Physical layer insecurity

Muriel Médard
Research Laboratory for Electronics
Massachusetts Institute of Technology
Cambridge, USA
medard@mit.edu

Ken R. Duffy
Hamilton Institute
Maynooth University
Maynooth, Ireland
ken.duffy@mu.ie

Abstract—In the classic wiretap model, Alice wishes to reliably communicate to Bob without being overheard by Eve who is eavesdropping over a degraded channel. Systems for achieving that physical layer security often rely on an error correction code whose rate is below the Shannon capacity of Alice and Bob's channel, so Bob can reliably decode, but above Alice and Eve's, so Eve cannot reliably decode. For the finite block length regime, several metrics have been proposed to characterise information leakage. Here we reassess a metric, the success exponent, and demonstrate it can be operationalized through the use of Guessing Random Additive Noise Decoding (GRAND) to compromise the physical-layer security of any moderate length code.

Success exponents are the natural beyond-capacity analogue of error exponents that characterise the probability that a maximum likelihood decoding is correct when the code-rate is above Shannon capacity, which is exponentially decaying in the code-length. In the finite blocklength regime, success exponents can be used to approximately evaluate the frequency with which Eve's decoding is correct in beyond-capacity channel conditions. Through the use of GRAND, we demonstrate that Eve can constrain her decoding procedure through a query-number threshold so that when she does identify a decoding, it is correct with high likelihood, significantly compromising Alice and Bob's communication by truthfully revealing a proportion of it.

We provide general mathematical expressions for the determination of success exponents in channels that can have temporally correlated noise as well as for the evaluation of Eve's query number threshold, using the binary symmetric channel as a worked example. As GRAND algorithms are code-book agnostic and can decode any code structure, we provide empirical results for Random Linear Codes as exemplars. Simulation results mimic the mathematical predictions, demonstrating the practical possibility of compromising physical layer security.

I. INTRODUCTION

Since Wyner's classic considerations [1], [2], [3], [4], there has been a rich literature on the topic of wiretap channels and associated codes [5], [6]. In particular, much of the work on physical layer security has relied on the premise of exploiting the difference in signal to noise ratio between the sender, Alice, and the intended receiver, Bob, and the pair formed by Alice and the eavesdropper, Eve. In the limit of long codes, the additional noise that Eve experiences can be transformed into an effect that acts like a partial one-time pad, obstructing Eve's attempts to decode. The premise behind operational proposals is the design of codes [7], [8], [9] that are decodable by Bob under lighter noise but not by Eve under heavier noise.

A natural question concerns the case when codes are not in the infinite limit setting and so concentration to the mean is no longer achieved with high probability, with short wiretap code constructions, of lengths of order 16, have gained attention [10], [11], [12].

As Bob seeks to have reliable communication with Alice, the relevant concern is to limit the cases where he decodes in error. For such events, there is a wealth of techniques to bound their probability, for example error exponents [13], [14], [15], [16], [17], [18]. For shorter codes, dispersion approximations and other considerations have been proposed [19], [20], [21].

For wiretap settings, both error exponents [22], [23], [24], [25], [26], as well as dispersion bounds and related finite blocklength analysis techniques [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [23] have been considered in the context of eavesdroppers. From the point of view of Eve, however, the security consideration is altogether different from reliable communication. Concern lies in the events where Eve is able to decode because the noise realization is advantageous as any successful decoding represents a failure of security [38].

We show in this paper that the success probability of Eve is an informative metric. While transmissions above capacity cannot all be decoded reliably, it does not mean that they are all decoded with probability near zero. Moreover, for a range of rates above capacity, we demonstrate that Eve can identify decodings that she is confident are not in error, compromising the security of Alice and Bob's communication.

In the context of developing Guessing Random Additive Noise Decoding (GRAND), Proposition 1 of [39] establishes success exponents, where the probability that a maximum likelihood decoder successfully decodes given the code-rate is above capacity decays exponentially in block-length [40], [41], for channels whose noise can have temporal correlation. These can be used to generate an estimate of the likelihood that Eve can correctly decode beyond capacity. Theorem 3 of [39] gives an additional result that provides Eve with a simple criterion to test whether she is confident in the proposed decoding. That is, not only can Eve decode correctly a fraction of the time, she can identify which decodings are likely to be correct.

In this paper, we explore Eve's ability to confidently and correctly decode moderate length codes acting beyond Shannon capacity when she uses GRAND. We consider random linear codes (RLCs), which achieve secrecy capacity in the case where the channel from Alice to Bob and the channel from Alice to Eve are both BSCs [42] and which have been previously considered for use in the wiretap channel setting

[22].

We note that while Bob generally seeks to be efficient in order to have a timely decoding for a well operating communications channel, Eve has no such constraint generally, so her guessing can be extensive. Our results show, however, that by using GRAND, Eve computational effort is minimal. Indeed, even though her signal to noise ratio is worse than Bob's, she can decode with a non-vanishing probability, which is sufficiently high to compromise the security of the wiretap system, while performing on average no more work that Bob, who cannot limit himself to decoding only in the most favorable noise realizations.

II. Success exponents - theory

Consider a simple version of the wiretap channel [1], [43] where Alice has binary data that she wishes to send Bob. Eve has an independent, noisier channel than Bob's. For both channels, we assume that the noise effect is independent of the transmitted code-word and additive but need not be independent and identically distributed. Both Bob and Eve have a statistical characterisation of their channels and perform hard detection decoding of Alice's error correcting code.

In this setting, Gallager's [44] error exponent results state that if a random, or random linear, code is used with a code-rate R that is less than the Shannon capacity of the channel, $C = 1 - H$, where H is the Shannon entropy rate of the noise, then the likelihood that a ML decoding is in error decreases exponentially in n at a speed that depends on R and C. The mirroring concept is success exponents, where the probability that a ML decoder successfully decodes given $R > 1 - H$ decays exponentially in n.

In particular, assume Alice transmits the coded information bits x^n and Eve receives a version corrupted by not-necessarily i.i.d. binary noise, $y^n = x^n \oplus N^n$, where $\oplus$ is modulo 2 summation. Eve performs GRAND decoding by sequentially taking, in order from most likely to least likely based on the noise statistics, putative noise effects, z^n, removing them from the received sequence and querying if what remains, $y^n \ominus z^n$, is in the code-book. The first instance where a code-book element is found is an ML decoding.

For code-rates less than capacity, Gallager's error exponent can be extracted from GRAND by analysing the likelihood that the number of queries until the true noise effect, N^n, is encountered is greater than the number of queries that would identify a non-transmitted code-word. For code-rates greater than capacity, success exponents can be extracted by analysing the likelihood that the true noise effect is encountered while querying before the first noise effect that would result in finding a non-transmitted codeword.

With all logs being base 2, to characterise the success exponent, define the Rényi entropy rate of the noise $\{N^n\}$ process with parameter $\alpha \in (0,1) \cup (1,\infty)$ to be

$$H_\alpha = \lim_{n \to \infty} \frac{1}{n} \frac{1}{1-\alpha} \log \left(\sum_{z^n \in \{0,1\}^n} P(N^n = z^n)^\alpha \right),$$

with $H = H_1$ being the Shannon entropy rate of the noise. Denote the min-entropy rate of the noise by $H_{\min} = \lim_{\alpha \to \infty} H_\alpha$. Using these definitions of H_α it has been established [45], [46], [47], [48] that the moments of the distribution of the number of queries required to identify a realization of the noise effect, N^n, when questions are asked in decreasing order of likelihood, scale exponentially with a rate that can be identified in terms of the Rényi entropy rates

$$\Lambda^N(\alpha) = \begin{cases} \alpha H_{1/(1+\alpha)} & \text{for } \alpha \in (-1,\infty) \\ -H_{\min} & \text{for } \alpha \leq -1. \end{cases}$$

Define the Legendre-Fenchel transform of Λ^N to be

$$I^N(g) = \sup_{\alpha \in \mathbb{R}} \left\{ g\alpha - \Lambda^N(\alpha) \right\},$$

which is the rate function for a large deviation principle of the scaled logarithm of guesswork [49], [48]. Proposition 1 of [39] proves that if $R > C$, the probability then an ML decoder provides a correct decoding decays exponentially in n with rate $I^N(1-R)$.

Theorem 3 of [39] gives a conditional result that if $0 < g < 1 - R$ is such that $I^N(g) < 1 - R - g$, then the probability of a correct decoding given GRAND made fewer than 2^{ng} queries converges to 1 as n increases. If the code rate $R > C$, then a sufficient condition for there to be an exponent for number of queries below which concentration to a correct result occurs is that $R < 1 - H_{\min} = C_{\min}$, where we will call $C_{\min}$ the min-capacity. Taken together, these results establish that to ensure that, when equipped with a hard detection decoder, Eve can never confidently decode any of the communication between Alice and Bob, it is necessary that $R > C_{\min}$ rather than $R > C$.

As a worked example, assume that the channel between Alice and Eve is a BSC with bit-flip probability p. In that case

$$\Lambda^N(\alpha) = \begin{cases} (1+\alpha) \log \left((1-p)^{\frac{1}{1+\alpha}} + p^{\frac{1}{1+\alpha}} \right) & \text{if } \alpha \in (-1,\infty) \\ \log(\max(1-p,p)) & \text{if } \alpha \leq -1, \end{cases}$$

and both the success exponent $I^N(1-R)$ and the exponent for the maximum number of code-book queries that would result in a confident decoding can be readily evaluated numerically.

Using those formulae to create finite block length approximations for codes of rate ≈ 0.91 and lengths $n = 64, 128, 192$ and 256, results in Fig. 1. The left hand panel shows the approximate likelihood that an ML decoding would be correct. The right hand panel shows $\log_2$ of the mathematically determined approximate maximum number of queries that can be made while ensuring that correct decoding is highly likely to be returned. These predictions can be compared with the empirical results that follow.

III. Success Probabilities - Practice

We first consider the natural analogue of the setting for the results in Fig. 1 where Alice and Bob are using a random linear [128,116] code. Eve decodes transmissions using GRAND and abandons after 2^a queries, where a is reported in figure
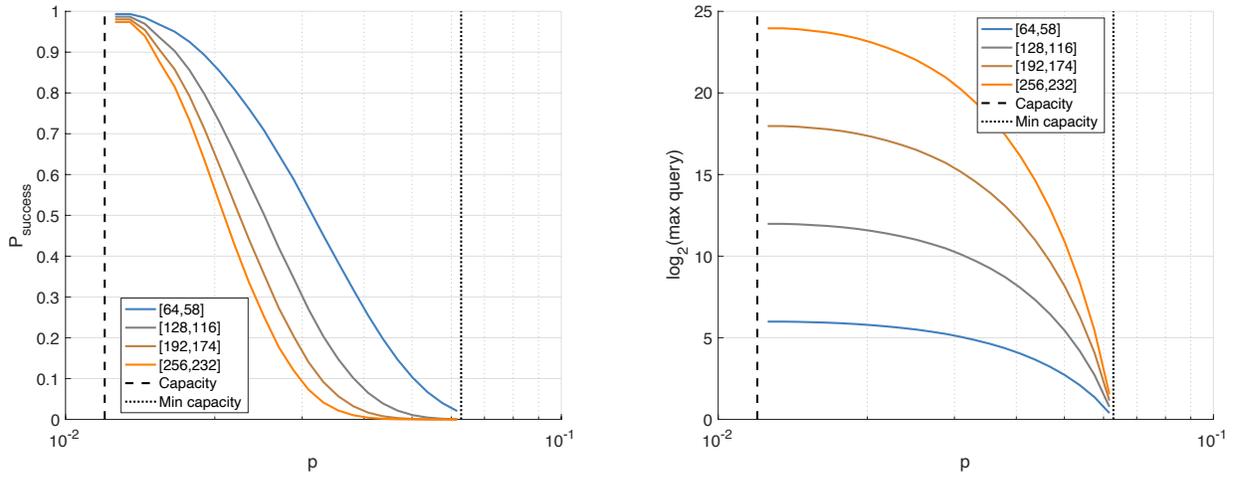
Fig. 1. For a BSC and four codes of different lengths, but the same rate rate of approximately 0.91, figures are plotted for channel conditions between Shannon capacity and min-capacity. Left hand panel: the approximate probability of a successful ML decoding as determined from the success exponent, $\exp(-nI^N(1-R))$, for the given BSC p. Right hand panel, theoretical predictions of $\log_2$ of the maximum query number that Eve should perform with GRAND to retain confidence in a correct decoding. Empirical results for random linear codes are presented later.
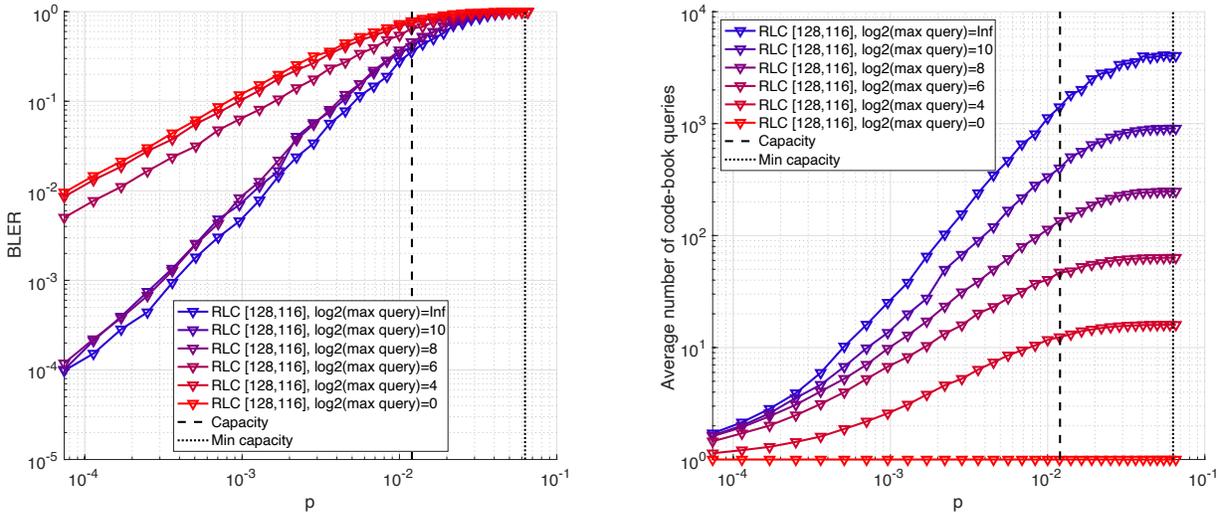

Fig. 2. A random linear [128, 116] code transmitted over a BSC with bit flip probability p decoded with GRAND. Left hand panel: block error rate. Right hand panel: average number of queries until a decoding is found or abandonment occurs. The blue line results from running hard detection GRAND-BSC without abandonment. As the colour gets redder, GRAND is abandoning earlier, at 2^a queries for the a stated in the legend, which is recorded as an error.

legends, returning an erasure rather than erroneous decoding, allowing her to discard decodings she would not trust.

Fig. 2 focuses on $R < C$ by showing Block Error Rate (BLER) against $-\log_{10}$ of the BSC's bit flip probability where abandonment counts as an incorrect decoding. As Theorem 2 of [39] establishes that all GRAND algorithms will identify an incorrect decoding after approximately $2^{n(1-R)} = 2^{n-k}$ queries, abandoning a little before then does not impact BLER performance when $R < C$ as decodings that would likely be in error are instead erasures. If abandonment happens too early, the full within-capacity decoding performance of the code is not realised. The right panel shows the average number of queries until a code-word is found or abandonment, where abandoning early can be seen to significantly reduce complexity.

The left panel of Fig. 3 replots the data in the first panel of Fig. 2 but focuses on the region where the code-rate is above capacity, $R > C$. It shows the likelihood that the decoding is correct, the success probability, where abandonment is counted as incorrect, and can be compared to the left hand panel of Fig. 1. This speaks to the success exponent for all ML decoders showing graceful degradation as code-rate passes through capacity.

The dashed lines in Fig. 3 are the success probability conditioned on not abandoning. By abandoning decoding early, the conditional success probability can be kept high for values of p well above Shannon capacity and up to min-capacity. The right panel of the figure shows the proportion of non-abandoned decodings, which decreases as the abandonment
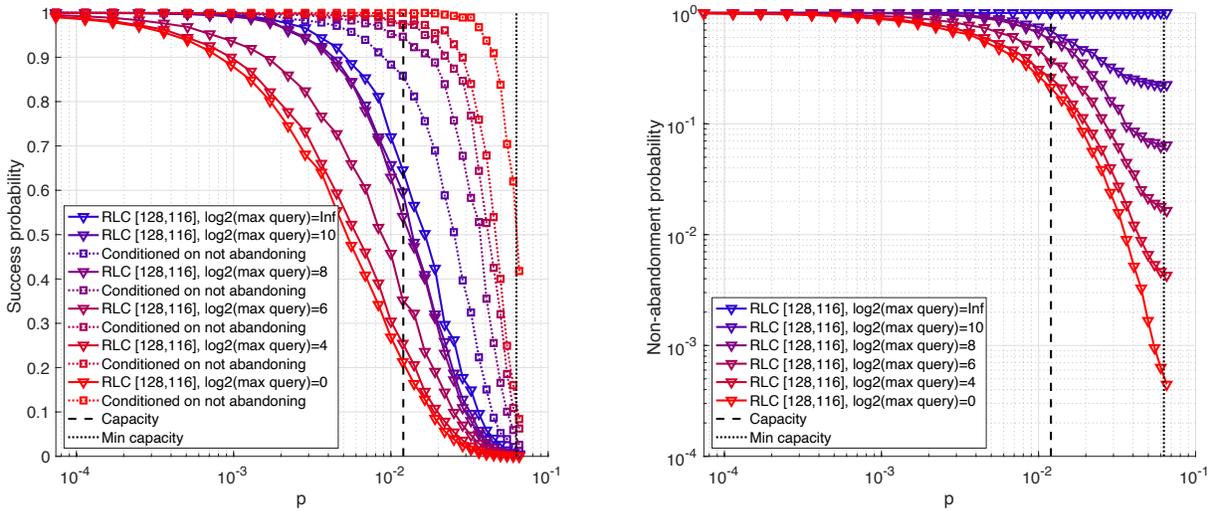
Fig. 3. Same setup as Fig. 2. Left hand panel: shows the likelihood that the decoding is correct, the success probability, where abandonment is counted as incorrect. The dotted lines are the success probability conditioned on not abandoning. Right hand panel: the proportion of non-abandoned decodings. The dashed black vertical line marks the capacity threshold, where $R < C$ to the left and $R > C$ to the right. The dotted black vertical line marks the min-capacity threshold, where $R < C_{\min}$ to the left and $R > C_{\min}$ to the right.

threshold is reduced, and is reflective of the fraction of Alice to Bob communications that Eve decodes rather than abandons.

Fig. 4, left panel, provides an indicator of how little work Eve is doing between non-abandoned decodings in terms of the total number of queries until she identifies a decoding she is confident in, where the early abandonment limits the effort used in decoding what would be untrustworthy decodings anyway. The right panel of Fig. 4 plots the mathematical determination of $\log_2$ of the maximum number of queries that Eve should be able to make while ensuring she only returns confident decodings (black lines - as determined using the formulae in Sec. II), while the red line identifies the empirical equivalent which ensures than more than 50% of Eve's decodings are correct. This establishes that, given knowledge of the bit-flip probability, Eve can use theory to guide her abandonment threshold. The observations from these results are that by only trusting decodings that are identified before a thresholded number of queries, when Eve does decode she can be confident that the decoding is correct, so long as $R < C_{\min}$, compromising Alice and Bob's communication.

For a longer [192,174] RLC of the same rate as the [128,116] code, the left hand panel of Fig. 5 shows analogous results to the left panel of Fig. 3 on the success probability and conditional success probability. Despite being a longer code that has greater total redundancy, the behavior is similar and consistent with theoretical predictions. The right hand panel is akin to that of Fig. 4, demonstrating the correspondence between the theoretical approximate evaluation of an appropriate abandonment threshold and the empirically identified one, where again good correspondence is observed.

IV. DISCUSSION

For codes whose rate are above Shannon capacity, we have demonstrated how success exponents can be used to estimate the fraction of correct decodings returned by a maximum likelihood decoder. We have illustrated how an eavesdropper, Eve, can use an abandonment threshold with GRAND, which can operate with any code, to identify decodings that are confidently correct to compromise Alice and Bob's communication.

For the BSC example used here, Eve's abandonment threshold can be related to a Hamming weight of the corresponding noise effect, but the mathematics and method can also be used for channels with memory where that would not be the case. Moreover, as GRAND algorithms search for the noise-effect, a BSC is essentially the worst case hard detection setting as the noise has minimal structure. In practice, channels are not memoryless but rendered synthetically so through interleaving, which is commonly part of the construction of wiretap systems [50], [51], [52], [53], [54]. Noise correlation, however, increases the effective SNR, possibly by multiple dBs, and has been demonstrated to be exploitable in the GRAND framework to improve decoding accuracy [39], [55]. Even if Bob uses a scheme that relies on interleaving, Eve can use statistical knowledge of the correlation of the noise, resulting in an effectively higher SNR, i.e. lesser degradation, of her channel relative to Bob's, while also using the mathematical formulation to inform her abandonment thresholds.

We have focused here on the simple case of a BSC, which is representative of DMCs, to which the approach can be applied. Hard-detection hardware implementations of GRAND for BSC and bursty channels have been published [56], [57], [58], [59] that demonstrate it is an efficient decoding algorithm for moderate redundancy codes. Fading channels can be more vulnerable than channels without fading [60]. In the setting where the channel noise is represented in a continuous domain, e.g. as Gaussian, the use of soft information, such as through ORBGRAND [61], [62], which is close to capacity achieving
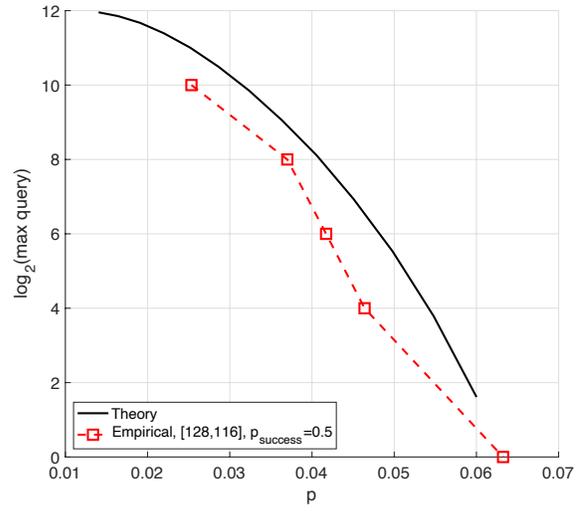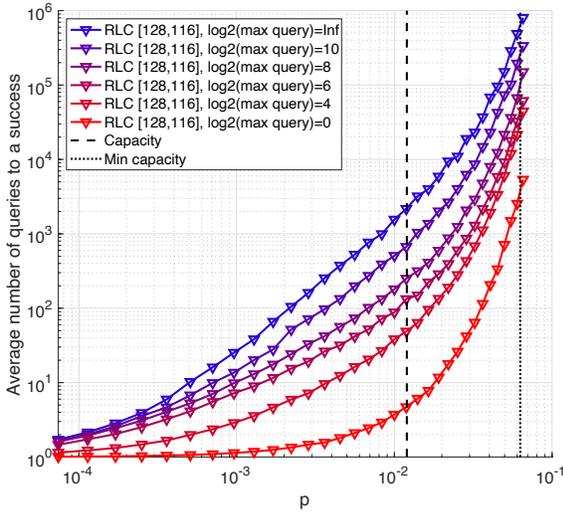
Fig. 4. Same setup as Fig. 2. Left hand panel: shows the average number of queries. including those that lead to an abandonment until a correct decoding. Right hand panel: black line is the theoretically determined number of queries that should be allowable while still concentrating on a correct decoding. The red line is the empirically determined value for which 50% of decodings given non-abandonment are correct for the abandonment criterion in the y-axis.
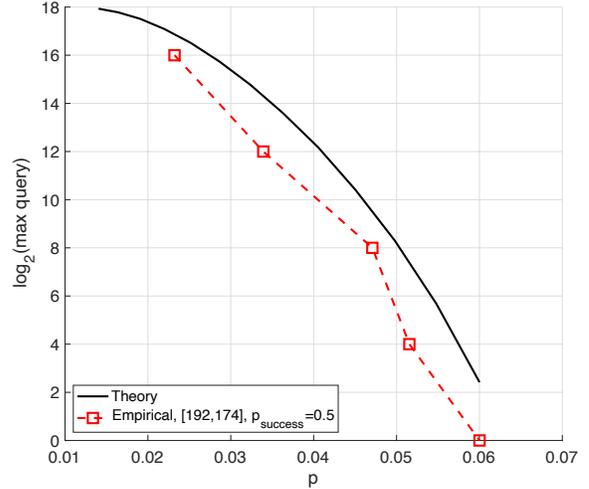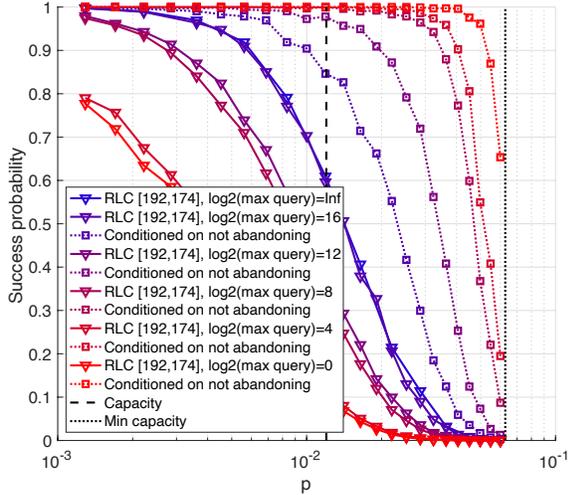

Fig. 5. Similar setup to Fig. 3, but for a [192,174] RLC. Left hand panel: the success probability, where abandonment is counted as incorrect. The dotted lines are the success probability conditioned on not abandoning. The dashed black vertical line marks the capacity threshold, where $R < C$ to the left and $R > C$ to the right. The dotted black vertical line marks the min-capacity threshold, where $R < C_{\min}$ to the left and $R > C_{\min}$ to the right. Right hand panel: black line is the theoretically determined number of queries that should be allowable while still concentrating on a correct decoding. The red line is the empirically determined value for which 50% of decodings given non-abandonment are correct for the abandonment criterion in the y-axis.

[63], [64] and practically implementable in hardware [65], [66], [67], would further aid Eve in compromising Alice and Bob's communication.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Labs Tech. J.*, vol. 63, no. 10, pp. 2135–2157, 1984.

[3] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel (corresp.)," *IEEE Trans. Info. Theory*, vol. 23, no. 3, pp. 387–390, 1977.

[4] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[6] X. S. Zhou, X. Wang, and M. Bloch, "Best readings in physical-layer security," Available at https://www.comsoc.org/publications/best-readings/physical-layer-security (2005/06/12), 2018.

[7] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[8] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[9] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 532–540, 2011.

[10] A. Nooraiepour and T. M. Duman, "Randomized convolutional codes for the wiretap channel," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3442–3452, 2017.

[11] A. Nooraiepour, S. R. Aghdam, and T. M. Duman, "On secure commu-

nications over Gaussian wiretap channels via finite-length codes," *IEEE Commun. Lett.*, vol. 24, no. 9, pp. 1904–1908, 2020.

[12] V. Rana and R. A. Chou, "Short blocklength wiretap channel codes via deep learning: Design and performance evaluation," *arXiv:2206.03477*, 2022.

[13] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: John Wiley & Sons, Inc., 1968.

[14] A. Wyner, "On the probability of error for communication in white Gaussian noise," *IEEE Trans. Inf. Theory*, vol. 13, pp. 86–90, 1967.

[15] R. McEliece and J. Omura, "An improved upper bound on the block coding error exponent for binary-input discrete memoryless channels (corresp.)," *IEEE Trans. Inf. Theory*, vol. 23, no. 5, pp. 611–613, 1977.

[16] S. B. Korada, E. Şaşoğlu, and R. Urbanke, "Polar codes: Characterization of exponent, bounds, and constructions," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6253–6264, 2010.

[17] A. Barg and G. Forney, "Random codes: minimum distances and error exponents," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2568–2573, 2002.

[18] R. G. Gallager, "The random coding bound is tight for the average code," *IEEE Trans. Inform. Theory*, vol. 19, no. 2, pp. 244–246, 1973.

[19] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.

[20] P. Mary, J.-M. Gorce, A. Unsal, and H. V. Poor, "Finite blocklength information theory: What is the practical impact on wireless communications?" in *IEEE Globecom (GC Wkshps)*, 2016, pp. 1–6.

[21] O. Kosut and J. Kliewer, "Finite blocklength and dispersion bounds for the arbitrarily- varying channel," in *IEEE ISIT*, 2018, pp. 2007–2011.

[22] M. Bastani Parizi, E. Telatar, and N. Merhav, "Exact random coding secrecy exponents for the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 509–531, 2017.

[23] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, 2006.

[24] M. Hayashi and R. Matsumoto, "Universally attainable error and information exponents, and equivocation rate for the broadcast channels with confidential messages," in *Proc. Allerton Conf.*, 2011, pp. 439–444.

[25] M. B. Parizi, E. Telatar, and N. Merhav, "Exact random coding secrecy exponents for the wiretap channel," in *IEEE ISIT*, 2016, pp. 1521–1525.

[26] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, 2011.

[27] R. Xu, D. Guo, B. Zhang, and G. Ding, "Finite blocklength covert communications in interweave cognitive radio networks," *IEEE Commun. Lett.*, vol. 26, no. 9, pp. 1989–1993, 2022.

[28] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, 2019.

[29] W. K. Harrison, "Exact equivocation expressions for wiretap coding over erasure channel models," *IEEE Commun. Lett.*, vol. 24, no. 12, pp. 2687–2691, 2020.

[30] W. K. Harrison and M. R. Bloch, "Attributes of generators for best finite blocklength coset wiretap codes over erasure channels," in *IEEE ISIT*, 2019, pp. 827–831.

[31] J. Pfister, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "Quantifying equivocation for finite blocklength wiretap codes," in *IEEE ICC*, 2017.

[32] A. Frank, H. Aydinian, and H. Boche, "Type II wiretap channel with an active eavesdropper in finite blocklength regime," in *IEEE WCNC*, 2016, pp. 1–6.

[33] M. Shoushtari and W. K. Harrison, "New dual relationships for error-correcting wiretap codes," in *IEEE ITW*, 2021, pp. 1–6.

[34] T.-X. Zheng, H.-M. Wang, D. W. K. Ng, and J. Yuan, "Physical-layer security in the finite blocklength regime over fading channels," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3405–3420, 2020.

[35] M. Shakiba-Herfeh, L. Luzzi, and A. Chorti, "Finite blocklength secrecy analysis of polar and reed-muller codes in BEC semi-deterministic wiretap channels," in *IEEE ITW*, 2021, pp. 1–6.

[36] C. Cao, H. Li, Z. Hu, W. Liu, and X. Zhang, "Physical-layer secrecy performance in finite blocklength case," in *IEEE GLOBECOM*, 2015.

[37] N. Arı, N. Thomos, and L. Musavian, "Performance analysis of short packet communications with multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6778–6789, 2022.

[38] N. Merhav, "Exact correct-decoding exponent of the wiretap channel decoder," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7606–7615, 2014.

[39] K. R. Duffy, J. Li, and M. Médard, "Capacity-achieving guessing random additive noise decoding," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4023–4040, 2019.

[40] S. Arimoto, "On the converse to the coding theorem for discrete memoryless channels (corresp.)," *IEEE Trans. Inform. Theory*, vol. 19, no. 3, pp. 357–359, 1973.

[41] G. Dueck and J. Korner, "Reliability function of a discrete memoryless channel at rates above capacity (corresp.)," *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 82–85, 1979.

[42] Y. Chen and A. Han Vinck, "On the binary symmetric wiretap channel," in *International Zurich Seminar on Communications*, 2010, pp. 17–20.

[43] E. Verriest and M. Hellman, "Convolutional encoding for Wyner's wiretap channel (corresp.)," *IEEE Trans. Info. Theory*, vol. 25, no. 2, pp. 234–236, 1979.

[44] R. Gallager, "The random coding bound is tight for the average code (corresp.)," *IEEE Tran. Inf. Theory*, vol. 19, no. 2, pp. 244–246, 1973.

[45] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans.Inf. Theory*, vol. 42, no. 1, pp. 99–105, 1996.

[46] D. Malone and W. G. Sullivan, "Guesswork and entropy," *IEEE Trans. Inf. Theory*, vol. 50, no. 4, pp. 525–526, 2004.

[47] C.-E. Pfister and W. Sullivan, "Rényi entropy, guesswork moments and large deviations," *IEEE Trans. Inf. Theory*, no. 11, pp. 2794–00, 2004.

[48] M. M. Christiansen and K. R. Duffy, "Guesswork, large deviations and Shannon entropy," *IEEE Trans. Inf. Theory*, vol. 59, pp. 796–802, 2013.

[49] E. Arikan, "Large deviations of probability rank," in *IEEE Int. Symp. Inf. Theory*, 2000, p. 27.

[50] I. Ajayi, Y. Medjahdi, L. Mroueh, and F. Kaddour, "Physical layer security by interleaving and diversity: Impact of imperfect channel state information," in *EECSI*, 2021, pp. 299–304.

[51] J. Pfeiffer and R. F. Fischer, "Multilevel coding for physical-layer security," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1999–2009, 2022.

[52] W. K. Harrison, J. Almeida, D. Klinc, S. W. McLaughlin, and J. Barros, "Stopping sets for physical-layer security," in *IEEE IYW*, 2010, pp. 1–5.

[53] A. Frank, H. Aydinian, and H. Boche, "Delay optimal coding for secure transmission over a burst erasure wiretap channel," in *IEEE WCNC*, 2019, pp. 1–7.

[54] W. Xiang, M. Johnston, and S. Le Goff, "Low-complexity power control and energy harvesting algorithms for wiretap channels employing finite-alphabet input schemes," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 318–326, 2018.

[55] W. An, M. Médard, and K. R. Duffy, "Keep the bursts and ditch the interleavers," *IEEE Trans. Commun.*, vol. 70, pp. 3655–3667, 2022.

[56] A. Riaz, V. Bansal, A. Solomon, W. An, Q. Liu, K. Galligan, K. R. Duffy, M. Médard, and R. T. Yazicigil, "Multi-code multi-rate universal maximum likelihood decoder using GRAND," in *IEEE ESSCIRC*, 2021, pp. 239–246.

[57] A. Riaz, M. Medard, K. R. Duffy, and R. T. Yazicigil, "A universal maximum likelihood GRAND decoder in 40nm CMOS," in *COMSNETS*, 2022, pp. 421–423.

[58] S. M. Abbas, T. Tonnellier, F. Ercan, and W. J. Gross, "High-throughput VLSI architecture for GRAND," in *IEEE SiPS*, 2020.

[59] S. M. Abbas, M. Jalaleddine, and W. J. Gross, "High-throughput VLSI architecture for GRAND Markov Order," in *IEEE SiPS*, 2021.

[60] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE ISIT*, 2006, pp. 356–360.

[61] K. R. Duffy, "Ordered reliability bits guessing random additive noise decoding," in *IEEE ICASSP*, 2021, pp. 8268–8272.

[62] K. R. Duffy, W. An, and M. Médard, "Ordered reliability bits guessing random additive noise decoding," *IEEE Trans. Signal Process.*, vol. 70, pp. 4528–4542, 2022.

[63] M. Liu, Y. Wei, Z. Chen, and W. Zhang, "ORBGRAND is almost capacity-achieving," *arxiv:2202.06247*, 2022.

[64] P. Yuan, K. R. Duffy, E. Gabhart, and M. Médard, "On the role of quantization of soft information in GRAND," *arXiv:2203.13552*, 2022.

[65] S. M. Abbas, T. Tonnellier, F. Ercan, M. Jalaleddine, and W. J. Gross, "High-throughput and energy-efficient vlsi architecture for ordered reliability bits GRAND," *IEEE Trans. Very Large Scale Integr. Syst.*, 2022.

[66] C. Condo, "A fixed latency ORBGRAND decoder architecture with LUT-aided error-pattern scheduling," *IEEE Trans. Circuits Syst. I Regul. Pap.*, 2022.

[67] A. Riaz, A. Yasar, F. Ercan, W. An, J. Ngo, K. Galligan, M. Médard, K. R. Duffy, and R. T. Yazicigil, "A sub-0.8pJ/b 16.3Gbps/mm^2 universal soft-detection decoder using ORBGRAND in 40nm CMOS," in *IEEE ISSCC*, 2023.