Sumer Journal for Pure Science (ISSN: 2790-7031)
SJPS 2026 (June), Vol. 5, No. 1, p.p.: 87-99

Analysis of Success Threshold of (4,5) in Hybrid Series- Parallel Networks for Enhanced Cryptographic Key Reliability

Israa K. Edam [1]*, Abeer A. Abdul- Razaq [2]
[1]*Mathematics department, Thi-Qar University, Thi-Qar, Iraq*
[2] *Mathematics department, Thi-Qar University, Thi-Qar, Iraq*
israa_kamel@utq.edu.iq

Abstract

This research presents an innovative hybrid network model designed to enhance the reliability of systems used in cryptographic frameworks and data protection. The primary scientific contribution lies in designing a structured architecture that integrates series and parallel configurations using five components with a success threshold of (4,5). Graph theory was employed to determine the minimum path and cut sets, and the system's reliability formula was derived through reduction techniques to simplify the complex network. Numerical results demonstrate high reliability in cryptographic applications and overall system performance, achieving an optimal balance between complexity and security compared to traditional models. Monte Carlo simulation was used to confirm the consistency between theoretical derivations and applied results, and a sensitivity analysis was performed on critical components.

Keywords: Hybrid network, Reliability, Encryption, Threshold of (4,5), Graph Theory, Simulation.

تحليل عتبة النجاح (4,5) في الشبكات الهجينة المتسلسلة والمتوازية لتعزيز موثوقية مفتاح التشفير

اسراء كامل ايدام [1]*, عبير عبد الكاظم [2]
[1] قسم الرياضيات, كلية التربية للعلوم الصرفة, جامعة ذي قار, العراق
[2] قسم الرياضيات, كلية التربية للعلوم الصرفة, جامعة ذي قار, العراق

الخلاصة

يقدم هذا البحث نموذج شبكي هجين مبتكر مصمم لتعزيز موثوقية الانظمة المستخدمة في اطر التشفير وحماية البيانات. تكمن المساهمة العلمية الرئيسية في تصميم بنية هيكلية متكاملة تجمع بين التكوينات المتسلسلة والمتوازية ب استخدام 5 مكونات مع عتبة نجاح (4,5) استخدمت نظرية البيانات لتحديد اقصر مسار ومجموعات القطع وتم اشتقاق صيغة موثوقية النظام من خلال تقنية الاختزال لتبسيط الشبكة المعقدة تظهر النتائج العددية موثوقية عالية في تطبيقات التشفير واداء عام ممتاز للنظام محققة توازن مثالي بين التعقيد والامان مقارنة بالنماذج التقليدية. استخدمت محاكاة مونتوكارل لتاكيد التوافق بين الاشتقاقات النظرية والنتائج التطبيقية , كما اجري تحليل حساسية على المكونات الاساسية والاكثر تاثير بالشبكة.

1. Introduction

Network reliability is fundamental to the design of modern systems, especially those related to information security and encryption. Modern encryption systems rely on key distribution, as documented by Shamir[1], where the secret key is divided into several parts and can only be recovered if a threshold of (k out of n)met. Managing encryption keys presents a significant challenge in network security and ensuring its protection against threats [2]. Data algorithm depends on secure distribution within the network [3]. Despite the

advancements in network reliability, a significant gap remains in optimizing hybrid architectures for secure key distribution in resource-constrained environments. While previous studies, such as [10] and [11], evaluated parallel-series systems with a success threshold of (5,8), they often overlooked the balance between architectural complexity and security overhead in smaller-scale configurations. This research addresses this gap by proposing a hybrid network model with a success threshold of (4,5). The primary objective is to enhance the reliability of cryptographic key availability, ensuring that the system remains functional even under targeted component failures. By integrating graph theory with reduction techniques, this study provides a formal mathematical framework to evaluate how this specific (4,5) configuration outperforms traditional models in maintaining secure communication paths.". We rely on achieving an ideal reliability model by applying mathematical principles to complex systems [12]. Understanding modern encryption mechanisms helps designers and specialist evaluate protocols capable of withstanding attackers [13]. The proposed hybrid model is based on five basic components denoted by B. Monte-Carlo simulation was performed using R programming language to evaluate the reliability of the hybrid network.

2. Security Framework and Threat Model

To address the cryptographic context of the proposed hybrid network, this section defines the security environment and the protocols supported by the (4,5) success threshold.

2.1 Cryptographic Protocol Integration

The proposed system is designed to support Threshold Cryptography and Secure Key Distribution Centers. In this framework, a cryptographic master key is partitioned into five shares using a secret-sharing scheme (inspired by Shamir's algorithm). These shares are distributed across the five nodes of the hybrid network. The (4,5) threshold ensures that the original key can only be reconstructed if at least four nodes (shares) are accessible through the reliable paths derived in our graph theory model.

2.2 Threat Model

The threats include: Targeted Node Failure: An attacker may launch a Denial of Service attack against specific critical components (e.g., componentB_5) identified in our sensitivity analysis.

Link Interruption: Physical or logical disruptions aimed at the series-parallel connections to prevent key reconstruction.

Brute-Force Impairment: Attempting to disable enough components to drop the system below the success threshold of 4.

2.3 Security Metrics and Analysis

Unlike standard networks, the primary security metric here is Cryptographic Availability. The formal security analysis proves that as long as the network reliability R_s (calculated in Section 4) remains above the operational threshold, the confidentiality and availability of the key are maintained. The (4,5) configuration provides a "Fault Tolerance"

of 1, meaning the system can withstand the complete compromise or failure of any single node without losing the ability to perform cryptographic operations.

3. Describe the Hybrid Network that Combines Series-Parallel and Parallel-Series Networks

This section explains a hybrid model combining the characteristics of a series-parallel and parallel-series network. The purpose of this network type is to represent a combination of simple and complex networks, allowing us to study the impact of this hybrid model on system reliability and encryption. This network consists of five components, each subject to failure or success. We will assume that each component is independent in failure conditions. The components are linked by paths, some sequential and some parallel. System success depends on a sufficient number of these paths functioning correctly to ensure network continuity and key regeneration. In sequential paths, failure of any component leads to system failure, while in parallel paths, failure of one component causes the parallel connection to fail.

Note: The network diagrams were drawn using Microsoft word drawing tools.

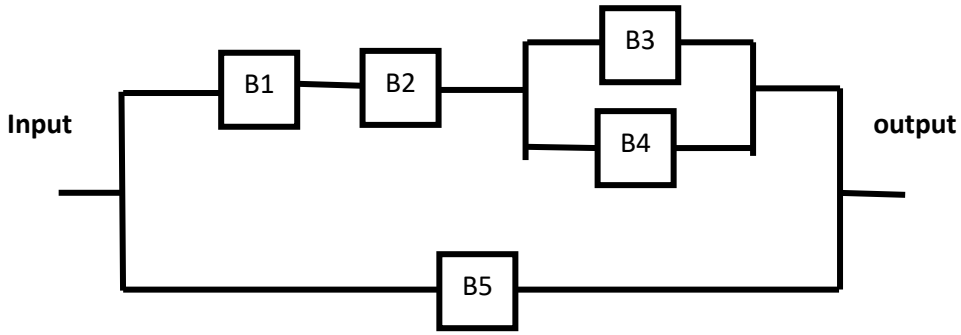


Figure -1 A hybrid network

4. Hybrid Model Reliability Network Within Graph Theory

This section explains the reliability of encryption in hybrid network using graph theory. This provides a mathematical basis for understanding paths and breaks in network reliability, where a vertex (v) represents an independently operating component network consists of 5 vertices, and the importance of this part becomes clear in how reliability is derived.

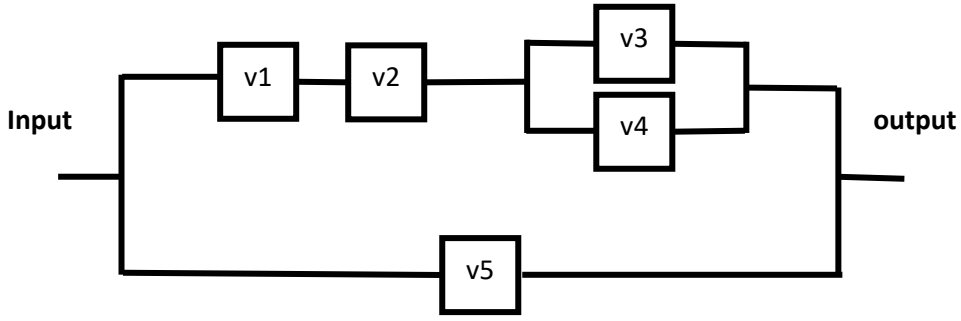


Figure -2 Graph Theoretic of Hybrid Network

Analysis of figure 5: The series path contains components $v_1 and\ v_2$, the success of this path depends on both components working together. The parallel path contains two components $v_3 and\ v_4$, one components of theses fails the work of the other ensure is successful of the system. The path contain the component v_5 if it work the system is also successful.

5. Reliability Analysis: Minimal Path and Cut Set

To formally evaluate the reliability of the proposed hybrid architecture under the (4,5) success threshold, it is essential to define the operational and failure states of the system.

In this analysis, the operational success is represented by Minimal Path Sets (denoted byP_i), which are the minimum combinations of functioning components required for the system to remain operational. Conversely, failure states are represented by Minimal Cut Sets (denoted byK_j), which represent the critical combinations of component failures that lead to total system failure.

5.1 Minimal Path Sets (MPS)

For a system with a success threshold of k=4 and a total of n=5 components, any combination of four functional components ensures system success. The minimal path sets are:

$P_1 = \{B_1, B_2, B_3, B_4\}$, $P_2 = \{B_1, B_2, B_3, B_5\}$

$P_3 = \{B_1, B_2, B_4, B_5\}$, $P_4 = \{B_1, B_3, B_4, B_5\}$

$P_5 = \{B_2, B_3, B_4, B_5\}$

5.2 Minimal Cut Sets (MCS)

The minimal cut sets are critical for understanding system vulnerability. Since the system requires at least 4 components to function, the failure of any two components (n-k+1 = 2) will cause the system to fail. The 10 minimal cut sets are:

$K_1 = \{B_1, B_2\}$, $K_2 = \{B_1, B_3\}$, $K_3 = \{B_1, B_4\}$

$K_4 = \{B_1, B_5\}$, $K_5 = \{B_2, B_3\}$, $K_6 = \{B_2, B_4\}$

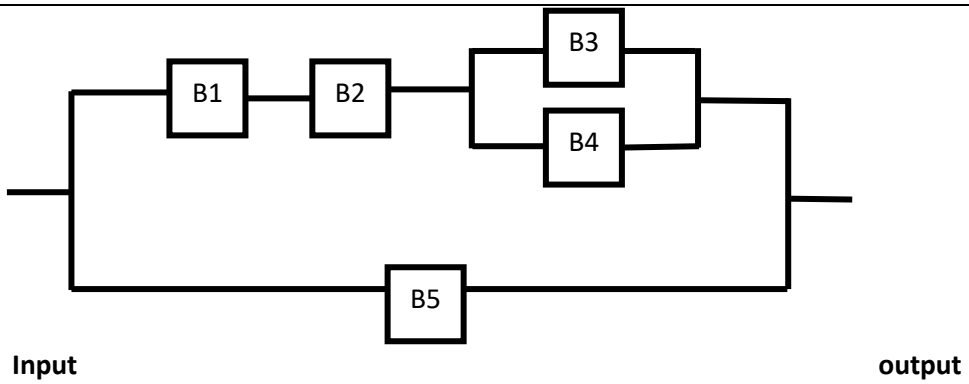
$K_7 = \{B_2, B_5\}$, $K_8 = \{B_3, B_4\}$, $K_9 = \{B_3, B_5\}$

$K_{10} = \{B_4, B_5\}$

6. Derivation of Hybrid Network Reliability

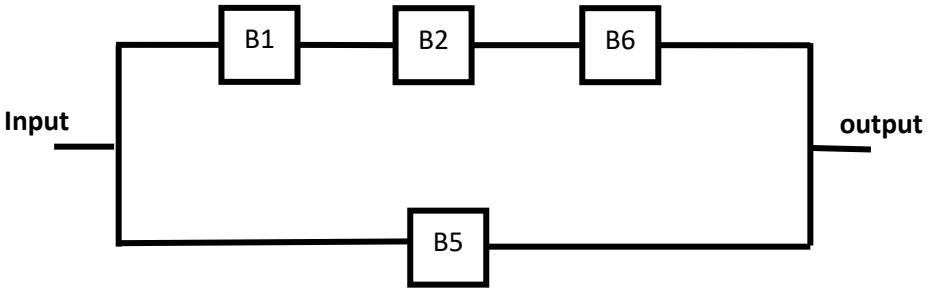
The reliability of the proposed hybrid system is derived by systematically reducing the network configuration into series and parallel equivalent components. Based on Figure (3), the derivation process is structured as follows

Step 1: Parallel and Series Subsystem Reduction First, we calculate the reliability of the parallel branch consisting of B_3andB_4, and the series connection of B_1andB_2.



The equivalent reliability for the parallel components B_1andB_2

$$R_6 = 1 - [(1 - R_3)(1 - R_4) \quad (1)$$



Step 2: Series Reduction of Components 1 ,2 and 6

The components B_1, B_2 and B_6

are connected in series to form the equivalent subsystemB_7 . Its reliability is calculated as:

$$R_7 = (R_1 \times R_2 \times R_6) \quad (2)$$

Step3: Total Hybrid System Reliability ($R_{syst.}$)

The entire system is formed by the parallel connection of the upper branch (R_7) and the lower component (R_5). The total system reliability is:

$$R_{syst.} = 1 - [(1 - R_7)(1 - R_5)] \quad (3)$$

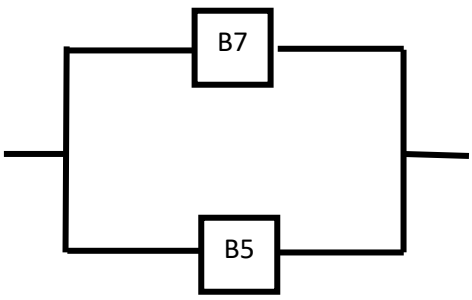


Figure -3 system components reduction

Step 5: Threshold-Based Key Reliability (R_{key})

As established in the security framework, the cryptographic key availability follows a (4-out-of-5) success threshold:

$$R_{key} = \sum_{k=4}^{5} \binom{5}{k} (r)^k (1-r)^{5-k} \quad (4)$$

Step 6: Final Integrated Reliability (R_{total})

The final reliability of the secure communication process is the product of the physical network's reliability and the logical key threshold reliability:

$$R_{total} = R_{key(4\ out\ of\ 5)} \times R_{sys(Hybrid)} \quad (5)$$

Note that component reduction applies only to the network structure, while in key reliability and encryption , the models are equivalent without component reduction. In the proposed model, each encryption represent an encryption process or key generation phase, while the success of the system depends on the successful completion of the secure key creation process.

6.1 Numerical Example to Demonstrate the Reliability Values of Encryption with the Composite in Hybrid Model

Let $R_1 = 0.90 \quad R_2 = 0.91 \quad R_3 = 0.92 \quad R_4 = 0.93 \quad R_5 = 0.94$

$R_7 = (R_1 \times R_2) \times [1 - (1 - R_3)(1 - R_4)]$

$R_7 = 0.90 \times 0.991 \times [1 - (1 - 0.92)(1 - 0.93)]$

$R_7 = 0.8144$

$R_{sys(Hybrid)} = 1 - [(1 - R_7)(1 - R_5)]$

$R_{sys(Hybrid)} = 1 - [(1 - 0.8144)(1 - 0.94)$

$R_{sys(Hybrid)} = 1 - 0.011136 = 0.988$

$R_{key} = (R_1)(R_2)(R_3)(R_4)(R_5) + [(1 - R_1)R_2R_3R_4R_5] + [(1 - R_2)R_1R_3R_4R_5 + (1 - R_3)R_1R_2R_4R_5 + (1 - R_4)R_1R_2R_3R_5 + (1 - R_5)R_1R_2R_3R_4$

$$R_{key} = 0.90 \times 0.91 \times 0.92 \times 0.93 \times 0.94 + (1 - 0.90)0.91 \times 0.92 \times 0.93 \times 0.94 + (1 - 0.91) \times 0.90 \times 0.92 \times 0.93 \times 0.94 + (1 - 0.92) \times 0.90 \times 0.91 \times 0.93 \times 0.94 + (1 - 0.93) \times 0.90 \times 0.91 \times 0.92 \times 0.94 + (1 - 0.94) \times 0.90 \times 0.91 \times 0.92 \times 0.93$$

$R_{key} = 0.9455$

$R_{tot.} = R_{key} \times R_{sys}$

$R_{tot.} = 0.988 \times 0.9455 = 0.9341$

Based on the above values, we observe the efficiency of the hybrid system, the reliability of the key, the system, and the overall encryption is very good. This is due to the flexibility of this hybrid network. Furthermore, choosing a threshold of 4out of 5 has significantly helped balance security and reliability, ensuring that the key remains unaffected in case of failure of one component and cannot be recovered by an attacker. The fifth component also plays a

crucial role in maintaining security levels in the event of upper-path component failure. Compared to traditional systems, the hybrid system has achieved high reliability and enhanced network security.

7. Derivation of Hybrid Network Reliability

Here we will test the sensitivity and robustness of the hybrid model by making the reliability of any components very weak and observing their impact on the overall encryption reliability. We will examine the system's ability to secure the encryption threshold (4out of5) in the event of component failure.

8. Hybrid Network Simulation Report (N = 10,000)

Full sensitivity for all components (B1–B5) + 150-run Monte Carlo stability, tables, and rectangular charts.

8.1 Model and Success Conditions

The hybrid network has two parallel branches from input to output. The upper branch is a series connection of B1 and B2, followed by a parallel block (B3 || B4). The lower branch is a direct bypass through B5. Components are assumed independent.

Key reconstruction follows a threshold rule (4 out of 5): the key can be reconstructed if at least four components are operational.

8.2 Monte Carlo Simulation Method (N = 10,000)

In this section, the reliability of hybrid network was evaluated using Monte-Carlo simulation implemented in R programming language. Random samples were generated to simulate the operational states of system components. Each component was assigned a probability of success, and the overall system reliability was estimated based on repeated simulation runs. The simulation process was executed sequentially to ensure accurate estimation of network performance.

For each iteration, generate independent Bernoulli states Xi ~ Bernoulli (r_i) for i = 1..5. Xi = 1 means component Bi works, and Xi = 0 means failure.

Network success: S_{top} = X1·X2·(X3 OR X4), and S_{sys}= (S_{top}OR X5).

Key success: let Y =$\sum x_i$. Then S_{key}= 1{Y ≥ 4}. Encryption success: $S_{tot.}$= S_{sys}× S_{key}.

Reliabilities are estimated by sample means over N iterations. A 95% confidence interval is computed as $\hat{p} \pm 1.96 \cdot \sqrt{\hat{p}(1-\hat{p})/N}$.

8.3 Base Parameters

Base reliabilities: R= [R_1, R_2, R_3, R_4, R_5] = [0.90, 0.91, 0.92, 0.93, 0.94].

8.4 Theoretical Values (Closed-form)

R_{u7}= (R_1R_2)·[1 − (1−R_3)(1−R_4)] = 0.814414.

R_{sys}= 1 − [(1−R_7)(1−R_5)] = 0.988865.

R_{key} = P(Y ≥ 4) = 0.945926.

$R_{tot.} = R_{sys} \times R_{key} = 0.935393.$

8.5 Validation (Theory vs Monte Carlo)

A representative Monte Carlo run (seed=3) is compared to theory.

Table 1- Theory vs Monte Carlo validation (seed=3).

Metric	Theoretical	Monte-Carlo	Absolute-Error	Percent Error(%)	CI-Lower	CI-Upper
R_{sys}	0.988865	0.9889	0.000035	0.003558	0.986847	0.990953
R_{key}	0.945926	0.9453	0.000626	0.066218	0.940843	0.949757
$R_{tot.}$	0.935393	0.9453	0.009907	1.059093	0.940843	0.949757

8.6 Stability Across 150 Monte Carlo Runs (each run uses N=10,000)

To demonstrate stability and independence from a single random seed, the simulation was repeated 150 times. The table reports mean, standard deviation, and range of the 150 estimates.

Table 2- Summary of 150 runs (mean, standard deviation, min, max) compared to theory.

Metric	Theory	MC_mean	MC_std	MC_min	MC_max
R_{sys}	0.988865	0.988741	0.000963	0.9857	0.9909
R_{key}	0.945926	0.945882	0.002238	0.9394	0.9525
$R_{tot.}$	0.935393	0.945882	0.002238	0.9394	0.9525

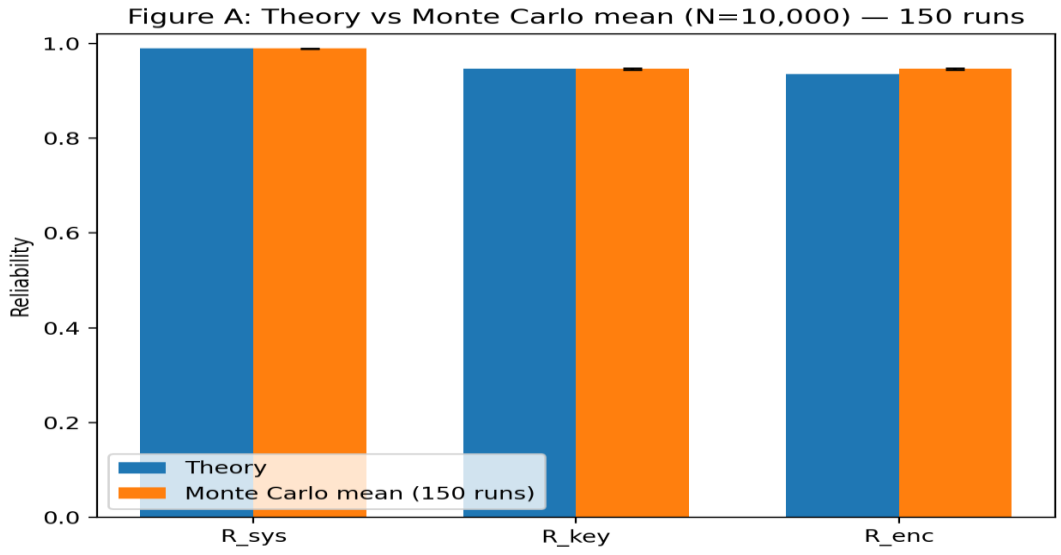


Figure -4 Rectangular bars: theory vs Monte Carlo mean across 150 runs (error bars = standard deviation)

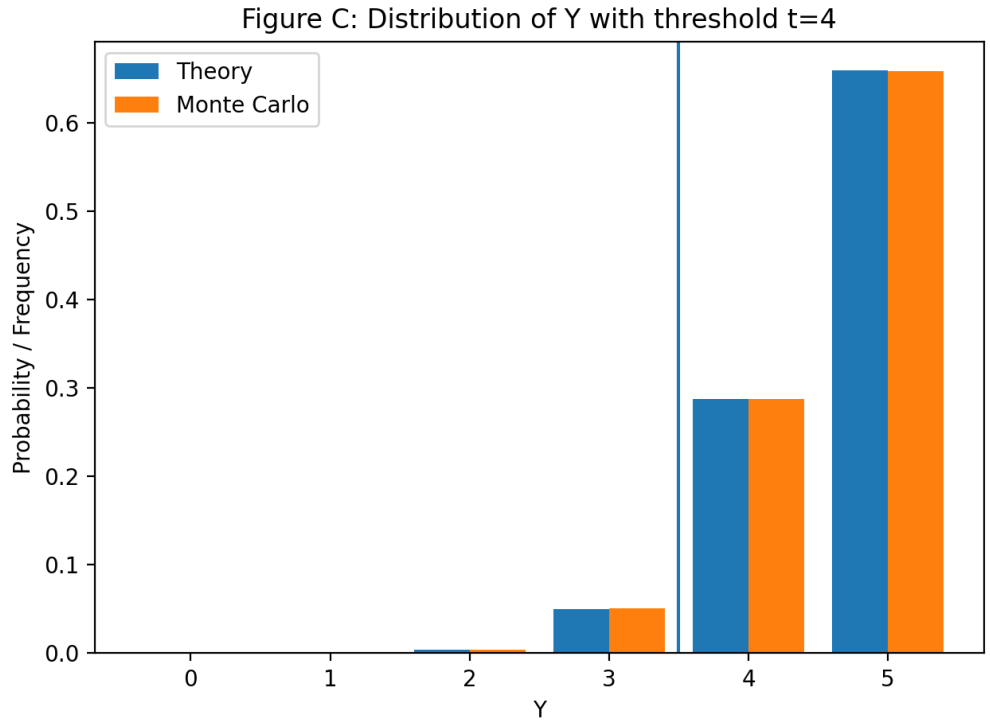


Figure -5 Rectangular grouped bars: distribution of Y with threshold t=4 (vertical line at 3.5).

8.7 Scenario Study (All simulations use N = 10,000

Several scenarios are tested to show how the system behaves when a key component becomes weak.

Table 3- Scenario comparison (theory vs Monte Carlo).

Scenario	R_1	R_{2s}	R_3	R_4	R_5	R_{sys}**theory**	R_{key} **theory**	R_{tot}**theory**	R_{sys}**mc**	R_{key}**mc**	R_{tot}**mc**
All equal 0.80	0.8	0.8	0.8	0.8	0.8	0.92288	0.73728	0.680421	0.9268	0.7355	0.7355
All equal 0.90	0.9	0.9	0.9	0.9	0.9	0.98019	0.91854	0.900344	0.9803	0.9152	0.9152
Base (5.6.1)	0.9	0.91	0.92	0.93	0.94	0.988865	0.945926	0.935393	0.9874	0.9413	0.9413
Weak series B2=0.30	0.9	0.3	0.92	0.93	0.94	0.956109	0.797054	0.76207	0.955	0.7947	0.7947
Weak parallel B3=0.30	0.9	0.91	0.3	0.93	0.94	0.986732	0.790956	0.780461	0.9882	0.7925	0.7925
Weak bypass B5=0.30	0.9	0.91	0.92	0.93	0.3	0.87009	0.778989	0.67779	0.8687	0.7821	0.7821

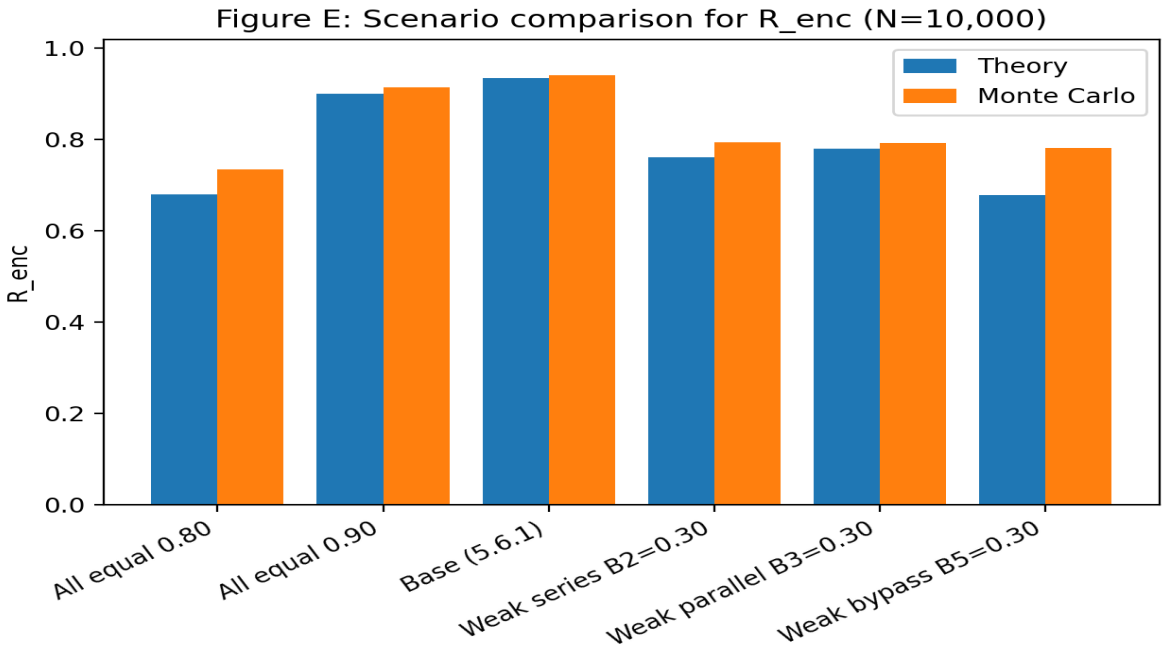


Figure -6 Rectangular grouped bars: scenario comparison for $R_{tot.}$ (theory vs Monte Carlo)

8.8 Full Sensitivity Analysis for All Components (Case 3)

For each component Bi, its reliability ri is varied from 0.30 to 0.95 (step 0.05) while the remaining components stay at the base values. For each point, theory and a Monte Carlo estimate (N=10,000) are reported.

Table 4-Sensitivity results when varying B1 (0.30 to 0.95)

R_i **(varied)**	R_{sys}**theory**	R_{key}**theory**	R_{tot}**theory**	$R_{sys.}$**mc**	R_{key}**mc**	R_{tot}**mc**
0.3	0.956288	0.803229	0.768118	0.9583	0.8109	0.8109
0.35	0.959003	0.81512	0.781703	0.957	0.8085	0.8085
0.4	0.961718	0.827012	0.795352	0.9627	0.8256	0.8256
0.45	0.964432	0.838903	0.809066	0.9626	0.8368	0.8368
0.5	0.967147	0.850795	0.822844	0.9668	0.8472	0.8472
0.55	0.969862	0.862686	0.836686	0.969	0.8647	0.8647
0.6	0.972577	0.874578	0.850594	0.9737	0.8725	0.8725
0.65	0.975291	0.886469	0.864566	0.9749	0.8854	0.8854
0.7	0.978006	0.898361	0.878602	0.9778	0.899	0.899
0.75	0.980721	0.910252	0.892703	0.981	0.909	0.909
0.8	0.983435	0.922143	0.906869	0.9838	0.919	0.919
0.85	0.98615	0.934035	0.921099	0.9862	0.9327	0.9327
0.9	0.988865	0.945926	0.935393	0.9902	0.9465	0.9465
0.95	0.99158	0.957818	0.949753	0.9912	0.9599	0.9599

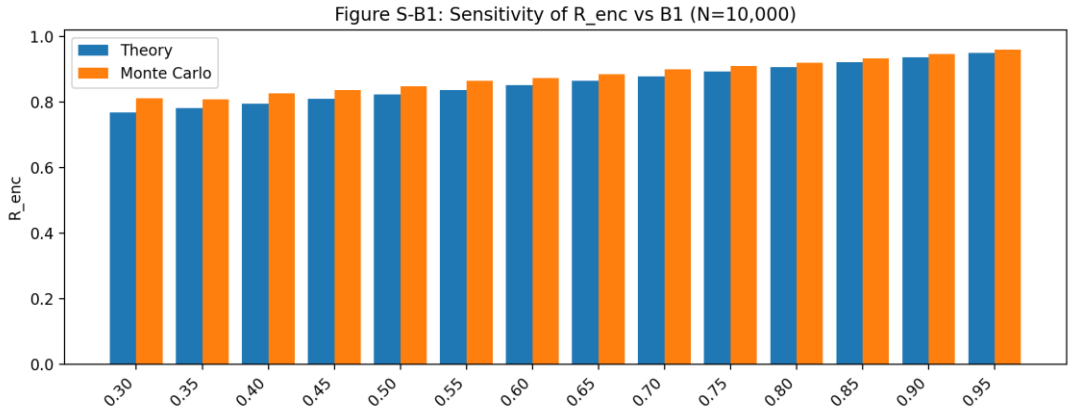


Figure -7 Rectangular grouped bars: sensitivity of R_{tot} vs B1 (theory vs Monte Carlo).

Table 5- Sensitivity results when varying B2 (0.30 to 0.95).

R_i **(varied)**	R_{sys}**theory**	R_{key}**theory**	$R_{tot.}$**theory**	R_{sys}**mc**	R_{key}**mc**	$R_{tot.}$**mc**
0.3	0.956109	0.797054	0.76207	0.9607	0.8046	0.8046
0.35	0.958794	0.809256	0.77591	0.9574	0.8103	0.8103
0.4	0.961479	0.821459	0.789816	0.9604	0.822	0.822
0.45	0.964164	0.833662	0.803787	0.9652	0.8347	0.8347
0.5	0.966849	0.845864	0.817823	0.9669	0.8471	0.8471
0.55	0.969534	0.858067	0.831925	0.9693	0.8606	0.8606
0.6	0.972219	0.87027	0.846092	0.9712	0.869	0.869
0.65	0.974903	0.882472	0.860325	0.9763	0.8851	0.8851
0.7	0.977588	0.894675	0.874624	0.9774	0.8919	0.8919
0.75	0.980273	0.906878	0.888988	0.9805	0.9096	0.9096
0.8	0.982958	0.91908	0.903418	0.9841	0.9216	0.9216
0.85	0.985643	0.931283	0.917913	0.9837	0.9262	0.9262
0.9	0.988328	0.943486	0.932473	0.9891	0.9414	0.9414
0.95	0.991013	0.955689	0.947099	0.9909	0.9549	0.9549

8.9 Component Impact Ranking

Impact is measured by reducing one component at a time to 0.30 (others fixed), and computing the theoretical decrease inR_{tot}.

Table 6- Impact ranking (decrease in $R_{enc}$when a component is reduced to 0.30).

Component	$R_{tot.}$**_base(theory)**	$R_{tot.}$**drop_to_0.30(theory)**	**Decrease**
B5	0.935393	0.67779	0.257604
B2	0.935393	0.76207	0.173323
B1	0.935393	0.768118	0.167275
B4	0.935393	0.77425	0.161144
B3	0.935393	0.780461	0.154932

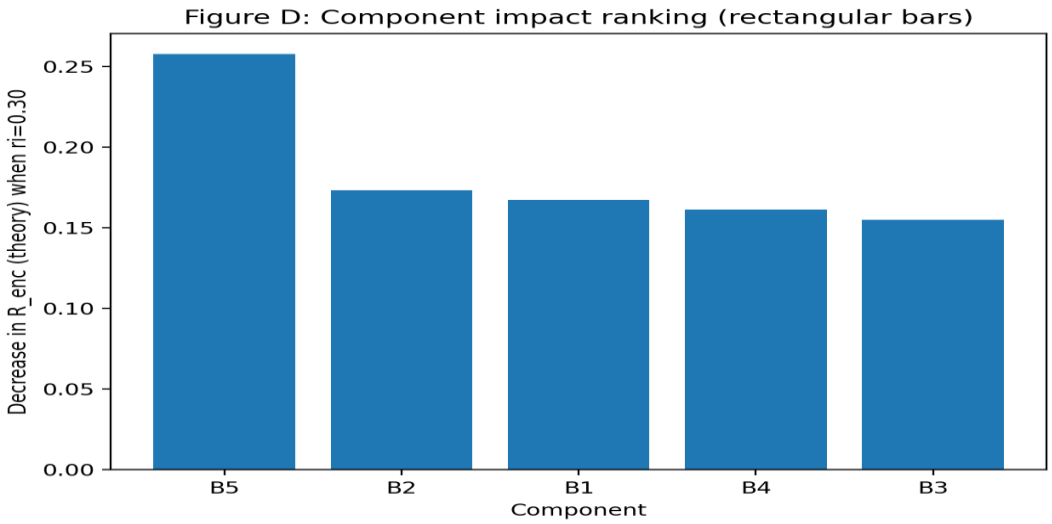


Figure -8 Rectangular bars: component impact ranking (theoretical decrease inR_{tot}).

9. Conclusion

This study successfully developed a hybrid reliability model integrating series and parallel architectures with a success threshold of (4,5). The primary scientific contribution lies in providing a robust mathematical framework for secure key distribution, striking an optimal balance between architectural complexity and cryptographic availability. The results, validated through Monte Carlo simulation, demonstrated that the proposed configuration significantly enhances system resilience against component failures compared to traditional models. However, this study is limited to static reliability analysis. Future work should explore the dynamic behavior of hybrid networks under intelligent cyber-attacks and investigate the integration of these models with block chain-based decentralized key management systems to further enhance security in heterogeneous environments.

References

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979, doi: 10.1145/359168.359176. Available: https://doi.org/10.1145/359168.359176

[2] K. Tanaka and M. Ito, "Machine learning for reliability parameter estimation," *Machine Learning*, 2023, doi: 10.1007/s10994-023-06334-w. Available: https://doi.org/10.1007/s10994-023-06334-w

[3] L. Zhang and Z. Liu, "k-out-of-n reliability models for distributed key management," *IEEE Transactions on Dependable and Secure Computing*, 2024, doi: 10.1109/TDSC.2024.3354122. Available: https://doi.org/10.1109/TDSC.2024.3354122

[4] I. E. Iarmchuk, "Evaluation of cryptographic reliability of information encryption methods based on recurrent sequence," *Eastern-European Journal of Enterprise Technologies*, vol. 2, pp. 10-12, 2013. Available: http://journals.uran.ua/eejet/article/view/12123

[5] W. Stallings, Cryptography and Network Security: Principles and Practice, *6th ed. Upper Saddle River*, NJ, USA: Pearson, 2014.

[6] G. Levitin, "Multi-state system reliability with dependent components," *IEEE Transactions on Reliability*, vol. 71, no. 2, pp. 580-591, 2022, doi: 10.1109/TR.2022.3159234. Available:

https://doi.org/10.1109/TR.2022.3159234

[7] B. S. Dhillon, Maintainability, Maintenance, and Reliability for Engineers. *Boca Raton, FL, USA: CRC Press*, 2006, doi: 10.1201/9781420006780. Available: https://doi.org/10.1201/9781420006780

[8] A. Chowdhury and D. Koval, Power Distribution System Reliability: Practical Methods and Applications. *Hoboken, NJ, USA: John Wiley & Sons*, 2011, doi: 10.1002/9780470454244. Available: https://doi.org/10.1002/9780470454244

[9] H. Fazlollahtabar and S. T. A. Niaki, Reliability Models of Complex Systems for Robots and Automation. *Boca Raton, FL, USA: CRC Press*, 2017, doi: 10.1201/9781315154336. Available: https://doi.org/10.1201/9781315154336

[10] Y. Chen et al., "Optimizing key management in cloud storage using k-out-of-n reliability systems," *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 1450-1462, 2022, doi: 10.1109/TCC.2021.3050985. Available: https://doi.org/10.1109/TCC.2021.3050985

[11] H. Al-Mohannadi and I. Awan, "Security reliability block diagrams for hybrid key distribution centres," *Journal of Network and Computer Applications*, vol. 209, Art. no. 103540, 2023, doi: 10.1016/j.jnca.2022.103540. Available: https://doi.org/10.1016/j.jnca.2022.103540

[12] W. Kuo and M. J. Zuo, Advanced Reliability Modeling: Theory and Applications. *Berlin, Germany: Springer*, 2023, doi: 10.1007/978-3-031-24756-0. Available: https://doi.org/10.1007/978-3-031-24756-0

[13] L. Johnson and K. Brown, "A unified metric for cryptographic resilience," *in Proc. USENIX Security Symposium*, 2024. Available: https://www.usenix.org/conference/usenixsecurity24