Leakage Thresholds and Security Trade-offs in Finite Blocklength Wiretap Channels

Shabnam Sodagari, *Senior Member, IEEE*

***Abstract*—This work discusses the bounds for the wiretap channel (WTC) in the finite blocklength regime, characterizing the behavior of the performance trade-off between information delivery to the legitimate receiver and information leakage to the eavesdropper as a function of blocklength. Since the error probability at the legitimate receiver is the same as that of a conventional point-to-point channel, the characterization of the former builds on the finite blocklength analysis for that case. The information leakage bound relies on the analysis of the corresponding leakage density. This paper extends these concepts by incorporating the use of the Berry-Esseen theorem in assessing the convergence rates of leakage and secrecy metrics to their asymptotic values, which provides a refined analytical tool to evaluate the performance of secrecy systems under finite blocklength constraints. Furthermore, this approach facilitates a quantification of the trade-offs involved, integrating concepts such as the aggregate leakage rate and empirical average leakage, thus enabling a more comprehensive understanding of how system parameters affect the overall secrecy performance. This allows for a more detailed exploration of the dependencies between blocklength, secrecy, and reliability trade-offs required to balance effective communication against security imperatives. These analyses also highlight the critical balance necessary between ensuring low probability of error for the legitimate receiver while maintaining stringent secrecy requirements against an eavesdropper. Furthermore, the study introduces metrics such as aggregate leakage rate and empirical average leakage, providing new insights into how these factors interplay to influence the overall performance of secure communication systems.**

***Index Terms*—finite blocklength, information theory, secrecy, security, wiretap channel.**

I. Introduction

In point-to-point communication with secrecy, a transmitter, Alice, seeks to transmit information to a legitimate receiver, Bob, with error probability at most ϵ while limiting the information leakage to the eavesdropper (Eve) to never exceed threshold δ. Fig 1 shows the wiretap channel (WTC) model [1], with M, X, Y, and Z representing the message, channel input, and channel outputs at the legitimate receiver and the eavesdropper, respectively. For the purpose of this work, the channel is memoryless by assumption.

The concept of a wiretap channel was first introduced by Wyner [1], marking a foundational development in the field of information-theoretic security. This model fundamentally addresses the challenge of secure communication over an insecure channel without relying on secret keys. In Wyner's original formulation, the main idea is to exploit the physical layer properties of communication channels to achieve secrecy.

Department of Computer Engineering Computer Science, California State University, Long Beach, CA 90840 USA (email:shabnam@ieee.org)

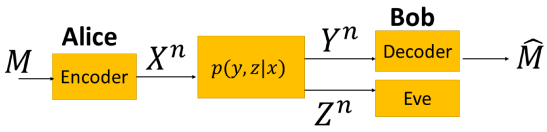

Fig. 1. The wiretap channel model

The model assumes that the eavesdropper's channel is a degraded version of the main channel to the legitimate receiver, which inherently limits the information that the eavesdropper can intercept.

Over the years, this model has been generalized and extensively studied, leading to the development of various coding strategies designed to maximize the rate at which information can be securely transmitted. The wiretap channel model has also inspired numerous applications in cybersecurity, wireless communication, and data privacy, demonstrating its broad impact on both theoretical and practical aspects of secure communication.

In [1], Wyner shows that it is possible to deliver information with a positive rate from Alice to Bob in a way that remains secret to Eve provided that the channel from Alice to Eve is a degraded version of the channel from Alice to Bob [1], meaning that $M \to X \to Y \to Z$ forms a Markov chain. In [2], Csiszar *et al.* extend Wyner's notion of secrecy by considering a broadcast channel with a confidential message (BCC) [2]. In the BCC, there is a common message to be broadcast to both Bob and Eve and a confidential message to be delivered to Bob but kept secret from Eve.

The notions of secrecy in Wyner's wiretap channel model and Csiszar *et al.*'s BCC model can both be expressed in terms of information leakage bounds, where information leakage characterizes how much Eve learns about the secret message. A formal definition appears in Section III. Both [1] and [2] examine secrecy in the limit as blocklength grows without bound.

In [3] the meta converse and random coding union (RCU) bound are used to derive finite blocklength bounds for a point-to-point channel. In [4], Yang *et al.* apply a similar strategy to derive non-asymptotic bounds for a simple wiretap channel with a perfect channel from Alice to Bob, under a total variation distance secrecy constraint.

Besser et al. [5], [6] focus on code design for fiber channels using neural networks, whereas our focus is on deriving the tradeoffs between blocklength, leakage, probability of error,

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

and channel parameters for general channels.

Unlike [7] we do not rely on the assumption that Eve knows the queue state of the legitimate transmitter (Alice), whether it is transmitting or not. Moreover, our method is broader and does not rely on a friendly jammer or a Rayleigh fading channel assumption. Additionally, Yang [8] exploits age of information to characterize the performance of short-packet in a wiretap channel. However, they consider permutation-based transmissions, whereas our approach is more general and may include permutation-based transmissions as a special case.

In this work, we seek to characterize the rate of convergence to Wyner's asymptotic capacity characterization for the discrete memoryless wiretap channel in the special case of the degraded wiretap channel. Like Wyner we employ an information leakage secrecy model.

The given finite blocklength analysis builds on the strategies and tools developed for the point-to-point channel in [3] and later applied to many other channel models (see, for example, [9]). Key to our analysis is the introduction of a new notion of leakage density analogous to the notion of information density. Leakage density is defined for each channel use and measures the incremental information about the transmitted message that an eavesdropper could potentially infer from the intercepted signal. Thus, the contributions of this paper can be summarized as follows:

- We leverage the concept of leakage density analogous to information density, which quantifies the incremental information leaked to an eavesdropper during each transmission. This approach provides a more granular perspective on security over finite blocklengths.
- We derive key relations between blocklength, information leakage, and the probability of error at the legitimate receiver. These relations are essential for understanding the security-performance trade-offs in finite blocklength communications.
- The paper identifies two distinct cases based on the channel dispersions of Alice-Bob and Alice-Eve. Each case provides a different insight into how the blocklength impacts the overall secrecy rate and error performance.
- The results are applicable to real-world scenarios like IoT and autonomous vehicles, where short-packet communication and stringent security are paramount. The findings help guide the design of secure communication systems that balance efficiency and leakage constraints.

The rest of the paper is organized as follows. Section II formally describes the discrete memoryless WTC and summarizes prior results. Section III discusses our proposed approach to bounding information leakage in the finite blocklength regime. Section IV discusses the use of hypothesis testing for the leakage rate secrecy constraint. Section V contains simulation results. Section VI concludes the paper.

II. Background and Problem Definition

A. Notation and Definitions

Definition 1. *A $(2^{nR}, n)$ wiretap channel code [10] comprises*

- *A uniformly distributed message set $\{1, \ldots, 2^{nR}\}$;*
- *A randomized encoder C that maps the message $M \in \{1, \ldots, 2^{nR}\}$ to a codeword $X^n(M)$ using a conditional pmf $p(x^n|M)$;*
- *A decoder that maps the received signal Y^n to*

$$\hat{M} \in \{1, \ldots, 2^{nR}\}.$$

We measure probability of error as $P_e^{(n)} = \mathbb{P}[\hat{M} \neq M]$, where $\mathbb{P}$ denotes the probability of an event. As shown in Fig. 2, the code employs a codebook comprising $2^{n\tilde{R}}$ codewords. The codewords are divided into 2^{nR} bins, each of size $2^{n(\tilde{R}-R)}$, with bin $C(m)$, $m \in \{1, \ldots, 2^{nR}\}$ containing the codewords $U^n(l)$ with $l \in [(m-1)2^{n(\tilde{R}-R)} + 1 : m2^{n(\tilde{R}-R)}]$. The encoder maps message $M \in \{1, \ldots, 2^{nR}\}$ to a codeword from bin $C(M)$. We denote the chosen codeword by $U^n(L)$, where L is chosen uniformly at random from $[(M-1)2^{n(\tilde{R}-R)} + 1 : M2^{n(\tilde{R}-R)}]$.

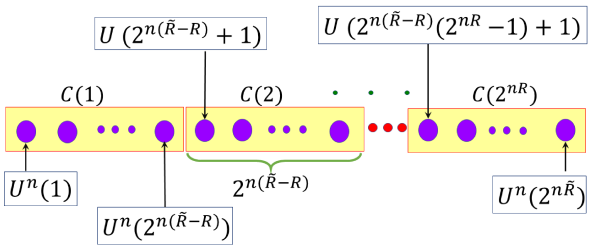

Fig. 2. Random Encoder for WTC

The item index L within bin $C(M)$ is the rate that Alice sacrifices to confuse Eve.

After the above step, the codeword X^n is chosen and transmitted according to a conditional pmf $\prod_{i=1}^n p_{X|U}(x_i|u_i)$. Joint typicality decoding is used in [10] for decoding in the achievability proof.

Definition 2. *The equivocation H experienced by eavesdropper Eve is defined as $\mathsf{E}^{(n)} = \mathsf{H}(L|Z^n)$, where H denotes entropy [10].*

Definition 3. *In the asymptotic case, a rate-equivocation pair (R, R_e) is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes, such that for probability of error $P_e^{(n)}$ and equivocation $\mathsf{E}^{(n)}$:*

$$\lim_{n\to\infty} P_e^{(n)} = 0$$

$$\lim_{n\to\infty} \frac{1}{n}\mathsf{E}^{(n)} \geq R_e^{(n)}$$

Definition 4. *Information leakage is defined as $\mathfrak{R}_L^{(n)} = \frac{1}{n}\mathrm{I}(M; Z^n)$, where I denotes mutual information. The weak secrecy condition is an asymptotic constraint on information leakage, which is given by [10]*

$$\lim_{n\to\infty} \mathfrak{R}_L^{(n)} = 0. \tag{1}$$

Definition 5. *The maximum secret rate $R^*(n, \delta, \epsilon)$ is the maximum rate between Alice and Bob in light of the constraint for average probability of error at Bob being $\mathbb{P}(M \neq \hat{M}) \leq \epsilon$.*

Additionally, δ is an upper bound threshold for a secrecy constraint at Eve.

Table I contains abbreviations and notation used in the paper.

TABLE I
NOTATION

X	Transmitted
Y	Received at Bob
Z	Received at Eve
n	Bocklength
L	Size of dummy messages in each bin for random binning to confuse Eve
$\|M\|$	Alphabet size of the message
$r_L^{(n)}$	Empirical avarege of leakage density over a block of size n
$R_L^{(n)}$	Upper bound on leakage rate
$r_{AL}^{(n)}$	Aggregate information leakage density over a block of size n
$R_{AL}^{(n)}$	Upper bound on aggregate leakage rate

B. Review of Degraded WTC Results

In [1] Wyner derives a lower bound for equivocation with a source encoder generating blocks of length k and a channel encoder generating blocks of length n. In [4], Yang *et al.* derive finite blocklength secrecy capacity bounds for point-to-point semi-deterministic WTC, where a WTC is called semi-deterministic if the channel between Alice and Bob is deterministic (perfect), while the channel from Alice to the eavesdropper is a discrete memoryless channel (DMC). For a semi-deterministic WTC the maximum secret rate $R^*(n,\epsilon,\delta)$ is

$$R^*(n,\epsilon,\delta) = C_s - \sqrt{\frac{V}{n}}Q^{-1}\left(\frac{\delta}{1-\epsilon}\right) + \mathcal{O}\left(\frac{\log n}{n}\right). \quad (2)$$

[4]. Here, C_s denotes the asymptotic channel capacity, while V is the channel dispersion. The analysis given employs a total variation distance secrecy constraint rather than information leakage metric, as employed in [1], [2].

In our finite blocklength analysis, we view the leakage through the lens of information density. This approach is well matched to earlier asymptotic strategies that relied on the mutual information.

C. Berry-Esseen Approximation

Theorem 1. ***Berry-Esseen Theorem*** *[11] (Sec. XVI. Theroem 1): Let X_i, $i \geq 1$ be i.i.d with $\mathrm{E}[X_1] = \mu$, $\mathrm{Var}[X_1] = V^2$, and $\beta_3 = \mathbb{E}|X_1 - \mu|^3$, Denote $S_n = \sum_i^n X_i$. Then, there exists a constant c (not depending on n or the distribution of X_i), such that*

$$\left|\mathbb{P}\left(\frac{S_n - n\mu}{\sqrt{nV}} \geq x\right) - Q(x)\right| \leq \frac{c\beta_3}{\sqrt{n}V^{3/2}}, \quad (3)$$

where $Q(x)$ is the standard normal complementary cdf.

If the leakage densities for each symbol transmitted by Alice are slightly skewed due to channel imperfections, the Berry-Esseen theorem allows us to estimate how this skew affects the sum over all transmissions in the block, and hence the total security leakage.

III. Proposed Approach for Approximation of Leakage in Finite Blocklength Degraded WTC

In the finite blocklength regime, the achievability translates into a rate-equivocation pair (R, R_e) such that;

$$P_e^{(n)} \leq \epsilon \quad (4)$$

$$\mathsf{E}^{(n)} \geq R_e - \epsilon \quad (5)$$

The approach taken in this work extends traditional analyses by integrating advanced statistical methods to more accurately predict and control information leakage within these constraints. Here, the Berry-Esseen theorem provides a critical tool for evaluating the deviation of leakage distributions from the normal, particularly over short blocklengths where asymptotic normality may not hold.

Definition 6. *An (n, R, R_e, ϵ) code in the finite blocklength regime is a coding scheme used for transmitting information, where n is the blocklength (the number of symbols per codeword), R is the transmission rate (bits per channel use), and R_e is the equivocation rate at the eavesdropper (bits per channel use), aiming to ensure secure communication. The parameter ϵ is a small positive number that bounds the maximum allowable probability of decoding error, $P_e^{(n)}$, at the receiver to be less than or equal to ϵ and requires the equivocation rate at the eavesdropper, $\mathsf{E}^{(n)}$, to be at least $R_e - \epsilon$, thereby balancing the trade-offs between reliability, rate, and security.*

Notice that in this secrecy problem, we have constraints on both the equivocation (or leakage) $\mathsf{E}^{(n)}$ and the reliability $P_e^{(n)}$.

To apply the Berry-Esseen to information density, note that $\frac{1}{n}\sum_{i=1}^n \imath(X,Z)$ approaches the expected value or leakage mutual information to the eavesdropper.

$$\imath(X,Z) = \log\frac{P_{XZ}}{P_X P_Z} \quad (6)$$

$$I(X,Z) = \mathbb{E}[\imath(X,Z)] = \sum_{x\in\mathcal{X}}\sum_{z\in\mathcal{Z}} P(X,Z)\log\frac{P(X,Z)}{P_X P_Z} \quad (7)$$

Consider the Markov chain

$$M \to X^n \to Z^n, \quad (8)$$

with M, X^n, and Z^n being the message, the encoder output, and the received signal at Eve; we define the leakage density as $\imath(X^n;Z^n)$, where for the DMC

$$\imath(X^n;Z^n) = \sum_{j=1}^n \imath(X_j,Z_j). \quad (9)$$

We use $r_L^{(n)}$ to define the empirical average of leakage density, i.e.,

$$r_L^{(n)} = \frac{1}{n}\sum_{j=1}^{n} \imath(X_j, Z_j). \tag{10}$$

The introduction of the empirical average leakage density $r_L^{(n)}$ and its analysis through the Berry-Esseen theorem in the context of wiretap channels, enables us to quantify the variance and skewness of leakage over finite blocklengths. This method not only refines the evaluation of security levels but also helps in designing codes that are robust against information leakage in practical scenarios.

The Berry-Esseen theorem then implies

$$\mathbb{P}\left(\frac{r_L^{(n)} - I(X;Z)}{\sqrt{V_L/n}} \geq R_L^{(n)}\right) \leq Q(R_L^{(n)}) + \frac{cT_L}{V_L^{3/2}\sqrt{n}}, \tag{11}$$

where $Q(x)$ is the probability that a standard normal random variable is greater than x, $R_L^{(n)}$ is an imposed upper bound on leakage rate, and

$$V_L = \text{var}\ [\imath(X_j; Z_j)]$$
$$T_L = \mathbb{E}|\imath(X_j; Z_j) - I(X_j; Z_j)|^3.$$

The leakage variance and third central moment in the Berry-Esseen theorem enable adjustments in the coding strategy to optimize the balance between communication efficiency and security. This is crucial for developing communication protocols that can effectively operate under stringent security requirements.

Choosing $R_L^{(n)}$ to satisfy

$$Q(R_L^{(n)}) + \frac{cT_L}{V_L^{3/2}\sqrt{n}} \leq \delta_L \tag{12}$$

guarantees a leakage probability bounded by target leakage bound δ_L giving

$$\mathbb{P}\left(\frac{r_L^{(n)} - I(X;Z)}{\sqrt{V_L/n}} \geq R_L^{(n)}\right) \leq \delta_L, \tag{13}$$

when

$$R_L^{(n)} \geq Q^{-1}\left(-\frac{cT_L}{V_L^{3/2}\sqrt{n}} + \delta_L\right). \tag{14}$$

This is equivalent to

$$V_L \geq \left(\frac{cT_L}{\delta_L - Q(R_L^{(n)})}\right)^{2/3} n^{-1/3}. \tag{15}$$

Building on this foundation, the finite blocklength relation applicable to the Alice-Bob channel, as established by [3], allows us to express the relationship as follows

$$\frac{1}{n}\log M^* = C - \sqrt{\frac{V}{n}}Q^{-1}(\epsilon).$$

This enables us to calculate the dispersion for the Alice-Bob channel, presented as:

$$V = \left(\frac{nC - \log M^*}{Q^{-1}(\epsilon)}\right)^2 \frac{1}{n}. \tag{16}$$

Given that the Alice-Eve channel is a degraded variant of the Alice-Bob channel, it follows that its dispersion V_L, for the same blocklength, is greater than that of the Alice-Bob channel, denoted as $V_L \geq V$. Therefore, depending on the choice of maximum leakage rate and other parameters, such as the error probability at Bob, and blocklength n, two distinct relations can be established from above equations, i.e., either the lower bound for V_L in Eq. (15) is greater than V in Eq. (16) or vice versa.

- Case 1: The upper bound for V_L

$$\left(\frac{cT_L}{\delta_L - Q(R_L^{(n)})}\right)^{2/3} n^{-1/3} \leq \left(\frac{nC - \log M^*}{Q^{-1}(\epsilon)}\right)^2 \frac{1}{n} \tag{17}$$

- Case 2

$$\left(\frac{cT_L}{\delta_L - Q(R_L^{(n)})}\right)^{2/3} n^{-1/3} > \left(\frac{nC - \log M^*}{Q^{-1}(\epsilon)}\right)^2 \frac{1}{n} \tag{18}$$

The above two cases capture the relation between the blocklength, leakage, and probability of error.

A. Aggregate Leakage Rate Over a Block of Length n

Instead of the empirical average of leakage, we can characterize the aggregate information leakage density $r_{AL}^{(n)}$, over a block of size n, and use the Berry-Esseen relation in its original form, as in Theorem 1.

$$r_{AL}^{(n)} = \sum_{j=1}^{n} \imath(X_j, Z_j). \tag{19}$$

Using Berry-Esseen:

$$\left|\mathbb{P}\left(\frac{r_{AL}^{(n)} - nI(X;Z)}{\sqrt{nV_A}} \geq x\right) - Q(x)\right| \leq \frac{cT_L}{\sqrt{n}V_A^{3/2}}, \tag{20}$$

where $V_A = \text{var}(i(X,Z))$ (channel dispersion) and $T_L = \mathbb{E}[|\imath(X,Z) - I(X,Z)|^3]$ is the third central moment of the channel.

Instead of x, we insert an upper aggregate rate for leakage or $R_{AL}^{(n)}$.

$$\mathbb{P}\left(\frac{r_{AL}^{(n)} - nI(X;Z)}{\sqrt{nV_A}} \geq R_{AL}^{(n)}\right) \leq Q(R_{AL}^{(n)}) + \frac{cT_L}{\sqrt{n}V_A^{3/2}}. \tag{21}$$

Setting

$$Q(R_{AL}^{(n)}) + \frac{cT_L}{\sqrt{n}V_A^{3/2}} \leq \delta_A. \tag{22}$$

guarantees that the leakage probability is bounded by target aggregate leakage upper bound δ_A

$$\mathbb{P}\left(\frac{r_{AL}^{(n)} - nI(X;Z)}{\sqrt{nV_A}} \geq R_{AL}^{(n)}\right) \leq \delta_A. \tag{23}$$

Therefore,

$$R_{AL}^{(n)} \geq Q^{-1}\left(-\frac{cT_L}{\sqrt{n}V_A^{3/2}} + \delta_A\right) \tag{24}$$

The above equation gives a lower bound for the dispersion V_A as follows:

$$V_A \geq \left(\frac{cT_L}{\delta_A - Q(R_{AL}^{(n)})}\right)^{2/3} n^{-1/3}. \tag{25}$$

Since the channel of Alice-Eve is a degraded version of the channel between Alice-Bob, we have $V_A \geq V$. Following the same line of reasoning to capture the blocklength, aggregate leakage, and error probability in one relation, we note that depending on the choice of these parameters and characteristics of the channel, e.g., its third central moment two cases can be distinguished:

- Case 1

$$\left(\frac{cT_L}{\delta_A - Q(R_{AL}^{(n)})}\right)^{2/3} n^{-1/3} \leq \left(\frac{nC - \log M^*}{Q^{-1}(\epsilon)}\right)^2 \frac{1}{n} \tag{26}$$

- Case 2

$$\left(\frac{cT_L}{\delta_A - Q(R_{AL}^{(n)})}\right)^{2/3} n^{-1/3} > \left(\frac{nC - \log M^*}{Q^{-1}(\epsilon)}\right)^2 \frac{1}{n} \tag{27}$$

IV. Leakage Converse via Hypothesis Testing

In this section we focus on the converse for the information leaked to Eve. We use the hypothesis testing approach, which is a tool used in non-asymptotic converse proofs [3] in place of the Fano's inequality.

Since the reliability condition (probability of error at the legitimate receiver) and the rate to the legitimate receiver are the same as the conventional point-to-point communication in the finite blocklength regime, we do not repeat the analysis here, for brevity. Nevertheless, we apply the resuls to Eve for leakage analysis.

More specifically, to characterize the leakage rate, we can apply the following meta-converse theorem proven in [3].

Theorem 2. *[3] Consider Z^n to be the signal received at the eavesdropper. For an arbitrary Q_{Z^n}, every (k, n, ϵ) code must satisfy:*

$$2^k \leq \frac{1}{\beta_{1-\epsilon}\left(P_{X^n}P_{Z^n|X^n}, P_{X^n}Q_{Z^n}\right)} \tag{28}$$

The above theorem implies that the leakage rate to Eve is upper bounded by

$$R_L \leq -\log_2\left(\beta_{1-\epsilon_e}\left(P_{X^n}P_{Z^n|X^n}, P_{X^n}Q_{Z^n}\right)\right) \tag{29}$$

Here, ϵ_e is the probability of error at Eve,

$$\beta_{1-\epsilon_e}(P_{X^n}, Q_{X^n}) = \inf_{P_{U|X^n}: P_{X^n}[U=0] \geq \alpha} Q_{X^n}[U=0],$$

where U is the output of a binary hypothesis testing to choose between a distribution P or an alternative Q.

If Eve uses the maximum likelihood decoder, the above leakage bound becomes tight. In general, if Eve uses jointly typical decoding, the above leakage bound holds with inequality, since jointly typical decoder is sub-optimal to ML decoder.

V. Simulation Results

In this section, we present the simulation results. The focus is on analyzing the leakage threshold (δ_L) as a function of blocklength (n) and error probability (ϵ). Specifically, the aim is to evaluate how the leakage threshold varies with different error probabilities at Bob while maintaining the channel's security against Eve.

The parameters for the simulation are selected as follows: Channel capacity at Bob is fixed at 1, and M^*, representing the size of the message set, is set to 2. The Berry-Esseen constant c is set to 0.4096, while T_L, the third central moment for the leakage density at Eve, is set to 0.3.

The simulation results, shown in Fig. 3, illustrate the relationship between the leakage threshold and blocklength n for different values of error probability ϵ. Each curve in the plot corresponds to a different value of ϵ, demonstrating how the leakage threshold changes with increasing blocklength under different error conditions.

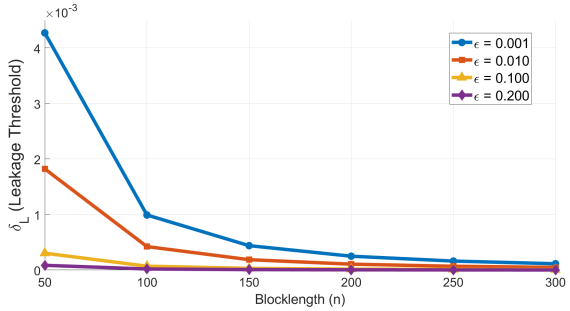

Fig. 3. Leakage Threshold vs Blocklength n for varying error probabilities ϵ.

In all cases, the leakage threshold decreases as the blocklength n increases. This is consistent with the fact that longer blocklengths provide better protection against information leakage to Eve, as the finite blocklength effects diminish with larger n.

The error probability ϵ has a significant effect on the leakage threshold. Lower values of ϵ correspond to looser secrecy conditions, which result in higher leakage thresholds. As ϵ increases, the system becomes more constrained in terms of leakage, with lower values of δ_L. The rate at which δ_L decreases with increasing blocklength is more pronounced for lower error probabilities. For higher values of ϵ, the curves flatten out, indicating that the improvement in leakage reduction slows down with larger blocklengths.

Next, we present the simulation results for δ_L (Leakage Threshold) vs. Blocklength for different values of the channel capacity C. The fixed parameters used are $R_L^{(n)} = 0.5$, $\epsilon = 0.1$, and $T_L = 0.3$. Additionally, the Berry-Esseen constant $c = 0.4096$ is used. The results are shown in Fig. 4.

Across the values of the channel capacity, we observe that the leakage threshold δ_L decreases as the blocklength n

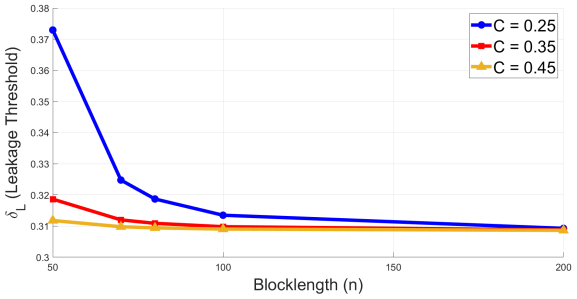

Fig. 4. Leakage threshold vs. blocklength for different values of channel capacity

increases. This is consistent with the expectation that larger blocklengths provide better security, as they allow for more robust encoding strategies that reduce the leakage of information to the eavesdropper. For instance, for $C = 0.25$, the leakage threshold starts at approximately 0.37 when $n = 50$ and decreases to nearly 0.32 when $n = 200$. A similar trend is observed for the other capacity values.

Additionally, higher capacity results in lower leakage: As the capacity increases, the leakage threshold generally decreases. This is due to the fact that a higher channel capacity allows for more efficient transmission of secure information, leaving less room for leakage to the eavesdropper. This trend holds across all blocklengths.

The curves for different values of C converge as the blocklength n increases. For larger blocklengths such as $n = 200$, the difference between leakage thresholds for different capacity values becomes minimal. This suggests that, for sufficiently large blocklengths, the impact of the channel capacity on the leakage threshold diminishes, and the system becomes more secure overall, regardless of the capacity. This aligns with the theoretical expectation that, in the asymptotic regime (large blocklengths), the system approaches its optimal performance, where the influence of finite blocklength effects is minimized.

These results highlight the critical role that both the blocklength and channel capacity play in determining the leakage threshold. The decreasing behavior of δ_L with increasing n illustrates that blocklength is a key parameter in improving security by reducing information leakage to the eavesdropper. Furthermore, increasing the capacity C enhances security by reducing δ_L, particularly for smaller blocklengths.

In practical terms, these findings suggest that in scenarios where the blocklength is constrained (e.g., in real-time communication systems with latency requirements), increased channel capacity can help mitigate the potential increase in leakage. Conversely, for applications that can tolerate larger blocklengths, the impact of channel capacity on leakage becomes less critical, and the system can achieve near-optimal security performance.

VI. Conclusion

We defined the notion of leakage density to analyze the information leaked to Eve in the finite blocklength regime. We specifically introduced the two notions of aggregate leakage and empirical average of leakage and used them in the Berry-Esseen theorem to bound the leakage in non-asymptotic Wiretap channels. Based on the choice of parameters, such as the blocklength, the channel charactersitics, the maximum leakage rate, probability of error, etc. we distinguished two cases that capture the interrelation of these parameters. We further applied the meta-converse to the channel from Alice to Eve to determine the leakage rate.

Practical applications of this study include IoT short-packet communications as well as ultra reliable low latency communication (URLLC) designed to adapt in real-time to changing conditions, ensuring that information leakage remains within acceptable bounds. Moreover, in the context of autonomous vehicles, fast and delay constrained non-asymptotic secure communication between vehicles and infrastructure is paramount to safety. Our analysis can be used to design communication systems that effectively prevent eavesdropping and ensure that control signals are transmitted securely and promptly, thus enhancing the safety and reliability of autonomous vehicle systems. Additionally, as computing moves closer to the edge of the network, ensuring the security of data processing at the edge—often in a resource-constrained environment—becomes crucial. Our analysis helps in designing security protocols that are both computation and bandwidth efficient, which is critical for edge devices processing sensitive data.

References

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

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

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

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

[5] K.-L. Besser, C. R. Janda, P.-H. Lin, and E. A. Jorswieck, "Flexible design of finite blocklength wiretap codes by autoencoders," in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 2512–2516.

[6] K.-L. Besser, A. Lonnstrom, and E. A. Jorswieck, "Neural network wiretap code design for multi-mode fiber optical channels," in *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2020, pp. 8738–8742.

[7] U. Somalatha, P. Mohapatra, and N. Pappas, "Performance analysis of the wiretap channel with a friendly jammer under finite blocklength," in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 239–244.

[8] Y. Yang, "Secure and timely status updates in the iot using short-packet permutation-based transmissions," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, 2023, pp. 1–6.

[9] S. Chen, M. Effros, and V. Kostina, "Lossless source coding in the point-to-point, multiple access, and random access scenarios," in *2019 IEEE International Symposium on Information Theory (ISIT)*, 2019, pp. 1692–1696.

[10] A. E. Gamal and Y. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[11] W. Feller, *An Introduction to Probability and Its Applications*. Wiley, 1971, vol. II.