The Gap to Practical MIMO Wiretap Codes

Anatoly Khina
EE Dept., CalTech
Pasadena, CA
Email: khina@caltech.edu

Yuval Kochman
School of CSE, HUJI
Jerusalem, Israel
Email: yuvalko@cs.huji.ac.il

Ashish Khisti
ECE Dept., U. of Toronto
Toronto, ON M5S 3G4, Canada
Email: akhisti@comm.utoronto.ca

The wiretap channel (WTC), introduced by Wyner [1], is composed of a sender ("Alice") who wishes to convey data to a legitimate user ("Bob"), such that the eavesdropper ("Eve") cannot recover any information of this data. In the multiple-input multiple-output (MIMO) Gaussian WTC, Alice is connected to Bob and Eve bi a MIMO broadcast channel. The capacity of this channel was found in [2]–[4].

Although the capacity of WTCs is well understood, construction of practical codes is still a challange. For the scalar Gaussian case, various approaches have been suggested. The recent work of Tyagi and Vardy in [5] is particularly appealing, since it uses a black-box approach: it takes any code that is good for the ordinary (non-secrecy) AWGN channel, and turns it into a good wiretap code using a hashing procedure.

However, assuming that we have such a code for the scalar case, how do we extend it to the vector case? Do we need to construct different codes for every channel matrix? In [6] we have presented a scheme based on scalar random-binning wiretap codes, in conjunction with a linear encoder and a successive interference cancellation (SIC) decoder, which approaches the MIMO wiretap capacity. In fact, it can be described as a variant of VBLAST/GDFE schemes, used in MIMO communication without secrecy [7], [8]. Interestingly, the proof that Eve cannot extract information also hinges on the optimality of the SIC procedure, this time in a "genie-aided" setting: after Eve extracts all possible information from a stream, the content of that stream is revealed to her for the sake of trying to decode the next streams.

Given the optimal SIC scheme for the MIMO WTC, it is natural to consider an explicit code construction, where the random-binning codes are replaced by ordinary AWGN codes, combined with some structured binning procedure, e.g. the hashing of [5]. Indeed, in [9] we have pursued this idea. The key point is that, as with random-binning codes, when any good set of codes is used, a "genie-aided" Eve cannot do better than follow a SIC process. Since at any stage of a SIC decoding process, the decoder sees a multiple-access channel (MAC) where the inputs are the streams that are not decoded yet, the optimality of the scheme is intimately related to that of a scheme for the MAC WTC [10]. However, the construction of good MAC WTC codes is also not immediate.

Even without secrecy, not any collection of good AWGN codes is good for any Gaussian MAC, see e.g. [11]: if the codebooks have structure (as they should, in a practical construction), the signal resulting from one codebook may not look as noise in the process of decoding the other, as for some channel coefficients the codes may align. This compromises MAC decoding, whose optimality is needed both for the "Bob" and "Eve" parts of the secrecy proofs. This effect can be circumvented by a dithering process, which makes sure that codewords play the part of "independent noise" when decoding a different codebook. We thus define a class of MAC WTC codes that have both good individual secrecy properties, and mutual independence; such codebook sets can be obtained from any set of good AWGN codebooks by a two-stage process of hashing and then dithering. However, this still does not yield a practical code construction, as dithering, which must be performed modulo a shaping region to retain optimality, inflicts decoding complexity that may be higher than that of the original code. Thus, in order to obtain a practical construction, we need to find a "simpler" procedure to perturb any given set of codebooks, such that the resulting codes are good for the MAC WTC. It is worth noting, that such a construction will also be theoretically significant in communication without secrecy constraints, as the problem of alignment already arises in VBLAST/GDFR schemes.

References

[1] A. D. Wyner, "The wiretap channel," *IEEE Trans. Info. Theory*, vol. 54, pp. 1355–1387, 1975.

[2] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," *IEEE Trans. Info. Theory*, vol. 56, pp. 5515–5532, 2010.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Info. Theory*, vol. 57, pp. 4961–4972, 2011.

[4] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Info. Theory*, vol. 55, pp. 2547–2553, 2009.

[5] H. Tyagi and A. Vardy, "Explicit capacity-achieving coding scheme for the Gaussian wiretap channel," in *ISIT*, Honolulu, HI, USA, June/July 2014.

[6] A. Khina, Y. Kochman, and A. Khisti, "Decomposing the MIMO wiretap channel," in *ISIT*, Honolulu, HI, USA, June/July 2014.

[7] P. W. Wolniansky, G. J. Foschini, G. D. Golden, and R. A. Valenzuela, "V-BLAST: an architecture for realizing very high data rates over the rich-scattering wireless channel," in *Proc. URSI Int. Symp. Sig., Sys., Elect. (ISSSE)*, Sep./Oct. 1998, pp. 295–300.

[8] J. M. Cioffi and G. D. Forney Jr., "Generalized decision-feedback equalization for packet transmission with ISI and Gaussian noise," in *Comm., Comp., Cont. and Sig. Proc.*, 1997, pp. 79–127.

[9] A. Khina, Y. Kochman, and A. Khisti, "From ordinary AWGN codes to optimal MIMO wiretap schemes," in *ITW*, Hobart, Tasmania, Australia, Oct./Nov. 2014.

[10] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Info. Theory*, vol. 54, pp. 5747–5755, 2008.

[11] F. Baccelli, A. El Gamal, and D. N. C. Tse, "Interference networks with point-to-point codes," *IEEE Trans. Info. Theory*, pp. 2582–2596, 2011.