Abstract—We study communication in the presence of a jamming adversary where quadratic power constraints are imposed on the transmitter and the jammer. The jamming signal is assumed to be a function of the codebook, and a noncausal but noisy observation of the transmitted codeword. For a certain range of the noise-to-signal ratios (NSRs) of the transmitter and the jammer, we are able to characterize the capacity of this channel under deterministic encoding. For the remaining NSR regimes, we determine the capacity under the assumption of a small amount of common randomness (at most $\tilde{O}(\log(n))$ bits in one sub-regime, and at most $\tilde{O}(n)$ bits in the other sub-regime) available to the encoder-decoder pair. Our proof techniques include a novel myopic list-decoding result for achievability and a Plotkin-type push attack for the converse in a subregion of the NSRs, which may be of independent interest.

A short video explaining our work is available at: https://youtu.be/0015_W_xhLM.

I. INTRODUCTION AND PRIOR WORK

Consider a point-to-point communication system where a transmitter, Alice, wants to send a message to a receiver, Bob, through a channel distorted by additive noise. She does so by encoding the message to a length-$n$ codeword, which is fed into the channel. The transmitted codeword is distorted by noise. Much of traditional communication and information theory has focussed on the scenario where the noise is independent of the transmitted signal and the coding scheme. We study the case where communication takes place in the presence of a malicious jammer (whom we call James) who tries to ensure that Bob is unable to recover the transmitted message. The channel is a discrete-time, real-alphabet channel, and the codeword transmitted by Alice is required to satisfy a quadratic power constraint. It is assumed that the coding scheme is known to all three parties, and James also observes a noisy version of the transmitted signal (hence the term myopic). The jamming signal is required to satisfy a separate power constraint, but otherwise can be a noncausal function of the noisy observation and the coding scheme.

This problem is part of the general framework of arbitrarily varying channels (AVCs), introduced by Blackwell et al. [1]. The quadratically constrained AVC (also called the Gaussian AVC) was studied in [2], which gave upper and lower bounds on the capacity of the channel under the assumption that James observes a noiseless version of the transmitted codeword (a.k.a. the omniscient adversary). This is closely related to the sphere-packing problem where the objective is to find the densest arrangement of identical $n$-dimensional balls of radius $\sqrt{\frac{n}{N}}$ subject to the constraint that the center of each ball lies within a ball of radius $\sqrt{nP}$. An exact characterization of the capacity of this problem is not known, though inner [2] and outer bounds [3], [4] are known. At the other end of the spectrum, [5], and later [6], studied the problem with an “oblivious” James who knows the codebook but does not see the transmitted codeword. They showed that if private randomness is available at the encoder, the capacity of the oblivious adversarial channel is equal to that of an additive white Gaussian noise (AWGN) channel (where the noise variance is equal to the power constraint imposed on James). If there is no common randomness, then the capacity exhibits a phase transition: It is equal to that of the corresponding AWGN channel for $N < P$, but 0 for $N \geq P$. These omniscient and oblivious cases are two extreme instances of the general myopic adversary that we study in this paper.

The work closest to that in this paper is by Sarwate [7], who characterized the capacity of this channel under the assumption that James knows a noisy version of the transmitted signal, but Alice’s codebook is shared only with Bob. This can be interpreted as a myopic channel with an unlimited amount of common randomness (or shared secret key) between Alice and Bob. A related model was studied in [8], where it was assumed that James knows the message, but not the exact codeword transmitted. In this setup, Alice has access to private randomness, but Alice and Bob do not share any common randomness. Game-theoretic versions of the problems have also been considered in the literature, notably by [9], [10], [11].

Communication in the presence of a myopic jammer has been studied in the discrete-alphabet case (see [12] and references therein). We would like to draw connections to the bit-flip adversarial problem where communication takes place over a binary channel, and James observes the codeword through a binary symmetric channel (BSC) with crossover probability $q$. He is allowed to flip at most $np$ bits, where $0 < p < 1/2$. Dey et al. [12] showed that when James is sufficiently myopic, i.e., $q > p$, the capacity is equal to $1 - H(p)$. In other words, he can do no more damage than an oblivious adversary. However, we observe that in the

Quadratically Constrained Myopic Adversarial Channels

Yihan Zhang*, Shashank Vatedka*, Sidharth Jaggi* and Anand D. Sarwate†

*Dept. of Information Engineering, The Chinese University of Hong Kong
†Dept. of Electrical and Computer Engineering, Rutgers, The State University of New Jersey

978-1-5386-4780-6/18/$31.00©2018 IEEE 611
quadratically constrained case, the capacity is always strictly less than the oblivious capacity.

![Diagram](image)

**Fig. 1:** The setup studied in this paper.

Let us formally describe the problem. The setup is illustrated in Fig. 1. Alice wants to send a message \( m \) to Bob. The message is assumed to be uniformly chosen from \( \{0, 1\}^n R \), where \( R > 0 \) is a parameter called the rate. Alice and Bob additionally have \( n_{\text{key}} \) bits of shared secret key, \( k \). This key is kept private from James. Alice encodes the message \( m \) (using \( k \)) to a codeword \( \tilde{x} \in \mathbb{R}^n \), which is transmitted across the channel. Let \( C \) denote the set of all possible codewords (the codebook). Due to potential randomness at the encoder either privately known only to the encoder (stochastic encoding) or shared secretly with the decoder (randomized encoding), the codebook rate \( R_{\text{code}} = \frac{1}{n} \log |C| \) could be different from the message rate \( R \) (which we sometimes simply refer to as the rate). The codebook must satisfy a power constraint of \( P > 0 \), i.e. \( \| z \|_2^2 \leq \sqrt{n} P \) for all \( z \in C \). James sees \( z = x + s_z \), where \( s_z \) is additive white Gaussian noise (AWGN) with mean zero and variance \( \sigma^2 \). He chooses a jamming vector \( s_y \in \mathbb{R}^n \) as a noncausal function of \( z \), the codebook \( C \), and private randomness. The jamming vector is also subject to a power constraint: \( \| s_y \|_2^2 \leq \sqrt{n} N \) for some \( N > 0 \). Bob obtains \( y = x + s_y \) and decodes this to a message \( \hat{m} \). The message is said to have been conveyed reliably if \( \hat{m} = m \). The probability of error, \( P_e \), is defined as the probability that \( \hat{m} \neq m \), where the randomness is over \( s_y \), the key \( k \), and the private random bits available to James. In all our codebook constructions, we will assume that Alice and Bob may share common randomness (kept secret from James), but the mapping from \((m, k)\) to \( x \) is deterministic. In other words, Alice does not possess any source of additional private randomness. Conversely, all our impossibility results are robust to the presence of private randomness at the encoder (since in some AVC scenarios, private randomness is known to boost capacity — e.g. [13]).

We will study the problem with different amounts of common randomness shared by Alice and Bob and unknown to James, and present results in each case.

We say that a rate \( R > 0 \) is achievable if there exists a sequence of codebooks of rate \( R_n \geq R \) for which \( P_e \rightarrow 0 \) as \( n \rightarrow \infty \). The supremum of all achievable rates is called the capacity of the channel.

II. CONTRIBUTIONS

In this article, we derive results for three different regimes of common randomness: (1) \( n_{\text{key}} = \Theta(n) \), (2) \( n_{\text{key}} = \Theta(\log n) \), and (3) \( n_{\text{key}} = 0 \). Due to space constraints, proofs and other technical details have been consigned to an extended version [14].

We prove a general result for list-decoding in presence of a myopic adversary. For an omniscient adversary, the list-decoding capacity is \(^1\)

\[
R_{\text{LD}} = \frac{1}{2} \log \left( \frac{(P + \sigma^2)(P + N) - 2P\sigma^2}{N\sigma^2} \right) > R_{\text{LD}}
\]

in a certain regime (depending on \( n_{\text{key}} \)) where \( \sigma^2 / P > P / N - 1 \). The achievable rates are illustrated in Fig. 2. With no common randomness, we can achieve \( R_{\text{LD}} \) and \( R_{\text{LD, myop}} \) in the red and blue regions of Fig. 2a respectively. If \( n_{\text{key}} = \Omega(n) \), then \( R_{\text{LD, myop}} \) is achievable in a larger region (e.g., Fig. 2b).

For \( n_{\text{key}} = \Omega(\log n) \), we combine our list-decoding result with [15, Lemma 2] to give achievable rates for reliable communication over the myopic adversarial channel. Suppose that \( n_{\text{key}} = nR \) for some \( R \) > 0. If \( R \geq \frac{1}{2} \log \left( 1 + \frac{P}{N} \right) - R_{\text{LD, myop}} \), then we are able to give a complete characterization of the capacity of the channel for all values of the NSRs. If \( R_{\text{key}} < \frac{1}{2} \log \left( 1 + \frac{P}{N} \right) - R_{\text{LD, myop}} \), then we are able to characterize the capacity in only a sub-region of the NSRs. This is illustrated in Fig. 3.

For \( n_{\text{key}} = \Theta(\log n) \) case, we are able to find the capacity in the red and blue regions in Fig. 4. In the dotted regions, we have nonmatching upper and lower bounds.

For \( n_{\text{key}} = 0 \), we require a different technique to find the capacity. Our results are illustrated in Fig. 5.

We show that if James is omniscient, then private randomness at the encoder does not help improve the capacity. This is based on a similar observation made in [13] for the bit-flip adversarial channel.

The variation of the regions of the noise-to-signal ratios (NSR) where we can obtain achievable rates is illustrated in Fig. 6. As seen in the figure, even \( \Theta(\log n) \) bits of common randomness is sufficient to ensure that the red and blue regions are expanded. An additional \( \Theta(n) \) bits can be used to expand the blue region even further, eventually covering the entire dotted region.

A. Novel proof techniques

Here we highlight the two most important proof techniques we introduce in our work.

1) Myopic list decoding: This is a central idea in our achievability proofs, and a novel contribution of this work. The broad idea is to show that James is unable to uniquely recover the transmitted codeword. We show that conditioned on \( z \), the transmitted codeword lies in a strip on the sphere of radius \( \sqrt{n}P \), approximately at a distance \( \sqrt{n\sigma^2} \) from \( z \). If

\(^1\)This is a folklore result. See, e.g., [14, Appendix B] for a proof.
the codebook rate exceeds \( \frac{1}{2} \log \left( 1 + \frac{P}{\sigma^2} \right) \), then this strip will contain exponentially many codewords. All these codewords are roughly at the same distance from \( \mathbf{z} \) and are therefore nearly indistinguishable from the one actually transmitted. Due to the confusion, no attack strategy by James is as bad as the one he could instantiate in the omniscient case. We study the list-decoding problem, where instead of recovering the transmitted message uniquely, Bob tries to output a poly\((n)\) sized list that includes the transmitted codeword. Since James is myopic, we could hope to achieve rates greater than the omniscient list-decoding capacity \( R_{LD} \). Even with \( n_{\text{key}} = 0 \), we can achieve a higher rate, equal to \( R_{LD,\text{myop}} \), in the blue region in Fig. 2a. The blue region can be expanded with a larger amount of common randomness, as seen in Fig. 2b.

2) Plotkin push attack/\( \mathbf{z} \)-aware symmetrization attack: The \( \mathbf{z} \)-aware symmetrization attack is a converse technique we use to show that the capacity is zero whenever \( n_{\text{key}} = 0 \) and \( \frac{\sigma^2}{P} < 4N/P - 2 \), and is inspired by a technique used to prove the Plotkin bound for bit-flip channels. We fix a strategy for James and analyse the resulting probability of error. James picks a codeword \( \mathbf{x} \) from Alice’s codebook uniformly at random and independently of \( \mathbf{z} \). He transmits \( (\mathbf{x} - \mathbf{z})/2 \) — since \( \mathbf{z} = \mathbf{x} + \mathbf{s}_\mathbf{z} \) for some vector \( \mathbf{s}_\mathbf{z} \) with \( N(0, \sigma^2) \) components, therefore Bob receives \( (\mathbf{x} + \mathbf{x}' - \mathbf{s}_\mathbf{z})/2 \). If \( \mathbf{x} \neq \mathbf{x}' \), then Bob makes a decoding error with nonvanishing probability. The \( \mathbf{z} \)-aware attack is novel in the context of myopic channels, but is also inspired by similar ideas in [16].
III. CAPACITY WHEN $n_{\text{key}} = \infty$

Define $R_{\text{LD,myop}} := \frac{1}{2} \log \left( \frac{P (P + \sigma^2) (P + N - 2 P \sqrt{N (P + \sigma^2)})}{N \sigma^2} \right)$.

Sarwate [7] showed the following:

**Lemma III.1** ([7]). The capacity of the myopic adversarial channel with an unlimited amount of common randomness is

$$C = \begin{cases} R_{\text{LD}} := \frac{1}{2} \log \frac{P}{N}, & \frac{\sigma^2}{P} \leq \frac{1}{N \sqrt{P}} - 1 \\ R_{\text{LD,myop}}, & \frac{\sigma^2}{P} \geq \max \left\{ \frac{1}{N \sqrt{P}} - 1, \frac{N}{P} - 1 \right\} \\ 0, & \frac{\sigma^2}{P} \leq \frac{N}{P} - 1 \end{cases}$$

We now give a formal description of our results.

IV. LINEAR AND LOGARITHMIC AMOUNTS OF COMMON RANDOMNESS

We discuss two possibilities: (1) $n_{\text{key}}$ is $\Theta(n)$, and (2) $n_{\text{key}}$ is $\Theta(\log n)$. The rate given by Lemma III.1 is an upper bound on the capacity for all values of $n_{\text{key}}$. We will show that this is achievable in a subregion of the NSRs.

A. List decoding

Consider the channel model in Fig. 1. In the list-decoding problem, the decoder is not required to recover the transmitted message exactly but instead output a (small) list of messages with the guarantee that the true message is in the list. We are typically interested in list sizes that are constant or grow as a low degree polynomial function of the blocklength.

**Definition IV.1.** Fix $R > 0$ and $n_{\text{key}} \geq 0$. A codebook $C = \{ x(m, k) : 1 \leq m \leq 2^n R, 1 \leq k \leq 2^{n_{\text{key}}(m)} \}$ is said to be $(P, N, L)$-list decodable at rate $R$ with $n_{\text{key}}$ bits of common randomness if

- $|x(m, k)|_2 \leq \sqrt{n P}$ for all $m, k$;
- for all possible randomized functions $s := s(C, z)$ satisfying
  $$P(\{ |s|_2 \leq \sqrt{n N} \} = 1, we have$$
  $$P(\{ B_{\{x, s\}} \cap C(k) > L \}) = o(1),$$

where $C(k) := \{ x(m, k) : 1 \leq m \leq 2^n R \}$. Here, the averaging is over the randomness in $\{ m, k, s \}$ and $z$. A rate $R$ is said to be achievable for $(P, N, L)$-list-decoding with $n_{\text{key}}$ bits of common randomness if $\exists$ sequences of codebooks (in increasing $n$) that are $(P, N, L)$-list decodable. The list-decoding capacity is the supremum over all achievable rates.

With an omniscient adversary ($\sigma = 0$) and $n_{\text{key}} = 0$, the capacity for $(P, N, O(\text{poly}(n)))$-list-decoding is equal to $R_{\text{LD}}$. (see [14, Appendix B] for a proof).

We now assume that $n_{\text{key}} = n R_{\text{key}}$, for some $R_{\text{key}} \geq 0$.

**Theorem IV.2.** Fix $\sigma > 0$. For $(P, N, O(n^3))$-list-decoding, the capacity is lower bounded as follows

$$C_{\text{LD,myop}} = \begin{cases} R_{\text{LD,myop}} = 1, & \frac{\sigma^2}{P} \geq \max \left\{ \frac{1}{N \sqrt{P}} - 1, \frac{N}{P} - 1 \right\} \\ R_{\text{LD,myop}} + R_{\text{key}} \geq \frac{1}{2} \log \left( 1 + \frac{P}{\sigma^2} \right), & \text{otherwise}. \end{cases}$$

These are summarized in Fig. 2.

The rate $R_{\text{LD}}$ is achievable even in presence of an omniscient adversary. The main contribution of this work is in showing that myopicity indeed does help, and we can obtain a higher rate of $R_{\text{LD,myop}}$ in a certain regime. It is interesting to note that even when $n_{\text{key}} = 0$, the myopic list decoding capacity is nonzero for $N > P$ and sufficiently large values of $\sigma^2/P$. Furthermore, increasing $R_{\text{key}}$ helps us achieve higher list-decoding rates as seen in Fig. 2.

Note that we are using an average probability of error in our work. This is different from a maximum probability of error, where the list size is required to be less than or equal to $L$ for every codeword. On the other hand, we are satisfied with this being true for all but a vanishingly small fraction of the codewords.
B. Achievable rate using $\Theta(n)$ bits of CR

Sarwate [15, Lemma 2] (originally proved by Langberg [17] for the bit-flip channel) showed that a list-decodable code can be converted to a uniquely decodable code with an additional $n_k = 2 \log(nL)$ bits of common randomness. If $L = n^{\Omega(1)}$, then the $n_k$ required is only logarithmic. We can therefore use this with Theorem IV.2 to obtain achievable rates. Combining this with the converse in [7],

\textbf{Lemma IV.3.} If Alice and Bob share $nR_{\text{key}}$ bits of common randomness, then the capacity is

\[
C = \begin{cases} 
R_{\text{LD,myop}}, & \text{if } \frac{\sigma^2}{P} \geq \max \left\{ \frac{1}{N_1^2 P}, \frac{N_1}{N_2^2 P} - 1 \right\} \\
R_{\text{LD}}, & \text{and } R_{\text{key}} > \frac{1}{2} \log (1 + \frac{P}{\sigma^2}) - R_{\text{LD,myop}} \\
0, & \frac{\sigma^2}{P} \leq \frac{1}{N_1^2 P} - 1
\end{cases}
\]

Furthermore, $R_{\text{LD}} \leq C \leq R_{\text{LD,myop}}$ if $\frac{\sigma^2}{P} \geq \max \left\{ \frac{1}{N_1^2 P}, \frac{N_1}{N_2^2 P} - 1 \right\}$ and $R_{\text{key}} < \frac{1}{2} \log (1 + \frac{P}{\sigma^2}) - R_{\text{LD,myop}}$. These results are pictorially summarized in Fig. 3.

Since $\Theta(\log n)$ bits are sufficient to distinguish the list, Theorem IV.2 for $R_{\text{key}} = 0$ gives us a result with $n_{\text{key}} = \Theta(\log n)$. Note that when $R_{\text{key}} = 0$, the condition $R_{\text{LD,myop}} + R_{\text{key}} > \frac{1}{2} \log (1 + \frac{P}{\sigma^2})$ reduces to $\frac{\sigma^2}{P} \geq 4 \frac{N_1}{N_2^2 P} - 1$.

\textbf{Lemma IV.4.} When $n_{\text{key}} = \Theta(\log n)$, the capacity of the myopic adversarial channel is:

\[
C = \begin{cases} 
R_{\text{LD,myop}}, & \text{if } \frac{\sigma^2}{P} \geq \max \left\{ \frac{1}{N_1^2 P}, 1 + \frac{N_1}{N_2^2 P} - 1 \right\} \\
R_{\text{LD}}, & \geq \frac{\sigma^2}{P} \leq \frac{1}{N_1^2 P} - 1 \\
0, & \text{or } \frac{\sigma^2}{P} \leq \frac{1}{N_1^2 P} - 1
\end{cases}
\]

Furthermore, $R_{\text{LD}} \leq C \leq R_{\text{LD,myop}}$ if $\max \left\{ \frac{1}{N_1^2 P}, \frac{N_1}{N_2^2 P} - 1 \right\} \leq \frac{\sigma^2}{P} \leq \frac{N_1}{N_2^2 P} - 1$. These results are summarized in Fig. 4.

V. NO COMMON RANDOMNESS

When Alice and Bob do not have access to a shared secret key, the achievable schemes above are not valid, and in some regions, tighter converses can be obtained. We have an improved converse using symmetrization arguments for the regimes $\frac{\sigma^2}{P} \leq 4 \frac{N_1}{N_2^2 P} - 2$ and $\frac{\sigma^2}{P} \geq 1$. For the other regimes, we use the converse in [7]. The techniques used to prove Lemmas IV.3 and IV.4 are not sufficient to prove the achievability part. This requires a different approach, and involves list-decoding, reverse list-decoding, and a “grid argument”. These ideas were introduced for the discrete case in [12]. Adapting these arguments for continuous channels involve a more careful handling of several error events and covering arguments. However, the ideas in [12] do not let us achieve rates higher than $R_{\text{LD}}$. To obtain improvements in the blue region, we need the ideas of myopic list decoding introduced in this paper. We are able to show the following.

\textbf{Theorem V.1.} The capacity of the myopic adversarial channel with no common randomness is given by

\[
C = \begin{cases} 
R_{\text{LD}}, & \text{if } \frac{1}{N_1^2 P} - 1 \leq \frac{\sigma^2}{P} \leq \frac{1}{N_1^2 P} - 1 \\
R_{\text{LD,myop}}, & \text{if } \frac{\sigma^2}{P} \geq \max \left\{ \frac{1}{N_1^2 P} - 1, \frac{N_1}{N_2^2 P} - 1 \right\} \\
0, & \text{if } \frac{\sigma^2}{P} \leq 4 \frac{N_1}{N_2^2 P} - 2 \text{ or } \frac{\sigma^2}{P} \geq 1
\end{cases}
\]

In the other regimes, we have

\[
R_{\text{LD}} \leq C \leq \begin{cases} 
R_{\text{LD}}, & \text{if } \frac{4 N_1}{N_2^2 P} - 2 \leq \frac{\sigma^2}{P} \leq \min \left\{ \frac{1}{N_1^2 P} - 1, \frac{N_1}{N_2^2 P} - 1 \right\} \\
R_{\text{LD,myop}}, & \text{if } \max \left\{ \frac{1}{N_1^2 P} - 1, \frac{N_1}{N_2^2 P} - 2 \right\} \leq \frac{\sigma^2}{P} \leq \frac{1}{N_1^2 P} - 1 \text{ and } \frac{N_1}{N_2^2 P} \leq 1
\end{cases}
\]

In summary, we are able to give a complete characterization of the capacity for certain values of the NSRs. The region where we can fully solve the problem expands with the amount of common randomness, and we can find the capacity for all values of the NSRs if $n_{\text{key}} = \Omega(n)$. Closing the gaps between the inner and outer bounds for smaller $n_{\text{key}}$ is ongoing work.

\textbf{REFERENCES}

[1] D. Blackwell, L. Breiman, and A. J. Thomasian, “The capacity of a class of channels under random coding,” Ann. Math. Statist., vol. 31, no. 3, pp. 558–567, 1960.

[2] N. Blachman, “On the capacity of bandlimited channel perturbed by statistically dependent interference,” IRE Trans. Inf. Theory, vol. 8, pp. 48–55, 1962.

[3] G. A. Kabatiansky and V. I. Levenshtein, “On bounds for packings on a sphere and in space,” Probl. Pered. Informatsi, vol. 14, no. 1, pp. 3–23, 1978.

[4] H. Cohn and Y. Zhao, “Sphere packing bounds via spherical codes,” Duke Math. J., vol. 163, no. 10, pp. 1965–2002, 2014.

[5] B. Hughes and P. Narayan, “Gaussian arbitrarily varying channels,” IEEE Trans. Inf. Theory, vol. 33, pp. 267–284, 1987.

[6] J. Csiszár and P. Narayan, “Capacity of the Gaussian arbitrarily varying channel,” IEEE Trans. Inf. Theory, vol. 37, pp. 18–26, 1991.

[7] A. Sarwate, “An AVC perspective on correlated jamming,” in Proc. IEEE Int. Conf. Signal Proc. and Comm., Bangalore, India, 2012.

[8] F. Haddadpour, M. Siavoshani, M. Bakshi, and S. Jaggi, “On AVCs with quadratic constraints,” IEEE Int. Symp. Inf. Theory, 2013.

[9] M. Mêdard, “Capacity of correlated jamming channels,” in Proc. Allerton Annual Conf. on Comm., Control and Computing, Allerton, USA, 1997.

[10] S. Shafi and S. Ulukus, “Mutual information games in multi-user channels with correlated jamming,” IEEE Int. Symp. Inf. Theory, vol. 55, pp. 4598–4607, 2009.

[11] C. Baker and I.-F. Chao, “Information capacity of channels with partially unknown noise,” J. Appl. Math., vol. 56, pp. 946–963, 1996.

[12] B. K. Dey, S. Jaggi, and M. Langberg, “Sufficiently myopic adversaries are blind,” in IEEE Int. Symp. Inf. Theory, 2015, pp. 1164–1168. [Online]. Available: https://arxiv.org/abs/1610.01287

[13] B. K. Dey, S. Jaggi, M. Langberg, and A. D. Sarwate, “The benefit of a 1-bit jump-start, and the necessity of stochastic encoding, in jamming channels,” Tech. Rep., February 2016. [Online]. Available: http://arxiv.org/abs/1602.02384

[14] Y. Zhang, S. Vatedka, S. Jaggi, and A. Sarwate, “Quadratically constrained myopic adversarial channels,” 2018. [Online]. Available: https://arxiv.org/abs/1801.05951

[15] A. D. Sarwate and M. Gastpar, “Rateless codes for AVC models,” IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3105–3114, July 2010.

[16] T. Li and S. Jaggi, “Quadratically constrained channels with causal adversaries,” submitted, ISIT 2018.

[17] M. Langberg, “Private codes or succinct random codes that are (almost) perfect,” in Proc. IEEE Symp. Found. Comp. Sci., Rome, Italy, 2004.