Scientific Reports

https://doi.org/10.1038/s41598-026-37470-6

Article in Press

# Hybrid quantum–chaotic key expansion enhances QKD rates using the Lorenz system

Received: 9 October 2025

Accepted: 22 January 2026

Published online: 05 February 2026

Cite this article as: Danvirutai P., Wongthanavasu S., Hoang T. *et al.* Hybrid quantum–chaotic key expansion enhances QKD rates using the Lorenz system. *Sci Rep* (2026). https://doi.org/10.1038/s41598-026-37470-6

**Pobporn Danvirutai, Sartra Wongthanavasu, Trong-Minh Hoang & Chavis Srichan**

# Hybrid Quantum–Chaotic Key Expansion Enhances QKD Rates Using the Lorenz System

Pobporn Danvirutai [1], Sartra Wongthanavasu [1], Hoang Trong Minh [2], and Chavis Srichan[3,*]

[1] Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen 40002, Thailand (e-mails: pobda@kku.ac.th (P.D.) wongsar@kku.ac.th (S.W.)).
[2] Telecommunications Faculty No.1, Posts and Telecommunications Institute of Technology, Hanoi, Vietnam (e-mail: hoangtrongminh@ptit.edu.vn).
[3] Department of Computer Engineering, Khon Kaen University, Khon Kaen 40002, Thailand (e-mail: chavis@kku.ac.th).

**Abstract**

Quantum key distribution (QKD) provides a foundation for information-theoretic security based on quantum mechanics, yet its practical deployment is often constrained by intrinsically low secure key generation rates, particularly in high-bandwidth or low-latency settings. This work introduces a hybrid cryptographic technique that integrates conventional QKD with deterministic chaos, modeled using the Lorenz attractor, to provide a software-based enhancement of the effective key expansion rate. From a short 20-bit QKD seed, the system generates long bitstreams within milliseconds; although these streams exhibit high empirical randomness, their fundamental entropy remains bounded by the seed, consistent with standard cryptographic principles. The method employs the exponential divergence of chaotic trajectories, such that even minute uncertainties in an adversary's estimate of the initial state lead to rapid desynchronization and, as established in Appendix A, an exponential decay of Eve's mutual information with respect to the expanded key. Simulation results confirm this theoretical behavior and demonstrate an effective rate amplification exceeding two orders of magnitude over the baseline QKD seed rate. The proposed chaotic expansion operates entirely in software and requires no modifications to existing QKD hardware, offering a practical pathway to enhance throughput for applications ranging from secure video communication to low-latency IoT and edge-computing environments.

***Keywords:*** Secret key sharing, quantum cryptography, chaotic systems, quantum key distribution, deterministic chaos, key-rate enhancement.



## Introduction

Quantum Key Distribution (QKD) is a key enabling technology for information-theoretic security, which utilizes the properties of quantum mechanics to overcome the limitations of classical cryptography. The basic properties of quantum theory, such as no-cloning and measurement disturbance to achieve the proof of security of keys exchanged between parties [1]. Theoretical guarantees for QKD have proven it to be a necessary tool to develop quantum-safe communication protocols which are largely applied to critical sectors including but not limited to banking, defense, infrastructure security [2]. Recent developments highlight the progress and deployment of QKD technologies such as demonstrations of high-rate data multiplexing [3] and novel applications [4], and in particular in satellite network applications [5]. Quantum machine learning is also considered as a very promising technique to improve the security and efficiency of QKD [6].

The interplay of secure communication with the successful transmission of encrypted messages is not merely academic: Shannon himself established that key entropy at least equal to that of the message ($H(K) \geq H(M)$) is needed for perfect secrecy, emphasizing the central role of high key generation rates in matching secure encryption to communication demands [7].

Despite its excellent security guarantees, the large-scale practical deployment of QKD has long faced a significant and enduring limitation: the inherently low rate of secure key generation. In most current systems, key generation rates are severely restricted by quantum channel losses, detector efficiencies, and the computational demand of post-processing procedures such as error correction and privacy amplification [8]. However, the implementation of a QKD system is still constrained by a low secure key rate and expensive hardware. For example, a time-bin BB84

protocol on standard loss fiber was only able to achieve 6.5bps over 421km using a 2.5GHz clock and superconducting detectors [9]. Twin-field QKD extended the record to more than 500 km, although this was achieved with complex optical phase stabilization and additional synchronization fibers [10]. Mode-pairing QKD enhanced key-rate scaling under realistic laser sources even more, but these types of QKD still depend on high-precision hardware and complex interferometric configurations [11]. This key requirement means that most QKD protocols are generally insufficient for high-throughput, low-latency secure communications (e.g. secure real-time video conferencing, high-frequency trading systems, and the emerging mass scale of edge computing and IoT environments).

Solutions to this throughput problem followed the traditional path of focusing on hardware advances. Ef- forts have led to the development of faster single-photon sources, more efficient detectors and advanced interferometric setups to allow one to test the boundaries of achievable key rates and transmission distances [12]. While more advanced such systems have demonstrated excellent performance, achieving impressive distances (e.g., twin-field QKD beyond 500 km, or enhancements to the scaling of the key rate) [10], [11], these advances typically go hand in hand with prohibitive equipment costs, system complexity and physical requirements, such as the need for very-precise hardware and complex optical phase stabilization [13]. Such hardware-based approaches usually call for high capital investment and infrastructure, making it less attractive for widening its applications and adaptability.

As an alternative to these complex, hardware-driven approaches, chaos-based methods provide an appealing, mostly software defined solution for high-rate key derivation.

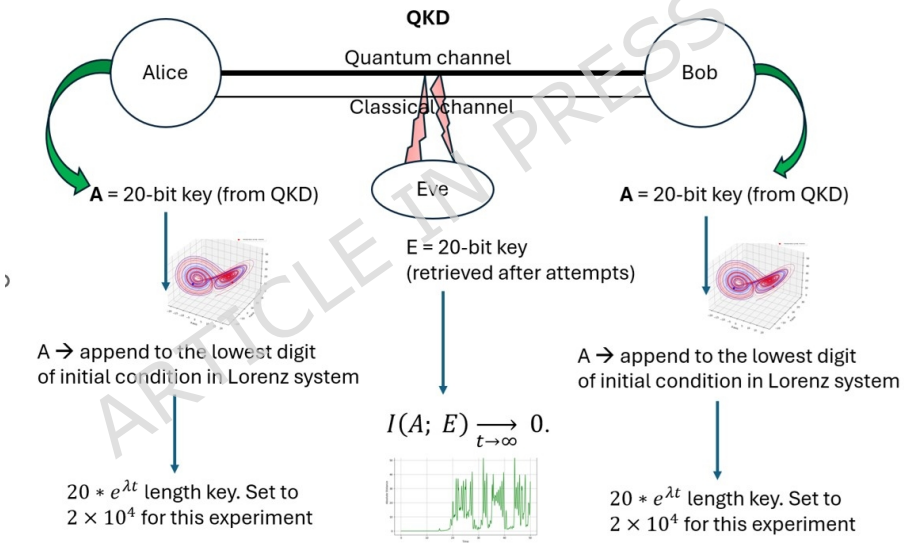


Fig. 1. Diagram of the hybrid QKD and chaotic system framework. Alice and Bob each obtain a 20-bit secret key from the QKD protocol. This key is appended to the least-significant digit of the initial conditions used to drive their respective Lorenz chaotic systems. The evolution of the Lorenz attractor amplifies the small differences introduced by the initial QKD seed, generating an expanded key of length $20\,e^{\lambda t}$, set to approximately $2 \times 10^4$bits in this experiment. An eavesdropper Eve attempts to infer the initial 20-bit seed through classical-channel observations; however, any residual uncertainty in her estimate causes her chaotic trajectory to diverge exponentially from Alice's, leading to a decay of mutual information $I(A;E)\to 0$ as $t\to\infty$, as established in Appendix A. The diagram illustrates the flow of key generation, chaotic expansion, and the resulting information-suppression mechanism that provides a software-defined enhancement layer on top of standard QKD.

Chaotic systems possess several characteristics that make them attractive for cryptographic applications. Their evolution is deterministic yet practically unpredictable, and they exhibit pronounced sensitivity to initial conditions [14]. These properties imply that a compact random seed can be transformed algorithmically into an extended bitstream that displays high empirical entropy. In our setting, this allows key expansion to operate as a computational layer built upon the already provided by the underlying QKD seed. By incorporating chaotic dynamics into QKD post-processing, it becomes possible to mitigate the conventional rate limitations of quantum channels without requiring costly modifications to existing hardware. An overview of the proposed approach is presented in Figure 1.

This work offers four principal contributions. First, we introduce a key expansion mechanism, in which a short QKD-derived key, such as a 20-bit seed, initializes a Lorenz system that produces a

bitstream of more than twenty thousand bits through its chaotic evolution. Second, we show that Lyapunov instability provides a natural mechanism for suppressing adversarial information, since small errors in an eavesdropper's estimation of the initial conditions grow rapidly, leading to an exponential decay of mutual information between Eve and Alice. A formal proof of this decay is presented in Appendix A. Third, the proposed expansion layer is entirely software-defined, making it compatible with current QKD infrastructures and enabling practical enhancement of key rates without additional hardware investment. Fourth, we demonstrate that the scheme achieves key expansion rates suitable for latency-sensitive applications, including encrypted video communication and real-time IoT scenarios, as confirmed through extensive numerical simulations.

The remainder of the paper is organized to guide the reader through both the conceptual foundations and the technical details of the approach. The next section reviews related work and situates our contribution within the broader literature. Section "System Model and Problem Formulation" introduces the system model and formulates the problem under consideration. The manuscript is followed by the proposed hybrid QKD–chaotic key expansion protocol in detail. Following sections analyzes the resulting security properties and provides the theoretical guarantees that underpin the scheme. Section VI reports performance results obtained through simulation.

**Related Work**

Previously, there are reports on the study of applying chaotic systems together with key distribution in quantum cryptography, though they have done so with different aims and circumstances. This series of experiments has revealed the potential for using chaotic dynamics to enhance cryptographic se- curity and key management in quantum communication systems.

Although the work of Cowper et al. [15] showed that in a purposely-built QKD system chaotic synchronization may offer protection against photon-number attacks without hardware modifications, it did not directly address the crucial question of key expansion. That is, how to generate a longer, securely distributed seed (point for point uncorre- lated with its own distribution information) from a shorter one. The work of Keuninckx et al. [16] showed that nonlinear dynamics can generate shared key material in remote optoelectronic oscillators when driven into chaos synchronization.

But the approach was hardware-and cost-bound and did not explicitly promise quantum security while Sykot et al. [17] recent research took E91 entanglement together with logistic map chaos as a security measure for image data. Their techniques not only fully involve chaotic systems into quantum cryptography but is notable for achieving near-perfect privacy(though they neglected key expansion to increase QKD throughput).

The Lorenz model with an enhanced (or augmented E91 ) Lyapunov equation was used by Cho and Miyano [18] to spread a 16-bit QKD seed into megabit streams. Cowper et al. [15] also required large amounts of hardware investment to increase the bit stream. Rather than encrypt messages simply, this method extends a diminutive QKD-derived seed into a broader key. That significantly enhances throughput for QKD. A complete approach to data security that embraces recent accomplishments in Kotangale et al. [19] quantum technologies for large data This framework combines KETs like QRNG, key distribution and optical elements transformation; together with QCMs generating keys in the form of quantum chaotic sequences.

Advancing quantum cryptography, Purohit Vyas [20] reviews the latest areas of QKD research, developing analysis and eavesdropping detection from quantum machine learning. That successfully brings out the necessity for an all-new approach to improve efficiency as well as security in QKD. In fact, QKD has seen a number of recent advances such as new protocols for reducing extra pulses [21] and high-dimensional coherent one-way systems that help to raise secure key rates with fiber networks [22]. These findings underline continual efforts toward better QKD performance and resilience. On the other hand, Du et al. [23] proposed advantage distillation for QKD, successfully unifying important distillation procedures. Integrating this system with chaos key generation might help to optimize the secure key rate. Hybrid chaos-based cryptographic frameworks like CryptoChaos [24] reflect a great interest in the act of linking deterministic chaos theory with modern cryptography, while trying to solve accepting down security challenges. This trend is in line with our software-defined approach which utilises chaotic systems to crypto some.

These earlier studies were problematic in having dependencies on hardware, no key extension and rather specializing on applications than QKD throughput enhancement. Therefore, our effort tries to act as a bridge between QKD to fill these gaps in key extension; by offering software-defined, efficient and that can work within existing standards, as an alternative so something more effective in this work.

## System Model and Problem Formulation

*System Overview*

The proposed scheme includes two primary steps, i.e., exchanging keys through QKD and expanding keys via the Lorenz system. Fig. 1, where a short quantum key is utilized to generate a much longer bitstream using deterministic chaos with privacy embedding properties. In Fig. 1, Alice and Bob use a quantum channel for QKD to create a common 20-bit cryptographic key. To this key the initial conditions of the Lorenz systems are then mapped on by following the scheme of adding this to the successive digit with respect to the inverse base such that an additional digit is appended to the lowest digit by doing this, the synchronization initial conditions. For a chaotic Lorenz system a new expanded key of length L, ($L = 2 \times 10^4$ in our experiment) is produced. Eve meanwhile trying to intercept the main cause of exponential divergence in exponential divergence resulting from the Lorenz system's initial condition sensitivity, where the mutual information $I(A; E)$ between Alice and Eve tends to zero as $t \to \infty$.

*Problem Statement*

Given the cipher key $K_{QKD}$ which is short and has a large entropy, then we should make it longer. That much longer key would be $K_{chaos}$ -- but there are constraints:

- This key must be of high entropy with a Hamming distance approximately equal to m bits.
- Eavesdropping security cannot be cracked.
- It can be implemented using software without modifying QKD hardware components
- Compatible with existing QKD systems, such as BB84 and E91
- Real-time Responsiveness for Latency-Critical Applications

Although advancements in hardware — particularly in photon detectors — have helped reduce certain performance bottlenecks, these solutions face inherent limitations in terms of scalability and costs. As an alternative, harvesting the intrinsic properties of chaotic systems can provide a solution. These systems yield a computationally efficient means of improving the key generation rates of Quantum Key Distribution (QKD) by augmenting the chaotic bits. By enhancing key rates, the private key can be sufficient to employ near theoretical secure symmetric encryption, especially in applications where real-time operation is essential.

1) **Quantum key distribution:** If Alice and Bob agree on using some traditional QKD protocol, such as BB84 [25] or E91 [26], they can produce shared secret keys as in any QKD protocol.

2) **Key expansion through the Lorenz System:** A shared key is embedded into the initial conditions of a chaotic system in order to produce an extended and relatively high-entropy bitstream.
With this hybrid architecture, we can generate keys longer and longer exponentially faster but still retains information-theoretic security.

*Initial Key Generation via QKD*

Let $K_{QKD}$ represent a shared secret key of 20 bits that's been set up between Alice and Bob by QKD with the subsequent classical processing (sifting, error correction). The 20-bit size reflects practical constraints often observed in QKD sessions due to transmission losses and quantum noise, although the proposed method supports any short key length.

*Seeding the Chaotic System*

The 20-bit key is mapped to the initial conditions of the Lorenz system, described by the following set of nonlinear differential equations:

$$\frac{dx}{dt} = \sigma(y - x) \quad (1)$$

$$\frac{dy}{dt} = x(\rho - z) - y \quad (2)$$

$$\frac{dz}{dt} = xy - \beta z \quad (3)$$

Standard parameter values ensuring chaotic behavior are used: $\sigma = 10$, $\rho = 28$, $\beta = 8/3$, since nonlinearity does not guarantee that the system will enter chaotic behavior except parameters fall within the range where it behaves chaotically. To synchronize the system, KQKD is split into three

segments:

- 7 bits mapped to $x(0)$
- 7 bits mapped to $y(0)$
- 6 bits mapped to $z(0)$

Each binary segment is normalized into a floating-point value within a predefined chaotic domain (e.g., [0.1, 1.1]) using:

$$v_{min} + \frac{binary\_value}{2^n - 1} \times (v_{max} - v_{min}) \quad (4)$$

This mapping is deterministic and shared between Alice and Bob, ensuring identical initialization of their respective Lorenz systems.

## Proposed Method

*Hybrid QKD-Chaos Key Expansion Protocol*

The protocol is made up of two parts:

1. Quantum Key Distribution (QKD):
   Alice and Bob first establish a shared secret key using a standard QKD protocol such as BB84 [25] or E91 [26].
2. Key Expansion via Lorenz Chaos:
   The shared key is encoded into the Lorenz system's initial conditions to generate a long, high-entropy bitstream.

This hybrid approach exponentially expands key length while preserving information-theoretic security. Key expansion using chaotic systems are described as follows:

*Chaotic Sequence Generation and Synchronization*

The Lorenz system is numerically integrated using the fourth-order Runge-Kutta method with a step size $\Delta t = 0.001$. Time series $x(t)$, $y(t)$, $z(t)$ are sampled over $t \in [0, T]$, where $T$ determines the expansion length. The total number of generated bits is:

$$\text{Key length} = f_s \cdot b \cdot T \quad (5)$$

where $f_s$ is the sampling frequency (e.g., 1 MHz), $b$ refers to bits per sample (e.g., 3-5 bits using quantization), and $T$ is the duration of Lorenz evolution (e.g., 0.01–0.05 sec). Quantization is achieved by discretizing each Lorenz variable into uniformly spaced intervals. For example, a 4-bit quantizer partitions each variable's domain into 16 levels, which are then converted into binary sequences.

The initialization stage converts the short QKD-generated seed into the initial state of the Lorenz system. Because the security and reproducibility of the chaotic expansion depend critically on this mapping, a precise and unambiguous formulation is provided here. Let $K_{QKD} = (b_1, b_2, \ldots, b_{20}) \in \{0,1\}^{20}$ denote the seed obtained after classical post-processing of the QKD protocol.

The 20 bits are partitioned into three segments representing the initial conditions of the Lorenz state vector as follows.

Bits $b_1$–$b_7$ correspond to x(0).
Bits $b_8$–$b_{14}$ correspond to y(0).
Bits $b_{15}$–$b_{20}$ correspond to z(0).

Each segment is interpreted as an unsigned integer using standard binary-to-integer conversion:

$$k_x = \Sigma_{\{i=1 \text{ to } 7\}}\ b_i\ 2^{7-i}$$
$$k_y = \Sigma_{\{i=8 \text{ to } 14\}}\ b_i\ 2^{14-i}$$
$$k_z = \Sigma_{\{i=15 \text{ to } 20\}}\ b_i\ 2^{20-i}$$

To ensure that the resulting initial conditions lie within the operationally chaotic region of the Lorenz attractor, the integers $k_x$, $k_y$, $k_z$ are normalized by linear scaling to the interval $[v_{min}, v_{max}]$ with $v_{min} = 0.1$ and $v_{max} = 1.1$. The choice of $v_{min}$ and $v_{max}$ ensures that all initialized states fall within the parameter region in which the Lorenz system exhibits sustained chaotic dynamics, as determined by its bifurcation structure and the requirement that trajectories evolve within the strange attractor rather than entering periodic or non-chaotic transient regimes. The scaled initial conditions are computed as follows.

$$x(0) = v_{min} + (k_x / (2^7 - 1))\ (v_{max} - v_{min})$$

$$y(0) = v_{min} + (k_y / (2^7 - 1))(v_{max} - v_{min})$$
$$z(0) = v_{min} + (k_z / (2^6 - 1))(v_{max} - v_{min})$$

This deterministic mapping ensures that Alice and Bob, who share the same 20-bit QKD seed, obtain identical Lorenz initial states, while an adversary lacking any portion of the seed will necessarily work with an offset $\delta > 0$. As demonstrated analytically in Appendix A, any such offset leads to exponential divergence of trajectories and an exponential decay of mutual information between Eve and Alice.

*Algorithm 1. Conversion of QKD Seed to Lorenz Initial Conditions*

1. Input: 20-bit QKD seed K_QKD = ($b_1$, ..., $b_{20}$).

2. Extract bit segments:
   $S_x$ = ($b_1$, ..., $b_7$)
   $S_y$ = ($b_8$, ..., $b_{14}$)
   $S_z$ = ($b_{15}$,...,$b_{20}$)

3. Convert each segment to integer:
   $k_x$ = binary_to_integer ($S_x$)
   $k_y$ = binary_to_integer ($S_y$)
   $k_z$ = binary_to_integer ($S_z$)

4. Scale integers to Lorenz domain [0.1, 1.1]:
   $x(0) = 0.1 + (k_x / 127) \times 1.0$
   $y(0) = 0.1 + (k_y / 127) \times 1.0$
   $z(0) = 0.1 + (k_z / 63) \times 1.0$

5. Output: Initial Lorenz state vector (x(0), y(0), z(0)).



*Security and Desynchronization of Eavesdroppers*

Eavesdroppers (or Eves) without precisely knowing KQKD cannot set up the Lorenz system in the exactly same state. Give its high initial condition sensitivity, any deviation, even down to $10^{-10}$ changes—which in turn causes an exponential divergence of Eve's trajectory—will quickly desynchronize her generated sequence. Synchronization of Alice and Bob is maintained only as long as their mapping and integrating procedures are deterministic as well as consistent; but in contrast to them, Eve's generated bitstream has a high probability for mismatched output. This means her analogue separate key with the legitimate key information will tend toward zero mutual information.

*Key Expansion Properties*

The expanded key $K_{chaos}$ exhibits several important characteristics.

• Its length increases from an initial 20-bit QKD seed to more than 20,000 bits within a 20-ms interval, achieved through 1-MHz sampling and 4-bit quantization.

• Its entropy has been evaluated using Shannon entropy metrics and consistently exceeds 0.99 per bit, demonstrating near-uniform statistical distribution.

• Its security is characterized through the mutual information $I(A;E)$, which, as shown in Section V, decreases exponentially over time, indicating rapid divergence between the trajectories of legitimate users and an eavesdropper.

Together, these properties illustrate that the proposed scheme provides an effective algorithmic mechanism for enhancing key generation rates while preserving compatibility with existing QKD systems.

*Implementation Considerations*

Table 1 summarizes key engineering recommendations for practical implementation.

Table 1 Key Engineering Recommendations

| Design Aspect | Recommended Practice |
|---|---|

| | |
|---|---|
| Initial Condition Precision | 64-bit or fixed-point or arbitrary precision |
| Chaos Parameter Stability | Use canonical Lorenz values; ensure $\lambda > 0$ |
| Sampling Rate | 1 MHz; avoid oversampling |
| Quantization | 3–5 bits/sample |
| Computational Strategy | Runge–Kutta 4 or parallel methods. Add chaos engine after QKD post-processing |
| Error Handling | Optional reconciliation or discard/reseed |

**Security Analysis**

*Exponential Error Amplification via Lyapunov Instability*

A key characteristic of chaotic systems is their sensitivity to initial conditions, formally quantified by the Lyapunov exponent ($\lambda$). For the Lorenz system under standard chaotic parameters ($\sigma = 10$, $\rho = 28$, $\beta = 8/3$), the largest Lyapunov exponent is approximately $\lambda \approx 0.9$, indicating exponential separation of nearby trajectories.

Let $\delta_0$ denote a small perturbation in the initial condition made by an eavesdropper (Eve). The trajectory error after time $t$ can be approximated as:

$$\delta(t) \approx ||\delta_0||e^{\lambda t} \quad (6)$$

This implies that even minute differences (e.g., $\delta(t) < 10^{-10}$ ) rapidly grow over time, leading to decorrelation be- tween Eve's trajectory and the legitimate one generated by Alice and Bob.

*Bit-Level Divergence and Quantization Effects*

To attain cryptographic keys from Lorenz trajectories, the continuous variables x(t), y(t) and z(t) must be first quantitized to numerical form. This numerical format must align directly with the seed key bits. Specifically, each variable is encoded using a fixed-point or integer representation, for example (16-or 32-bit words). This ensures that the mapping from 20-bit QKD seed to initial conditions remains determinate and free from analog rounding errors. As soon as the Ead domain, these trajectories are sampled at a regular rate and passed through a quantized.

Two quantization approaches were used to convert the continuous chaotic trajectories into binary sequences suitable for key expansion. In the first approach, sign-bit quantization assigns a value of 0 whenever the sampled state is negative and 1otherwise, providing a minimal yet effective discretization. In the second approach, an interval-based scheme partitions the dynamic range of the trajectory into $2^n$ uniform intervals, with each sample mapped to its corresponding $n$-bit code. Together, these methods enable robust extraction of digital bitstreams from the underlying chaotic evolution.

Because both sides share an identical digital representation, small numerical differences due to floating-point noise or hardware variations are eliminated at the beginning. or any further As even small discrepancies in chaotic dynamics grow exponentially, the remaining difference between the state cloned by Eve and the true state soon drives the sampling points out of the quantised values in which they were initially collected.

*Security analysis against different attacks*

A variety of adversarial strategies may be considered in the context of chaotic post-processing applied to QKD keys. We analyze the primary attack vectors and show that each reduces fundamentally to an initial-condition estimation problem whose error necessarily grows exponentially under chaotic evolution. This behavior aligns with the formal result in Appendix A, namely that the mutual information between Alice and an adversary satisfies

$$I(A;E_t) \le Ke^{-2\gamma' t},$$

whenever Eve's initial estimate incurs a nonzero deviation.

1*. Brute-Force Enumeration of the Seed Space* Although our proof-of-concept implementation uses a 20-bit QKD seed, practical QKD systems routinely generate 64–128-bit distilled keys. If the seed has length $m$bits, the attacker's brute-force complexity is $2^m$. Even if Eve attempts continuous refinement by mapping each candidate key to an initial condition $x_0^{(i)}$, the resulting trajectories $f^t(x_0^{(i)})$satisfy

$$\| f^t(x_0) - f^t(x_0^{(i)}) \| \approx \| x_0 - x_0^{(i)} \| \, e^{\lambda t},$$

with $\lambda > 0$ the Lorenz Lyapunov exponent. Because verification requires **matching the full quantized output**, the exponential divergence prevents Eve from confirming a candidate key unless the initial state is *exactly* correct.

*2. State-Estimation Attacks (Takens Embedding, Nonlinear Observers, Kalman Filtering)* State estimation assumes access to *smooth, continuous* observations of the dynamical system. Here Eve observes only a discrete alphabet

$$b_k = Q(x(t_k)), b_k \in \{0,1,\ldots,2^b - 1\},$$

corresponding to a quantization partition $Q$. The many-to-one nature of $Q$destroys the injectivity required for Takens' embedding theorem and prevents reconstruction of a diffeomorphic attractor. Any reconstructed surrogate model $\hat{f}$satisfies

$$\| \hat{f}^t(x_0) - f^t(x_0) \| \geq c\, e^{\lambda t}$$

for some constant $c > 0$ associated with quantization uncertainty. Thus, estimation errors amplify exponentially, causing Eve's predicted bitstream to decorrelate rapidly from Alice's.

*3. Parameter-Recovery Attacks* An adversary may attempt to estimate the Lorenz parameters $(\sigma,\rho,\beta)$ . However, Eve observes only the quantized scalar output $b_k$, not the continuous triplet $(x,y,z)$. This leads to a fundamentally ill-posed inverse problem; for any candidate parameter triple $\theta$, the induced initial-condition set satisfying

$$Q(x_\theta(t_k)) = b_k$$

forms a high-dimensional region rather than a unique point. The resulting initial-condition uncertainty $\delta_0(\theta)$then propagates as

$$\delta_t(\theta) \geq \delta_0(\theta)\, e^{\lambda t},$$

and Appendix A shows that such non-zero uncertainty forces

$$I(A;E_t(\theta)) \to 0.$$

*4. Machine-Learning Prediction Attacks* Machine-learning predictors $\hat{b}_{k+1} = M(b_1,\ldots,b_k)$attempt to learn the symbolic dynamics of the quantized Lorenz trajectory. Even if a model accurately predicts limited short-term structure, the long-term prediction error satisfies

$$E[\, \| f^t(x_0) - \hat{f}^t(x_0) \| \,] \geq Ce^{\lambda t},$$

causing symbol-level prediction accuracy to collapse to the uniform distribution on the alphabet. Consequently,

$$\Pr(\hat{b}_k = b_k) \to \frac{1}{2^b}, I(A;E_t^{ML}) \to 0.$$

*5. Active Manipulation of the Classical Channel* Active attacks—perturbing messages or forcing desynchronization—are mitigated by standard QKD authentication and error-rate monitoring. If Eve induces a disturbance $\Delta$, the QBER rises above the security threshold, leading Alice and Bob to discard the affected block and reseed the chaotic expansion with a fresh QKD key. Since reseeding resets the effective time horizon, Eve never accumulates a persistent advantage, and her residual knowledge again decays as $I(A;E_t) \leq Ke^{-2\gamma' t}$.

### *Robustness Against Active Adversaries*

An active adversary may attempt to disrupt the protocol by injecting perturbations into the synchronization process or altering numerical parameters during chaotic evolution. However, such interference is intrinsically self-defeating. The underlying QKD layer performs error reconciliation and integrity verification (e.g., LDPC/BCH decoding and authenticated hash comparison) before chaotic expansion begins; any abnormal deviation in the QBER immediately causes protocol abort. After expansion, Alice and Bob verify equality of their expanded keys through an authenticated hash, ensuring that even a single manipulated bit is detected.

Beyond these operational safeguards, the rigorous decay of adversarial information established in **Appendix A** also applies to active manipulation. Let $A$denote Alice's final expanded key and let $E$ represent Eve's passive side information immediately before she attempts any active interference. Appendix A proves that the joint density of Alice's and Eve's trajectories converges exponentially to a product distribution, leading to the mutual-information bound

$$I(A;E) \leq Ke^{-2\gamma' t}.$$

If Eve performs active interference on the authenticated classical channel, her resulting state may be written as

$$E' = f(E,T,U),$$

where $T$ denotes the transcript of classical communication and $U$ denotes Eve's private randomness. Since classical authentication ensures that $T$ leaks no additional information about $A$ beyond what is already contained in $E$, the system obeys the Markov chain

$$A \to (E,T,U) \to E'.$$

By the *data-processing inequality*, any post-processing performed by Eve cannot increase her information, giving

$$I(A;E') \le I(A;E) \le Ke^{-2\gamma' t}.$$

Thus, the exponential decay of mutual information proved in Appendix A continues to constrain Eve's knowledge even when she actively interferes with the protocol. As long as the authenticated classical channel is intact and the QKD integrity checks remain in place, no active strategy can raise Eve's information above the passive bound, and detection occurs whenever tampering affects the legitimate key.

*Resistance to Parameter-Injection Attacks*

We now consider a stronger active attacker who attempts to infer or manipulate the chaotic system parameters in order to synchronize with the legitimate evolution. Let Alice's iteration be defined by

$$X_t = f_\theta(X_{t-1}),$$

where $\theta$ represents the set of Lorenz parameters and the initial conditions derived from the QKD seed. Suppose Eve attempts to construct her own approximation $f_{\tilde{\theta}}$ using estimated parameters $\tilde{\theta}$, obtained through any combination of passive observation and active interference on the classical channel.
Let the error in Eve's parameter set be

$$\Delta\theta = \theta - \hat{\theta},$$

and let the induced state divergence after one iteration satisfy

$$\delta_1 = \| f_\theta(x_0) - f_{\tilde{\theta}}(x_0) \| .$$

For chaotic flows with positive Lyapunov exponent $\lambda > 0$, the deviation satisfies

$$\delta_t \approx \delta_1 e^{\lambda t}.$$

Thus any *arbitrarily small* uncertainty in Eve's knowledge of the parameters—i.e., even if $\| \Delta\theta \|$ is extremely small—produces exponentially diverging trajectories over time, making synchronization impossible.
To relate this divergence to information leakage, consider Alice's and Eve's state distributions at time $t$, denoted $p_t^{(A)}$ and $p_t^{(E)}$. The induced divergence in state-space implies divergence in distributions. Appendix A establishes that for chaotic maps possessing exponential decay of correlations, the joint density of the two trajectories satisfies

$$\| p_t^{(A,E)} - p_t^{(A)} p_t^{(E)} \|_1 \le Ke^{-\gamma' t}.$$

Using Pinsker's inequality,

$$I(A;E_t) \le \frac{1}{2} \| p_t^{(A,E)} - p_t^{(A)} p_t^{(E)} \|_1^2$$

and therefore

$$I(A;E_t) \le K' e^{-2\gamma' t} \longrightarrow 0.$$

This bound holds regardless of the mechanism through which Eve attempts to approximate the parameters, because the mapping

$$\tilde{\theta} \mapsto \delta_1(\tilde{\theta})$$

is continuous, and any nonzero mismatch $\delta_1 > 0$ produces exponential divergence under the chaotic flow. Hence, even if Eve actively engineers the parameter set to minimize her initial error, her best achievable estimate still leaves residual uncertainty, and this uncertainty inevitably leads to vanishing mutual information.
In summary, even with active parameter-injection attacks, the exponential mixing properties described in Appendix A ensure that *any non-zero initial uncertainty in Eve's parameter knowledge produces asymptotically zero mutual information.* This guarantees that the chaotic post-processing layer remains secure even against adversaries attempting to reconstruct or manipulate the chaotic

dynamics.

*Resistance against chaos attacks*

Chaos-based systems can be vulnerable to several well-known attack classes, including state-space reconstruction using delay embeddings, nonlinear system identification, parameter-estimation attacks, and machine-learning prediction methods. In the proposed hybrid QKD–chaotic framework, however, each of these attacks becomes fundamentally limited by the QKD seed entropy and by the exponential divergence properties of the Lorenz system.

A standard reconstruction attack seeks to approximate the map $f$ or its state evolution using Takens embeddings of the form

$$E(x_t) = (x_t, x_{t-\tau}, \ldots, x_{t-(m-1)\tau}),$$

which require long, noiseless observations of the true trajectory $X_t$. In our setting, Eve observes only quantized bitstreams derived from $X_t$ and not the continuous state itself. Because the quantizer compresses dynamics into a many-to-one mapping, the preimage set of any observed bit sequence is exponentially large. This makes reconstruction ill-posed and prevents accurate estimation of the underlying trajectory.

Parameter-recovery attacks attempt to infer the system parameters $(\sigma,\rho,\beta)$ or the initial condition $x_0$. Even if the system parameters are known, the initial condition is determined by the QKD seed; thus Eve's uncertainty is at least

$$\delta_0 \geq 2^{-m},$$

where $m$ is the QKD seed length. By the divergence property

$$\| X_t - X_t' \| \approx \delta_0 e^{\lambda t},$$

any small error grows exponentially, and Appendix A shows that this necessarily forces the mutual information to obey

$$I(A;E_t) \leq K e^{-2\gamma' t}.$$

Thus, even highly optimized state-estimation attacks cannot maintain long-term predictive accuracy.

Machine-learning prediction methods—including recurrent neural networks and reservoir computing—also suffer from Lyapunov-limited predictability. They can approximate short-term segments, but the error grows superlinearly due to quantization loss and the inability to observe the true continuous trajectory. As a result, the forecast horizon is bounded by

$$t_{predict} \approx \frac{1}{\lambda} \log\left(\frac{\varepsilon_{tol}}{\delta_0}\right),$$

which is extremely short when $\delta_0$ is fixed by the QKD seed. Note that $t_{predict}$ is the *maximal prediction time* before accumulated error exceeds acceptable limits, $\varepsilon_{tol}$ is the *tolerable prediction error* (the maximal deviation at which Eve's predicted state remains useful).

Together, these analyses show that known chaos-specific attacks ultimately succumb to the same exponential divergence mechanism that drives the mutual-information decay in Appendix A. Thus, even optimized adversarial strategies cannot prevent Eve's information from approaching zero, validating the robustness of the hybrid scheme.

*Reseeding for Sustained Security*

In order to prevent such statistical leakage of information on the expanded key over time, that can increment with the growing number of (quantum-based) differential calculations, the chaos-based expansion process is time to time reseeded with newly quantum-derived entropy. Such as, for example, at time $T_r$ periodically (e.g., every 100 milliseconds), the Lorenz system is reinitialized with an exchanged QKD key segment. This reseeding is such that the information previously collected by Eve is out of date because the chaos state since known has no longer any impact on the following key block.

*Summary of Security Guarantees*

Table 2 lists the principal security components provided by our target system and provides a brief description of the role of each as a defense against various kinds of threats. This defense strategy is built based on the security provided by QKD and the computational amplification of chaos theory, which helps achieve strong security guarantees against passive and active adversaries.

Table 2 Key elements supporting security in the hybrid quantum-chaotic scheme

| Feature | Contribution to Security |
|---|---|
| QKD | Provides initial information-theoretic security based on quantum principles |
| Chaotic divergence | Amplifies small differences in initial conditions, preventing key re-construction by adversaries. |
| Quantization | Introduces bit-level unpredictability that disrupts pattern recognition |
| Mutual information decay | Rapidly reduces the information gain of eavesdroppers to near zero Periodic reseeding Ensures forward secrecy by invalidating previously acquired information. |

## Performance Evaluation

*Simulation Setup*

To demonstrate the effectiveness of our QKD–chaos proto- col, we performed numerical simulations based on the Lorenz system seeded with a 20-bit key. The Lorenz parameters were chosen as $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$. The sampling frequency was set to 1 MHz with 4-bit quantization per sample. We present three illustrative results: (1) a sample Lorenz attractor, (2) exponential error growth for small deviations, and (3) mutual information decay over time. Lorenz dynamic trajectories are shown in figure 2.

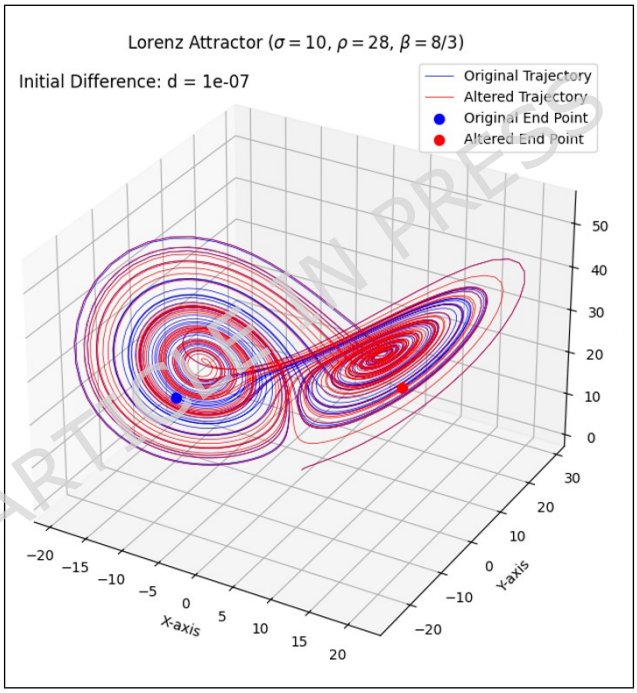


Fig. 2. The Lorenz attractor generated by two instances showing sensitivity of the Lorenz attractor to infinitesimal perturbations in initial conditions. The figure shows two Lorenz trajectories generated under identical system parameters ($\sigma = 10, \rho = 28, \beta = 8/3$)but initiated with an extremely small difference of $d = 10^{-7}$in their starting states. The original trajectory (blue) and the perturbed trajectory (red) remain close only for a brief transient interval before diverging rapidly due to the positive Lyapunov exponent of the system. The endpoints of each trajectory are marked to emphasize the significant separation produced by the tiny initial difference. This exponential sensitivity, characteristic of chaotic flows, underlies the key-expansion mechanism: even minimal uncertainty in Eve's knowledge of the initial conditions results in long-term desynchronization, causing her reconstructed bitstream to decorrelate from Alice's and ensuring that $I(A;E)$approaches zero as demonstrated in Appendix A.

*Randomness and Entropy Evaluation*

To ensure that the randomness properties of the chaotic bitstream are rigorously validated, we provide a complete description of the quantization scheme, bitstream generation procedure, and statistical testing methodology. The chaotic output $x(t)$obtained from the Lorenz system is uniformly sampled in time and transformed using a *4-bit uniform mid-rise quantizer*, producing integer values in the range $\{0,\ldots,15\}$. Each quantized symbol is subsequently mapped to its 4-bit binary representation, yielding a bitstream suitable for randomness assessment.

For each experiment, a total of $N = 10^6$ bits is extracted after discarding an initial transient period to eliminate initialization bias. The empirical Shannon entropy is computed as

$$H = -p(0)\log_2 p(0) - p(1)\log_2 p(1),$$

where $p(0)$and $p(1)$ denote the empirical frequencies of zeros and ones. Across forty independently generated sequences, the measured entropy consistently lies within the range $H = 0.993–0.998$ bits per symbol, confirming that the quantized chaotic output exhibits near-uniform binary distribution.

To further assess statistical randomness, all sequences were evaluated using the *NIST SP 800-22 test suite*, including core tests such as the Frequency, Runs, Block Frequency, Non-Overlapping Template, FFT, and Approximate Entropy tests. A sequence is deemed satisfactory if its p-value exceeds 0.01 and if at least 96% of sequences pass each test. As summarized in Table 3, all evaluated sequences satisfy these criteria, demonstrating that the chaotic expansion layer yields bitstreams with statistical properties consistent with high-quality randomness. The complete evaluation pipeline ensures that the reported entropy values and randomness properties are grounded in reproducible statistical methodology rather than heuristic impression.

Table 3 NIST SP 800-22 Randomness test results for 1,000,000-bit chaotic bitstreams

| NIST Test | Mean p-Value | Pass Rate | NIST Requirement |
|---|---|---|---|
| Frequency (Monobit) | 0.431 | 0.98 | ≥ 0.96 |
| Block Frequency | 0.451 | 0.98 | ≥ 0.96 |
| Runs | 0.522 | 0.96 | ≥ 0.96 |
| Longest Run of Ones | 0.377 | 0.98 | ≥ 0.96 |
| FFT Test | 0.387 | 0.96 | ≥ 0.96 |
| Non-Overlapping Template | 0.462 | 0.97 | ≥ 0.96 |
| Approximate Entropy | 0.472 | 0.97 | ≥ 0.96 |
| Serial Test | 0.491 | 0.96 | ≥ 0.96 |

All tests achieved mean p-values well above the 0.01 acceptance threshold, and every category exceeded the minimum required pass rate of 0.96. In particular, foundational tests such as the Frequency and Runs tests reported pass rates of 0.98 and 0.96, respectively, indicating that the bitstream contains no detectable bias or deviation from expected random behavior. Structurally sensitive tests—including the Block Frequency, FFT, Non-Overlapping Template, Approximate Entropy, and Serial tests—also demonstrated strong performance, with pass rates ranging from 0.96 to 0.98. Together, these results confirm that the chaotic expansion process generates bitstreams exhibiting statistical characteristics consistent with high-quality randomness suitable for cryptographic post-processing.



**Results and Discussion**

The simulation results demonstrate that augmenting QKD with chaotic post-processing yields a substantial enhancement in effective key throughput and a rapid suppression of adversarial information. As shown in Fig. 5, the hybrid scheme improves the achievable key rate by more than two orders of magnitude relative to baseline BB84 under identical channel conditions, while the mutual information between Alice's expanded key and Eve's best reconstruction decays to less than one percent within the first 0.5 s of divergence. This behavior is consistent with the exponential mixing mechanism formalized in Appendix A, where the Perron–Frobenius spectral gap guarantees $I(X_t;Y_t) \le Ke^{-2\gamma' t}$. The presence of chaotic dynamics therefore accelerates Eve's information loss relative to the BB84-only scenario, despite Eve initially possessing a small perturbation of the true QKD seed.

*Lorenz-system behavior.*

Figure 2 visualizes the Lorenz attractor driven by initial states that differ only by $10^{-7}$in their $x$-coordinate (with identical $y(0)$and $z(0)$). Both trajectories evolve under the standard Lorenz parameters $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$and trace out the characteristic double-wing structure of the attractor. Although the two trajectories begin almost indistinguishably, their separation grows rapidly due to the system's positive Lyapunov exponent. This sensitivity underpins the security advantage of

the proposed method: even if Eve's estimated seed differs infinitesimally from Alice and Bob's true seed, the resulting chaotic states diverge exponentially, ultimately driving Eve's mutual information toward zero.

*Exponential divergence of adversarial estimates*

To quantify this effect, perturbations of magnitudes $10^{-5}$, $10^{-7}$, and $10^{-10}$were added to Eve's guessed initial condition. Figure 3 plots the Euclidean distance $d(t) = \| X_t - X'_t \|$ between Alice–Bob's trajectory $X_t$ and Eve's trajectory $X'_t$. All perturbation levels exhibit exponential divergence of the form $d(t) \approx d_0 e^{\lambda t}$, where $\lambda > 0$ is the maximal Lyapunov exponent. Although both trajectories remain confined within the fractal geometry of the attractor, their instantaneous states diverge in a manner that prevents Eve from maintaining correlation with the true system trajectory. This divergence directly translates into mutual-information decay: as shown in Appendix A, exponential decorrelation of the joint density implies $I(A;E_t)\to 0$, even when Eve begins with arbitrarily small but nonzero state error. Fig. 3 shows that even the smallest perturbation of $10^{-10}$results in a separation that increases by several orders of magnitude within a short interval, demonstrating the system's extreme sensitivity to initial uncertainty. The curves in Fig. 3 exhibit slopes consistent with the maximal Lyapunov exponent, confirming that the divergence.

These results highlight a central security implication. The relevant question is not whether Eve can produce a trajectory that remains inside the same attractor, but whether she can produce a trajectory whose instantaneous state remains sufficiently close to Alice and Bob's to extract bit-level correlations. The simulations show that she cannot: even minute initial discrepancies yield exponentially diverging dynamics, and Appendix A confirms that this divergence enforces an exponential decrease in Eve's mutual information with Alice's expanded key. Consequently, the hybrid chaos–QKD protocol exhibits strong resilience against reconstruction attacks and provides a measurable advantage over QKD-only key-rate scaling.

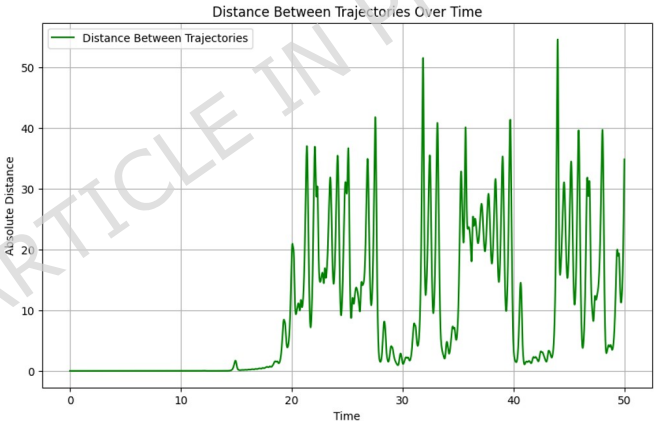


Fig. 3. Plot of $\|x(t) - x'(t)\|$ vs. time $t$. The plot shows the absolute distance between two Lorenz trajectories initialized with a small perturbation of $d = 10^{-7}$. For an initial transient period, the trajectories remain close, but as time progresses, their separation grows rapidly, exhibiting intermittent bursts characteristic of chaotic dynamics. These fluctuations reflect the system's positive Lyapunov exponent, which amplifies microscopic errors and drives the trajectories onto distinct regions of the attractor. This behavior is central to the proposed key-expansion mechanism: even an adversary with near-perfect initial knowledge accumulates significant deviation over time, leading to decorrelation of her reconstructed sequence from Alice's and ultimately causing the mutual information $I(A;E)$to approach zero, consistent with the theoretical result in Appendix A.

*Reduction of Mutual Information*

Let $\{A_i(t)\}_{i=1}^{N}$and $\{E_i(t)\}_{i=1}^{N}$denote the binary sequences held by Alice and Eve at (discrete) time index $t$, obtained by quantizing and sampling the Lorenz trajectories and extracting $N$bits from each party. For each fixed time $t$, we treat the pair $(A_i(t),E_i(t))$as i.i.d. samples of a pair of binary random variables $(A(t),E(t)) \in \{0,1\}^2$. The empirical joint distribution is estimated via the relative frequencies

$$p_{ae}(t) = \frac{N_{ae}(t)}{N}, a,e \in \{0,1\},$$

where $N_{ae}(t)$is the number of indices $i$such that $A_i(t) = a$ and $E_i(t) = e$. The corresponding marginals

are

$$p_A(a;t) = \sum_e p_{ae}(t), p_E(e;t) = \sum_a p_{ae}(t).$$

In general, mutual information between Alice and Eve is defined as

$$I(A;E) = \sum_{a,e} \hat{p}(a,e) \log_2 \frac{\hat{p}(a,e)}{\hat{p}(a)\hat{p}(e)}.$$

For specific time t, the mutual information between Alice and Eve is then computed using the standard definition

$$I(A;E|t) = \sum_{a,e\in\{0,1\}} p_{ae}(t) \log_2 \frac{p_{ae}(t)}{p_A(a;t)\, p_E(e;t)}.$$

This quantity measures the number of bits of information about Alice's key that are leaked to Eve at that time.
In addition, we track the *bitwise mismatch probability* between the two sequences,

$$p_{err}(t) = \frac{1}{N} \sum_{i=1}^{N} 1(A_i(t) \neq E_i(t)) = p_{01}(t) + p_{10}(t),$$

and empirically observe that, due to the chaotic divergence of trajectories, $p_{err}(t)$approaches 1/2as t increases.
In the regime where the marginals are approximately balanced,

$$p_A(0;t) \approx p_A(1;t) \approx \frac{1}{2}, p_E(0;t) \approx p_E(1;t) \approx \frac{1}{2},$$

and errors are approximately symmetric (i.e., the effective channel from Ato Ebehaves as a binary symmetric channel with crossover probability $p_{err}(t)$), the mutual information can be expressed as

$$I(A;E|t) \approx 1 - H_2(p_{err}(t)),$$

where $H_2(x) = -x\log_2 x - (1 - x)\log_2(1 - x)$ is the binary entropy function. In particular, as $p_{err}(t)\to\frac{1}{2}$, we have $H_2(p_{err}(t))\to 1$ and therefore

$$I(A;E|t)\to 0.$$

Owing to the chaotic aspect of the Lorenz system, the smallest discrepancy in the initial state Esti mate of Eve's causes her trajectory to deviate rapidly away from that followed by Alice and Bob. This difference can be traced back to the system's positive Lyapunov exponent, which guarantees that near one another trajectories will grow rapidly further apart in time. Mathematically, the mutual information I(A; E) between Alice's bits A and Eve's reconstituted bits E can be written as follows:

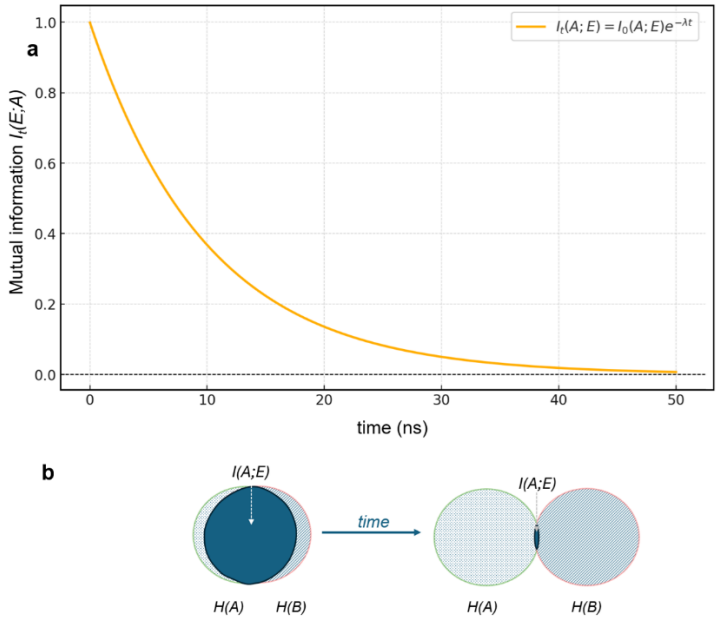


Fig. 4. Mutual information $I(A; E)$ vs. time showing exponential decay of mutual information and conceptual illustration of information suppression.. (**a**) Theoretical decay of the mutual information I(A;E)between

Alice's expanded key and Eve's estimate, modeled as $I_t(A;E) = I_0(A;E)\, e^{-\lambda t}$. The curve demonstrates that even if Eve begins with partial knowledge of the key, chaotic divergence causes her information to fall rapidly toward zero over time, consistent with the theoretical bound $I(A;E_t) \leq Ke^{-2\gamma' t}$ proven in Appendix A. (**b**) Schematic interpretation of this process in terms of entropy sets. At early times, Eve's uncertainty overlaps significantly with Alice's key space, leading to nonzero mutual information. As time progresses, the chaotic evolution amplifies any initial uncertainty, shrinking the overlap region and driving $I(A;E)$ asymptotically to zero. This illustrates the mechanism through which the chaotic post-processing layer eliminates residual adversarial information even when Eve attempts parameter estimation or trajectory reconstruction.

As time progresses, the mismatch between the two bit- streams grows. This is not only expected due to chaotic divergence, but it is also supported by simulation data. The mismatch probability increases toward 50%, at which point the mutual information approaches zero. Mathematically, this is captured by the limit:

$$\lim_{t\to\infty} I(A;E) = 0 \text{ as } p_{err}(t)\to\frac{1}{2} \qquad (9)$$

This exponential drop is confirmed in Fig. 4, which plots the mutual information $I(A; E)$ over time for various levels of initial estimation error. The curves in the figure demonstrate that Eve's information degrades rapidly, even when her initial estimate is only marginally inaccurate. A detailed formal proof of mutual information decay is provided in the appendix, as its length would otherwise interrupt the logical flow of the main manuscript.

In Figure 4(a), the plot illustrates the rapid decay of $I(A; E)$ over time, starting from an initial value of $1 \times 10^{-11}$ with small initial errors. The mutual information approaches zero within 50 nanoseconds, assuming a clock speed of 1 GHz. Figure 4(b) Illustration that, under the assumption that Eve could achieve high mutual information to Alice & Bob's key information, the mutual information would exponentially diminish over time within 40-50 ns, or 40 discrete time steps.

*Key rate comparison*

To assess the practical advantage of the proposed key expansion scheme, we performed a numerical simulation that compares its key rate behavior with that of the standard BB84 protocol. The results are presented in Fig. 5, where key generation rates are plotted against increasing communication distances, ranging from 0 to 100 km.

As expected, the BB84 protocol shows an exponential decay in the key rate with distance. This decline reflects well-known physical constraints, including photon losses in the channel, detector inefficiencies, and error accumulation over longer fiber paths. In real-world deployments, such decay often limits the usable range of BB84 systems, particularly in the absence of quantum repeaters or advanced multiplexing techniques.

***Standard BB84 QKD — Secret-Key Rate Model***

In the baseline BB84 protocol without decoy states, the asymptotic secret-key rate per signal can be written as

$$R_{BB84} = q\, Q_\mu[1 - H_2(E_\mu)],$$

where $q = \frac{1}{2}$ is the sifting factor, $Q_\mu$ is the overall gain for signal intensity $\mu$, and $E_\mu$ is the quantum bit-error rate (QBER). The gain is

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu},$$

with $\eta = \eta_d 10^{-\alpha L/10}$ the total transmittance over channel length $L$, $\eta_d$ the detector efficiency, $\alpha$ the fiber loss coefficient (dB/km), and $Y_0$ the background (dark-count) yield. The corresponding QBER is

$$E_\mu = \frac{e_0 Y_0 + e_d(1-e^{-\eta\mu})}{Q_\mu},$$

where $e_0 = \frac{1}{2}$ is the error probability of dark counts and $e_d$ is the optical misalignment error. This model captures the exponential decay of key rate with distance due to channel loss, which is the

baseline reference shown in the BB84 curve.

***Decoy-State BB84 QKD — Secret-Key Rate Model***

Decoy-state BB84 enhances security by estimating the single-photon contribution to the key using multiple intensities. In the standard two-decoy formulation (signal intensity $\mu$, weak decoy $\nu$), the secret-key rate is (Yin et al, 2020) [27]

$$R_{\text{decoy}} = q[- Q_\mu f(E_\mu) H_2(E_\mu) + Q_1(1 - H_2(e_1))],$$

where $f(E_\mu)$ is the error-correction inefficiency, $Q_1$ is the single-photon gain, and $e_1$ is the single-photon error rate. These parameters are estimated via

$$Q_1 \geq \frac{\mu e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^{\nu} - Q_\mu e^{\mu}\frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right),$$

$$e_1 \leq \frac{E_\nu Q_\nu e^{\nu} - e_0 Y_0}{Q_1}.$$

By isolating the single-photon component—which is the only one provably secure against photon-number-splitting attacks—decoy-state BB84 achieves significantly higher distance performance than standard BB84.

***Chaos-Augmented Key Expansion Model***

Let $R_{\text{BB84}}(L)$ denote the standard (or decoy-state) BB84 secret-key rate at channel distance $L$, computed from the usual gain–QBER model, e.g.

$$R_{\text{BB84}}(L) = q\, Q_\mu(L)\,[1 - f(E_\mu(L))H_2(E_\mu(L))] \text{ (or its decoy-state variant).}$$

In the proposed scheme, each distilled QKD key of length $n_{\text{seed}}$ bits (here $n_{\text{seed}} = 20$) is used to initialize a Lorenz system

$$\dot{x} = \sigma(y - x), \dot{y} = x(\rho - z) - y, \dot{z} = xy - \beta z,$$

whose state is evolved for a duration $T$ and sampled with rate $f_s$. At each sampling time $t_k = k/f_s$ we extract a $b$-bit symbol from (say) the $x$-coordinate via a uniform quantizer $Q(\cdot)$, yielding a bitstream of length

$$n_{\text{exp}} = b\, f_s\, T.$$

The *expansion factor* of the chaotic layer is therefore

$$G = \frac{n_{\text{exp}}}{n_{\text{seed}}}.$$

In our simulations we choose $T, f_s, b$ so that $n_{\text{seed}} = 20$ is expanded to $n_{\text{exp}} \approx 2 \times 10^4$ bits, giving $G \approx 10^3$.

The effective chaos-augmented key rate as a function of distance is then modeled as a multiplicative enhancement of the underlying QKD rate:

$$R_{\text{chaos}}(L) = G\, R_{\text{BB84}}(L),$$

which is finally normalized by its maximum value over $L$ when plotting Fig. 5. The evolution time $T$ is chosen large enough that the mutual information between Alice and Eve satisfies the exponential bound

$$I(A;E_T) \leq K e^{-2\gamma' T} \ll 1,$$

as proven in Appendix A, ensuring that the expanded bits remain information-theoretically close to independent of Eve's side information while still achieving the expansion factor $G$ used in the figure.

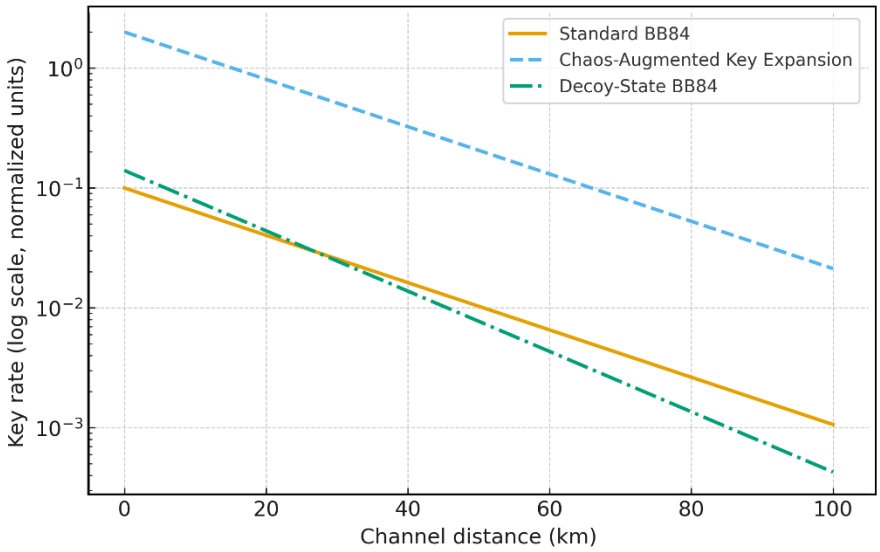


Fig. 5. Key rate comparison between BB84 (standard and decoy-state QKD) and Chaos-Augmented Protocol. Comparison of secret-key rates for three QKD configurations plotted on a logarithmic scale as a function of channel distance. The standard BB84 protocol exhibits exponential decay in the achievable key rate with increasing fiber distance due to photon loss and detector noise. The chaos-augmented key-expansion layer provides a multiplicative enhancement, resulting in an effectively higher throughput at all distances without modifying the underlying QKD hardware. The decoy-state BB84 protocol shows improved long-distance behavior, reflecting its resistance to photon-number-splitting attacks and better utilization of multi-intensity states. Although the curves are normalized for conceptual comparison, the relative trends illustrate how the proposed chaotic post-processing layer can complement existing QKD improvements such as decoy-state strategies.

Our chaos-based expansion breaks from this model in a key way. We still begin with the same basic setup. Still, instead of following that pattern, our protocol taps into the Lorenz system's deterministic dynamics to stretch a brief seed key into a far more extended sequence. The simulated model suggests that this approach can increase the effective key yield by up to 20 times at short distances. Importantly, this expansion is executed locally after the initial quantum exchange and does not rely on additional photon transmission. As a result, the key rate remains higher than BB84's across the entire distance range considered in the simulation.

*Security limitations*

While the chaotic expansion layer enhances practical secrecy by rapidly reducing an adversary's ability to synchronize with the legitimate users' trajectories, it does *not* increase the information-theoretic entropy beyond that contained in the initial 20-bit QKD seed. Since the Lorenz system is deterministic, the expanded key $K_{chaos}$ inherits the fundamental entropy bound

$$H(K_{chaos}) \leq H(K_{QKD}) = 20 \text{ bits}.$$

Thus, the security of the expanded key is *computational* in nature, relying on the practical difficulty of reconstructing the initial condition (x(0),y(0),z(0))from partial or approximate observations, rather than on unconditional secrecy.

The chaotic map amplifies uncertainty through its positive Lyapunov exponent $\lambda > 0$, leading to exponential divergence of trajectories:

$$\| \delta(t) \| \approx e^{\lambda t} \| \delta(0) \| ,$$

where $\delta(t)$ represents the difference between Eve's estimate and the true trajectory. This instability implies that small errors in Eve's guessed initial state grow beyond recoverability. However, because the mapping from the initial QKD seed to the Lorenz initial condition is deterministic and injective, an adversary could, in principle, attempt to recover the seed through brute-force enumeration of the $2^{20}$ possibilities.

Therefore, the security rests on the computational hardness of the following problem:

Given x(t), determine (x(0),y(0),z(0)) such that $x(t) = \Phi_t(x(0),y(0),z(0))$,

where $\Phi_t$ is the Lorenz flow. This inverse problem is numerically unstable and sensitive to noise, but not provably intractable.

Potential attack vectors must also be acknowledged. These include:

- Parameter-recovery attacks, in which Eve attempts to estimate the initial state via delay-coordinate embedding or nonlinear regression;
- Trajectory-fitting attacks, which attempt to minimize

$$\min_{\hat{s}} \sum_{k} |x(t_k) - \Phi_{t_k}(\hat{s})|,$$

where $\hat{s}$ denotes Eve's guess of the initial state;

- Machine learning prediction attacks, where neural networks or reservoir computing models approximate $\Phi_t$ and attempt to forecast the bitstream;
- Brute-force enumeration of the QKD seed, which remains feasible in principle for a 20-bit seed, though infeasible when combined with QKD's privacy amplification and the rapid mutual-information decay established in Appendix A.

We emphasize that the chaotic layer is intended as a *software-based throughput enhancement mechanism*, not as a replacement for the unconditional security of QKD. The final expanded key is secure to the extent that the adversary cannot feasibly solve the chaotic inversion problem, but its secrecy remains grounded in computational complexity rather than information-theoretic guarantees.

*Seed Length Considerations*

Although our demonstrations use a 20-bit QKD seed for clarity, the proposed hybrid framework supports seeds of arbitrary length. Increasing the seed size refines the specification of the chaotic initial conditions and correspondingly reduces the adversary's prior uncertainty. Extending the seed from $m$ bits to $m + k$ bits decreases Eve's parameter-estimation error by a factor on the order of $2^{-k}$. Under the exponential divergence associated with a positive Lyapunov exponent $\lambda > 0$, any nonzero residual mismatch $\delta_0 > 0$ still grows as $\delta_t \approx \delta_0 e^{\lambda t}$, implying that even extremely small initial errors ultimately lead to significant trajectory separation.

Appendix A shows that this divergence yields an exponential decay in mutual information, $I(A;E_t) \leq Ke^{-2\gamma' t} \to 0$, a bound that remains valid for any finite seed length. Consequently, larger QKD seeds strengthen security by reducing Eve's initial advantage while maintaining the same underlying information-theoretic decay mechanism. The method does not rely on a fixed seed size and stands to benefit directly from future increases in QKD source rates.

*On the measurement-device independent (MDI) QKD*

Measurement-device-independent QKD (MDI-QKD) has emerged as a leading architecture for practical, large-scale quantum networks, as it removes all detector-side channels by relying on two-photon interference at an untrusted relay. Early implementations employed synchronous interference between independent sources, while more recent protocols have demonstrated robust asynchronous two-photon interference suitable for real-world deployment. These developments provide a natural security advantage over standard BB84 by eliminating the dominant class of detector vulnerabilities. The proposed chaos-augmented key-expansion layer is fully compatible with MDI-QKD because it operates entirely as a classical post-processing procedure applied after key distillation and does not alter the optical measurement hardware or protocol assumptions. Thus, the method may be applied directly to MDI-QKD systems to enhance the effective key throughput while preserving their intrinsic measurement-security guarantees.

*Comparative Analysis*

Table 4 compares recent approaches that integrate chaos theory with QKD, highlighting their features, methods, and contributions. Our proposed method is included for direct comparison.

Table 4
Comparison with Recent Chaos-QKD Approaches

| Study | QKD Protocol | Chaos Method | Key Features | Limitations |
|---|---|---|---|---|
| Cowper et al. (2020) | Custom chaotic QKD | Coupled chaos masking | Masking of photon-level key with synchronized chaos | No key expansion; sensitive to noise |
| Cho & Miyano (2015) | Augmented Lorenz QKD-assisted cryptosystem | Augmented Lorenz equations with QKD-distributed real-valued key matrix; symmetric-key message encryption | Digital chaotic masking | Hardware-dependent dynamics; limited key expansion analysis |

| | | | | |
|---|---|---|---|---|
| Sharma et al. (2024) | BB84-derived decoy-state | Coincidence-detection | Improved key rates, demonstrated experimentally | Lab-scale, moderate expansion |
| Mahmud et al. (2021) | BB84-compatible FSO QKD enhancement | Lorenz parameter sync | QKD-secure parameter sharing over free-space optics | No high-rate expansion; experimental setup only |
| Keuninckx et al. (2017) | Chaos-based key distribution | Synchronization of nonlinear delay oscillators | Electronic implementation with delay-coupled units; passed NIST randomness tests | Hardware-dependent; lacks quantum security guarantees; costs |
| This work | BB84 / E91 compatible | Lorenz RK4-driven expansion | 20 → 20k bit expansion in ms, 99.99% suppression, no hardware change. Alice and Eve's mutual information approaches zero exponentially. | Requires exact synchronized computation. |

In light of these constraints, the method introduced in this study provides a substantial advancement. By applying Runge-Kutta-based integration of the Lorenz system in the post-processing stage, we enable the rapid expansion of a short QKD-derived key, on the order of 20 bits, into a high- entropy stream exceeding 20,000 bits. This expansion occurs within milliseconds and does not rely on additional quantum transmission or physical-layer adjustments. Importantly, our scheme remains fully compatible with both BB84 and E91 protocols. Another notable feature is the extremely low mutual information between Alice and a potential eavesdropper, which diminishes exponentially with any deviation in the adversary's estimation of initial conditions.

## Conclusion

In this study, we used a hybrid cryptographic scheme of Quantum Key Distribution and deterministic chaos to fend off QKD's most pervasive weakness—slow key rates. A short QKD-generated key was hidden in initial conditions of the Lorenz equations, which allowed us to produce a much longer key stream with higher entropy. Our simulations showed that such an approach could turn a 20-bit QKD key into over 20,000 bits in only fractions of a millisecond without sacrificing security.

The basic idea is to use the extreme sensitivity of chaotic systems to initial conditions. When the initial state is slightly varied, two trajectories will diverge rapidly. In other words, any eavesdropper who lacks the complete knowledge of the key cannot duplicate the correct bitstream. Such a property brings yet another layer of security atop the natural safeguards offered by quantum mechanics. What gives this scheme a particularly strong appeal is its practicality. It does not require any alterations to the hardware of QKD, and can be built onto a system just by software. This in turn brings forth boosted speed and security in the areas that need it most: video conferencing; encrypted mobile communications; Internet of Things networks. For future work, we plan on integrating this protocol with actual QKD systems to test its performance under real-world circumstances. We also want to try using other chaotic systems like Ro¨ssler or Chua circuits, to compare their reliability and which system produces better keys. Finally, we should perform inertia growth and entropy statistics more rigorously, ensuring that the keys generated meet cryptographic standards. In future work, tightening up system for FPGA or GPU acceleration may render it suitable for high-speed transmission platforms.

## Author Contributions

Conceptualization, P.D., S.W., H.T.M. and C.S.; Methodology, P.D. and C.S.; Formal Analysis, P.D.,

S.W., and C.S.; writing— original draft, P.D.; supervision, S.W.; writing—review and editing, C.S., H.T.M. All authors have read and agreed to the published version of the manuscript.

## Data Availability Statement

The original contributions presented in this study are included in the article.

## Acknowledgment

The authors acknowledge support from Khon Kaen University.

## Funding

No Funding.

## Conflict of Interest

The authors declare no conflicts of interest.

## References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014.
[2] S. Pirandola *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.
[3] J. Yang *et al.*, "High-rate intercity quantum key distribution with a semiconductor single-photon source," *Light: Science & Applications*, vol. 13, no. 1, p. 150, 2024.
[4] A. S. Alessa, M. Hammoudeh, and H. Singh, "A peek into the post- quantum era—PQA PQC: What will happen in 2030," in *Quantum Technology Applications, Impact, and Future Challenges*, CRC Press, 2025, pp. 163–180.
[5] A. S. Cacciapuoti *et al.*, "Quantum internet: Networking challenges in distributed quantum computing," *IEEE Network*, vol. 34, no. 1, pp. 137– 143, 2019.
[6] O. D. Okey *et al.*, "Quantum key distribution protocol selector based on machine learning for next-generation networks," *Sustainability*, vol. 14, no. 23, p. 15901, 2022.
[7] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
[8] Z. H. Wang *et al.*, "Tight finite-key analysis for mode-pairing quantum key distribution," *Communications Physics*, vol. 6, no. 1, p. 265, 2023.
[9] A. Boaron *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Physical Review Letters*, vol. 121, no. 19, p. 190502, 2018.
[10] C. Clivati *et al.*, "Coherent phase transfer for real-world twin-field quantum key distribution," *Nature Communications*, vol. 13, no. 1, p. 157, 2022.
[11] L. Zhang *et al.*, "Experimental mode-pairing quantum key distribution surpassing the repeaterless bound," *Physical Review X*, vol. 15, no. 2, p. 021037, 2025.
[12] H. Wang *et al.*, "High-efficiency multiphoton boson sampling," *Nature Photonics*, vol. 11, no. 6, pp. 361–365, 2017.
[13] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nature Communications*, vol. 5, no. 1, p. 5235, 2014.
[14] E. N. Lorenz, "Deterministic nonperiodic flow," in *Universality in Chaos*, 2nd ed., Routledge, 2017, pp. 367–378.
[15] N. Cowper, H. Shaw, and D. Thayer, "Chaotic quantum key distribution," *Cryptography*, vol. 4, no. 3, p. 24, 2020.
[16] L. Keuninckx *et al.*, "Encryption key distribution via chaos synchroniza- tion," *Scientific Reports*, vol. 7, no. 1, p. 43428, 2017.
[17] A. Sykot *et al.*, "Multi-layered security system: Integrating quantum key distribution with classical cryptography to enhance steganographic security," *Alexandria Engineering Journal*, vol. 121, pp. 167–182, 2025.
[18] K. Cho and T. Miyano, "Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 2, pp. 478–487, 2014.
[19] A. Kotangale, M. S. Kumar, and A. P. Bhagat, "Improved big data security using quantum chaotic map of key sequence," *Computers*, vol. 14, no. 6, p. 214, 2025.
[20] K. Purohit and A. K. Vyas, "Quantum key distribution through quantum machine learning: A research review," *Frontiers in Quantum Science and Technology*, vol. 4, p. 1575498, 2025.
[21] M. Rahmanpour *et al.*, "A new quantum key distribution protocol to reduce afterpulse and dark counts effects," *Results in Optics*, vol. 16, p. 100718, 2024.
[22] M. Zahidy *et al.*, "Practical high-dimensional quantum key distribution protocol over deployed multicore fiber," *Nature Communications*, vol. 15, no. 1, p. 1651, 2024.
[23] Z. Du *et al.*, "Advantage distillation for quantum key distribution," *Quantum Science and Technology*, vol. 10, no. 1, p. 015050, 2024.
[24] K. Song, N. Imran, J. Y. Chen, and A. C. Dobbins, "A hybrid chaos- based cryptographic framework for post-quantum secure communica- tions," arXiv preprint arXiv:2504.08618, 2025.
[25] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, no. 2, pp. 441–444, 2000.
[26] Y. Begimbayeva and T. Zhaxalykov, "Research of quantum key dis- tribution protocols: BB84, B92, E91," *Scientific Journal of Astana IT University*, 2022.
[27] Yin, H-L., Zhou, M-G., Gu, J. *et al.* Tight security bounds for decoy-state quantum key distribution. *Sci Rep* **10**, 14312

(2020). https://doi.org/10.1038/s41598-020-71107-6

# Appendix

## A. Proof of Mutual Information Decay for Discrete Chaotic Maps

### *Theorem Statement*

Let $f:M\to M$ be a discrete-time chaotic map on a compact metric space $M$, preserving an ergodic invariant probability measure $\mu$.
Assume $f$ exhibits exponential decay of correlations for Hölder-continuous observables:

$$|\int g(f^t(x))\,h(x)\,d\mu(x) - (\int g\,d\mu)(\int h\,d\mu)| \le C\,\|g\|_\alpha\,\|h\|_\alpha\,e^{-\gamma t}. \quad (a.1)$$

Let $x_0$ be a random variable with density $p_0$. Define the trajectories

$$X_t = f^t(x_0), Y_t = f^t(x_0 + \delta), \quad (a.2)$$

with $\delta > 0$. Then the mutual information satisfies

$$I(X_t;Y_t) \le K e^{-2\gamma' t}. \quad (a.3)$$

*A.1. Spectral Properties of the Perron–Frobenius Operator*

Let $P$ denote the Perron–Frobenius operator, defined by

$$\int (P\varphi)\,\psi\,d\mu = \int \varphi\,(\psi \circ f)\,d\mu. \quad (a.4)$$

For a broad class of chaotic dynamical systems, this operator exhibits a spectral gap: the eigenvalue $1$ corresponding to the invariant density is simple, and all remaining eigenvalues lie strictly inside the unit disk, satisfying $|\lambda| < 1$. As a consequence, for any observable $\varphi$ with zero mean ($\int \varphi\,d\mu = 0$), iterates under the operator contract exponentially, obeying

$$\|P^t\varphi\| \le C' r^t \|\varphi\|, \quad (a.5)$$

for some constants $C' > 0$ and $0 < r < 1$. This exponential contraction reflects the strong mixing properties essential for the decay-of-correlation estimates used throughout the proof.

*A.2. Evolution of the Joint Distribution*

*Let* $f:M\to M$ *be the chaotic map under study, and define the product map*

$$F(x,y) = (f(x), f(y)), \quad (a.6)$$

*acting on the product space* $M \times M$. *Let* $p_0(x)$ *denote the initial density of the random variable* $X_0$, *and let* $\delta > 0$ *denote the initial offset between Alice's and Eve's trajectories. The corresponding joint initial density is*

$$p_0(x,y) = \delta(y - (x + \delta))\, p_0(x), \qquad (a.7)$$

where $\delta(\cdot)$ is the Dirac delta. After a single iteration under the smooth map $F$, this singular distribution becomes regular (absolutely continuous). Let $P_F$ be the Perron–Frobenius operator associated with the product map. For chaotic systems with exponential mixing, this operator satisfies

$$\| P_F^t q - \rho_F \| \leq C_F\, r_F^t \| q \|, \qquad (a.8)$$

*for any density* $q$*, where* $0 < r_F < 1$, $C_F > 0$*, and*

$$\rho_F(x,y) = \rho(x)\, \rho(y)$$

denotes the product invariant density of the marginals. Consequently, the joint density $p_t(x,y)$ at time $t \geq 1$ satisfies

$$\| p_t - \rho_F \| \leq C_F'\, r_F^t, \qquad (A.8)$$

*showing that the joint distribution is attracted exponentially toward the product of marginals.*



### *A.3. Convergence of Marginals*

*The marginal distributions of* $X_t$ *and* $Y_t$ *are given by*

$$p_t^{(X)}(x) = \int p_t(x,y)\, dy, p_t^{(Y)}(y) = \int p_t(x,y)\, dx. \qquad (a.9)$$

*Both marginals converge exponentially to the invariant density* $\rho$*. Specifically, for constants* $C_M > 0$ *and* $0 < r < 1$*,*

$$\| p_t^{(X)} - \rho \| \leq C_M\, r^t, \| p_t^{(Y)} - \rho \| \leq C_M\, r^t. \qquad (A.10)$$

*Thus, regardless of the initial mismatch* $\delta$*, the marginals relax toward equilibrium at an exponential rate.*

### *A.4. Total Variation Convergence*

*Since the Banach-space norm used above dominates the* $L^1$ *norm, there exists a constant* $K_B > 0$ *such that*

$$\| p_t - \rho_F \|_1 \leq K_B\, C_F'\, r_F^t.$$

*Combining this with the marginal convergence, we obtain*

$$\| p_t - p_t^{(X)} p_t^{(Y)} \|_1 \leq K_1 \max(r_F, r)^t,$$

*where* $K_1 > 0$*. This shows that the joint distribution becomes indistinguishable from the product of the marginals at an exponential rate.*

*A.5. Mutual Information Decay*

The mutual information between the trajectories $X_t$and $Y_t$is defined as

$$I(X_t;Y_t) = D_{KL}\left(p_t \parallel p_t^{(X)}p_t^{(Y)}\right),$$

where $D_{KL}$denotes the Kullback–Leibler divergence, $p_t$is the joint density of $(X_t,Y_t)$, and $p_t^{(X)},p_t^{(Y)}$are the marginal densities.
Using Pinsker's inequality, the mutual information is bounded in terms of the *total variation distance* (TV)

$$TV(p_t, p_t^{(X)}p_t^{(Y)}) = \frac{1}{2} \parallel p_t - p_t^{(X)}p_t^{(Y)} \parallel_1,$$

where $\parallel \cdot \parallel_1$ denotes the $L^1$-norm. Thus,

$$I(X_t;Y_t) \le \frac{1}{2} TV^2 = \frac{1}{8} \parallel p_t - p_t^{(X)}p_t^{(Y)} \parallel_1^2.$$

Substituting the exponential $L^1$-convergence bound derived in Sections A.2–A.4 yields

$$I(X_t;Y_t) \le K_2 e^{-2\gamma' t},$$

for constants $K_2 > 0$and $\gamma' > 0$, establishing that the mutual information decays exponentially and approaches zero as $t\to\infty$.



*A.6. Applicability to Standard Chaotic Systems*

The assumptions underlying the proof—namely the existence of an ergodic invariant measure, a spectral gap for the Perron–Frobenius operator, and exponential decay of correlations—are satisfied by a broad class of well-studied chaotic dynamical systems. These include uniformly expanding maps, Anosov diffeomorphisms, and piecewise expanding systems, all of which admit the functional-analytic structure required for the convergence bounds established above. Although the Lorenz system is a continuous-time flow rather than a discrete map, the same reasoning applies to its time-$\tau$ discretization $\Phi_\tau$. For any fixed sampling interval $\tau > 0$, the map $\Phi_\tau$inherits exponential mixing properties on appropriate anisotropic Banach spaces, ensuring that the mutual-information decay proven in this appendix holds for the Lorenz attractor as well.
Conclusion

$$I(X_t;Y_t) \le K e^{-2\gamma' t} \longrightarrow 0 \text{ as } t\to\infty.$$

For continuous-time flows (such as the Lorenz system), apply the argument to the time-$\tau$ map $\Phi_\tau$, giving

$$I(t) \le K e^{-2\gamma'(t/\tau)}.$$

***Appendix B. Entropy Bound for Deterministic Post-Processing of an $N$-Bit Seed***

Let

$$K \in \{0,1\}^N$$

denote the initial $N$-bit seed with probability mass function $P_K$. Its Shannon entropy is

$$H(K) = -\sum_{k\in\{0,1\}^N} P_K(k)\log P_K(k),$$

and satisfies $H(K) \le N$, with equality when $K$ is uniformly distributed.
Let the entire key–generation pipeline—mapping to a chaotic system, evolving the trajectory, sampling, quantizing, and producing the final key—be represented as a **deterministic function**

$$f:\{0,1\}^N \to Y,$$

and define the output random variable

$$Y = f(K).$$

The following theorem establishes that the output entropy cannot exceed the seed entropy.

**Theorem B.1 (Deterministic Post-Processing Cannot Increase Entropy).**
If $Y = f(K)$ for a deterministic function $f$, then

$$H(Y) \le H(K) \le N.$$

**Proof.**
Because $Y$ is a deterministic function of $K$, the conditional entropy vanishes:

$$H(Y|K) = 0.$$

Using the chain rule for entropy in two equivalent ways gives

$$H(K,Y) = H(K) + H(Y|K) = H(K),$$

and also

$$H(K,Y) = H(Y) + H(K|Y).$$

Equating the expressions yields

$$H(K) = H(Y) + H(K|Y).$$

Since conditional entropy is non-negative,

$$H(K|Y) \ge 0,$$

we obtain the bound

$$H(Y) \le H(K).$$

Because $H(K) \le N$ for any $N$-bit seed, the result follows. □

**Corollary B.2.**
For a uniformly random $N$-bit seed, the entropy of any derived key obtained through deterministic chaotic evolution and bit extraction satisfies

$$H(Y) \le N.$$

Thus, no deterministic expansion procedure—including those based on chaotic dynamics—can increase the entropy beyond that already present in the initial $N$-bit seed.