the complement of this set in $\mathcal{Y}^n$. Let $\mathbf{x}_i := f(i)$. Given transmitted message i and state $\mathbf{s}$, we define the probability of error for authentication code (f, ϕ) as:

$$e(i, \mathbf{s}) = \begin{cases} W(\phi^{-1}(i)^c \mid \mathbf{x}_i, \mathbf{s}) & \text{if } \mathbf{s} = \mathbf{s}_0 \\ W(\phi^{-1}(\{i, 0\})^c \mid \mathbf{x}_i, \mathbf{s}) & \text{else.} \end{cases}$$

An appropriate measure of error probability should take into account our assumption that the adversary has knowledge of the codebook but not the particular message being transmitted. We assume each message in $[M] := \{1, 2, \ldots, M\}$ is transmitted with equal probability, so the average probability of error over all possible messages for a given state $\mathbf{s}$ is

$$e(\mathbf{s}) = \frac{1}{M} \sum_{i=1}^{M} e(i, \mathbf{s}).$$

We say a rate R is *achievable* if there exists a sequence of $(2^{nR}, n)$ authentication codes such that

$$\max_{\mathbf{s} \in \mathbb{F}_2^n} e(\mathbf{s}) \to 0 \text{ as } n \to \infty.$$

Notice that $\max_{\mathbf{s}} e(\mathbf{s})$ is the highest error probability the adversary can hope for without knowledge of the transmitted message. The *authentication capacity* C_{auth} is the supremum of all achievable rates. Let C denote the capacity in the no-adversary setting (i.e., $\mathbf{s} = \mathbf{s}_0$).

In [6], it was shown that a channel property called *overwritability* exactly determines when the authentication capacity is nonzero. An adversarial channel $W_{Y|X,S}$ with no-adversary state s_0 is *overwritable* if there exists a distribution $P_{S|X}$ such that $\sum_{\mathbf{s}} P_{S|X}(s \mid x')W(y \mid x, s) = W(y \mid x', s_0)$ for all x, x', y.

Theorem II.1. *[6] If a channel is not overwritable, then $C_{auth} = C$; if it is overwritable, then $C_{auth} = 0$.*

Intuitively, over an overwritable channel, an adversary can seamlessly make their own false message appear legitimate to the receiver without being detected. This should be compared with symmetrizability for the standard AVC problem [5]: $W_{Y|X,S}$ is *symmetrizable* if there exists $P_{S|X}$ such that $\sum_s P_{S|X}(s \mid x')W(y \mid x, s) = \sum_s P_{S|X}(s \mid x)W(y \mid x', s)$ for all x, x', y. In [6] it was shown that overwritability implies symmetrizability, but that the converse does not hold.

The methods of proving Theorem II.1, as well as the analogous results for the general AVC case [5], rely on random coding techniques. In this paper, we demonstrate more structured authentication codes whose rates are arbitrarily close to the non-adversarial capacity.

In the remainder of the paper, a binary (M, n) *code* is a (non-linear) code with M codewords and block length n, and an $[n, k]$ *code* is a binary linear code of block length n and dimension k. The rate of a code is given by $\log_2(M)/n = k/n$ in the linear case. Appending one vector to another will be denoted by $\|$.

III. Main Results

In this section, we present structured authentication codes which can achieve the authentication capacity, $C_{\text{auth}} = C$, of the considered, non-overwritable channels. It should be noted that the BSC and BEC, while non-overwritable, are symmetrizable; we emphasize that we are restricting our focus to the authentication setting. The structure of our argument is as follows: in Section III-A, we show that a positive-rate code with bounded-complexity decoding is achievable; in Section III-B, we prove that we may use shared randomness to construct such codes with a higher rate. Finally, in Section

III-C we prove that these codes can be combined to form a deterministic capacity-achieving keyless authentication code with bounded-complexity decoding.

A. Positive-rate code

We begin by designing a sequence of authentication codes with positive rate such that $\max_{\mathbf{s}} e(\mathbf{s})$ approaches 0 as n goes to infinity. Each message $i \in [2^k]$ corresponds to a binary vector of length k, which we will denote $\mathbf{m}_i$. Our strategy will be to append a hash vector of length k to each message. In the non-deterministic case (i.e. $W(y \mid x, s) \in (0, 1)$ for some choice of y, x, s), we will then encode the resulting message-hash vector using a linear error-correcting code. First, we show that there exists a hash function that renders unique the state required to shift between any two message-hash vectors:

Lemma III.1. *There exists a hash function $h : \mathbb{F}_2^k \to \mathbb{F}_2^k$ such that*

$$[\mathbf{m}_1 \| h(\mathbf{m}_1)] + [\mathbf{m}_2 \| h(\mathbf{m}_2)] \neq [\mathbf{m}_3 \| h(\mathbf{m}_3)] + [\mathbf{m}_4 \| h(\mathbf{m}_4)] \quad (1)$$

for distinct $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4 \in \mathbb{F}_2^k$.

Proof. With a slight abuse of notation, let $h(\mathbf{m}) := \mathbf{m}^3$, where the calculation is done in $\mathbb{F}_{2^k}$ using the isomorphism between $\mathbb{F}_2^k$ and $\mathbb{F}_{2^k}$, and then converted back to a vector in $\mathbb{F}_2^k$ (see, e.g., [11], Chapter 13). We claim this h has the desired property.

Suppose, by way of contradiction, that

$$[\mathbf{m}_1 \| h(\mathbf{m}_1)] + [\mathbf{m}_2 \| h(\mathbf{m}_2)] = [\mathbf{m}_3 \| h(\mathbf{m}_3)] + [\mathbf{m}_4 \| h(\mathbf{m}_4)]$$

for some distinct $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4 \in \mathbb{F}_2^k$. Then

$$\mathbf{m}_1 + \mathbf{m}_2 + \mathbf{m}_3 + \mathbf{m}_4 = \mathbf{0}, \text{ and } \mathbf{m}_1^3 + \mathbf{m}_2^3 + \mathbf{m}_3^3 + \mathbf{m}_4^3 = \mathbf{0}. \quad (2)$$

The intersection of the equations in (2) gives $\mathbf{m}_1^3 + \mathbf{m}_2^3 + \mathbf{m}_3^3 + (\mathbf{m}_1 + \mathbf{m}_2 + \mathbf{m}_3)^3 = \mathbf{0}$, which reduces to

$$(\mathbf{m}_1 + \mathbf{m}_2)(\mathbf{m}_1 + \mathbf{m}_3)(\mathbf{m}_2 + \mathbf{m}_3) = \mathbf{0}.$$

However, this cannot be the case, as the $\mathbf{m}_i$'s were chosen to be distinct. We conclude that $[\mathbf{m}_i \| h(\mathbf{m}_i)] + [\mathbf{m}_j \| h(\mathbf{m}_j)]$ is distinct for each pair $\mathbf{m}_i, \mathbf{m}_j \in \mathbb{F}_2^k$.

□

Remark III.2. *For the hash function $h(\mathbf{m}) = \mathbf{m}^3$ given in the proof of Lemma III.1, determining whether a particular binary vector of length $2k$ is a valid message-hash combination consists of calculating $\mathbf{m}^3$. This requires a calculation in $\mathbb{F}_{2^k}$, but does not require any stored information regarding hash function values at either the sender or receiver. We present this particular function to demonstrate one possibility. Other hash functions may, of course, have the desired property of Lemma III.1 and be utilized here, with trade-offs in the length of the output hash vector, computational complexity, storage requirements, etc.*

By appending a hash whose existence is given by Lemma III.1, we have established a sequence of positive-rate codes for the case in which the channel $W_{Y|X,S}$ is deterministic (i.e. there is no channel noise in addition to the adversary's state choice). This is formalized in the following theorem.

Theorem III.3. *Consider the sequence of $(2^k, 2k)$ codes described by $f(i) = [\mathbf{m}_i \| h(\mathbf{m}_i)]$, where h is as in Lemma III.1, and $\phi(\mathbf{y}) = j$ if $f(j) = \mathbf{y}$, and $\phi(\mathbf{y}) = 0$ else. Let $W(y \mid x, s) = 1$ if $y = x + s$, and zero otherwise. Then*

$$\max_{\mathbf{s}} e(\mathbf{s}) \leq \frac{2}{2^k}.$$

Proof. Notice that for a fixed $\mathbf{s} \neq \mathbf{s}_0$, there are at most two valid codewords whose difference from another codeword is precisely $\mathbf{s}$. Indeed, suppose there are more than two, and $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ are three such distinct codewords. Then it must be the case that either $\mathbf{x}_2 + \mathbf{s} \neq \mathbf{x}_1$ or $\mathbf{x}_3 + \mathbf{s} \neq \mathbf{x}_1$ (or both). Without loss of generality, suppose the former. Because we are working over a field of characteristic 2, $\mathbf{x}_1, \mathbf{x}_1 + \mathbf{s}, \mathbf{x}_2$, and $\mathbf{x}_2 + \mathbf{s}$ are all distinct. However, $(\mathbf{x}_1 + \mathbf{s}) + \mathbf{x}_1 = \mathbf{s} = (\mathbf{x}_2 + \mathbf{s}) + \mathbf{x}_2$, contradicting our choice of h as having the property in (1).

Thus, $e(i, \mathbf{s}) = 1$ for at most two values of i, and 0 for all other values. For $\mathbf{s} = \mathbf{s}_0$ over this deterministic channel, $e(i, \mathbf{s}) = 0$ for all i. Together, this gives us:

$$\max_{\mathbf{s}} e(\mathbf{s}) = \max_{\mathbf{s}} \left(\frac{1}{2^k} \sum_{i=1}^{2^k} e(i, \mathbf{s}) \right) \leq \frac{2}{2^k}.$$

□

In order to protect against channel noise in the case where $\mathbf{s} = \mathbf{s}_0$, we encode the message-hash vector of Theorem III.3 using a linear error-correcting code. The encoding process, f, now consists of two steps: appending an appropriate hash of the message, and encoding using the chosen linear code. Decoding consists of decoding according to the linear code, and then determining whether the resulting word contains a valid message-hash combination. We will call a codeword of the inner linear code that is the encoding of a valid message-hash vector a *valid codeword.*

First, we observe that encoding using a linear code does not have an effect on the property given by (1).

Lemma III.4. *Let $h : \mathbb{F}_2^k \to \mathbb{F}_2^\ell$, where $\ell \geq k$, have the property in (1), and let $C : \mathbb{F}_2^{k+\ell} \to \mathbb{F}_2^n$ be an $[n, k+\ell]$ code. For $i \in [2^k]$, let $f(i) = C([\mathbf{m}_i \| h(\mathbf{m}_i)])$. Then the difference vector $f(i) - f(j)$ uniquely identifies $i, j \in [2^k]$.*

Proof. This is a clear consequence of the linearity of C. □

Theorem III.5. *Consider the authentication code of length n described by $f(i) = C([\mathbf{m}_i \| h(\mathbf{m}_i)])$ for $i \in [2^k]$, where $h : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is as in Lemma III.1, and C is an $[n, 2k]$ code with average decoding error probability for $W_{Y|X}$ bounded above by $P_e(C)$. Let $\mathcal{D} : \mathcal{Y}^n \to \mathbb{F}_2^n$ be the decoding function of C, and suppose $\mathcal{D}(\mathbf{y}) = C([\mathbf{m}_j \| \hat{\mathbf{h}}])$. Let $\phi(\mathbf{y}) = j$ if $h(\mathbf{m}_j) = \hat{\mathbf{h}}$, and let $\phi(\mathbf{y}) = 0$ otherwise. Then the rate of the authentication code (f, ϕ) is k/n, and*

$$\max_{\mathbf{s}} e(\mathbf{s}) \leq \max \left\{ P_e(C), \frac{2}{2^k} \right\}.$$

Proof. The rate of the authentication code follows from the length of the message vectors k and the final block length of the code n. Notice that the rate of the authentication code is half the rate of the chosen inner linear code C. For ease of notation, let $M := 2^k$ and $\mathbf{x}_i := f(i)$. When $\mathbf{s} = \mathbf{s}_0$, the success of the decoder depends entirely on the protection of C:

$$e(\mathbf{s}_0) = \frac{1}{M}\sum_{i=1}^{M} W(\phi^{-1}(i)^c \mid \mathbf{x}_i, \mathbf{s}_0) \le P_e(C).$$

Next, suppose $\mathbf{s} \neq \mathbf{s}_0$. For $0 \le t \le 2^{2k}-1$, let $\delta_{i,t}$ be equal to $W(\mathcal{D}^{-1}(\mathbf{x}_i + \mathbf{c}_t) \mid \mathbf{x}_i, \mathbf{s})$ for codeword $\mathbf{c}_t \in C$, where $\mathbf{c}_0 = \mathbf{0}$. That is, $\delta_{i,t}$ is the probability that the output of the channel with input $\mathbf{x}_i + \mathbf{s} \in \mathbb{F}_2^n$ decodes under $\mathcal{D}$ to the codeword $\mathbf{x}_i + \mathbf{c}_t \in C$, so that $\sum_{t=0}^{2^{2k}-1} \delta_{i,t} = 1$. Then,

$$\begin{aligned} e(i,\mathbf{s}) &= W(\phi^{-1}(\{i,0\})^c \mid \mathbf{x}_i, \mathbf{s}) \\ &= \sum_{t=1}^{2^{2k}-1} W(\mathcal{D}^{-1}(\mathbf{x}_i + \mathbf{c}_t) \mid \mathbf{x}_i, \mathbf{s}) \cdot \mathbf{1}_{i,t} \\ &= \sum_{t=1}^{2^{2k}-1} \delta_{i,t} \cdot \mathbf{1}_{i,t} \end{aligned}$$

where the indicator function $\mathbf{1}_{i,t}$ is equal to 1 when $\mathbf{x}_i + \mathbf{c}_t$ is a valid codeword (notice $t \neq 0$), and zero otherwise. From our assumption in Section II on the symmetry of the decoder, $\delta_{i,t} = \delta_{j,t}$ for all $i, j \in [M]$ (but it is not necessarily the case that $\mathbf{1}_{i,t} = \mathbf{1}_{j,t}$). So,

$$\begin{aligned} e(\mathbf{s}) &= \frac{1}{M}\sum_{i=1}^{M}\sum_{t=1}^{2^{2k}-1} \delta_t \cdot \mathbf{1}_{i,t} \\ &\le \frac{1}{M}\left(\sum_{t=1}^{2^{2k}-1} 2\delta_t\right) \le \frac{2}{M} \end{aligned} \tag{3}$$

where (3) follows from the fact that at most two values of i yield a valid codeword $\mathbf{x}_i + \mathbf{c}_t$ for a fixed $t \neq 0$ (see Lemma III.4 and the proof of Theorem III.3), and hence $\mathbf{1}_{i,t} = 1$ for at most two values of i. □

B. Coding with shared randomness

The rate of a code constructed as in Section III-A is upper bounded by half the non-adversarial channel capacity. However, the non-adversarial capacity is achievable. We next present a sequence of codes that, given a small amount of shared randomness in the form of a shared secret key, allows for authentication with $\max_{\mathbf{s}} e(\mathbf{s}) \to 0$ as $n \to \infty$ while maintaining a high rate. In particular, we achieve the non-adversarial capacity at the cost of requiring a shared key.

The encoding of our authentication code is as follows: to each message $i \in [2^k]$, represented by $\mathbf{m}_i \in \mathbb{F}_2^k$, we append a short vector which is a function of the message itself as well as a small amount of shared randomness; we denote this function by h. As in Section III-A, we may then further protect against channel noise using a linear inner code. This entire encoding process is encapsulated in the authentication code encoding function $f_{\mathbf{u},\mathbf{v}} : [2^k] \to \mathbb{F}_2^n$, where $(\mathbf{u}, \mathbf{v})$ is the shared key between sender and receiver.

We propose a particular choice for the function $h : \mathbb{F}_2^k \times \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell$, where the shared random information is in $\mathbb{F}_2^\ell \times \mathbb{F}_2^\ell$ (equivalently, $\mathbb{F}_2^{2\ell}$). Letting $\Delta_{2,\ell} : \mathbb{F}_2^\ell \to \mathbb{F}_{2^\ell}$ be the bijective map implied by the isomorphism between the two fields, define

$$\begin{aligned} h : \mathbb{F}_2^k \times \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell &\to \mathbb{F}_2^\ell \\ (\mathbf{m}, \mathbf{u}, \mathbf{v}) &\mapsto \Delta_{2,\ell}^{-1}\left(\sum_{j=1}^{k} m_j \Delta_{2,\ell}(\mathbf{u})^j\right) + \mathbf{v} \end{aligned} \tag{4}$$

where m_j is the jth coordinate of the vector $\mathbf{m}$, and $\Delta_{2,\ell}(\mathbf{u})^j$ indicates the jth power of $\Delta_{2,\ell}(\mathbf{u})$ in $\mathbb{F}_{2^\ell}$. The choice of function given in (4) is similar to one used in [12]; its structure leads to an efficient decoder $\phi_{\mathbf{u},\mathbf{v}}$ based on the shared information $(\mathbf{u}, \mathbf{v})$. Let $\mathcal{D} : \mathcal{Y}^n \to \mathbb{F}_2^n$ be the decoding rule of the inner linear code $C : \mathbb{F}_2^{k+\ell} \to \mathbb{F}_2^n$. The function $\phi_{\mathbf{u},\mathbf{v}}$ first decodes $\mathbf{y}$ according to $\mathcal{D}$, then decides if the result is a valid codeword. Denote the subset of C which is valid for shared $\mathbf{u}, \mathbf{v}$ by $C_{\mathbf{u},\mathbf{v}}$. If the decoded codeword is valid, $\phi_{\mathbf{u},\mathbf{v}}(\mathbf{y})$ is the corresponding message in $[2^k]$. Otherwise, $\phi_{\mathbf{u},\mathbf{v}}(\mathbf{y}) = 0$.

To see how the validity of a codeword may be determined, we first note that a codeword is in $C_{\mathbf{u},\mathbf{v}}$ if and only if, when unencoded using C^{-1} (the inverse map from the image of C back into $\mathbb{F}_2^{k+\ell}$) the result is a valid message-hash vector. Define

$$\mathbf{Q}_1 := \sum_{j=1}^{k} C^{-1}(\mathcal{D}(\mathbf{y}))_j \Delta_{2,\ell}(\mathbf{u})^j + \Delta_{2,\ell}(\mathbf{v}), \tag{5}$$

$$\mathbf{Q}_2 := \Delta_{2,\ell}\left(C^{-1}(\mathcal{D}(\mathbf{y}))_{k+1}^{k+\ell}\right), \tag{6}$$

where $C^{-1}(\cdot)_{k+1}^{k+\ell}$ is the last ℓ coordinates of $C^{-1}(\cdot)$, and $C^{-1}(\cdot)_j$ is the jth coordinate of $C^{-1}(\cdot)$. The value $\mathbf{Q}_1$ is the the correct value in $\mathbb{F}_{2^\ell}$ of h, given by the first k coordinates of $C^{-1}(\mathcal{D}(\mathbf{y}))$; $\mathbf{Q}_2$ is the observed value in $\mathbb{F}_{2^\ell}$ of h.

If $\mathbf{Q}_1 = \mathbf{Q}_2$, we will declare that the message is authentic and output as $\phi_{\mathbf{u},\mathbf{v}}(\mathbf{y})$ the value in $[2^k]$ corresponding to the first k coordinates of $C^{-1}(\mathcal{D}(\mathbf{y}))$. If $\mathbf{Q}_1 \neq \mathbf{Q}_2$, we will declare adversarial interference and output $\phi_{\mathbf{u},\mathbf{v}}(\mathbf{y}) = 0$.

Next, we give results on the reliability of this scheme in a noisy channel setting. The following theorem easily reduces to the noiseless case.

Theorem III.6. *Let the shared random vectors* $\mathbf{u}$ *and* $\mathbf{v}$ *each be chosen uniformly at random from* $\mathbb{F}_2^\ell$*, and let* $P_e(C)$ *be an upper bound on the average probability of decoding error over* $W_{Y|X}$ *of the* $[n, k+\ell]$ *linear inner code* C*. Then for the authentication code* $(f_{\mathbf{u},\mathbf{v}}, \phi_{\mathbf{u},\mathbf{v}})$ *described above,*

$$\max_{\mathbf{s}} e(\mathbf{s}) \le \max\left\{P_e(C), \frac{k}{2^\ell}\right\}.$$

Proof. Let $M := 2^k$ and $\mathbf{x}_{i,\mathbf{u},\mathbf{v}} := f_{\mathbf{u},\mathbf{v}}(i)$. If $\mathbf{s} = \mathbf{s}_0$,

$$e(\mathbf{s}_0) = \frac{1}{M \cdot 2^{2\ell}} \sum_{i=1}^{M}\sum_{\mathbf{u},\mathbf{v}} W(\phi_{\mathbf{u},\mathbf{v}}^{-1}(i)^c \mid \mathbf{x}_{i,\mathbf{u},\mathbf{v}}, \mathbf{s}_0) \le P_e(C).$$

Now, let $\mathbf{s} \neq \mathbf{s}_0$. For $0 \le t \le 2^{k+\ell} - 1$, let $\delta_{i,\mathbf{u},\mathbf{v},t}$ be equal to $W(\mathcal{D}^{-1}(\mathbf{x}_{i,\mathbf{u},\mathbf{v}} + \mathbf{c}_t) \mid \mathbf{x}_{i,\mathbf{u},\mathbf{v}}, \mathbf{s})$ for codeword $\mathbf{c}_t \in C$, where $\mathbf{c}_0 = \mathbf{0}$. That is, $\delta_{i,\mathbf{u},\mathbf{v},t}$ is the probability that the output of the channel with input $\mathbf{x}_{i,\mathbf{u},\mathbf{v}} + \mathbf{s} \in \mathbb{F}_2^n$ decodes to the codeword $\mathbf{x}_{i,\mathbf{u},\mathbf{v}} + \mathbf{c}_t \in C$ under $\mathcal{D}$, so that $\sum_{t=0}^{2^{k+\ell}-1} \delta_{i,\mathbf{u},\mathbf{v},t} = 1$. We let $\mathbf{1}_{i,\mathbf{u},\mathbf{v},t}$ be equal to

1 if $\mathbf{x}_{i,\mathbf{u},\mathbf{v}} + \mathbf{c}_t \in C_{\mathbf{u},\mathbf{v}}$, and zero otherwise. As in the proof of Theorem III.5, $\delta_{i,\mathbf{u},\mathbf{v},t}$ is independent of $\mathbf{x}_{i,\mathbf{u},\mathbf{v}}$ for our class of decoders, so we have $\delta_{i,\mathbf{u},\mathbf{v},t} = \delta_t$, and

$$\begin{aligned} e(\mathbf{s}) &= \frac{1}{M \cdot 2^{2\ell}} \sum_{i=1}^{M} \sum_{\mathbf{u},\mathbf{v}} W(\phi_{\mathbf{u},\mathbf{v}}^{-1}(\{i,0\})^c \mid \mathbf{x}_{i,\mathbf{u},\mathbf{v}}, \mathbf{s}) \\ &= \frac{1}{M \cdot 2^{2\ell}} \sum_{i=1}^{M} \sum_{t=1}^{2^{k+\ell}-1} \delta_t \sum_{\mathbf{u},\mathbf{v}} \mathbf{1}_{i,\mathbf{u},\mathbf{v},t} \\ &\leq \frac{k}{M \cdot 2^{\ell}} \sum_{i=1}^{M} \sum_{t=1}^{2^{k+\ell}-1} \delta_t \qquad (7) \\ &\leq \frac{k}{M \cdot 2^{\ell}} \sum_{i=1}^{M} 1 = \frac{k}{2^{\ell}}, \end{aligned}$$

Observe that each codeword $\mathbf{x}_{i,\mathbf{u},\mathbf{v}} + \mathbf{c}_t$ is in $C_{\mathbf{u},\mathbf{v}}$ if and only if

$$\sum_{j=1}^{k} C^{-1}(\mathbf{x}_{i,\mathbf{u},\mathbf{v}} + \mathbf{c}_t)_j \Delta_{2,\ell}(\mathbf{u})^j + \Delta_{2,\ell}(\mathbf{v}) = \Delta_{2,\ell}\left(C^{-1}(\mathbf{x}_{i,\mathbf{u},\mathbf{v}} + \mathbf{c}_t)_{k+1}^{k+\ell}\right),$$

where $C^{-1}(\cdot)_{k+1}^{k+\ell}$ is the last ℓ coordinates of $C^{-1}(\cdot)$, and $C^{-1}(\cdot)_j$ is the jth coordinate of $C^{-1}(\cdot)$. This holds if and only if $\Delta_{2,\ell}(\mathbf{u})$ is a root of the degree (at most) k polynomial $\Delta_{2,\ell}(C^{-1}(\mathbf{c}_t)_{k+1}^{k+\ell}) - \sum_{j=1}^{k} C^{-1}(\mathbf{c}_t)_j X^j \in \mathbb{F}_{2^\ell}[X]$. For fixed t, this occurs for at most k choices of $\mathbf{u}$. We may then bound $\sum_{\mathbf{u},\mathbf{v}} \mathbf{1}_{i,\mathbf{u},\mathbf{v},t} \leq \sum_{\mathbf{v}} k = 2^{\ell} k$, giving (7). □

C. Final coding scheme

Finally, we put the results of the previous two subsections together in order to arrive at a code of high rate that may accomplish authentication without the use of a shared key. Loosely, we use the positive rate code of Section III-A to encode the shared randomness needed for the code in Section III-B, and send both codes across the adversarial channel.

Theorem III.7. *Let (f_p, ϕ_p) denote the positive-rate code of Section III-A, and let $(f_{r,\mathbf{u},\mathbf{v}}, \phi_{r,\mathbf{u},\mathbf{v}})$ denote the code with shared randomness of Section III-B. Let $C_{n'}^{(p)}$ and $C_n^{(r)}$ be the $[n', R_p n']$ and $[n, R_r n]$ linear inner code sequences chosen for the two encoding procedures, respectively, and assume each has average error probability approaching zero as $n \to \infty$. Let $(\mathbf{u}, \mathbf{v})$ be the shared randomness for $(f_{r,\mathbf{u},\mathbf{v}}, \phi_{r,\mathbf{u},\mathbf{v}})$, chosen uniformly at random from $\mathbb{F}_2^{\ell} \times \mathbb{F}_2^{\ell}$, where ℓ is such that $\ell = o(R_r n)$ and $\ell = \omega(log(R_r n))$.*

Let $j \in [2^{2\ell}]$ correspond to $[\mathbf{u} \| \mathbf{v}] \in \mathbb{F}_2^{2\ell}$. Then, the code described by $[f_p(j) \| f_{r,\mathbf{u},\mathbf{v}}(i)]$ has rate approaching R_r and error probability approaching zero as block length goes to infinity.

Proof. Let $\mathbf{y}_j$ be the channel output of the first portion of the transmitted word, corresponding to input $f_p(j)$, and $\mathbf{y}_i$ the output of the second portion, corresponding to input $f_{r,\mathbf{u},\mathbf{v}}(i)$. First decode $\mathbf{y}_j$ according to ϕ_p. If the decoder outputs "0" (i.e. detects adversarial interference), output 0. Otherwise, decode $\mathbf{y}_i$ according to $\phi_{r,\hat{\mathbf{u}},\hat{\mathbf{v}}}$, where $[\hat{\mathbf{u}} \| \hat{\mathbf{v}}]$ corresponds to the output message $\hat{j}$ of ϕ_p.

By Theorem III.5, the first decoder succeeds with probability at least $1 - \max\{P_e(C_{4\ell/R_p}^{(p)}), \frac{2}{2^{2\ell}}\}$ (notice here that the message length of the positive-rate code is 2ℓ, the required shared randomness of the code $(f_{r,\mathbf{u},\mathbf{v}}, \phi_{r,\mathbf{u},\mathbf{v}})$). Given that this code is successful, the code $f_{r,\mathbf{u},\mathbf{v}}$ succeeds with probability at least $1 - \max\{P_e(C_n^{(r)}), \frac{R_r n - \ell}{2^\ell}\}$ by Theorem III.6. In all, the probability of success is bounded below by the product of these. As $n \to \infty$, $\ell \to \infty$, and the probability of success converges to 1 given our assumptions on the asymptotic growth of ℓ.

The rate of the code is given by $R = (R_r n - \ell)/(n + \frac{4\ell}{R_p})$. Since $\ell = o(R_r n)$, as $n \to \infty$, $R \to R_r$. □

Remark III.8. *Observe that the decoding complexity of this scheme is bounded above by the sum of the decoding complexities of the chosen linear inner codes, and the complexities of three polynomial calculations in $\mathbb{F}_{2^\ell}$ (to verify the message-hash vectors in the codes of Sections III-A and III-B). The asymptotic rate R_r of this scheme is derived from the rate of the linear code used in constructing the randomized code in Section III-B. Since capacity-achieving linear codes exist for the underlying symmetric channel, the capacity of our scheme can approach the non-adversarial capacity.*

IV. Conclusions

We presented a structured coding scheme utilizing linear codes for authentication over binary-input, symmetric adversarial channels. This strategy allows for coding rates up to the non-adversarial capacity of the underlying channel, and for bounded-complexity decoding. Expanding our work to a broader class of adversarial channels is ongoing work.

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] 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.

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

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

[5] 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.

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

[7] V. Guruswami and A. Smith, "Codes for computationally simple channels: Explicit constructions with optimal rate," in *2010 IEEE 51st Annual Symp. on Found. of Computer Science*, 2010, pp. 723–732.

[8] J. L. Massey, "Applied digital information theory," *Lecture notes*, vol. 19, 1998.

[9] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. on Inf. Theory*, vol. 47, no. 2, pp. 599–618, 2001.

[10] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. on Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[11] D. S. Dummit and R. M. Foote, *Abstract Algebra*. Wiley Hoboken, 2004, vol. 3.

[12] P. Tian, S. Jaggi, M. Bakshi, and O. Kosut, "Arbitrarily varying networks: Capacity-achieving computationally efficient codes," in *2016 IEEE Int'l Symp. on Inf. Theory (ISIT)*, July 2016, pp. 2139–2143.