Shahid Bahonar University of Kerman
Journal of Mahani Mathematical Research
Print ISSN: 2251-7952 Online ISSN: 2645-4505

APPLICATION OF TSALLIS ENTROPY IN DEFINING A NEW GENERALIZED STRONG AND WEAK SECRECY

S. Jalayeri, G.R. Mohtashami Borzadaran ✉, and M. Khorashadizadeh

Article type: Research Article
(Received: 10 September 2025, Received in revised form 20 March 2026)
(Accepted: 18 May 2026, Published Online: 19 May 2026)

Abstract. In this paper, we explore the diverse applications and distinctive properties of Tsallis entropy by introducing generalized definitions of strong and weak secrecy. Tsallis entropy suggests that generalized weak secrecy and strong secrecy are commonly employed in information-theoretic security challenges. Additionally, we examine the interplay between Tsallis entropy and the criteria for strong and weak secrecy. The primary motivation behind this study is to elucidate the concept of "generalized weak secrecy," a widely utilized notion. Also, this research delves into the precise relationship between conditional entropy and the minimum adversarial error probability, illustrating how generalized weak security can be translated into practical guarantees. For static and memoryless sources, it is demonstrated that the vanishing of the leakage rate requires the adversarial error probability to reach its upper bound. Moreover, generalized strong security, characterized by the vanishing of the variational distance, results in the complete operational failure of the adversary. These findings underscore the critical role of Tsallis entropy in assessing the security of systems.

Keywords: Weak secrecy, Strong secrecy, Adversary, Average symbol error probability, Block error probability, Conditional Tsallis entropy.
2020 MSC: 94A08, 94A17, 62P99, 68M25.

1. Introduction and Preliminaries

Information-theoretic security is a crucial concept, and the connection between conditional Tsallis entropy and security is an important topic to discuss. The term "security" refers to being free from danger or feeling safe. It is often used in compound words like "security measure", "security check", or "security guard." This text explores security from two different perspectives: strong secrecy and weak secrecy. Let X_n be the n-length encoded sequence of a message transmitted by the transmitter, and let Y_n denote the eavesdropper's information. Hence the message is said to be very safe, if

$$\lim_{n\to\infty} I(X_n, Y_n) = 0,$$

✉ grmohtashami@um.ac.ir, ORCID: 0000-0002-8841-1386
https://doi.org/10.22103/jmmr.2026.25899.1867
Publisher: Shahid Bahonar University of Kerman
How to cite: S. Jalayeri, G.R. Mohtashami Borzadaran, M. Khorashadizadeh, *Application of Tsallis entropy in defining a new generalized strong and weak secrecy*, J. Mahani Math. Res. 2026; 15(2): 477-498.

and weakly secure if

$$\lim_{n\to\infty} n^{-1} I(X_n, Y_n) = 0,$$

where $I(X_n, Y_n) = \sum_x \sum_y P_{X_n Y_n} \ln \frac{P_{X_n Y_n}}{P_{X_n} P_{Y_n}}$ is Shannon mutual information, for more information which one can refer to [4] and [20]. Strong and weak secrecy have diverse applications. This topic has been explored in various studies across different domains such as:

- Multimodal biometric authentication systems [28]:
  These systems identify individuals using biological features such as fingerprints, facial recognition, or iris patterns. Strong security in these systems is essential to prevent forgery and unauthorized access. Additionally, using multiple different models can enhance accuracy and reliability.

- Eavesdropping channels [26]:
  In digital communications, eavesdropping channels can gain access to sensitive information. Strong security in this area requires encryption and security protocols to prevent intrusion and data theft. Furthermore, examining vulnerabilities in these channels can help improve security methods.

- Physical layer security in wireless communication systems [14]:

- Physical layer security in instantaneous capacity channels [9]:
  In channels such as wireless networks, the presence of physical threats can easily lead to unauthorized access. Thus, strengthening security at this layer is crucial for protecting vital information.

- Wired networks [22]:
  Security in wired networks also faces challenges, including physical attacks and unauthorized access to equipment. Utilizing security protocols and encryption can help reinforce this security.

Additionally, studies have shown that there is a fundamental tradeoff between security and privacy in biometric security systems [10]. Moreover, reliability metrics analogous to information-theoretic security have also been considered in source or channel coding ([3]; [35]). [11] has also studied the interplay between Shannon information measures and reliability metrics.

The limitations of Shannon entropy in addressing certain anomalies observed in the realm of communication physics have sparked considerable interest. Although Shannon entropy enjoys widespread application across various disciplines, it often struggles to effectively capture the complexities of nonlinear

phenomena. A key attribute of Tsallis entropy is its non-additive quality, which indicates that it cannot be obtained simply by summing the entropies of its constituent parts. This unique characteristic allows for the exploration and modeling of novel and varied behaviors within intricate, nonlinear systems. Therefore, choosing Tsallis entropy as an alternative to Shannon entropy provides a more robust framework for accurately representing complex phenomena. This strategy not only deepens our comprehension of irregularities and system behaviors but also guides us toward more nuanced and precise scientific insights. In light of the significant relationship between strong and weak security frameworks and information theory, we propose a definition for generalized strong and weak secrecy *(generalized strong and weak secrecy)* rooted in Tsallis entropy, a well-known generalization.

The necessity of this research is to clarify the concept of weak secrecy, which is widely used but has not been clearly explained. generalized Weak secrecy alone is insufficient to show that the adversary's error probability is maximized, unless the secret is generated from a stationary and memoryless source. Furthermore, the relation among different reliability criteria with secrecy must be clarified, such as vanishing equivocation and vanishing error probability. Vanishing equivocation (equivocation refers to the conditional entropy of the secret given the adversary's knowledge, i.e., the ambiguity is directly related to the secrecy level of the secret.) is shown to be a stronger reliability criterion than vanishing error probability. It should be noted that the role of equivocation in information security is central and vital, as this metric provides a measure of the adversary's uncertainty about the secret and serves as a key indicator of the system's success in concealing information. Moreover, the precise relationships between secrecy metrics such as generalized weak and strong secrecy and their operational implications, such as maximizing the adversary's probability of error and determining the secrecy level of the secrets, are examined. This framework enables more comprehensive analysis and the design of more efficient security systems. These results must be used to generalize the channel coding theorem for discrete memoryless channels by utilizing different reliability criteria. So, this work explores the interactions between Tsallis entropy and the criteria defining both generalized strong and weak secrecy. [8] introduced an extension of entropy and [4] proposed the generalization of the entropy by hypothesizing a non-extensive entropy, (i.e., Tsallis entropy), which covers Shannon entropy in specific cases. Also, [24] defined the Tsallis entropy of degree $\alpha > 0, \alpha \neq 1$

$$T_\alpha(X) = \frac{1}{1-\alpha}\left(\sum_x P(x)^\alpha - 1\right),$$

and a form of conditional Tsallis entropy was introduced by

$$T_\alpha(X|Y) = \sum_y P(y)^\alpha T_\alpha(X|y),$$

where $T_\alpha(X|y) = \frac{1}{1-\alpha}\left(\sum_x P(x|y)^\alpha - 1\right)$.
The conditional Tsallis entropy was introduced based on the conditional Rényi entropy. [17] presented conditional entropic uncertainty relations for Tsallis entropy. Many researchers have studied on Tsallis entropy, such as [2], [31], [16], [23], [34], [29], [27], [21] and [15].

The parameter directly influences the security of systems. In systems utilizing Tsallis entropy, by adjusting this parameter, we can gain a deeper understanding of potential risks and vulnerabilities that may pose threats. This insight enables us to develop more effective security interfaces to safeguard our information and systems. The impact of α on information security is as follows:
1. In systems with $\alpha < 1$, sensitivity to rare and unusual information can pose a security risk. Such information may unexpectedly compromise system security. For instance, cyberattacks exploiting uncommon vulnerabilities can be particularly effective against these systems.
2. When α equals 1, information distribution is conventional, predictable, and measurable. It typically provides greater security as standard protection measures like encryption and conventional security protocols can be effectively employed.
3. In systems with α greater than 1, performance generally improves, and due to intrinsic organizational logic and structure, they can exhibit greater resilience to attacks. It is expected that systems be designed to minimize errors and weaknesses.
For example, consider a security system with two states: failure and operational. If the probability of failure is very low ($e.g., (p = 0.01)$) and the probability of being operational is $(1 - p = 0.99)$:
1. If $\alpha > 1$, then $T_\alpha(0.01, 0.99) = 0.0198$ when $\alpha = 2$. In this case, the system shows less sensitivity to such changes (errors), meaning that errors may have a minimal impact on the overall system performance.
2. If $\alpha < 1$, then $T_\alpha(0.01, 0.99) = -0.19$ when $\alpha = 0.5$. The system is sensitive to sudden and rare changes, which can quickly compromise its capabilities and make it more vulnerable to attacks.
3. If $\alpha = 1$, then $T_\alpha(0.01, 0.99) \approx 0.08$. In this case, Tsallis entropy converges to Shannon entropy, a common measure of uncertainty that indicates a balanced sensitivity to all events.

The Tsallis entropy and the conditional Tsallis entropy converge to Shannon entropy and conditional Shannon entropy as α approaches 1, respectively. Hence, taking $\alpha \to 1^+$ and evoking L'Hôpital's rule, for $\alpha > 1$, $I_\alpha^T(X_n, Y_n) \to$

$I(X_n, Y_n)$, where $I_\alpha^T(X_n, Y_n) = T_\alpha(X_n) - T_\alpha(X_n|Y_n)$ is Tsallis mutual information for $\alpha > 1$ defined by [33] and [7]. The role of equivocation in information security is central and vital, as this metric provides a measure of the adversary's uncertainty about the secret and serves as a key indicator of the system's success in concealing information. Moreover, the precise relationships between secrecy metrics such as weak and strong secrecy and their operational implications, such as maximizing the adversary's probability of error and determining the secrecy level of the secrets, are examined. This framework enables more comprehensive analysis and the design of more efficient security systems. In Section 2, we introduce the basics and initial concepts regarding strong and weak secrecy. Also, in the Section 3, we have considered the connection between different reliability criteria based on Tsallis entropy and studied connections of the conditional Tsallis entropy with secrecy.

2. **Main results**

Consider a common discrete source, from which $S^k = (S_1, S_2, ..., S_k)$ is generated to create a message. According to the received information, the recipient generates an estimate $\hat{S}^k = (\hat{S}_1, \hat{S}_2, ..., \hat{S}_k)$. Thus, the average symbol error probability and the block error probability can be respectively defined by [36] and [11]

$$\lambda_k = \frac{1}{k} \sum_{j=1}^{k} P(S_j \neq \hat{S}_j),$$

$$\mu_k = P(S^k \neq \hat{S}^k).$$

Also, let $\tilde{S}^k = (\tilde{S}_1, \tilde{S}_2, ...\tilde{S}_k) = F^*(\hat{S}^k)$, where

$$F^* = \underset{F^*}{argmin}\, P(S^k \neq (\hat{S}^k)),$$

where, F^* is the optimal decoder ($MaximumLikelihoodDecoder$) that minimizes the block error probability. Therefore, for the decoder, the modified average symbol error probability and modified the block error probability can be characterized respectively by [11]

$$\tilde{\lambda}_k = \frac{1}{k} \sum_{j=1}^{k} P(S_j \neq \tilde{S}_j),$$

$$\tilde{\mu}_k = P(S^k \neq \tilde{S}^k).$$

Let X and Y be two random variables taking values in the same, possibly countably infinite, alphabet $\chi = \{1, 2, ...\}$ and let $f(.)$ be an arbitrary function, then

$$\varepsilon = P(X \neq Y) = 1 - \sum_{w \in \chi} P_{XY}(w, w)$$

where $\varepsilon \leq 1 - P_X(1)$. If Y takes values on χ' which is not necessarily equal to χ consider

$$\begin{aligned} \hat{\varepsilon} &= \min_{f:\chi' \to \chi} P(X \neq f(Y)) \\ &= \sum_y P_Y(y)(1 - \max_z P_{X|Y}(z|y)) \\ &\leq 1 - \max_z P_X(z). \end{aligned}$$

Now, for any given P_X, we assume $P_X(i) \geq P_X(j)$ if $i < j$. If $0 < \eta \leq 1 - P_X(1)$ (This threshold η determines which of the primary probabilities of the distribution P_X (except the maximal probability $P_X(1)$) are bounded in the auxiliary distribution R.), the following Auxiliary probability distributions defined by [10]

$$R(P_X, \eta) = (1 - \eta, q_1, q_2, ...), \tag{1}$$

and

$$Q(P_X, \eta) = (\eta^{-1}q_1, \eta^{-1}q_2, ...),$$

so that the probability distribution is

$$q_j = \begin{cases} \theta & \text{if } P_X(j+1) > \theta \\ P_X(j+1) & \text{if } P_X(j+1) \leq \theta \end{cases}, \tag{2}$$

where, $0 < \theta < P_X(1)$, $Q(P_X, \eta)$ is a distribution and for $j \geq 1$

$$\eta = \sum_j q_j,$$

the key role of is to represent the minimum error probability. Since the Tsallis entropy of $R(P_X, \eta)$ denoted by $\phi_X^{T\alpha}(\eta) = T_\alpha(R(P_X, \eta))$ for $\alpha > 1$ is a concave, continuous and $\phi_X^{T\alpha}(\eta)$ is a strictly increasing function in η. Furthermore, $\phi_X^{T\alpha}(0) = 0$ and $\phi_X^{T\alpha}(1 - P_X(1)) = T_\alpha(P_X)$. Here, the main goal is to define a boundary function $\phi_X^{T\alpha}(\eta)$ that is used to obtain a tight bound on the conditional Tsallis entropy (equivocation) as a function of the minimum error probability.

Now, we present a few helpful Lemmas and Theorems. For a given marginal P_X and a given minimal error probability, in particular, we obtain the tightest upper bound on equivocation (conditional Tsallis entropy; $T_\alpha(X|Y)$) in terms of $\varepsilon = P(X \neq Y)$.

Lemma 2.1. ([31]) The generalized mutual entropy for $\alpha > 1$ is defined as,

$$I_\alpha^T(X, Y) = T_\alpha(Y) - T_\alpha(Y|X) = T_\alpha(X) - T_\alpha(X|Y),$$

where

$$T_\alpha(X|Y) = -\sum_x \sum_y P(x, y)^\alpha ln_\alpha P(x|y) = \frac{1}{1-\alpha} \sum_y P(y)^\alpha \sum_x P(x|y)^\alpha - 1.$$

Note that $\ln_\alpha(x) = \frac{x^{1-\alpha}-1}{1-\alpha}$. Also $T_\alpha(X|Y,Z) \leq T_\alpha(X|Z)$ and $T_\alpha(X|Y) \leq T_\alpha(X)$.

Theorem 2.2. Let X and Y be random variables taking values in the same, possibly countably infinite, alphabet. If $\varepsilon = P(X \neq Y) \leq 1 - P_X(1)$ for $\alpha > 1$ then

$$T_\alpha(X|Y) \leq h_\alpha(\varepsilon) + \varepsilon^\alpha T_\alpha(Q(P_X, \varepsilon)), \tag{3}$$

where

$$h_\alpha(\varepsilon) = -\varepsilon^\alpha \ln_\alpha(\varepsilon) - (1-\varepsilon)^\alpha \ln_\alpha(1-\varepsilon)$$

.

Proof. According to the Lemma 2.1, for ε and $\alpha > 1$,

$$T_\alpha(X|Y) = T_\alpha(X) - I_\alpha^T(X,Y) \tag{4}$$

$$\leq T_\alpha(X) - \min_{P_{X|Y}: P(X\neq Y)\leq\varepsilon} I_\alpha^T(X,Y). \tag{5}$$

Let the integer k and $P_X(k+1) < \theta < P_X(k)$ are chosen so that

$$\sum_{j=1}^{k} P_X(j) = (k-1)\theta + 1 - \varepsilon. \tag{6}$$

Similar works done by [12] and [6], for $\theta \leq P_k$, we have

$$\min_{P_{X|Y}=P(X\neq Y)\leq\varepsilon} I_\alpha^T(X,Y) = \frac{1}{1-\alpha}[\sum_{P_k\geq\theta} P_k^\alpha - 1] - \left[\frac{1}{1-\alpha}[(k-1)\theta^\alpha + (1-\varepsilon)^\alpha - 1\right]],$$

so,

$$T_\alpha(X) - \min_{P_{X|Y}=P(X\neq Y)\leq\varepsilon} I_\alpha^T(X,Y) \quad \frac{1}{1-\alpha}[\sum_{P_k<\theta} P_k^\alpha + (k-1)\theta^\alpha + (1-\varepsilon)^\alpha - 1]$$

$$= T_\alpha(R(P_X, \varepsilon)).$$

On the other hand, for $\alpha > 1$, we have

$$h_\alpha(\varepsilon) + \varepsilon^\alpha T_\alpha(Q(P_X,\varepsilon)) = \frac{\varepsilon^\alpha + (1-\varepsilon)^\alpha - 1}{1-\alpha} + \varepsilon^\alpha \left(\frac{(k-1)(\frac{\theta}{\varepsilon})^\alpha + \sum_{j=k+1}^{\infty} (\frac{P_j}{\varepsilon})^\alpha - 1}{1-\alpha} \right)$$

$$= T_\alpha(R(P_X,\varepsilon)).$$

□

Example 2.3. *Let X be a binary random variable with distribution $P_X(1) = 0.6$ and $P_X(2) = 0.4$. Also assume $\epsilon = P(X \neq Y) = 0.2$. According to the above theorem, R is a distribution constructed from P_X and ϵ. For $\epsilon = 0.2$ and $\theta = 0.2$, the distribution R is obtained as $\{0.8, 0.2\}$. We now compute the numerical values of the bound for different values of α: As can be observed, as α increases from 1.5 to 3, the upper bound on $T_\alpha(X|Y)$ decreases from 0.425*

α	$h_\alpha(0.2)$	$T_\alpha(Q)$	ϵ^α	*Upper bound on* $T_\alpha(X\|Y)$
1.5	0.390	0.390	0.0894	0.425
2	0.32	0.32	0.04	0.3328
3	0.24	0.24	0.008	0.2419

TABLE 1. Numerical values of the upper bound in Theorem 2.2 for $\epsilon = 0.2$ and different α

to 0.242. *This demonstrates that for a fixed error probability, a larger* α *yields a tighter bound, and consequently* T_α *converges to zero more rapidly.*

Remark 2.4. For $\varepsilon < 1 - P_X(1)$, the upper bound in (2) is sharp when $P_{XY}(k,s)$ is given by

$$P_{XY}(k,s) = \begin{cases} 0 & s = w+1, ... \\ P_X(k)\frac{P_X(s)-\theta}{1-\varepsilon-\theta} & s = 1, ..., w; k = w+1, .. \\ \theta\frac{P_X(s)-\theta}{1-\varepsilon-\theta} & s = 1, .., w; k = 1, .., w; k \neq s, \\ (1-\varepsilon)\frac{P_X(s)-\theta}{1-\varepsilon-\theta} & s = k = 1, .., w \end{cases} \tag{7}$$

that defined by

$$P_Y(s) = \begin{cases} \frac{P_X(s)-\theta}{1-\varepsilon-\theta} & s = 1, ..., w \\ 0 & Otherwise, \end{cases}$$

and

$$P_{X|Y}(k|s) = \begin{cases} P_X(k) & k = w+1, ... \\ \theta & k = 1, ..., w; k \neq s, \\ (1-\varepsilon) & k = s = 1, ..., w \end{cases}$$

where θ depends on ε and P_X through (2).

Example 2.5. Suppose $P_X = \{0.5, 0.4, 0.05, 0.05\}$ and $\varepsilon = 0.3$, then using (6) and (7) via $\theta = 0.2$ leads to

$$P_{XY} = \begin{bmatrix} 0.42 & 0.08 & 0 & 0 \\ 0.12 & 0.28 & 0 & 0 \\ 0.03 & 0,02 & 0 & 0 \\ 0.03 & 0.02 & 0 & 0 \end{bmatrix},$$

so, we have $P[X \neq Y] = 0.08 + 0.12 + 0.03 + 0.03 + 0.02 + 0.02 = \varepsilon$ which shows that equality can be attained in Inequality (2).

The next result generalizes Theorem 2.2 upper bounding $T_\alpha(X|Y)$ in terms of $\hat{\varepsilon} = \min_f P(X \neq f(Y))$. The following Theorem establishes a precise mathematical framework connecting equivocation to the adversary's minimum error probability. This connection is crucial because it allows the weak security metric to translate into practical security guarantees. Specifically, since $\phi_X^{T_\alpha}(.)$ is strictly increasing, the lemma ensures that if the adversary's error probability

is small, the equivocation must also be small. This implies that controlling the conditional entropy directly and mathematically bounds the adversary's error probability (the operational metric).

Theorem 2.6. Let X and Y be random variables taking the same values, possibly countably infinite, alphabet. For $\alpha > 1$ then

$$T_\alpha(X|Y) \leq \phi_X^{T_\alpha}(\min_f P(X \neq f(Y)) \tag{8}$$

$$\leq \phi_X^{T_\alpha}(P(X \neq Y)). \tag{9}$$

Proof. Let $f^* = \underset{f^*}{argmin}\, P(X \neq f^*(Y))$ and $Z = f^*(Y)$. Then $\varepsilon = P(X \neq Z) \leq 1 - P_X(1)$ and

$$T_\alpha(X|Y) = T_\alpha(X|Y,Z) \tag{10}$$

$$\leq T_\alpha(X|Z) \tag{11}$$

$$\leq T_\alpha(R(P_X, \hat{\varepsilon})), \tag{12}$$

where $T_\alpha(R(P_X, \hat{\varepsilon})) = h_\alpha(\hat{\varepsilon}) + \hat{\varepsilon}^\alpha T_\alpha(Q(P_X, \hat{\varepsilon})$ and (12) proves similar to the above Theorem. The second inequality follows $\phi_X^{T_\alpha}(\eta)$, which is a strictly increasing function in η. □

Example 2.7. *Assume our source has four symbols with the following probabilities (probabilities must be in descending order):* $P_X(1) = 0.5, \quad P_X(2) = 0.3, \quad P_X(3) = 0.1, \quad P_X(4) = 0.1$. *Suppose the adversary has gained information such that their minimum guessing error probability for the secret is* $\epsilon = 0.4$. *According to references, to calculate the function* $\Phi_x(0.4)$, *we must construct a new probability distribution named* $R(P_X, \epsilon)$.

We need to find θ *such that* $\sum \min(\theta, P_X(i+1)) = \epsilon$. *If we take* $\theta = 0.2$, *then:*

$$q_1 = \min(0.2, 0.3) = 0.2, ; q_2 = \min(0.2, 0.1) = 0.1, ; q_3 = \min(0.2, 0.1) = 0.1$$

, where the sum of q_i *equals 0.4. The distribution* R *is defined as* $\{1 - \epsilon, q_1, q_2, q_3\} = \{0.6, 0.2, 0.1, 0.1\}$. *The goal is to compute the Tsallis entropy with* $\alpha = 2$ *for this distribution, which provides an upper bound on the conditional entropy* $T_2(X|Y)$ *in terms of Tsallis entropy.*
Calculating the Tsallis entropy for distribution R:
$\sum p_i^2 = 0.6^2 + 0.2^2 + 0.1^2 + 0.1^2 = 0.36 + 0.04 + 0.01 + 0.01 = 0.42$,
$T_2(R) = 1 - 0.42 = 0.58$.
For comparison, the Tsallis entropy of the original source:
$\sum p_i^2 = 0.5^2 + 0.3^2 + 0.1^2 + 0.1^2 = 0.25 + 0.09 + 0.01 + 0.01 = 0.36$,
$T_2(X) = 1 - 0.36 = 0.64$.
If the adversary's error probability is 0.4, their maximum uncertainty (conditional entropy) in terms of Tsallis entropy cannot exceed 0.58. This bound is meaningful because it is lower than the Tsallis entropy of the source (0.64).

These calculations show that, for any amount of information leakage, we can precisely determine the physical limitations the adversary faces in guessing the secret.

Example 2.8. *(Investigating the effect of block length n and parameter α on the upper bound of conditional Tsallis entropy) Let the source X have four symbols with distribution $P_X = \{0.5, 0.3, 0.1, 0.1\}$. In a practical scenario with block length n, the minimum error probability $\epsilon_n = e^{-n/100}$ decreases exponentially with n. For each pair (n, α), the upper bound on $T_\alpha(X|Y_n)$ is obtained through the auxiliary distribution $R(P_X, \epsilon_n)$, which is constructed according to the method in Example 2.7. The numerical results are reported in the following table.*

n	ϵ_n	$\alpha = 1.5$	$\alpha = 2$	$\alpha = 3$
100	$e^{-1} \approx 0.3679$	0.710	0.520	0.330
200	$e^{-2} \approx 0.1353$	0.452	0.298	0.164
400	$e^{-4} \approx 0.0183$	0.121	0.058	0.021

For a fixed α, increasing n (decreasing ϵ_n) significantly reduces the bound T_α. Also, for a fixed n, increasing α makes the bound smaller; for example, at $n = 200$, we have:

$$T_{1.5} \approx 0.452, \quad T_2 \approx 0.298, \quad T_3 \approx 0.164,$$

which indicates that the larger the α, the faster the conditional Tsallis entropy converges to zero.
Following [6], P_{X^*} is majorized by P_X if for all k,

$$\sum_{j=1}^{k} P_{X^*}(j) \leq \sum_{j=1}^{k} P_X(j).$$

Theorem 2.9. If P_{X^*} is majorized by P_X, then for any $\alpha > 1$ and $0 < \eta \leq 1 - P_X(1)$, we have:

$$\phi_{X^*}^{T\alpha}(\eta) \geq \phi_X^{T\alpha}(\eta).$$

Proof. Since P_{X^*} majorized by P_X, the result follows from Lemma 4 in [11]. As shown by [13], for $\alpha > 1$, the function $\phi_{X^{T\alpha}}(\eta)$ is concave. Therefore, according to [6], the proof is completed. □

The following theorem shows the relation between the block equivocation $\frac{1}{k}T_\alpha(S^k \mid \hat{S}^k)$ and the average symbol error probability $\tilde{\lambda}_k$.

Theorem 2.10. There exists a random variable S such that $T_\alpha(S) < \infty$and P_S is majorized by P_{S_i} for all i. Then for $\alpha > 1$, we have

$$\frac{1}{k}T_\alpha(S^k \mid \hat{S}^k) \leq \phi_X^{T\alpha}(\tilde{\lambda}_k).$$

Proof. Note that

$$\frac{1}{k}T_\alpha(S^k|\hat{S}^k) = \frac{1}{k}\sum_{j=1}^{k} T_\alpha(S_j|S^{j-1},\hat{S}^k) \tag{13}$$

$$\leq \frac{1}{k}\sum_{j=1}^{k} T_\alpha(S_j|\hat{S}^k) \tag{14}$$

$$\leq \frac{1}{k}\sum_{j=1}^{k} \phi_{S_j}^{T\alpha}(\min_f P[S_j \neq f(\hat{S}^k)]) \tag{15}$$

$$\leq \phi_{S_j}^{T\alpha}(\frac{1}{k}\sum_{j=1}^{k} \min_f P[S_j \neq f(\hat{S}^k)]) \tag{16}$$

$$\leq \phi_S^{T\alpha}(\tilde{\lambda}_k), \tag{17}$$

where (13), (14) and (15) follows from [24] and (Theorem 2.2) respectively. Inequality (16) implies from the concavity of $\phi_X^{T\alpha}$ for $\alpha > 1$, and (17) follows from Theorem 2 as P_S is majorized by P_{S_i}. □

Example 2.11. *Assume that the data source S (The block length (k) is 1000 bits.) is a stationary and memoryless source with uniform distribution $P_s = \{0.5, 0.5\}$. Based on the above lemma, the relation $\frac{1}{k}T_2(S^k|\hat{S}^k) \leq \Phi_S(\tilde{\lambda}_k)$ holds. Suppose the system is in a weak security state and the information leakage rate $\frac{1}{k}I_2^T(S^k,\hat{S}^k)$ is very small and equal to 0.05. Now, according to the definition of mutual information, the block equivocation is calculated as follows:*

$$\frac{1}{k}I_2^T(S^k,\hat{S}^k) = T_2(S) - \frac{1}{k}T_2(S^k|\hat{S}^k).$$

Therefore,

$$0.05 = 0.5 - \frac{1}{k}T_2(S^k|\hat{S}^k) \Rightarrow \frac{1}{k}T_2(S^k|\hat{S}^k) = 0.45.$$

Since the function $\phi_S^{T_2}(\lambda)$ is exactly equal to the Tsallis entropy function $T_2(\lambda)$ with error probability λ, we have

$$0.45 \leq T_2(\tilde{\lambda}_k).$$

We need to find a value for the average symbol error probability $\tilde{\lambda}_k$ such that its entropy is at least 0.45. By solving the inverse of the entropy function, $\tilde{\lambda}_k$ must be at least 0.342.

The above calculations prove that if the information leakage rate of your system is 0.05 bits per symbol, then in a block of 1000 bits, the adversary will, on average, guess at least 342 bits incorrectly. This example shows how, as we move towards perfect security by reducing the leakage from 0.05 to 0, the adversary's error probability approaches its theoretical upper bound of 0.5 (500 errors in 1000 bits).

Example 2.12. *(Investigating the effect of block length k and parameter α in a binary source) Consider a stationary and memoryless source with uniform binary distribution $P_S = \{0.5, 0.5\}$ and block length k. Assume the system is in a weak security state, and the Tsallis mutual information rate decreases as follows:*

$$\frac{1}{k} I_\alpha^T(S^k, \hat{S}^k) = 0.1\, e^{-k/500}.$$

From the definition of Tsallis mutual information, we have

$$\frac{1}{k} I_\alpha^T(S^k, \hat{S}^k) = T_\alpha(S) - \frac{1}{k} T_\alpha(S^k|\hat{S}^k),$$

where $T_\alpha(S)$ for the uniform binary distribution is given by

$$T_\alpha(S) = \frac{1 - 2^{1-\alpha}}{\alpha - 1}, \quad \alpha \neq 1.$$

Specifically, $T_{1.5}(S) = \frac{1-2^{-0.5}}{0.5} = 2(1-2^{-0.5}) \approx 0.5858$, $T_2(S) = 0.5$, $T_3(S) = \frac{1-2^{-2}}{2} = 0.375$. *Therefore,*

$$\frac{1}{k} T_\alpha(S^k|\hat{S}^k) = T_\alpha(S) - 0.1e^{-k/500}.$$

According to the above theorem, the upper bound for this quantity is given by $\phi_S^{T_\alpha}(\tilde{\lambda}_k)$. For a uniform binary source, $\phi_S^{T_\alpha}(\tilde{\lambda}_k) = T_\alpha(\tilde{\lambda}_k)$, hence

$$T_\alpha(\tilde{\lambda}_k) \geq T_\alpha(S) - 0.1e^{-k/500}.$$

The following table presents the numerical values of $\frac{1}{k} T_\alpha$ for several k and α:

k	$\frac{1}{k} I_\alpha^T$	$\frac{1}{k} T_{1.5}$	$\frac{1}{k} T_2$	$\frac{1}{k} T_3$
500	$0.1e^{-1} \approx 0.0368$	$0.5858 - 0.0368 = 0.5490$	$0.5 - 0.0368 = 0.4632$	$0.375 - 0.0368 = 0.3382$
1000	$0.1e^{-2} \approx 0.0135$	$0.5858 - 0.0135 = 0.5723$	$0.5 - 0.0135 = 0.4865$	$0.375 - 0.0135 = 0.3615$
2000	$0.1e^{-4} \approx 0.0018$	$0.5858 - 0.0018 = 0.5840$	$0.5 - 0.0018 = 0.4982$	$0.375 - 0.0018 = 0.3732$

As k increases, the normalized conditional entropy approaches $T_\alpha(S)$ (information leakage decreases). For a fixed k, increasing α reduces the value of $\frac{1}{k} T_\alpha$, indicating faster convergence.

The provided bounds depend on the block length n and decrease as n increases (i.e., as the error probability decreases). The parameter α has an inverse effect on the bounds: the larger the α, the smaller the bound and the faster the convergence of T_α to zero.

Theorem 2.13. For X defined on an arbitrary, possible infinite alphabet with finite entropy, for $\alpha > 1$, f the minimum error probability $\min_f P(X \neq f(Y_n)) \to 0$, tends to zero, then

$$T_\alpha(X|Y_n) \to 0,$$

Proof. We now proceed to obtain the tightest lower bound on error probability for a fixed P_X. Let

$$\phi_X^{T\alpha}(\hat{\varepsilon}) = T_\alpha(R(P_X, \hat{\varepsilon})),$$

where R is defined in (1). Since entropy is Schur-concave ([13]) and $R(P_X, \hat{\epsilon})$ is majorized by $R(P_X, \delta)$ if $\hat{\epsilon} > \delta$,$\phi_X^{T\alpha}(\hat{\epsilon})$ is a strictly increasing function. It can be verified that $\phi_X^{T\alpha}(\hat{\epsilon})$ is continuous and hence, ${\phi_X^{T\alpha}}^{-1}(.)$ exists. By Theorem 2.2 and $\phi_X^{T\alpha}(\hat{\varepsilon}) = T_\alpha(R(P_X, \hat{\varepsilon}))$, we have

$$(18) \qquad {\phi_X^{T\alpha}}^{-1}(T_\alpha(X|Y_n)) \leq \min_f P(X \neq f(Y_n)).$$

Furthermore, for any givenP_X, and $0 \leq \tau \leq T_\alpha(X) < \infty$,

$$(19) \qquad \min_{P_{Y|X}: T_\alpha(X|Y)=\tau} \min_f P(X \neq f(Y_n)) = {\phi_X}^{{T\alpha}^{-1}}(\tau).$$

Although an analytical expression for ${\phi_X^{T\alpha}}^{-1}$ is unknown, it can be readily found numerically. Note that both ${\phi_X^{T\alpha}}^{-1}(w)$ and $\frac{d}{dw}{\phi_X^{T\alpha}}^{-1}(w)$ are equal to 0 when $w = 0$. As an application of (18), consider a random process $\{X_n\}_{n=-\infty}^{\infty}$, taking values on a finite or countably infinite alphabet. Consider the minimum prediction error

$$\hat{\varepsilon}_n = \min_f p(X_n \neq f(X^{n-1})),$$

where $X^{n-1} = (X_1, ..., X_{n-1})$. Then the predictability of the process of [22] is defined as

$$\Pi = \lim_{n\to\infty} \hat{\varepsilon}_n.$$

It easily follows from the continuity of ϕ that the entropy rate $\lim_{n\to\infty} T_\alpha(X_n|X_1^{n-1})$ and the predictability satisfy

$$(20) \qquad \lim_{n\to\infty} T_\alpha(X_n|X_1^{n-1}) \leq \phi_X^{T\alpha}(\Pi),$$

when the process is stationary, where X stands for the distribution of X_n. According to (19), for any P_X, there exists a process with a first-order distribution P_X, whose predictability and entropy rate satisfy (20) with equality □

3. *Connections of conditional entropy with secrecy*

Note that in a cryptosystem, the amount of resources utilized to generate a secret X_n is represented by n, and the adversary somehow knows Y_n. Now, n can be considered as the number of observations, the number of channels used, storage size, etc. This definition allows secrets to be produced from either serial or non-serial sources. If a secret is created from a serial source, then the source output is indicated by $S^n = (S_1, S_2, ..., S_n)$, and the adversary produces an estimate $\hat{S}^n = (\hat{S}_1, \hat{S}_2, ..., \hat{S}_n)$. We show that generalized strong security is significantly stronger than the zero-variation-distance criterion; in other words, vanishing variation distance (the discriminability criterion) alone

suffices to guarantee the minimum adversary error probability. Then the relationship between generalized weak security and the maximum adversary error probability is specified.

3.1. **Generalized strong secrecy.** *$I_\alpha^T(X_n, Y_n)$ quantifies the amount of information shared or leaked about the secret, strictly constraining this quantity to zero yields an absolute leakage bound. So, we define generalized strong secrecy as follow*

$$\lim_{n\to\infty} I_\alpha^T(X_n, Y_n) = 0, \tag{21}$$

which can more over be represented in terms of the Kullback-Leibler divergence. By three important relations from q-deformed algebra expressed in [32], we have

$$\begin{aligned} D_\alpha^T(P_{XY}||P_X \times P_Y) &= -\sum_x \sum_y P_{XY} Ln_\alpha \frac{P_X P_Y}{P_{XY}} \\ &= -\sum_x \sum_y P_{XY}(Ln_\alpha P_Y + P_Y^{1-\alpha} Ln_\alpha \frac{1}{P_{Y|X}}) \\ &= -\sum_y P_Y Ln_\alpha P_Y + \sum_x \sum_y (P_Y P_X)^{1-\alpha} P_{XY}^\alpha Ln_\alpha P_{Y|X} \\ &\leq -\sum_y P_Y^\alpha Ln_\alpha P_Y + \sum_x \sum_y P_{XY}^\alpha Ln_\alpha P_{Y|X} \\ &= T_\alpha(Y) - T_\alpha(Y|X) \\ &= I_\alpha^T(X, Y). \end{aligned}$$

The inequality is satisfied because $P_Y^\alpha \leq P_Y$ for any y and $\alpha > 1$, and $Ln_\alpha(t) \leq 0$ for any $0 \leq t \leq 1$ and $\alpha > 1$, then

$$I_\alpha^T(X, Y) \geq D_\alpha^T(P_{XY}||P_X \times P_Y).$$

By our definition (21), if generalized strong secrecy is satisfied, then

$$D_\alpha^T(P_{XY}||P_X \times P_Y) \to 0, \tag{22}$$

this means that X_n and Y_n can be expressed as asymptotically independent in Kullback-Leibler divergence.

At that point, it is natural to regard vanishing other divergence measures, e.g., the variation distance. Let $V(P;Q) = \sum_{x,y} |P_{X_n,Y_n}(x,y) - P_{X_n}(x)P_{Y_n}(y)|$ be the total variation distance, then for any $\alpha \in (0;1]$,

$$\ln \sum_{x\in\chi} P_X^\alpha Q_X^{1-\alpha} \leq \sum_{x\in\chi} P_X^\alpha Q_X^{1-\alpha} - 1,$$

and

$$\frac{1}{1-\alpha} l \sum_{x\in\chi} P_X^\alpha Q_X^{1-\alpha} \leq \frac{1}{\ln 2(1-\alpha)} \left(\sum_{x\in\chi} P_X^\alpha Q_X^{1-\alpha} - 1 \right),$$

therefore $D_\alpha(P||Q) \leq \frac{1}{\ln 2} D_\alpha^T(P||Q)$, *and* $\frac{\alpha}{2} V^2(P,Q) \leq D_\alpha(P||Q)$ *then,*

$$\frac{\alpha \ln 2}{2} V^2(P,Q) \leq D_\alpha^T(P||Q),$$

equality occurres whenever $\sum_{x\in\chi} P_X^\alpha Q_X^{1-\alpha} = 1$. *According to the above inequality*

$$V(P_{X_n,Y_n}, P_{X_n} P_{Y_n}) \to 0.$$

$\rho_\alpha^T(X_n, Y_n)$ *indicates a kind of correlation between* X *and* Y. *[7] defined a parametrically extended correlation coefficient in terms of Tsallis mutual information such that*

$$\rho_\alpha^T(X_n, Y_n) = \frac{I_\alpha^T(X_n, Y_n)}{T_\alpha(X_n, Y_n)},$$

for $T_\alpha(X_n) > 0$, $T_\alpha(Y_n) > 0$ *and* $\alpha > 1$. *Hence, if generalized strong secrecy is satisfied and also* $T_\alpha(X_n, Y_n) > 0$, *then* $\rho_\alpha^T(X_n, Y_n) \to 0$. *So,* X_n *and* Y_n *can be expressed as asymptotically independent in a parametrically extended correlation coefficient. In the following, [7] defined an entropic distance between* X *and* Y *by*

$$\tilde{d}_\alpha(X_n, Y_n) = 1 - \rho_\alpha^T(X_n, Y_n),$$

for $T_\alpha(X_n) > 0$, $T_\alpha(Y_n) > 0$ *and* $\alpha > 1$. *Hence, if generalized strong secrecy is satisfied, then* $\tilde{d}_\alpha(X_n, Y_n) \to 1$. *Therefore,* X_n *and* Y_n *can be expressed as asymptotically independent at an entropic distance.*

Also, [7] defined another correlation coefficient in terms of Tsallis mutual information by

$$\hat{\rho}_\alpha^T(X_n, Y_n) = \frac{I_\alpha^T(X_n, Y_n)}{max\left\{T_\alpha(X_n), T_\alpha(Y_n)\right\}},$$

for $T_\alpha(X_n) > 0$, $T_\alpha(Y_n) > 0$ *and* $\alpha > 1$. *Hence, if generalized strong secrecy is satisfied then* $\hat{\rho}_\alpha^T(X_n, Y_n) \to 0$. *Thus,* X_n *and* Y_n *can be expressed as asymptotically independent. In the following, [7] defined an entropic distance between* X *and* Y *by*

$$\hat{d}(X_n, Y_n) = 1 - \hat{\rho}_\alpha^T(X_n, Y_n),$$

for $T_\alpha(X_n) > 0$, $T_\alpha(Y_n) > 0$ *and* $\alpha > 1$. *Hence, if generalized strong secrecy is satisfied, then* $\hat{d}_\alpha(X_n, Y_n) \to 1$. *So,* X_n *and* Y_n *can be expressed as asymptotically independent at an entropic distance.*

To relate the criterion of indistinguishability (vanishing change distance) and information leakage, it can be stated that strong security (vanishing mutual information) requires the disappearance of change distance. This leads to complete operational failure for the adversary.

Lemma 3.1. Consider a system with a serial source then the followings are equivalent

1. $\lim_{n\to\infty} V(P_{S_n,\hat{S}_n}, P_{S_n}P_{\hat{S}_n}) = 0$
2. $V(P_{S_m,\hat{S}_m}, P_{S_m}P_{\hat{S}_m}) = 0, \forall m$
3. $I_\alpha^T(S_m, \hat{S}_m) = 0, \forall m$
4. $\lim_{n\to\infty} I_\alpha^T(S_n, \hat{S}_n) = 0$

Proof. From the Theorem 2 of [11], for all $n > m$ where fix m, (1) follows (2). If (2) is true, then for all b and c such that $P_{S_m\hat{S}_m}(b,c) > 0$,

$$P_{S^m,\hat{S}^m}(b,c) = P_{S^m}(b)P_{\hat{S}^m}(c).$$

Therefore, $I_\alpha^T(S_m, \hat{S}_m) = 0$ and (2) implies (3). By taking $m \to \infty$ (3) follows (4). Eventually, (4) implies (1) due to Pinsker's inequality. □

When a system with a serial source is needed to satisfy strong secrecy, it is proportionate to requiring S_m and $\hat{S}_m$ are independent for all finite m.

3.2. **Generalized weak secrecy.** *We define generalized Weak secrecy for $\alpha > 1$ as follow*

$$\lim_{n\to\infty} n^{-1} I_\alpha^T(X_n, Y_n) = 0. \tag{23}$$

The leakage rate is achieved when the mutual information rate $I_\alpha^T(X_n, Y_n)$ between the secret X^n and the adversary's knowledge Y^n tends to zero. Here, note that a serial source is stationary with a positive entropy rate. Then the weak secrecy is equivalent to

$$\lim_{k\to\infty} k^{-1} I_\alpha^T(S_k, S_k) = 0. \tag{24}$$

For a general secrecy system, weak secrecy in (24) *is compared with secure criteria*

$$\lim_{n\to\infty} \frac{T_\alpha(X_n|Y_n)}{T_\alpha(X_n)} = 1, \tag{25}$$

The following theorem compares the criterion of perfect privacy $\lim_{n\to\infty} \frac{T_\alpha(X_n|Y_n)}{T_\alpha(X_n)}$ with weak security and determines the conditions under which they are equivalent. It should be noted that if $\lim_{n\to\infty} \frac{T_\alpha(X_n|Y_n)}{T_\alpha(X_n)} = 1$, then the adversary has not gained any meaningful information about the secret.

Theorem 3.2. Assume X_n and Y_n are defined on the same alphabet, then
1. if $\lim_{n\to\infty} \frac{T_\alpha(X_n|Y_n)}{T_\alpha(X_n)} = 1$ implies $\lim_{n\to\infty} \frac{1}{n} I_\alpha^T(X_n, Y_n) = 0$.
2. if $\frac{T_\alpha(X_n)}{n} > 0$ $\lim_{n\to\infty} \frac{T_\alpha(X_n|Y_n)}{T_\alpha(X_n)} = 1$ if and only if

$$\lim_{n\to\infty} \frac{1}{n} I_\alpha^T(X_n, Y_n) = 0.$$

Proof. 1) If $\lim_{n\to\infty} \frac{T_\alpha(X_n|Y_n)}{T_\alpha(X_n)} = 1$, then $\lim_{n\to\infty} \frac{T_\alpha(X_n|Y_n)-T_\alpha(X_n)}{T_\alpha(X_n)} = 0$. So,

$$\lim_{n\to\infty} \frac{I_\alpha^T(X_n, Y_n)}{T_\alpha(X_n)} = 0.$$

2) The proof of the "if" part is obvious from Section 1 of the theorem. On the other hand since $T_\alpha(X_n) \leq \ln n \leq n-1 \leq n$ then,

$$\frac{I_\alpha^T(X_n, Y_n)}{T_\alpha(X_n)} \geq \frac{I_\alpha^T(X_n, Y_n)}{n} \geq 0.$$

Also, for the second part, we indicate,

If $\lim_{n\to\infty} \frac{1}{n} I_\alpha^T(X_n, Y_n) = 0$ then $\frac{1}{n} \lim_{n\to\infty} T_\alpha(X_n|Y_n) = \frac{1}{n} \lim_{n\to\infty} T_\alpha(X_n)$.

Hence $n^{-1}T_\alpha(X_n) > 0$, so $\lim_{n\to\infty} \frac{T_\alpha(X_n|Y_n)}{T_\alpha(X_n)} = 1$. □

This maximum probability of error ($\tilde{\lambda}_{\max}$) means that the adversary has the minimal possible advantage in guessing the message. Strong security always ensures that the adversary reaches the maximum probability of error. By contrast, weak security alone is not sufficient to guarantee the maximum error probability unless the secret source is stationary and memoryless. The following theorem shows that weak secrecy, under the assumption that the secret source is stationary and memoryless, guarantees the adversary's maximum probability of error.

Theorem 3.3. Let (the maximum average symbol error probability) $\tilde{\lambda}_{\max} = 1 - \max_s P_S(s) > 0$, if (25) is satisfied For any discrete stationary memoryless source with distribution P_S, then

$$\lim_{k\to\infty} \tilde{\lambda}_k = \tilde{\lambda}_{\max}.$$

Proof. If $\lim_{k\to\infty} \frac{1}{k} I_\alpha^T(S^k, \hat{S}^k) = 0$, then

$$\lim_{k\to\infty} \frac{1}{k} T_\alpha(S^k|\hat{S}^k) = \lim_{k\to\infty} \frac{1}{k} T_\alpha(S^k) = T_\alpha(S).$$

Together with $\phi_S^{T\alpha}(\tilde{\lambda}_k) \geq k^{-1}T_\alpha(S^k|\hat{S}^k)$ from Theorem 2.9, $\lim_{k\to\infty} \phi_S^{T\alpha}(\tilde{\lambda}_k) \geq T_\alpha(S)$. Since $\phi_S^{T\alpha}(.)$ is continuous, and we know $\phi_S^{T\alpha}(\lambda_{\max}) = T_\alpha(S)$. So,

$$\lim_{k\to\infty} \frac{1}{k} I_\alpha^T(S^k, \hat{S}^k) = 0 \Rightarrow \lim_{k\to\infty} \tilde{\lambda}_k = \tilde{\lambda}_{\max}.$$

□

The above theorem shows that for a static and memoryless source, weak security (vanishing information leakage rate) leads to a practical outcome. It is proved that weak security requires the average probability of adversarial symbolic error to reach its maximum value ($\lambda_{\max}$). This result transforms weak security into a strong, stringent barrier where the adversary faces the highest

possible error in detecting information.
The following theorems consider different reliability criteria for source or channel coding. First, in the following theorem, the connection between vanishing error probability and vanishing normalized equivocation is summarized.

Theorem 3.4. For any general discrete source, if there exists S such that $T_\alpha(S) < \infty$ and P_S is majorized by P_{S_i} for all i, then the followings are satisfied:

1. $\lim_{k\to\infty} \mu_k = 0$
2. $\lim_{k\to\infty} \lambda_k = 0$
3. $\lim_{k\to\infty} \frac{1}{k} \sum_{j=1}^{k} T_\alpha(S_j|\hat{S}^k) = 0$
4. $\lim_{k\to\infty} \frac{1}{k} T_\alpha(S^k|\hat{S}^k) = 0$

Proof. Equation (1) implies (2) which results from the Theorem 5 of [11]. Since $0 < \tilde{\lambda}_k \leq \lambda_k$ (2) implies $\lim_{k\to\infty} \tilde{\lambda}_k = 0$ and hence $\lim_{k\to\infty} \phi_S^{T\alpha}(\tilde{\lambda}_k) = 0$. Together with Theorem 2 (2) implies (3). Since

$$\frac{1}{k} T_\alpha(S^k|\hat{S}^k) = \frac{1}{k} \sum_{j=1}^{k} T_\alpha(S_j|S^{j-1}, \hat{S}^k) \leq \frac{1}{k} \sum_{j=1}^{k} T_\alpha(S_j|\hat{S}^k),$$

(3) implies (4). □

Theorem 3.5. For any general discrete source, if there exists S such that $T_\alpha(S) < \infty$ and P_S is majorized by P_{S_i} for all i, then the following are satisfied

1. $\lim_{k\to\infty} \tilde{\mu_k} = 0$
2. $\lim_{k\to\infty} \tilde{\lambda_k} = 0$
3. $\lim_{k\to\infty} \frac{1}{k} T_\alpha(S^k|\hat{S}^k) = 0$

Proof. Equation (1) implies (2) which results from Theorem 6 of [11]. By Theorem 2 (2) implies (3). □

Example 3.6. Let

$$\hat{S}_k = \begin{cases} S_k & \text{with probability } \frac{1}{2} \\ \bar{S}_k & \text{with probability } \frac{1}{2}, \end{cases}$$

where $\bar{S}_i = 1 - S_i$. Let S_k be generated by a stationary memoryless source with distribution $P_S = \{0.5; 0.5\}$ for example $\alpha = 2$. Then $\frac{1}{k} T_\alpha(S^k|\hat{S}^k) = \frac{3}{8k} \to 0$ but $T_\alpha(S_i|\hat{S}_i) = \frac{3}{8}$ for all i and $\lambda_k = \mu_k = \frac{1}{2}$.

So, this example demonstrates that the implications stated in Theorem 3.4 do not hold in the reverse direction.
The following example, based on Theorem 3.3, considers a cryptographic key distribution system and shows how Tsallis criteria (mutual information and conditional entropy) relate to adversarial reliability measures (probability of error).

Example 3.7. *A security entity (such as a digital identity provider) generates long binary cryptographic keys Sk from a stationary, memoryless source with a probability distribution* $P_S = \{0.5, 0.5\}$. *The adversary observes the side information* $\hat{S}_k$ *and uses the maximum-likelihood decoding method to guess the key.* $T_\alpha(S) = \frac{1}{2}$ *and* $\tilde{\lambda}_{\max} = 1 - \max(\frac{1}{2}, \frac{1}{2}) = \frac{1}{2}$ *determine the maximum uncertainty that the system can impose on the adversary in the best case. According to Theorem 3.3,* $\lim_{k\to\infty} k^{-1} I_\alpha^T(S_k, S_k) = 0$ *requires* $\lim_{k\to\infty} \tilde{\lambda}_k = \tilde{\lambda}_{\max}$. *If weak secrecy is satisfied, the normalized ambiguity tends to the source's entropy rate,*

$$\lim_{k\to\infty} \frac{1}{k} T_\alpha(S^k|\hat{S}^k) = T_\alpha(S) = \frac{1}{2}.$$

Thus, the calculations show that if the system can maintain weak secrecy, it guarantees that the adversary, in the best case, will have at most a %50 *symbol error rate (average symbol error rate). This is the maximal security reliability that can be achieved for a uniformly random source.*

4. *Conclusion*

Secrecy is a fundamental concept in information theory, with strong and weak secrecy finding numerous applications in areas such as wiretap channels, wireline networks, and bidirectional broadcast channels. In this paper, we aim to define generalized forms of strong and weak secrecy, which are extensively utilized in information-theoretic security challenges. The primary motivation for this study is to assess system security based on Tsallis entropy within the context of information-theoretic security problems. Through the establishment of precise mathematical bounds, this work establishes a direct connection between equivocation (uncertainty) and operational reliability. Specifically, it demonstrates that in stationary memoryless systems, the attainment of weak secrecy suffices to guarantee that the adversary's symbol and block error probabilities reach their upper bounds. Furthermore, it emphasizes that strong secrecy results in a vanishing variational distance, thereby effectively eliminating any potential guessing advantage for the adversary.

In future work, it is essential to identify the conditions under which Tsallis-based secrecy is more advantageous in specific areas (distributions, channel models, and -values). Furthermore, we propose that the insights derived from this study, along with a comprehensive investigation of information-theoretic security and generalized coding theorems, can guide the development of robust

communication and security systems. Future research could enhance Tsallis-based security measures by combining hyper MV-algebras and statistical mechanics to reduce parameter dependence and establish precise security bounds (For further study, refer to [1] and [5]). Additionally, we will connect Tsallis-based security definitions to practical measures, such as adversary advantage and information leakage bounds, to enhance understanding and application.

5. *Declarations*

The authors declare that there are no conflicts of interest.

6. *Aknowledgement*

We would like to thank the reviewers for their thoughtful comments and efforts towards improving our manuscript.

References

[1] Balogh, S. G., Palla, G., Pollner, P., & Czégel, D. (2020). Generalized entropies, density of states, and non-extensivity. Scientific reports, 10(1), 15516. https://doi.org/10.1038/s41598-020-72421-9

[2] Beck, C. (2009). Generalised information and entropy measures in physics. Contemporary Physics, 50(4), 495-510. https://doi.org/10.1080/00107510902823517

[3] Cover, T. M., & Thomas, J. A. (1991). Elements of Information Theory. New York: Wiley-Interscience. https://doi.org/10.1002/0471200611

[4] Csiszár, I., & Körner, J. (1978). Broadcast channels with confidential messages. IEEE Transactions on Information Theory, 24(3), 339-348. https://doi.org/10.1109/TIT.1978.1055892

[5] Ebrahimi, M., & Mehrpooya, A. (2014). An application of geometry in algebra: uncertainty of hyper MV-algebras. In Proceedings of the 7th seminar on geometry & topology, Tehran (pp. 529-534). https://dorl.net/dor/20.1001.1.23453942.1393.0.0.8.8

[6] Erokhin, V. (1958). ϵ-entropy of a discrete random variable. Theory of Probability and Its Applications, 3(1), 97-100. https://doi.org/10.1137/1103009

[7] Furuichi, S. (2006). Information theoretical properties of Tsallis entropies. Journal of Mathematical Physics, 47(2), 023302. https://doi.org/10.1063/1.2165740

[8] Havrda, J., & Charvát, F. (1967). Quantification method of classification processes. Concept of structural α-entropy. Kybernetika, 3(1), 30-35. https://dml.cz/handle/10338.dmlcz/125229

[9] He, B., Zhou, X., & Swindlehurst, A. L. (2016). On secrecy metrics for physical layer security over quasi-static fading channels. IEEE Transactions on Wireless Communications, 15(10), 6913-6924. https://doi.org/10.1109/TWC.2016.2591518

[10] Ho, S. W., & Verdú, S. (2008, July). Conditional entropy and error probability. In 2008 IEEE International Symposium on Information Theory, 1622-1626. https://doi.org/10.1109/ISIT.2008.4595316

[11] Ho, S. W. (2009). On the interplay between Shannon's information measures and reliability criteria. In 2009 IEEE International Symposium on Information Theory, 154-158. https://doi.org/10.1109/ISIT.2009.5205597

[12] Ho, S. W., & Verdu, S. (2010). On the interplay between conditional entropy and error probability. IEEE Transactions on Information Theory, 56(12), 5930-5942. https://doi.org/10.1109/TIT.2010.2079130

[13] Ho, S. W., & Verdú, S. (2015). Convexity/concavity of Rényi entropy and α-mutual information. In 2015 IEEE International Symposium on Information Theory (ISIT), 745-749. https://doi.org/10.1109/ISIT.2015.7282577

[14] Hyadi, A., Rezki, Z., & Alouini, M. S. (2016). An overview of physical layer security in wireless communication systems with CSIT uncertainty. IEEE Access, 4, 6121-6132. https://doi.org/10.1109/ACCESS.2016.2607706

[15] Jamalzadeh, J., & Ghasemi, K. (2024). Tsallis entropy of fuzzy -algebras. International Journal of Nonlinear Analysis and Applications, 15(12), 385-395. https://doi.org/10.22075/ijnaa.2024.33021.4709

[16] Jurkowski, J. (2013). Quantum discord derived from Tsallis entropy. International Journal of Quantum Information, 11(01), 1350013. https://doi.org/10.1142/S0219749913500134

[17] Kurzyk, D., Pawela, Ł., & Puchała, Z. (2018). Conditional entropic uncertainty relations for Tsallis entropies. Quantum Information Processing, 17(8), 1-12. https://doi.org/10.1007/s11128-018-2009-4

[18] Lai, L., Ho, H. W., & Poor, H. V. (2008). Privacy-security tradeoffs in biometric security systems. In 2008 46th Annual Allerton Conference on Communication, Control, and Computing, 268-273. https://doi.org/10.1109/ALLERTON.2008.4797572

[19] Marshall, A. W., Olkin, I., & Arnold, B. C. (1979). Inequalities: theory of majorization and its applications. New York: Academic Press. https://doi.org/10.1016/C2010-0-64839-5

[20] Maurer, U., & Wolf, S. (2000, May). Information-theoretic key agreement: from weak to strong secrecy for free. In International Conference on the Theory and Applications of Cryptographic Techniques, 351-368. Springer, Berlin, Heidelberg.

[21] Mohamed, M. S., Barakat, H. M., Al Mutairi, A., & SidAhmed, M. (2023). Further properties of Tsallis extropy and some of its related measures. AIMS Mathematics, 8(12), 28219-28245. https://doi.org/10.3934/math.20231445

[22] Mojahedian, M. M., Gohari, A., & Aref, M. R. (2017, June). On the equivalency of reliability and security metrics for wireline networks. In 2017 IEEE International Symposium on Information Theory (ISIT), 2713-2717. https://doi.org/10.1109/ISIT.2017.8007007

[23] Rajagopal, A. K., Sudha, Nayak, A. S., & Devi, A. U. (2014). From the quantum relative Tsallis entropy to its conditional form: separability criterion beyond local and global spectra. Physical Review A, 89(1), 012331. https://doi.org/10.1103/PhysRevA.89.012331

[24] Rastegin, A. E. (2013). Bounds of the Pinsker and Fannes types on the Tsallis relative entropy. Mathematical Physics, Analysis and Geometry, 16(3), 213-228. https://doi.org/10.1007/s11040-013-9125-2

[25] Rastegin, A. E. (2015). Further results on generalized conditional entropies. RAIRO-Theoretical Informatics and Applications, 49(1), 67-92. https://doi.org/10.1051/ita/2015004

[26] Shah, S. M., & Sharma, V. (2015, March). Achieving Shannon capacity region as secrecy rate region in a multiple access wiretap channel. In 2015 IEEE Wireless Communications and Networking Conference (WCNC), 759-764. https://doi.org/10.1109/WCNC.2015.7127592

[27] Shrahili, M., & Kayid, M. (2023). Residual Tsallis entropy and record Values: some new insights. Symmetry, 15(11), 2040. https://doi.org/10.3390/sym15112040

[28] Singh, S. P., & Tiwari, S. (2023). A dual multimodal biometric authentication system based on WOA-ANN and SSA-DBN techniques. Sci, 5(1), 10. https://doi.org/10.3390/sci5010010

[29] Tian, D. (2023). Pricing principle via Tsallis relative entropy in incomplete markets. SIAM Journal on Financial Mathematics, 14(1), 250-278. https://doi.org/10.1137/22M1491710

[30] Tsallis, C. (1988). Possible generalizations of Boltzmann-Gibbs Statistics. Journal of Statistical Physics, 52(1), 479-487. https://doi.org/10.1007/BF01016429
[31] Venkatesan, R. C. (2007). Generalized Statistics Framework for Rate Distortion Theory with Bregman Divergences. arXiv preprint cond-mat/0701218. https://arxiv.org/abs/cond-mat/0701218
[32] Venkatesan, R. C., & Plastino, A. (2011). Scaled Bregman divergences in a Tsallis scenario. Physica A: Statistical Mechanics and Its Applications, 390(15), 2749-2758. https://doi.org/10.1016/j.physa.2011.03.009
[33] Vila, M., Bardera, A., Feixas, M., & Sbert, M. (2011). Tsallis mutual information for document classification. Entropy, 13(9), 1694-1707. https://doi.org/10.3390/e13091694
[34] Vilasini, V., & Colbeck, R. (2019). Analyzing causal structures using Tsallis entropies. Physical Review A, 100(6), 062108. https://doi.org/10.1103/PhysRevA.100.062108
[35] Yeung, R. W. (2008). Information Theory and Network Coding. Springer. https://doi.org/10.1007/978-0-387-79234-7
[36] Wyner, A. D. (1975). The wire tap channel. Bell System Technical Journal, 54(8), 1355-1387. https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

S. Jalayeri
Orcid number: 0000-0002-8464-5871
Department of Statistics
Ferdowsi University of Mashhad
Mashhad, Iran
Email address: samira.jalayeri@mail.um.ac.ir

G.R. Mohtashami Borzadaran
Orcid number: 0000-0002-8841-1386
Department of Statistics
Ferdowsi University of Mashhad
Mashhad, Iran
Email address: grmohtashami@um.ac.ir

M. Khorashadizadeh
Orcid number: 0000-0001-7732-1599
Department of Statistics
University of Birjand
Birjand, Iran
Email address: m.khorashadizadeh@birjand.ac.ir