SLECP-SDN: A Secure and Lightweight Communication Protocol in a Software-Defined Network (SDN)

Aladesote Olomi Isaiah, *Member, IAENG*, Azizol Abdullah, *Member, IAENG*, Normalia Samian and Zurina Mohd. Hanapi

Abstract— This study presents a novel protocol, the Secure and Lightweight Communication Protocol in Software-Defined Networks (SLECP-SDN), leveraging Elliptic Curve25519 to enhance security and efficiency in SDN Southbound Interface (SBI) communication. Unlike the existing cryptographic solutions, SLECP-SDN integrates computational efficiency, robust security, and energy optimization to address vulnerabilities in SBI. Using a Lightweight Elliptic Curve Diffie-Hellman (ECDH) approach, the proposed protocol ensures secure exchange and session establishment while mitigating critical security threats, including impersonation, replay, packet injection, and Man-in-the-middle (MITM) attacks. To evaluate the system performance, the Contiki Cooja Simulator was employed to model SDN communication among 20 hosts, incorporating various mod(p) values to assess encryption/decryption performance, energy consumption, and throughput. The Automated Validation of Internet Security Protocols and Applications (AVISPA) tool was also utilized for security verification. Using the High-Level Protocol Specification Language (HLPSL), AVISPA tested the mutual authentication protocol against three attack models: On-the-Fly Model-Checker (OFMC), Constraint Logic-based Attack Searcher (CL-AtSe), and Tree Automata-based Protocol Analyzer (TA4SP). The results demonstrated that SLECP-SDN achieves a throughput of 1224.43 MBps at a 138-bit modulus, outperforming RSA and hybrid AES+RSA algorithms. Single topology configurations delivered the fastest transmission times for encrypted files. These findings validate the effectiveness of SLECP-SDN in maintaining high-security standards without compromising network performance, making it a viable option

Index Terms: Data Security, Elliptic Curve25519, Software-defined network, Southbound Interface, Throughput, Topology.

I. INTRODUCTION

Software-defined network (SDN) has emerged as a transformative technology that decouples the control and

Manuscript received August 31, 2024; revised February 13, 2025.

This work was supported and funded by Universiti Putra Malaysia (UPM).

Aladesote Olomi Isaiah is a Ph.D. student in the Department of Computer Communication and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), Serdang 43400, Malaysia (phone: +2348030657156; e-mail: gs57427@student.upm.edu.my and isaaladesote@fedpolel.edu.ng)

Azizol Abdullah is an Associate Professor in the Department of Computer Communication and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), Serdang 43400, Malaysia (e-mail: azizol@upm.edu.my)

Normalia Samian is a Senior Lecturer in the Department of Computer Communication and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), Serdang 43400, Malaysia (e-mail: normalia@upm.edu.my)

Zurina Mohd. Hanapi is an Associate Professor in the Department of Computer Communication and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), Serdang 43400, Malaysia (e-mail: zurinamh@upm.edu.my)

data planes, enabling centralized network management and enhanced flexibility [1], [2]. Unlike traditional networks, control logic and data forwarding are tightly integrated [3], [4]. SDN separates these functions, allowing for programmable and scalable network architectures [5]–[7]. This integration hampers network management and restricts adaptability. The paradigm shifts facilitate rapid innovation in network management and optimization, but they also introduce new security challenges, particularly at the Southbound Interface (SBI).

SDN relies on four key interfaces: Southbound, Northbound, Eastbound, and Westbound [8], [9]. The Southbound API is essential, facilitating communication between the control and data planes [10]. Northbound APIs offer a standardized interface for application development by providing critical insights into the underlying devices [11]. Eastbound APIs manage communication between distributed controllers, while Westbound APIs integrate legacy network devices with the SDN controller. These interfaces enable SDN to deliver more flexible and manageable network operations.

The SBI, a critical component of SDN, facilitates communication between the control plane and data plane devices, such as switches and routers. While this interface is essential for SDN's functionality, it is highly vulnerable to various attacks, including unauthorized access, man-in-the-middle (MiTM), packet injection, and impersonation attacks. Securing the SBI is crucial to ensuring the integrity, confidentiality, and availability of SDN operations [12]–[14].

Existing approaches to securing SBI communication rely on cryptographic techniques such as RSA, AES, or hybrid encryption methods. However, these methods often have significant computational and energy costs, making them unsuitable for resource-constrained environments. Moreover, some solutions lack robust mechanisms for mutual authentication, leaving networks susceptible to impersonation and replay attacks. These limitations necessitate the development of a more secure and efficient protocol tailored to SDN's unique requirements.

This study proposes the Secure and Lightweight Communication Protocol in Software-Defined Networks (SLECP-SDN) to address these challenges. SLECP-SDN leverages the Elliptic Curve25519 algorithm to provide a high-security, low-overhead solution for securing the SBI. Unlike the traditional methods, the protocol incorporates a lightweight mutual authentication mechanism, ensuring trust between communicating entities and mitigating key security threats. Additionally, SLECP-SDN employs efficient encryption and decryption processes, enabling secure data

exchange without compromising network performance. The main contributions of the study are as follows:

- 1. Development of SLECP-SDN, a protocol that utilizes Elliptic Curve25519 for securing SBI communication with strong cryptographic guarantees.
- 2. Introduction of a mutual authentication mechanism that mitigates various attacks, such as impersonation, MiTM, replay, and packet injection attacks, thereby ensuring robust device identity verification.
- 3. Performance evaluation of SLECP-SDN using encryption and decryption times, energy consumption, and throughput across various file sizes and modulus values.
- 4. Comparative analysis with traditional cryptographic algorithms, demonstrating SLECP-SDN's superior balance of security and efficiency.

The remainder of this paper is organized as follows: Section 2 reviews related work on SBI security. Section 3 presents the proposed SLECP-SDN methodology. Section 4 also introduces the experimental setup and evaluates the results. Section 5 compares SLECP-SDN's performance with existing methods. Finally, section 6 concludes the study and suggests directions for future research.

II. LITERATURE REVIEW

Securing communication in SBI in SDN is a critical challenge, as malicious switches pose significant threats by disobeying rules, colluding with other compromised entities, or falsifying information. Recent research has introduced defense mechanisms, such as encryption and authentication techniques, to address these vulnerabilities. These approaches enhance security and preserve network integrity by leveraging SDN's programmability and centralized control. This review explores these mechanisms, highlighting their effectiveness (potential) to mitigate threats and safeguard SDN environments.

Chao et al. [15] synthesized realistic network topologies and flow entries derived from real-world datasets to evaluate the techniques on virtual SDN networks created using Mininet. While the active probing technique effectively reduced the required number of test packets and achieved practical fault localization times, the techniques involving statistics checking and packet obfuscation require further evaluation and optimization to address their inherent weaknesses and challenges.

Ghaly and Abdullah [16] addressed the security of data transmission in software-defined networks (SDNs) by implementing robust encryption algorithms to mitigate potential security vulnerabilities arising from the separation of control and data planes, which can compromise data integrity and confidentiality. It proposes a hybrid encryption approach combining the Advanced Encryption Standard (AES) symmetric-key algorithm and the Rivest-Shamir-Adleman (RSA) asymmetric-key algorithm. The approach encrypts the original data using AES with a 256-bit key length and then encrypts the AES key using RSA with a 4096-bit public key. The hybrid approach demonstrates better encryption time and throughput compared to RSA alone. Furthermore, the single topology scenario exhibits the lowest transmission time compared to linear and tree topologies when sending encrypted files through the SDN

Similarly, Alemami *et al.* [17] addressed the critical issue of data security in cloud computing, where resource sharing

among clients poses risks like data theft and leakage. To mitigate these risks, the study investigates encryption techniques, including AES, DES, Blowfish, RSA, and IDEA, which transform data into cipher text. The comparative analysis evaluates these algorithms based on security, encipherment capacity, memory usage, and encryption speed. The results show that AES and Blowfish are the most efficient based on speed and memory usage, while RSA and IDEA are less secure.

Varadharajan and Tupakula [18] proposed a two-pronged security architecture to mitigate the threats posed by compromised end hosts in SDNs. This architecture aims to detect and prevent attacks targeting both the control plane (SDN controller) and the data plane (network switches) before they can reach and impact these critical components. The first part is the Security Management Application (SMA), a software component in the SDN controller. The SMA specifies and evaluates security policies leveraging the controller's global network visibility, while the second part consists of the Switch Security Components (SSCs) implemented within the network switches. The SSCs enforce the security policies the SMA defines by performing functions like flow mapping, state validation of end hosts, traffic inspection, and flow encryption if required.

Al-Hamdani and Bhaya [19] proposed a new key management scheme to address the challenges of securing communication in SDN environments due to the separation of control and data planes. This scheme ensures the secure distribution of RSA certificate keys without compromising network performance. It utilizes the RSA algorithm for key generation, a hierarchical system for key distribution, and a novel approach to prevent unauthorized access to keys. However, the proposed scheme relies heavily on the central controller for key generation and management, which could become a single point of failure or a bottleneck in larger networks.

To address the vulnerabilities from unencrypted communication channels, which allow eavesdropping and tampering between controllers and switches in OpenFlowenabled devices, Gray et al. [20] introduced a new authentication mechanism using device fingerprinting to secure SDN environments. Experimental results show that this approach prevents unauthorized access and ensures network security. However, attackers can exploit this by mimicking static features, deceiving the SDN controller into recognizing malicious entities as legitimate switches. Mockingly examining handshake messages between the controller and switches enhanced the quality of secure sessions in the SDN data plane. This approach ensures secure communication but increases overhead, as the controller must scrutinize every message sent and received. This additional scrutiny, necessary for maintaining communication integrity and security, increases processing demands on the controller and may affect overall network performance and efficiency.

Ranjbar *et al.* [21] enhanced the quality of secure sessions in the SDN data plane by meticulously examining handshake messages between the controller and the switches, which enhanced the quality of secure sessions. The study ensures secure communication but increases overhead, as the controller must scrutinize every message sent and received.

Yigit et al. [22] proposed the secure distribution and management of cryptographic keys in SDN to prevent

unauthorized access and maintain high performance. It uses asymmetric key generation and distribution using RSA algorithms by generating keys at a central controller and distributing them securely through SSL channels. The experimental results using an SDN testbed show that the proposed cryptography key management approach effectively secures SDN environments. However, the CPU-intensive nature of the encryption process could delay regular switch operations, and the need to store keys at the controller introduces a single point of failure.

Peng et al. [23] introduced QKDFlow, a solution that combines quantum key distribution (QKD) with a one-time pad (OTP) encryption algorithm to secure OpenFlow protocol messages. This approach is designed to prevent Man-in-the-Middle (MitM) attacks and enhance the secure communication between the control and data planes in SDN.

Adhikari et al. [24] addressed the lack of mandatory security measures like Transport Layer Security (TLS) in the OpenFlow protocol, which makes the Southbound Interface (SBI) vulnerable to MiTM attacks. They propose a combination of Elliptic-curve Diffie-Hellman (ECDH) key exchange and Advanced Encryption Standard (AES) 256 encryption to secure communication between the SDN controller and switches. The study uses Bettercap with SSLStrip to simulate MiTM attacks and validate the effectiveness of the encryption approach. However, while secure, the initial key exchange process depends on the assumption that the public keys are exchanged without interception.

The research presents the SAF-Secure Authentication framework aiming to heighten security and optimize services for entities within the SDN-IoT network. Utilizing hashing algorithms (Keccak-256) and digital certificates (Bliss-B), the study ensures the validity of entities. It assesses the proposed architecture's performance by considering computation overhead and resource utilization. The SAF architecture demonstrates enhanced security performance, improving the efficiency of message encryption. However, there is a necessity for deeper exploration into system constraints regarding authentication, particularly focusing on computation overhead and resource utilization [25]

The study in [26] addresses the lack of data plane authentication, a vulnerability that can cause controller malfunctions. Their proposed prototype, Mynah, effectively mitigates this issue with only a 4.5% increase in communication latency. Mynah introduces a novel controller and switch architecture, making it the first solution to tackle this problem.

The literature review highlights several critical research gaps in securing data planes in SDNs that need further investigation. These include optimizing statistics checking and packet obfuscation techniques, understanding the performance impact of hybrid encryption methods, and providing a tailored analysis of encryption techniques for SDNs. Centralized key management schemes present risks of single points of failure, and current authentication mechanisms are susceptible to sophisticated impersonation attacks. Enhanced security measures often increase overhead, and processing demands, affecting network efficiency, and the security of initial key exchanges relies on potentially vulnerable assumptions.

Addressing these gaps is essential for developing more effective and efficient security solutions for SDNs.

Introducing Elliptic Curve25519 [27] to secure communication can address some of these gaps due to its high performance and strong security with relatively low computational overhead. Its robust cryptographic properties make it highly resistant to attacks, including impersonation, and it minimizes the additional overhead associated with enhanced security measures. Curve25519 also supports efficient key exchange management, further strengthening the security of SDNs.

III METHODOLOGY

This study introduces the Secure and Lightweight Communication Protocol for SDN (SLECP-SDN), designed to secure communication between the data plane (DP) and the control plane (CP). The proposed approach employs a pre-computed curve points strategy, enhancing computational efficiency and memory usage. It maintains robust 192-bit security while using 128-bit encrypted keys.

The protocol uses Elliptic Curve25519 for efficient, high-security encryption and key exchange, ensuring robust data transfer protection within the SDN. Additionally, integrating the GMP library boosted the performance of scalar multiplication and reduced the cost of generating large prime numbers. The study uses Elliptic Curve25519 for its cryptographic strength and efficiency. Figure 1 presents the secure communication flow of SLECP-SDN. SLECP-SDN involves the following phases: key generation, key exchange, encryption and decryption, simulation, and mutual authentication.

A). Key Generation

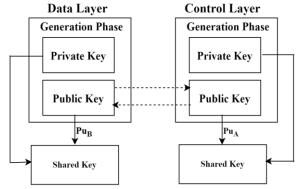


Fig. 1. Secure Communication Flow in SLECP-SDN

In this phase, both the control plane (CP) and the data plane (DP) dynamically generate private-public key pairs using Elliptic Curve Cryptography (ECC). A secure cryptographically strong pseudo-random number generator (CSPRNG), implemented via Python's os.urandom(), generates the private keys, while public keys are derived through scalar multiplication of the private key and curve base point G, as represented in equation [1]:

$$P = K * G \tag{1}$$

Where P is the public key, K is the private key, and G is the base point. The algorithm for scalar multiplication is detailed in Algorithm 1, which ensures efficient point addition and doubling using modular arithmetic.

This curve, defined by the equation $y^2 = x^3 + 486662x^2 + x \mod(p)$ (Montgomery, 1987), operates over a prime finite field, ensuring strong encryption using modular arithmetic, specifically:

$$P = 2^{255} - 19 (2)$$

The curve's base point serves as the foundation for generating all other points on the curve, which are crucial for encryption and decryption processes. Each SDN device is assigned unique elliptic curve points generated as part of the encryption system.

Algorithm 1: Point Addition and Point Doubling

Input: Point X = (x_1, x_2) ; Point Y = (y_1, y_2) **Output:** Point Z= (x_3, y_3)

- 1. If X is the point at infinity
- 2. return Y
- 3. end If
- 4. If Y is the point at infinity
- 5. return X
- 6. end if
- 7. If $x_1 = x_2$ and $y_1 \neq y_2$
- 8. return the point at infinity.
- 9. end if
- 10 If $x \neq Y$, calculate slope m
- 11. $m = \frac{y_2 y_1}{x_2 x_1}$
- 12. else if x = y, calculate
- 13. $m = \frac{3x_1^2}{2y_1}$
- 14. end if
- 15. calculate the coordinates of Z
- 16. $x_3 = m^2 x_1 x_2$
- 17. $y_3 = m(x_1 x_3) y_1$
- 18. End

Algorithm 1 outlines the process of scalar multiplication (point addition and point doubling) on Elliptic Curve 25519 using modular arithmetic. It takes two input points, X and Y, each with two coordinates, and produces an output point, Z. Special cases are handled first: if either X or Y is at infinity, the algorithm returns the other point, and if the x-coordinates of X and Y are the same but their y-coordinates differ, it returns the point at infinity. For other cases, the slope m is calculated. If the points are different, the slope is $m = \frac{y_2 - y_1}{x_2 - x_1}$; if they are the same (point doubling), the slope is $\frac{3x_1^2}{2y_1}$. Finally, the coordinates (x, y) of the output point Z are calculated using $m^2 - x_1 - x_2$ and $m(x_1 - x_3) - y_1$

From Fig. 1, let the data plane be A and the control plane be B. The private keys for A and B are represented as Pk_A and Pk_B , respectively. The corresponding public keys for A and B are given by:

$$Pu_{A} = Pk_{A} * G \tag{3}$$

$$Pu_{R} = Pk_{R} * G \tag{4}$$

Where G is a predefined generator point on the elliptic curve.

B). Key Exchange Phase

The protocol employs the Elliptic Curve Diffie-Hellman (ECDH) method to enable CP and DP to establish a shared secret over an insecure channel. During the exchange,

Device A (DP1) sends its public key (Pu_A) to Device B (CP1), which responds by sending its public key (Pu_B) to Device A. In the shared secret exchange, A computes its shared secret (sPu_A) using B's public key (Pu_B) and A's private key (Pk_A) , as shown in equation (5). Similarly, B calculates its shared secret (sPu_B) by using A's public key (Pu_A) and B's private key (Pk_B) , as shown in equation (6). Both calculations result in the same shared secret key, enabling secure communication between A and B. This protocol ensures that the DP and CP can derive a shared secret, even over an insecure communication channel, as depicted in Fig. 2.

$$sPu_A = Pk_A * Pu_B \tag{5}$$

$$sPu_B = Pk_B * Pu_A \tag{6}$$

These principles also apply to DP2 and CP2, ensuring consistent exchange security. The public key is openly shared, while the private key remains confidential.

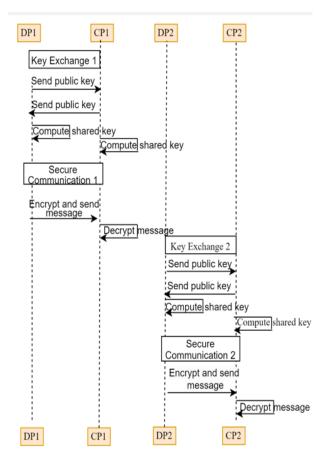


Fig. 2. Sequence diagram for public key exchange in SLCEP-SDN

C). Encryption and Decryption

Once the shared key is established, it is used for encryption and decryption. Encryption is performed as follows:

$$ECC(Char(i)) = Shared_{Key} + Char(i)$$

$$Encrypted\ Message = \sum_{i=1}^{n} (Shared_{key} + Char(i))$$
 (8)

Decryption reverses this process to recover the original plaintext:

$$Decrypted Message = \sum_{i=1}^{n} (Encrypted Message - Shared_{key})$$
(9)

$$Char(i) = (Encrypted\ Message\ (i) - Shared_{key})\ (10)$$

The sender (DP) encrypts the plaintext using the shared key, turning it into ciphertext, and then transmits it over the network. Upon receiving the ciphertext, the recipient (CP) uses the same shared key to decrypt it and recover the original plaintext. This process ensures the confidentiality of the communication, protecting the transmitted messages from an unauthorized access.

D). Simulation and Authentication

The system was modelled using Contiki's Cooja simulator, simulating SDN communication between 20 hosts. The protocol's robustness against attacks was verified using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, employing High-Level Protocol Specification Language (HLPSL). It ensured resistance against attack models like On-the-Fly Model-Checker (OFMC), Constraint Logic-based Attack Searcher (CL-AtSe), and Tree Automata-based Protocol Analyzer (TA4SP).

E). Proposed Mutual Authentication Technique

This section details the key features of the proposed approach. The technique aims to ensure optimal performance in constrained networks while providing the most cost-effective security for hosts in SDN networks. It addresses fundamental security components, including confidentiality, authentication, and data integrity. The data transfer process between the sender and receiver hosts is described as follows:

- a. To create trust, a host must authenticate the relevant device before sending or receiving data to or from an adjacent host. The sending and receiving hosts will execute an ECDH-based authentication key agreement protocol to authenticate mutually.
- b. For the ECDH process, host_1 and host_2 generate their' private keys such that Host1's private key is Prv_H1 and Host_2's private key is Prv_H2.
- c. The receiving host must ensure that the data received has not been altered during transmission once the mutual authentication has been established. Similarly, data must be protected from eavesdroppers and Man in the Middle (MiTM) during transmission. End-to-end encryption is typically used to protect data from these types of assaults.

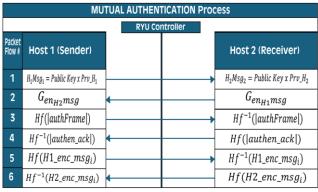


Fig. 3. Proposed Lightweight Mutual Authentication Process

d. Encryption is employed during the key exchange stages, enabling secure end-to-end encryption between the two constrained SDN hosts. The keys used in this procedure are public keys such as embedded network keys (Net_k = Network_id + Public_Key), which are the same for one network only.

The data flow of ECDH-based mutual authentication is shown in Figure 3, where the notations used in the proposed technique are shown and elaborated upon in Table 1.

TABLE 1 NOTATIONS IN THE PROPOSED SCHEME

| Notations | Description | Generator Size | Key pair Size |
|-------------------------|---|-------------------|------------------|
| $H_1 M s g_1$ | Host_1 message | 64*d | 128*d |
| H_2Msg_2 | Host_2 message | 64*d | 128*d |
| $Public_{key}$ | Public key | 64 | 128 |
| Prv_H_1 | Private Key of Host 1 | 64 | 128 |
| Prv_H_2 | Private Key of Host 2 | 64 | 128 |
| N_k | Unique Network key | 32 | 64 |
| $G_{en_{H_1}msg}$ | Generator message by Host 1 | 64 | 128 |
| $G_{en_{H_2}msg}$ | Generator message of Host 2 | 64 | 128 |
| authFrame | Authentication Frame string | 128*d | 256*d |
| authen_ack | Authentication acknowledge Frame string | 128*d | 256*d |
| Hf(i) | The hash function for Encryption | 64*c | 128c |
| $Hf^{-1}(i)$ | Inverse Hash for decryption | 64*c | 128c |
| $H1_enc_msg_i$ | Sender encrypted data block | 64*d | 128*d |
| H2_enc_msg _i | Receiver encrypted data block | 64*d | 128*d |

Note: d is the number of data block characters. c is the number of ASCII characters

Data transmission and authentication steps are stated below:

- 1. Host 1 sends the message, H_1Msg_1 , encrypted through the private key Prv_H_1 of host 1.
- 2. Host 2 receives the message, makes knowledge of Prv_H_1 , adds Prv_H1 with the message, H_1Msg_1 and sends a reply of H_2Msg_2 .
- 3. Host 1 has both privates at this stage. It now encrypts and sends an authentication frame, |authFrame|, which is encrypted using both private keys.
- 4. Host 2 receives and decrypts the message using Prv_H_1 , adds Prv_H_2 , reads |authFrame|, and sends an authentication acknowledgement frame, $|authen_ack|$.
- 5. After a successful acknowledgement frame, Host 1 encrypts and sends a real message $G_{en_{H_1}msg}$ using hash function Hf(i). The encrypted block is now $H1_enc_msg_i$.
 6. Host 2 receives the encrypted block, $H1_enc_msg_i$,
- 6. Host 2 receives the encrypted block, $H1_enc_msg_i$, decrypts it, $G_{en_{H1}msg}$ through $Hf^{-1}(i)$ and sends $H2_enc_msg_i$ as completion of this session.

F). Experimental Setup

The protocol was tested on a Dell Inspiron 5402 with an 11th Gen Intel® Core™ i7-1165G7 @ 2.8GHz processor and 16GB RAM, running Ubuntu 18.04, Python 3.8, Mininet, and Ryu 4.12. Three SDN topologies—single, linear, and tree—were modelled. Performance evaluation

included encryption/decryption times for varying text file sizes. The gmpy2 library (version 2.2.0) with mini-GMP was employed to optimize cryptographic operations.

IV RESULTS AND DISCUSSION

This section presents our findings on securing communication between the data plane and the control layer using the Elliptic Curve25519.

A). Reference Table

The Reference Table lists ASCII characters for message encryption, with each character mapped to a unique point on the elliptic curve. These curve points are pre-calculated to minimize runtime computation, unlike the secret key (SK). Table II includes all 128 ASCII characters, such as uppercase and lowercase English letters, digits (0–9), punctuation marks, and control characters (e.g., carriage return and line feed).

Each character is associated with a large random prime integer, which serves as a generator point (G) on the curve. These points are derived using scalar multiplication from a set generator value, which can vary depending on network settings, a public key, or periodic updates. The generator number for each ASCII character is calculated using a large random prime integer. This is essential for determining the curve's specific (x, y) coordinates, starting from G with x =9 and y = 6248, under the modulus 1019532643. Table 2 provides data on cryptographic operations, including private key generation and elliptic curve point coordinates. It includes columns for iteration numbers, ASCII values, and the x and y coordinates of the curve points. The randomness in the data shows that the cryptographic processes were carried out securely and unpredictably. This randomness is critical for security, as any patterns in key generation or curve points could be exploited by attackers, making the system vulnerable.

B). Avalanche Effect

The avalanche effect refers to the time taken to encrypt and decrypt data blocks and the changes in bit patterns before and after encryption. Fig. 4 shows a scatter plot with ASCII values on the x-axis and PDF values on the y-axis. The data points cluster around low PDF values, indicating uniformity, unpredictability, equal probability, and randomness in the data across the ASCII range. The graph shows a near-normal distribution, where each byte has an equal chance of occurring. This uniformity is crucial in encrypted data, as it prevents patterns that attackers could exploit.

C). Computational Performance of Encryption and Decryption Time

This section highlights the computational performance of the Elliptic Curve25519 algorithm for encrypting and decrypting text files of various sizes with different mod(p) values. Table III shows that encryption time increases with file size and varies across different mod(p) values. For instance, encrypting a 106MB file takes between 375.1931 μ s (mod(p) = 18) and 638.905 μ s (mod(p) = 108). Decryption times also differ and do not always match encryption times, with the same 106MB file taking between 348.4432 μ s (mod(p) = 138) and 774.9815 μ s (mod(p) = 108), as shown in Figure 5.

D). Energy Consumption for Encryption and Decryption

This section presents the energy consumption during encryption and decryption for various input values, as Table IV depicts. The data reveals that energy usage increases with file size and longer cryptographic keys. Larger files and longer bit-length keys require more computational power and time, leading to higher energy consumption. For example, Curve25519, with a 138-bit key, offers greater security but consumes more energy for encryption than shorter keys. CPU power usage, reflected in energy consumption, generally rises with file size and mod(p) values. For instance, encrypting an 11.804MB file at mod(p) 138 uses 0.01207141 mJ/s, nearly double the 0.00651434 mJ/s at mod(p) 18. However, the relationship between mod(p) values and computational time is inconsistent. Larger mod(p) values enhance security but require more time and energy.

E). Throughput

Throughput measures how efficiently encryption operates without creating performance bottlenecks. In SDN, the controller must quickly respond to data plane events, and any delay can degrade performance. Table 5 and Figure 6 show the throughput (in MBps) for various modulus bit lengths in Curve25519 operations. The 138-bit modulus achieves the highest throughput at 1224.43 MBps, offering the best balance between security and efficiency. In contrast, the 108-bit modulus has the lowest throughput at 984.24 MBps due to more computationally intensive operations. Throughput also drops for larger and smaller bit lengths, with the 253-bit modulus at 1073.31 MBps and the 72-bit modulus at 1102.67 MBps. This indicates that bit lengths above 138 increase computational load without significant security gains, while shorter bit lengths may boost speed but weaken security.

F). Comparison of Throughput Results Across Different Algorithms

Figure 6 shows that Curve25519, with a 138-bit modulus, achieves the highest throughput at 1224.43 MBps, while RSA has the lowest at 33.52 MBps. The hybrid AES + RSA algorithm consumes more memory despite its low throughput. Curve25519's high throughput highlights its superior computational performance and fastest encryption times among the compared algorithms. Larger keys offer stronger security by requiring more computation to break the encryption. High throughput is crucial for optimal performance in high-speed networks like data centres and SDNs, which handle large data volumes. Curve25519 consistently outperforms algorithms like those used by Ghaly and Abdullah [16], providing better performance in these environments.

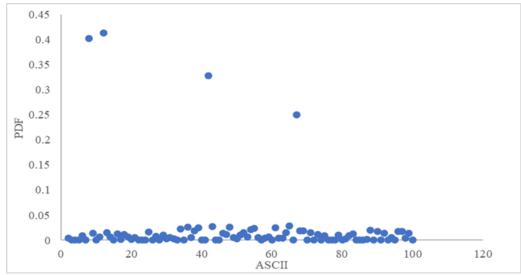


Fig. 4. Uniformity in encrypted frames

TABLE II REFERENCE TABLE RESULTS

| Ci | ASCII | REFERENCE TABLE RESUL Curve point (x) | Curve point (y) |
|----------|--------------|--|--|
| 1 | \x00 | 149726810710315296553937312724301 | 24600957519473220769194735521699 |
| 2 | \x01 | 163174634229599258874334183193398 | 85130006238113929278204390999710 |
| 3 | \x02 | 780558091608003967686489978491883 | 72839741149170059733587718842234 |
| 4 | \x03 | 137801430053945588459731715413622 | 158648653400952353340375015959402 |
| 5 | \x04 | 173922987490323721209269691240318 | 101020736503289960385653001016359 |
| 6 | \x05 | 157320079731207275078488946584733 | 121136843483945486248145127716954 |
| 7 | \x06 | 156151758736574461367152050556143 | 109986854106365416332928871443683 |
| 8 | \x07 | 191958799062696965345711303387942 | 132703531872930875468252346052149 |
| 9 | \x08 | 8400387075025926071918878726382 | 45446136002036367512488286630135 |
| 10 | \t | 121743830913937608230457439173814 | 72403069454975549149926810602113 |
| 11 | \n | 197371859685415251780241189082531 | 55644391545652875760106396344570 |
| 12 | \x0b | 43287691868693190418946629180498 | 48203497305583214396591157548082 |
| 13 | \x0c | 1605531985446277787491027134457727 | 12493726006699614011029499893107 |
| 14 | \r | 98866145589130550589368806894057 | 132327937137858778593395070483899 |
| 15 | \x0e | 9071825616161890397453917942257 | 195010370010647726939696191003798 |
| 16 | \x0f | 197771975788040659340258421333968 | 150828200468320200456797791741440 |
| 17 | \x10 | 159706020404494218147144263608179 | 107469284392674855392862852139385 |
| 18 | \x10 \x11 | 51569769450651939011773900111107 | 1275543270979720175632549870553 |
| 19 | \x12 | 34681501817146951098488246606362 | 117347760686959690165580149303838 |
| 20 | \x13 | 5964526546791930670855312116629 | 28351474552900309024095183355180 |
| 20 | \x13 \x14 | 24750915065416558059577050971126 | 118634230687814148512214991106033 |
| 22 | \x14 \x15 | 191925054553661560390367578452552 | 47297171615120066510971033239849 |
| 23 | \x16 | 48654887353283405174044353107653 | 189971426246448134522211951351040 |
| 23 24 | \x16 \x17 | 12987369635410323020661696141373 | 56370959838297157328022881778406 |
| | | | |
| 25 | \x18 | 58921890190933091573959672700960 | 131430224725100888345881575668680 |
| 26 27 | \x19 | 90844289010019972680798400225182 | 174417308842853290691526996724895 |
| 28 | \x1a | 33422292471199233754465466573700 819393018769986793912755029787 | 3992493444415362507375971279785 186589913907986804354355941385297 |
| 28 29 | \x1b | | |
| | \x1c | 16828623595101960755138331981848 | 194730759428046342543014793804 |
| 30 | \x1d | 43754598955246394193836544665671 | 157067047071810528446825274677245 |
| 31 | \x1e | 135551855283630705269492082093937 | 168102183784710518283377434124348 |
| 32 | \x1f | 169834897400631511353146427474768 | 13517088884723521426700603369916 |
| 33 | | 67366257666644977822771863279316 | 12756379734990538064447403923278 |
| 34 | ! | 1890153007922555264921718603 | 137838611113022894684741228810054 |
| 35 | | 192928265730552011736012122413142 | 84764903331782183678801377123774 |
| 36 | # | 109844769974466109803877548361161 | 109407167209614069729454097758486 |
| 37 | \$ | 18311938370555316803776127250489 | 30606541599324377379447354480753 |
| 38 | % | 153015475417273965582569868444936 | 28011654104320990542643794927009 |
| 39 | & | 55048963593969599965163775948594 | 153617908701962226084569434909194 |
| 40 | " | 165825161646636817757748097178322 | 359174189846693826053564977105581 |
| 41 | (| 150867669022016994007908950114126 | 28246445392313803021013769527197 |
| 42 |) | 163098789831733149520901723958754 | 14112116185099818521028844627014 |
| 43 | * | 8069656439222140138900532800081 | 175941373947063280950157049086165 |
| 44 | + | 174131584438625841897229171361424 | 156877929374343254571461590487940 |
| 45 | , | 139189422720162185628505107465436 | 36076575012238035568208634535353 |
| 46 | - | 105275389736211994004716149622018 | 66489180054101744788362967225974 |
| 47 | • | 88102741523736263776853556938104 | 121204768434919897842262997584153 |
| 48 | / | 15094530751156508767749357961716 | 4256256178318410073087145156241 |
| 49 | 0 | 19665573300053478380044888782393 | 74235560923948052540267765007707 |
| 50 | 1 | 20518402432411406354108180054620 | 71702364481054182937196396316535 |

Engineering Letters

| \$1 | | | | |
|--|-----|----------|------------------------------------|-----------------------------------|
| 52 3 6 07270278975645188997554457557 33 4 0101995605027217107998757183991 34 5 6 8223380002853039534027252121401 35 6 223711829105801072232899522994 35 7 0947606046227291013700122899522944 36 11280605027291013700122899522944 37 11613109105704252032551412 38 9 1827668137980184886228993372941 38 9 1827668137980184886228993372941 39 1 107599524645755463795158563770115 30 1 11060690680101243478064851261088104 2 286391452910128471064851261088104 2 2864049058879949848136867040014 2 2864049058879949848136870400014 2 2864049058879949848136870400014 2 2864049058879949848136870400014 2 2864049058879949848136870400014 2 2864049058879949848136870400014 2 2864049058879949848136870400014 2 286404905887994984812808570400014 2 286404905887994984812808570400014 2 286404905887994984812808570400014 2 28640490588794984812808570400014 2 28640490588791280907998848986881368103 3 2 2326356699852340996442790858044 3 28640498481311845156622870792544 3 2865048689879148181818181818181818181818181818181818 | 51 | 2 | 177509877541323754009262777497781 | 93913153114224778021042901992043 |
| 53 4 610139955002761716199987715185991 54 5 852289002852039849272524124101 55 6 77 604760640022791017501003516142 57 88 3546003253091750021223192329742 58 1 3546003253091750021223192327742 58 1 3546003253091750021223192327742 59 1 1079975246475554637515151051003516142 59 1 1079975246475554637515155503770315 50 1 112000649058791093935955155503770315 50 1 1120006490587910938455367649014 51 11200064905879109393595515503770315 51 1200649058879049938405367649014 52 2 2 9 446884267599913531187906959418411 61 2 1 1006990580012487909993839968031 62 2 3 7 4935792649323599999339968031 62 2 3 7 4935792649323599999339968031 63 2 3 7 4935792649323599997839968033 64 77 186547808481786498578632220000176 65 2 3 5 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | | | | |
| 55 6 22573 ILSQ1030510 02252899523954 | | | | |
| 55 6 228731182910589511053251053253053253954 | | | | |
| 56 7 694760040627279101750108316142 285330453391092722770844611432 575 8 5346605325407536262223193239742 143408884835769379322326793923367 575 8 534606352467536262223193239742 143408884835769379357923236793923367 575 975 975 975 975 975 975 975 975 97 | 54 | | 85223808028520395349272524121401 | |
| 56 7 0947600400227291017501083516142 57 8 53466035254017536082794221319329742 58 9 1827266811798081488622391932931 59 1 107095244075546795158637701515 50 1 1120664916470644923448151515515515515515515515515515515515515 | 55 | 6 | 22873118291058051063228939523954 | 116313090570426320851072204819663 |
| 57 8 5.146003524-003728-0222319239742 58 9 1827266813799814682289939359311 1738229032837166631798222952684591073 59 1 1075995246457554673951586826370015 157534235571666312725072684591073 60 1 110009008006128479098451261088124 61 2 946683267599153181790699384511 173534235571666312725072684591073 61 2 946683267599153181790699384611 173647372964108982775 62 3 94668326759915318179069938411 1736473728561 173651 1736521 1736 | 56 | 7 | 69476060406227291017501083516142 | |
| 58 9 18272668179908149886228939352931 17128279023883796829888212123894 59 : 10759052464755467991535187067901531 1575362835716014 228666410525676792799641 (08987775 61 < 110006690060102797590153118706905948212 222265666952025676792799641 (08987775 62 - 946488267599153118706905944811 138371720556071367960262837824565 63 > 74957972642923190999833980013 1226236566952924314314516242707254 64 7 8 8645789726429319096003 65 8 9 1000366289311765590902256491925 158680713537014134437772741017062747106176 66 8 12079374272917904068046231806290 158680713537014004002667014706705666 200904474707077905900333999723 1807496981325490528514190490526701677166 67 8 12079374272917904068046231806290 1586807135390140000567016706701670670 158198322995638889596072885135899 12834920669088076497852092205056 10000696060620060200608167016701670670 159192670701140416728808897174713244267458691797701404167288088971471324426745865117587055552690 75428078566571754011246137627752 10006966066200602009660660520095707011404167288088971471324426745865117587055552690 75428078566571754011246137627752 172244183623700095851119999727071 14016728808987147132442674505855558119999727071 14016728808987147132442674505855558119999727071 1401672880898714713244267459859187067067067067067067067067067067067067067 | | | | |
| 99 : 1079992444755467395158567370315 17538423557166631272502684891073 60 : 11200690680012847809483151088124 61 : 100690680012847809483151088124 62 : 946488426759913115780695348411 1881720556071360926479720285014 63 : 74925792642933298979983195808013 64 : 2 18557944475784497784977853273606776 65 : 100690680012847807832239069776 66 : 2 1855794447578449778549785325466776 67 : 1006906800128478087832239069776 68 : 2 1906906497877832239069776 69 : 1006906490889117855909922548491035 69 : 1 190690649088917855909922548491035 60 : 1 190690649088917855909925254849035 60 : 1 190690649088917855909925254849035 60 : 1 190690649088917855909925254849035 61 : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | | | | |
| 60 : 112000649015470949938403567040014 228664150256679279904510898775 616 61 | | | | |
| 61 - | 59 | : | 107599524645755463795155863770315 | 157534235571666312725026848591073 |
| 61 < 110096098606012847809848151 23226255669982304996442790284666 29446760798048181 138517055690718369060264878224666 3 | 60 | ; | 112060649054870949938405367040014 | 22866415025676792799644108987775 |
| 62 = 944688476759915311870965914811 1385172055620713629062264378234664 ? 18654780481786464983768321230696176 7396541484580720718176825071709254 65 @ 254476679580604084872193510767878 141523845921732744017794474141619 9 1000306029311768509092526491925 156480713533070104902867091671716 66 A 19003050629311768509092526491925 156480713533070104902867091671716 67 B 12079374272179709059003350995723 180374909813254870833114806192967 70 F 19003050629311768509092526491925 156480713533070104902867091671716 70 F 19044255421165000281671061401125 1026475788160827854464807062843 71 F 16775864395535381617587035536007 180374909813254870833114806192967 71 F 16775864395353581617587035536007 180374909813254870837175864395353581617587035536007 1803747599244251814869595881617587035536007 18037474579244261814865965887560 17778643495353581617587035536007 180374745792442618148659658887560 17778643495353581617587035536007 180374457924445181486596588877560 177786434953535816175870355550007 18037445792444518148659658877124711323416043 27548070178070857177785783059407 1778747807481848922331874161058 17787846748746747857846748747867478747874787478747874787478 | 61 | | 110069068060128478094851261088124 | 23226356669582304996442750285034 |
| 63 > 749357964293359899799853986913 64 47 186457804817564937683223696176 65 66 2544766795860084048721935076978 66 A 1900836028931175650090255691925 67 B 120793742729179040680426231806730 68 C 355900444767079050003350995723 68 C 355900444767079050003350995723 69 D 1 58193822996235883956072885135849 69 D 1 58193822996235883956072885135849 60 D 1 58193822996235883956072885135849 61 1 61 1 61 1 61 1 61 1 61 1 61 1 61 | | | | |
| 64 | | | | |
| 66 A 19003030629311775859092556491925 67 B 12079374279179040680402351806730 68 C 355900444760790509003359095723 68 C 355900444760790509003359095723 69 D 1 518193822959635885956672885135849 60 E 2944295421450500201867106410125 61 C 365900444760790590030350995723 61 E 294429542145050028187106410125 61 C 3659004447607905900359093707 61 E 294429542145050050815101909920707 62 C 1630306060662300555119899920707 63 C 163036060662300555119899920707 64 D 1 10868610102778647093246493092521 64 C 1 10868610102778647093246493092521 65 C 1 1 10868610102778647093246493092521 65 C 1 1 1 1086861010277864703246493092521 66 C 1 1 1 108686101027786032491341313 67 K 1 1 10868610102778602349343831131 67 K 2 1 1 10868610102778602349343831131 68 C 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | | | | |
| 66 A 1900303602931176559092256491925 67 B 102793742721790406804023515650730 68 C 355900447476077905909035099573 68 C 3559004474760779059090359095733 69 D 1881932299953658959672885135849 70 E 2944295421562060281671061401125 71 F 16779624959535885956072885135849 71 F 16779624959535858596672885135849 72 G 163036966065206095551119899927071 72 G 163036966065206052551119899927071 73 H 77287431836275070782818615636859 74 1 108686101027758470932644930592531 75 J 10233160765408867712471123231 76 K 3764906438995812031282888101590 77 L 12857816620018787212471123431134 77 L 128578166201878762209493478471 78 M 16458736163411862953209498478471 79 N 1254619411186993790774698094171 88 O 700928164566051678881486094171 89 P 99715569579597974989789471 80 O 7009281645660516788814786069417 81 S 16958325557404074828958117978664 82 P 997155695779578957957959580949178 83 C 14951464718096982998112786964 84 S 16868235557404069882898112786964 85 C 1192370792948145811093 85 C 1 1192370792948158917589664 86 U 1192370792948158917589664 87 V 2009617634958004229933137914355 86 U 11923707929481498118699841738966 87 V 2009617634958004229933137914355 88 V 73851922491522264668488904897 89 V 467163065742922154684888904897 89 V 467163065742933137914355 80 U 119237079294814891389159918918918999990999098187786966966366632355579491491899099918919999999999999999999999 | 64 | | 186547804817864498376832230696176 | 73965414845807207181768267176051 |
| 66 A 1900304602931176S590992526491925 67 B 10279374272179046804603451806730 68 C 355900447476077905990035099723 68 C 355900447476077905990035099723 69 D 188193229963658859667238815849 70 E 2944295421562060281671061401125 71 F 16779624959535885956072388158549 72 G 16303696606520095551119899527071 72 G 16303696606520095551119899527071 73 H 772874318382579607082818615663559 74 1 108686101027758470932464309592531 75 J 10233160765408877124711232416043 76 K 3764906438995812033282888101500 77 L 12887681662001878778281881133 77 L 12887681662001878728381811536043748742612868958955059491 78 M 16485736165411860595209498478471 79 N 125461941186099539921195418781 80 O 700928104856095167880348070113 81 P 997135595779549730074668069417 82 P 997135595779549730074668069417 83 P 997135595779549730074668069417 83 P 9971355957795470074668069417 84 P 9971355957795470074668069417 85 P 9971355957795470074668069417 85 P 9971355957795470074668069417 86 P 9971355957795470074668069417 87 V 2009617464958000088599811278664 87 V 200961746495800088299811278664 88 W 73851922491522256684885069417 89 X 4 4240411072908807673884892855727 89 X 2 4240411072908807673884892855727 90 X 2 1415573867620913991843778964 90 Y 4 46716005674987817819869497999999999999999999999999999999999 | 65 | (a) | 25447667958600840488721935076978 | 14152845921732743401774474241639 |
| 67 B 12079374272917904068042531800730 | 66 | | 190030360289311768509092526491925 | 156480713533070104902867091671716 |
| 68 C 3559004474760779059000335995723 | | | | |
| D | | | | |
| 70 E 29442954415c0002816710c1401125 102c47578816630278546146307062843 | | | | |
| 71 F 16777962495555581617587035526309 754280783605717748011246137627752 G 1630366606620695551119895927071 H041672880889717431241246778581 73 H 77287431836257600783818615663859 18239774579244261218685965885755 75 J 1023316765406887124711322416043 2754807017807085717728573050491 76 K 376490634589951203328288101506 8676226889616665203675493240 77 L 128876816620018786723409443831133 4505440472855675210916708266093 78 M 16485736165341186295320949847471 313251770659558000493496131506744 79 N 12546194118609935993211954318781 1470027525457064008732160426829 | 69 | | 158193822959635885956072885135849 | 12834920660988076497852092205056 |
| 72 G 163036960606320695551119899527071 | 70 | E | 29442954241562060281671061401125 | 102647578816308278544643697662843 |
| 72 G 163036960606320695551119899527071 | 71 | F | 167779624595535581617587035526309 | 75428078360571754011246137627752 |
| 73 H 77287431836257600783818615663859 182397745792442612186859058857506 74 I 10836610102758476932464909952521 75 J 102331607654068877124711323416043 27548070178070857177285783050491 75 K 3746906318899811023328588101506 8767262689996168685754932049 77 L 128876816620018786723049343831133 45054404728556752109167082660893 78 M 164857361653411866993539211954318781 132517065995800408188131506744 79 N 12546194311866993539211954318781 14700275254570640087321604268291 80 O 7009281048566905399211954318781 14700275254570640087321604268291 81 P 997138549577959437700974698049417 1538294242068501173170322913931 82 Q 14481150416 10080610688400118736 16131953487314269256736012126260 83 R 24490514050144509882908182786064 69503727540034617742601551359424 84 S 1658623555679467238678381511003 85 T 171024704622051136504135867359394 96334338737065967688644328597686 84 S 1658623555679467238678381511003 85 T 171024704622051136504135867359394 96334338737065967688644328597686 86 U 1193370792294153601795251564688888504947 44792649990851875761246532 87 V 20206176349800422933137914355 10735812669445783224200882070166 87 V 202061763498004229931991842855 10735812669445783224200882070166 88 W 773851923049152221564648888804947 1606731844561434267802047379 89 X 42404110729088076738834802855577 1651953200809561511692730858504214 90 Y 44671633065744993013991842731806 1295576732878270907373326467007253 91 Z 14215573856724039113660431281586 1463548486032347781264707787870778787978979789799999999999999 | | | | |
| Texas | | | | |
| 75 J 102331607654068877124711223416043 27548070178070857177225783050491 76 K 3764906438998512033282858101506 86762268989616863575493204 77 L 128878616620018786723049943831133 45064404728556752109167082669093 | | | | |
| 76 K 37649063438995812033282888101506 8676226898066166883236573493204 77 L 128876816620018786723094943813133 45054404728557521001670826660893 78 M 1648573616524118629323209494878471 13251770659580004936491831507674 79 N 125461943118669953593121954518781 147007252544570640016204268291 80 O 7009281048565051667880348070113 264325863996228910611854446532822 81 P 997188495779694370097468049417 15382942340688301132224018931 82 Q 14481150461500850160884091078736 1613195348731426922265736012122626 83 R 2419051490144508982908182787366 69505727540034617551353942 84 S 165863255567946723867583381511093 192306387060460792280187761246352 85 T 1710237042229514568483535353 1933535353331791435353 1933512664947893252740686 86 U 1192370722944155001795256163547 44792644990818175745316344191302 87 V 202095176349580042293315991842731553 1933522068095478832410755925441753550046150200074764 88 T 73656712424993315991842735355 | 74 | | 108686101027758476932464390592521 | 7247780024318848925331871461058 |
| 77 L 128876816620018786723049943831133 4050440472855675210916708260899 78 M 125461943118669935393211954318781 14700275254570640087321604268291 80 O 7099281048565011667884034970113 264232863996232491831506744 81 P 99713854957795943700074698049417 153829437406843501173170224913831 82 Q 14481150461500866106988401078736 161319534873146922265736012122626 83 R 24190514050144509882908182786964 69503727540034617742601551359424 84 S 16586325567940521867583381511093 192306587004460792228018771246352 85 T 17102470462946722867583381511093 192306587004460792228018771246352 86 U 119237079229441536917595551683547 4479264999038175743316547686 87 V 2022661763495004229351379143555 1073581260934783224208082070166 88 W 738519232491522215546848850489947 166673183445614345241076592647378 99 Y 467163036574429930319591842731896 129576732878270970737326467007253 90 Y 467163036574429930319591842731896 129576732878270970737326467007253 91 Z 142155738676240393113660413181856 14635484360232124647078704776 92 [135670151295696880690932601466280 16289727055287748969089132929163 93 W 34516693003651721285338558617494 762261521398544932212647078704776 95 ^ 1152550744650129537967389812907 6085828438972644602277357065 96 | 75 | J | 102331607654068877124711323416043 | 27548070178070857177285783050491 |
| 77 L 128876816620018786723049943831133 4050440472855675210916708260899 78 M 125461943118669935393211954318781 14700275254570640087321604268291 80 O 7099281048565011667884034970113 264232863996232491831506744 81 P 99713854957795943700074698049417 153829437406843501173170224913831 82 Q 14481150461500866106988401078736 161319534873146922265736012122626 83 R 24190514050144509882908182786964 69503727540034617742601551359424 84 S 16586325567940521867583381511093 192306587004460792228018771246352 85 T 17102470462946722867583381511093 192306587004460792228018771246352 86 U 119237079229441536917595551683547 4479264999038175743316547686 87 V 2022661763495004229351379143555 1073581260934783224208082070166 88 W 738519232491522215546848850489947 166673183445614345241076592647378 99 Y 467163036574429930319591842731896 129576732878270970737326467007253 90 Y 467163036574429930319591842731896 129576732878270970737326467007253 91 Z 142155738676240393113660413181856 14635484360232124647078704776 92 [135670151295696880690932601466280 16289727055287748969089132929163 93 W 34516693003651721285338558617494 762261521398544932212647078704776 95 ^ 1152550744650129537967389812907 6085828438972644602277357065 96 | 76 | K | 37649063438995812033282888101506 | 8676226898966166863236575493204 |
| 78 M | | | | |
| N | | | | |
| 80 O 700928104856901667880348070113 2243258699622891061185448632822 N 1 P 99713854977995437009747808049417 1538294320485317303224913931 82 Q 14481150461500860169884091078736 161319534873142692265736012122660 | | | | |
| 81 P 99713854957795943700974698049417 82 Q I448115046150086109881092736 83 R 24190514050144590882908182786964 84 S 16586325567946723867583381511093 85 T 171024704622051136504113568735294 86 U 119237079229441536917595501683547 87 V 2029617634958004293351379143335 88 W 73881923249152221564684885048947 89 X 42404110729088076738843892855727 16973183445614345241076592647379 90 Y 46716303657442930319591842731896 12 Z 14215573865740393113660431381586 13 365867041536115064631381586 14 12828799314404994855106002747104 25 [135670151295696880609032601466280 26 [12828799314404994855106002747104 27 447167386816939219649 28] 1 2282879931404994855106002747104 28 37693419417456801293571876398123097 29 [3479831076541798806518919219649 30] 2 47938197654179880651891919649 31 [3479831076541798806518919219649 32 [3479831076541798806518919219649 3479831076541798806518919219649 3479831076541798806518919219649 35 [3479831076541798806518919219649 36 [3479831076841798806581891919649 36 [3479831076841798806581891919649 37 [3479831076541798806581891919649 38 [3479831076541798806581891919649 39 [3479831076541798806581891919649 39 [3479831076541798806581891919649 30 [3479831076541798806581891919649 30 [3479831075641798806581891919649 30 [3479831076541798806581891919649 30 [3479831076541798806581891919649 30 [3479831076541798806581891919649 30 [3479831076541798806581891919649 30 [3479831076541798806688185864848952466440535055977933 30 [347983107654179806561891919649 30 [347983107654179806561891919649 30 [347983107654179806561891919649 30 [347983107654179806561891919649 30 [347983107654179806661891919649 30 [3479831076614078066981919649 30 [3479831076614078066981919649 30 [34798310766147806986918919649 30 [34798310766147806986918919649 30 [347983107661478069868818878789698688188789786868888888888 | 79 | N | 125461943118669953593211954318781 | 14700275254570640087321604268291 |
| 81 P 99713854957795943700974698049417 82 Q I448115046150086109881092736 83 R 24190514050144590882908182786964 84 S 16586325567946723867583381511093 85 T 171024704622051136504113568735294 86 U 119237079229441536917595501683547 87 V 2029617634958004293351379143335 88 W 73881923249152221564684885048947 89 X 42404110729088076738843892855727 16973183445614345241076592647379 90 Y 46716303657442930319591842731896 12 Z 14215573865740393113660431381586 13 365867041536115064631381586 14 12828799314404994855106002747104 25 [135670151295696880609032601466280 26 [12828799314404994855106002747104 27 447167386816939219649 28] 1 2282879931404994855106002747104 28 37693419417456801293571876398123097 29 [3479831076541798806518919219649 30] 2 47938197654179880651891919649 31 [3479831076541798806518919219649 32 [3479831076541798806518919219649 3479831076541798806518919219649 3479831076541798806518919219649 35 [3479831076541798806518919219649 36 [3479831076841798806581891919649 36 [3479831076841798806581891919649 37 [3479831076541798806581891919649 38 [3479831076541798806581891919649 39 [3479831076541798806581891919649 39 [3479831076541798806581891919649 30 [3479831076541798806581891919649 30 [3479831075641798806581891919649 30 [3479831076541798806581891919649 30 [3479831076541798806581891919649 30 [3479831076541798806581891919649 30 [3479831076541798806581891919649 30 [3479831076541798806688185864848952466440535055977933 30 [347983107654179806561891919649 30 [347983107654179806561891919649 30 [347983107654179806561891919649 30 [347983107654179806561891919649 30 [347983107654179806661891919649 30 [3479831076614078066981919649 30 [3479831076614078066981919649 30 [34798310766147806986918919649 30 [34798310766147806986918919649 30 [347983107661478069868818878789698688188789786868888888888 | 80 | O | 7009281048565051667880348070113 | 26432586399622891061185448632822 |
| 82 Q 144811504615008860169884091078736 83 R 249051405014450988290818278694 84 S 165863255567946723867583381511093 1923063873060460792280187761246352 85 T 171024704622051136504113568735294 86 U 1192370792294415369172955561683547 87 V 20296176349580042293351379143355 88 W 73851923249152221546484885048947 89 X 42404110729088076738834892855727 89 X 42404110729088076738834892855727 89 Y 4476163036574429303193991842731896 90 Y 467163036574429303193991842731896 91 Z 1421557385672409393113660431381886 162897270552877489690891329239163 92 [135670151295696880609032601466280 93 W 34516693003651721285338558617494 94] 1 12828799314404994855106002747104 95 A 11555574461536010570004985062981 96 A 34798310765417988065618919219649 97 A 403119174568012935178167398123097 98 A 2 5201534919257264972352785531958 98 A 2 5201534919257264972352785531958 99 B 785333393400904418699292881578 99 B 785333393400904418699292881578 99 B 785333393400904418699292881578 99 B 785333393400904418699292881578 99 B 878533393900904418669292881578 99 B 878533393900904418669392881578 99 B 87853339390090441866980929881578 99 B 878533393900904418669392881578 99 B 87853339390090441866936565561491919191 10 D 380797033816962066751962246663486 10 C 1425734268628390459788711491791 10 D 38079703381696206751962246663486 10 C 1425734268628390459788771491791 10 D 3807970338169620675196224663486 10 C 1425734268628390459788771491791 10 D 3807970338169620675196224663486 10 C 1425734268628390459788771491791 10 D 38079703381696260675196224663486 10 C 14257342686283904597887714917919665300666440535055597303394806155 10 C 1425734268628390459788771491791 10 D 3807373381696266348666155 2061534557575962246663486 10 C 1425734268628390459788771491791 10 D 380737381696266663486 10 C 142573426862839045978877149179191 10 D 38073738169626666155 2061534575759657916979739066 11 1436461476740777579066114797799066 11 149861430436335348949497079799066520566555878949086653551766643866155 20615345757998799162676508937977161992494670 21 147862860939352509757161992494670 21 1478688988999 | 81 | | 99713854957795943700974698049417 | 153829432406835011731703224913931 |
| 83 R 24190514050144509882908182788964 69503727540034617742601551359424 84 S 1658632556794672386758381511093 192206387060792280187761246352 85 T 171024704622051136504113568735294 96334538737065967688644328597688 60 U 119237079229414536017595561683547 44792649490972280187761246352 87 V 20296176349580042293351379143355 10735812669345783224208082070166 88 W 7385192324915221564684885048947 169673183445614345241076592647379 89 X 4240411072088076738834892855727 1651935200805161169273085540214 90 Y 46716303657442930319591842731896 129576732878270970737326467007253 91 Z 142155738657240930131660431381586 146554834052324778212647078074776 92 [135670151295696880690932601466280 162897270552877489690891329239163 3 4351669300365172128338558617494 762261521329343440420127357065 93 W 3451669300365172128338558617494 76226152132933444042017357065 94] 12828799314404994855106002747104 33800368572130824532557541672 95 ^ 115555074461536016570004985062981 178697207467364283889873192226170038 96 _ 34798310765417988065618919219649 58414861312588046947029245178854 97 | | | | |
| 84 S 165863255567946723867583381511093 192306387060460792298187761246352 85 T 17102470462201136567589443949958175745316344191302 87 V 20296176349580042293351379143355 10735812669345783224208082070166 87 N 20296176349580042293351379143355 10735812669345783224208082070166 87 N 20296176349580042293351379143355 10735812669345783224208082070166 87 N 20296176349580042293351379143355 10735812669345783224208082070166 87 N 20296176349580042293351379143555 10735812669345783224208082070166 97 N 20206176349580042293351379143555 10735812669345783224208082070166 97 Y 46716330657442903015991842731896 12959767322790707373264760707253 91 Z 142155738567240393113660431381586 146354843602324778212647078704776 92 [135670151295696880690932601466280 16289727027874969098192939163 93 34516693003651721285338558617494 76226152132985243346402217357065 94] 1282879931440499485516007247104 3580036863572130892939163 93 34516693003651721285338558617494 76226152132985243346402217357065 95 ^ 11555074615366101570004985062981 178697204763642838897319226170038 96 _ 34798310765417988065618919219649 5841486131258804947029245178854 97 * 40311917456801293571876398123097 60885234843327217078888283435943 94966530064782038769405025518 100 C 14257342686283904597888711491791 45202597864746255202589240987424 101 D 38079703381696206275196224663486 584006854128525677670706755377545 102 E 45754318113363907213290807399706 16280413937603654834952246241157 103 F 54603626980736375626574917973966 13452747470170595478748680068925 104 G 8831030015061460340342884086615 5 320613545557392469064267288040072170519780611947 10524854414529365338667179720579 56350336757626433679739085552294 106 I 110524854114529365338667179739966 13452747470170595878784860068925 104 G 8831030015061460340342884086615 5 3206135455573924690642672458040077171010 M 762840946939325957516107897806155 32061354555799249670 1614797301646880772170519780611947 101 M 7628409469393259075761607697893377 1353766464688077893392890665189174701 101 M 76284094693932506066129973870710 17147802633978457630938745 | | Ď | | |
| 86 U 11923709229415361917595561683547 47926490581757451516375864191302 87 V 20296176349580042293351379143355 10735812669345783224208082070166 88 W 73851923249152221564684885048947 169673183445614345241076592647379 89 X 4420411072908807673883489285727 165193520080956151169273088540214 90 Y 46716303657442930319591842731896 122 1421557348567240393113660431381586 1429576732878270970737326467007253 142155738567240393113660431381586 146354843224778212467078704776 92 [135670151295696880609032601466280 162897270552877489960981329239163 93 | 83 | | 24190514050144509882908182786964 | 69503727540034617742601551359424 |
| 86 U 11923707922941536917592561682547 87 V 20296176349580042293351379143355 1075812669345783224208082070166 88 W 73851923249152221564684885048947 169673183445614345241076592647379 89 X 42404110729088076738834892855727 165193520080956151169273085540214 90 Y 46716330657442993013991842731896 1229576723279070737326467007253 91 Z 142155738567240393113660431381586 146354843602324778212647078704776 92 [135670151295696880609032601466280 1628972705528774896908913292239163 93 \(\) 34516693003651721285338558617494 7622615213298524334602217357065 94] 12828799314404994855106002747104 35800368635721308244532557541672 95 ^ 11555507461536010570004985062981 1786972047634628388973192226170038 96 _ 34798310765417988065618919219649 58414861312588046947029245178854 97 ^ 4031917456801293571876398123097 6058523483469272052245178854 99 B 7853383294300904418699292881578 9496653006064782308769405025518 100 C 14257342686283904597888711491791 45202597866464035555957933 100 C 14257346268283904597888711491791 10 D 38079703381696206275196224663486 584006854128526776707067555377545 102 E 45754318113363097213290807399706 16280413936364344932546441157 103 F 54603626980736375626574917973966 13452747470170595478748680068925 104 G 88310300150614603403428840866155 32061354555739246904267228044012 105 B 114962103490535324894198774726010 52106929978961837973595788332568 106 I 114962103490535324894198774726010 52106929978961837933980552294 106 I 114962103490535324894198774726010 5210692997896183793398832568 107 J 178525573965101425925678525983891 59328016211192139963932800748481171 100 L 25644472604057487620160279983372 153746726294407072170519780611947 101 M 76284094693932509757161992494670 161447730164668807420454834490151419980483234 108 K 136893011504697995122275622579664 134515225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 101 M 76284094693932509757161992494670 171478026300233976547344007394712 101 D 1897105588814649040604444888484948948749484848484848484848484 | 84 | S | 165863255567946723867583381511093 | 192306387060460792280187761246352 |
| 86 U 11923707922941536917592561682547 87 V 20296176349580042293351379143355 1075812669345783224208082070166 88 W 73851923249152221564684885048947 169673183445614345241076592647379 89 X 42404110729088076738834892855727 165193520080956151169273085540214 90 Y 46716330657442993013991842731896 1229576723279070737326467007253 91 Z 142155738567240393113660431381586 146354843602324778212647078704776 92 [135670151295696880609032601466280 1628972705528774896908913292239163 93 \(\) 34516693003651721285338558617494 7622615213298524334602217357065 94] 12828799314404994855106002747104 35800368635721308244532557541672 95 ^ 11555507461536010570004985062981 1786972047634628388973192226170038 96 _ 34798310765417988065618919219649 58414861312588046947029245178854 97 ^ 4031917456801293571876398123097 6058523483469272052245178854 99 B 7853383294300904418699292881578 9496653006064782308769405025518 100 C 14257342686283904597888711491791 45202597866464035555957933 100 C 14257346268283904597888711491791 10 D 38079703381696206275196224663486 584006854128526776707067555377545 102 E 45754318113363097213290807399706 16280413936364344932546441157 103 F 54603626980736375626574917973966 13452747470170595478748680068925 104 G 88310300150614603403428840866155 32061354555739246904267228044012 105 B 114962103490535324894198774726010 52106929978961837973595788332568 106 I 114962103490535324894198774726010 52106929978961837933980552294 106 I 114962103490535324894198774726010 5210692997896183793398832568 107 J 178525573965101425925678525983891 59328016211192139963932800748481171 100 L 25644472604057487620160279983372 153746726294407072170519780611947 101 M 76284094693932509757161992494670 161447730164668807420454834490151419980483234 108 K 136893011504697995122275622579664 134515225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 101 M 76284094693932509757161992494670 171478026300233976547344007394712 101 D 1897105588814649040604444888484948948749484848484848484848484 | 85 | T | 171024704622051136504113568735294 | 96334538737065967688644328597686 |
| 87 V 20296176349780042293351379143555 10735812669345783224208082070166 88 W 73851923249152221564684888048947 16967313445613453614076592647379 89 X 42404110729088076738834892855727 165193520080956151169273085540214 90 Y 46716303657442930319591842731896 129576732878270970737326467007253 91 Z 142155738567240939113660431381586 146354840323247782126447078704776 92 [135670151295696880690932601466280 162897270552877489690891329239163 93 Y 34516693003651721285338558617494 76226152398524334602217357065 94] 12828799314404904855106002747104 35800368635721308244532557841672 95 ^ 115555074461536010570004985062981 78697204763462838897319226170038 96 _ 34798810765417988065618919219649 584148613125880469947029245178854 97 | | | | |
| 88 W 738519232491522215646584885048947 | | | | |
| 89 X 42404110729088076738834892855727 165195220080956151169273085540214 90 Y 46716303657442930319591842731896 1 Z 142155738567240393113660431381586 146354843602324778212647078704776 92 [13567015129566880609032601466280 162897270552877489690891329239163 93 W 34516693003651721285338558617494 94] 12828799314404994855106002747104 35800368635721308244532557365 94] 12828799314404994855106002747104 35800368635721308244532557541672 95 ^ 115555074461356010570004985062981 17869720476346202217857065 96 _ 34798310765417988065618919219649 97 | | | | |
| 90 Y 46716303657442930319591842731896 1295767332878270970737326467007253 91 Z 142155738567240393113660431381586 146554843602324778212647078704776 92 [135670151295696880609032601466280 162897270552877489609891329239163 93 | 88 | | 73851923249152221564684885048947 | 169673183445614345241076592647379 |
| 91 Z 142155738567240393113660431381586 1463548431602324778212647078704776 92 [13567015129569688069032601466280 162897270552877489690891329239163 93 | 89 | X | 42404110729088076738834892855727 | 165193520080956151169273085540214 |
| 91 Z 142155738567240393113660431381586 1463548431602324778212647078704776 92 [13567015129569688069032601466280 162897270552877489690891329239163 93 | 90 | Y | 46716303657442930319591842731896 | 129576732878270970737326467007253 |
| 92 | | | | |
| 93 | | | | |
| 94 | | | | |
| 95 | 93 | | 34516693003651721285338558617494 | 76226152132985243346402217357065 |
| 95 | 94 | 1 | 12828799314404994855106002747104 | 35800368635721308244532557541672 |
| 96 | 95 | Ā | 115555074461536010570004985062981 | 178697204763462838897319226170038 |
| 97 | | | | |
| 98 A 2520153491925726497235278531958 156943284483372127078888283435943 99 B 785383294300904418699292881578 94966530060641782308769405025518 100 C 14257342686283904597888711491791 45202597864762652025089240987424 101 D 38079703381696206275196224663486 58400685412852677670706755377545 102 E 45754318113363907213290807399706 162804139376036548434952246241157 103 F 54603626980736375526574917973966 13452747470170595478748680068925 104 G 88310300150614603403428840866155 32061354555739246906426728504402 105 H 110324834114529365338627179220579 56350336757626433679739085552294 106 I 1149621034003635324894198774726010 5210692997896183759738532568 107 J 178352557396510142592676825983891 59328012611119213963933924806248 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383303345801074816170176780 1459511931110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 1146883188336332858967325555033990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199886482324 297089498026756017553411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 910236982956724016017887233116128 20288898129341375329981035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 1251075238568806012794623663678891 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 253573454092706588216983128123 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067990954797590 126 1138 | | | | |
| 99 B 7853383294300904418699292881578 94966530060641782308769405025518 100 C 14257342686283904597888711491791 4520259786472652025089240987424 101 D 38079703381696206275196224663486 58400688412852677670706755377545 102 E 45754318113363907213290807399706 162804139376036548434952246241157 103 F 54603626980736375626574917973966 13452747470170595478748680068925 104 G 88310300150614603403428840866155 32061354555739246906426728504402 105 H 1103248341145293653338627179220579 56350336757626433679739085552294 106 I 114962103403635324894198774726010 52106929978961837597359788332568 107 J 178352557396510142592676825983891 593280126111192139639333924806248 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 762840946939325097571619922494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 1459511931109847628374127256437 114 Q 18639805895196284566081462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235995426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078655993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979990190619891943 79447158932388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 1397276845143973511973336984785237 1936240161395541997893631283412203 2 116992063625517654738613317717161 82003517206186342382599394505019 4 { 60294121170902891455939443181336 87038905202294191487610086311196 125 253573454092706588216983128121 153098601307678423067909547975790 127 ~ 11387995585517660791168964790177 1011597410318412326682658555654540 | | | 4031191/4508012935/18/639812309/ | |
| 100 C | | | | |
| 101 D 38079703381696206275196224663486 58400685412852677670706755377545 102 E 45754318113363907213290807399706 162804139376036548434952246241157 103 F 54603626980736375626574917973966 13452747470170595478748680068925 104 G 88310300150614603403428840866155 3206135455739246906426728504402 105 H 110324834114529365338627179220579 56350336757626433679739085552294 106 I 114962103403635324894198774726010 52106929978961837597359788332568 107 J 178352557396510142592676825983891 59328012611119213963933924806248 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 1570820467412250109111661968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 19362401613955819978863128341203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 124 { 60294121170902891455939443181336 87038905202294191487610086311196 2535733454092706588216983128121 150908601307678423206799547975790 127 1138799558551766579168646791077 1011597410318412326826258555654540 12674000000000000000000000000000000000000 | 99 | | 7853383294300904418699292881578 | 94966530060641782308769405025518 |
| 101 D 38079703381696206275196224663486 58400685412852677670706755377545 102 E 45754318113363907213290807399706 162804139376036548434952246241157 103 F 54603626980736375626574917973966 13452747470170595478748680068925 104 G 88310300150614603403428840866155 3206135455739246906426728504402 105 H 110324834114529365338627179220579 56350336757626433679739085552294 106 I 114962103403635324894198774726010 52106929978961837597359788332568 107 J 178352557396510142592676825983891 59328012611119213963933924806248 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 1570820467412250109111661968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 19362401613955819978863128341203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 124 { 60294121170902891455939443181336 87038905202294191487610086311196 2535733454092706588216983128121 150908601307678423206799547975790 127 1138799558551766579168646791077 1011597410318412326826258555654540 12674000000000000000000000000000000000000 | 100 | C | 14257342686283904597888711491791 | 45202597864762652025089240987424 |
| 102 E 45754318113363907213290807399706 162804139376036548434952246241157 103 F 54603626980736375626574917973966 13452747470170595478748868068925 104 G 88310300150614603403428840866155 32061354555739246906426728504402 105 H 110324834114529365338627179220579 56350336757626433679739085552294 106 I 114962103403635324894198774726010 52106929978961837597359788332568 107 J 178352557396510142592676825983891 59328012611119213963933924806248 108 K 136893011504697995122275622579664 1434152225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 161479730146468807420454884406518 111 N 170958508014520504665129973870710 171147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 18639805895196246144532991 13694061216853841 | 101 | | 38079703381696206275196224663486 | 58400685412852677670706755377545 |
| 103 F 54603626980736375626574917973966 13452747470170595478748680068925 104 G 88310300150614603403428840866155 32061354555739246906426728504402 105 H 110324834114529365338627179220579 56350336757626433679739085552294 106 I 114962103403635324894198774726010 52106929978961837597359788332568 107 J 178352557396510142592676825983891 59328012611119213963933924806248 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 19516838303345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 534220786569931509286612804033664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 2 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 2 535734540927065882169831281213 153325678348891734881602883923566 1300821195445152927098860222837111 150908601307678423067909547975790 127 11387995585517660791168964790177 101159741031841232682625855654540 | | | | |
| 104 G 88310300150614603403428840866155 32061354555739246906426728504402 105 H 110324834114529365338627179220579 56350336757626433679739085552294 106 I 114962103403635324894198774726010 52106929978961837597359788332568 107 J 178352557396510142592676825983891 59328012611119213963933924806248 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 1211962466060322260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 1092081766580952559426144532991 1369406121 | | | | |
| 105 H | | | | |
| 106 | | | 88310300150614603403428840866155 | |
| 107 J 178352557396510142592676825983891 59328012611119213963933924806248 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979990918061991943 79447158 | 105 | Н | 110324834114529365338627179220579 | 56350336757626433679739085552294 |
| 107 J 178352557396510142592676825983891 59328012611119213963933924806248 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979990180619891943 79447158 | 106 | I | 114962103403635324894198774726010 | 52106929978961837597359788332568 |
| 108 K 136893011504697995122275622579664 143415225557196245248243287418171 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 15170820467412250109111661968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129 | | | | 59328012611119213963933924806248 |
| 109 L 25644472604057487620160279983372 153746726294407072170519780611947 110 M 76284094693932509757161992494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 13972768451499735519736947412988 125107523856 | | | | |
| 110 M 76284094693932509757161992494670 161479730146468807420454834406518 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 1397276845143973351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523 | | | | |
| 111 N 170958508014520504665129973870710 17147802630023397634734007394712 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 202888898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517 | | | | |
| 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 1862107012035744510341998966482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 870389052 | 110 | M | 76284094693932509757161992494670 | 161479730146468807420454834406518 |
| 112 O 121196246606032260496084437330837 79058571393105006032715524873461 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 1862107012035744510341998966482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 870389052 | 111 | N | 170958508014520504665129973870710 | 17147802630023397634734007394712 |
| 113 P 195168383030345801074816170176780 145951193110984762837294127256437 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348 | | | | |
| 114 Q 186398058951962845660831462230733 155837808768653032308876190617550 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307 | | | | |
| 115 R 174194187340190280319970993056211 114683818833633285896732555053990 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 1011597410318 | | | | |
| 116 S 109208176658095235959426144532991 136940612168538418999112306803345 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923366 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | | | |
| 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | 115 | | 174194187340190280319970993056211 | 114683818833633285896732555053990 |
| 117 t 186210701203574451034199896482324 29708949802675601753411873075099 118 u 53422078656993150928661280403664 151708204674122501091116616968566 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | 116 | S | 109208176658095235959426144532991 | 136940612168538418999112306803345 |
| $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | | | | |
| 119 v 16273862062814979909180619891943 7944715892388243628941844281573 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | | | |
| 120 w 91023698295672401601788723116128 20288898129341375329081035179403 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | | | |
| 121 x 139727684514397351197336984785237 193624016139554199783631283412203 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | | | |
| 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | W | | |
| 122 y 194505428411659469405109674142988 125107523856880602179462363678891 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | 121 | X | 139727684514397351197336984785237 | 193624016139554199783631283412203 |
| 123 z 116992063625517654738613317717161 82003517206186342382599394505019 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | | | |
| 124 { 60294121170902891455939443181336 87038905202294191487610086311196 125 2535734540927065882169831281213 153325678348891734881602883923566 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | | | |
| 125 2535734540927065882169831281213 153325678348891734881602883923566 126 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | <u>L</u> | | |
| 126 } 130082119544515292709886022837111 150908601307678423067909547975790 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | <u>{</u> | | |
| 127 ~ 11387995585517660791168964790177 101159741031841232682625855654540 | | | | |
| | 126 | } | 130082119544515292709886022837111 | 150908601307678423067909547975790 |
| | 127 | ~ | 11387995585517660791168964790177 | 101159741031841232682625855654540 |
| 0311374040723710012307107123711002330170720730 | | | | |
| | 120 | \A / I | 1/0/2/100/2/2070/20/2010/120/17200 | 05115 120202725771002550170720750 |

G). Securing Data

Safeguarding sensitive data is very crucial with the evolving cybersecurity threats. One of the most robust and efficient methods of securing data, especially in SDN networks, requires a reliable algorithm, which ECC is one which offer strong encryption while minimizing computational overhead. The elliptic curve 25519 has exceptional security properties and performance characteristics compared to the various ECC curves. Implementing elliptic curve25519 to secure data in SDN requires striking the right balance

between security and computational efficiency. Analysis, as presented in Table V and Fig. 7, reveals that adopting a 138-bit mod(p) value with curve25519 balances robust encryption and efficient computation. The transmission of files encrypted with a 138-bit mod(p) value of the ECC curve25519 occurs through the SDN network using the Ryu controller with three topologies: single, linear, and tree. Table 6 presents the transmission times (milliseconds) for encrypted text files across network topologies.

TABLE III
COMPUTATIONAL TIME PERFORMANCE OF ENCRYPTION AND ENCRYPTION

| Text file | P-value | Bit Size | Encryption Time | Decryption Time |
|-----------|--|------------|------------------|------------------|
| 915KB | 137849 | 18 | 28.17 | 17.33 |
| | 5171003929967 | 43 | 24.83 | 15.50 |
| | 3044861653679985063343 | 72 | 13.71 | 14.48 |
| | 198211423230930754013084525763697 | 108 | 12.85 | 13.07 |
| | 276602624281642239937218680557139826668747 | 138 | 15.07 | 14.97 |
| | 1447401115466452442794637312608598848160326 3447650325797860494125407373907997 | 253 | 15.16 | 16.67 |
| 5.384MB | 137849 | 18 | 30.25 | 35.12 |
| | 5171003929967 | 43 | 29.10 | 29.22 |
| | 3044861653679985063343 | 72 | 25.92 | 49.47 |
| | 198211423230930754013084525763697 | 108 | 30.87 | 30.21 |
| | 276602624281642239937218680557139826668747 | 138 | 29.12 | 27.24 |
| 11.000 | 1447401115466452442794637312608598848160326 3447650325797860494125407373907997 | 253 | 28.77 | 31.56 |
| 11.804MB | 137849 | 18 | 65.14 | 64.18 |
| | 5171003929967 | 43 | 71.99 | 66.51 |
| | 3044861653679985063343 | 72 | 70.03 | 66.29 |
| | 198211423230930754013084525763697 | 108 | 84.37 | 62.67 |
| | 276602624281642239937218680557139826668747 | 138 | 120.71 | 76.51 |
| | 1447401115466452442794637312608598848160326 344765032579786049412540373907997 | 253 | 57.20 | 58.05 |
| 35.350MB | 137849 | 18 | 229.99 | 334.31 |
| | 5171003929967 | 43 | 241.77 | 206.49 |
| | 3044861653679985063343 | 72 | 206.49 | 234.83 |
| | 198211423230930754013084525763697 | 108 | 160.30 | 172.52 |
| | 276602624281642239937218680557139826668747 | 138 | 171.81 | 230.41 |
| | 1447401115466452442794637312608598848160326 344765032579786049412540373907997 | 253 | 245.98 | 228.07 |
| 59.809MB | 137849 | 18 | 360.77 | 333.67 |
| | 5171003929967 | 43 | 346.11 | 349.67 |
| | 3044861653679985063343 | 72 | 410.10 | 303.10 |
| | 198211423230930754013084525763697 | 108 | 405.74 | 410.98 |
| | 276602624281642239937218680557139826668747 | 138 | 319.92 | 472.83 |
| 106MB | 1447401115466452442794637312608598848160326 344765032579786049412540373907997 | 253 18 | 245.65 | 316.53 |
| 100MB | 137849 | | 375.19 | 383.95 |
| | 5171003929967 | 43 | 440.82 | 402.22 |
| | 3044861653679985063343 | 72 | 438.37 | 459.07 |
| | 198211423230930754013084525763697 | 108 | 638.90 | 774.98 |
| | 276602624281642239937218680557139826668747 1447401115466452442794637312608598848160326 344765032579786049412540373907997 | 138 253 | 417.70 632.83 | 348.44 654.76 |

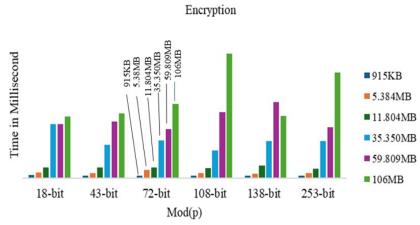


Fig. 5. Graphical Analysis of Encryption Computational Time Performance

TABLE IV ENERGY CONSUMPTION OF ECC CURVE25519 FOR ENCRYPTION AND DECRYPTION

| Text File | P-value | Bit | Encryption Energy | Decryption Energy |
|-----------|---|------|-------------------|-------------------|
| Text File | r-value | Size | Encryption Energy | Decryption Energy |
| | 137849 | 18 | 0.0028 | 0.0017 |
| | 5171003929967 | 43 | 0.0025 | 0.0015 |
| | 3044861653679985063343 | 72 | 0.0014 | 0.0014 |
| | 198211423230930754013084525763697 | 108 | 0.0013 | 0.0013 |
| | 276602624281642239937218680557139826668747 | 138 | 0.0015 | 0.0015 |
| | 144740111546645244279463731260859884816032 | | | |
| 915KB | 63447650325797860494125407373907997 137849 | 253 | 0.0015 | 0.0017 |
| | 5171003929967 | 18 | 0.0030 | 0.0035 |
| | 3044861653679985063343 | 43 | 0.0029 | 0.0029 |
| | 198211423230930754013084525763697 | 72 | 0.0026 | 0.0049 |
| | | 108 | 0.0031 | 0.0030 |
| | 276602624281642239937218680557139826668747 | 138 | 0.0029 | 0.0027 |
| 5.384MB | 144740111546645244279463731260859884816032 63447650325797860494125407373907997 | 253 | 0.0029 | 0.0032 |
| | 137849 | 18 | 0.0065 | 0.0064 |
| | 5171003929967 | 43 | 0.0072 | 0.0067 |
| | 3044861653679985063343 | 72 | 0.0070 | 0.0066 |
| | 198211423230930754013084525763697 | 108 | 0.0084 | 0.0063 |
| | 276602624281642239937218680557139826668747 | 138 | 0.0121 | 0.0077 |
| | 144740111546645244279463731260859884816032 | 150 | 0.0121 | 0.007,7 |
| 11.804MB | 6344765032579786049412540373907997 | 253 | 0.0057 | 0.0058 |
| | 137849 | 18 | 0.0230 | 0.0334 |
| | 5171003929967 | 43 | 0.0242 | 0.0206 |
| | 3044861653679985063343 | 72 | 0.0235 | 0.0160 |
| | 198211423230930754013084525763697 | 108 | 0.0164 | 0.0173 |
| | 276602624281642239937218680557139826668747 | 138 | 0.0172 | 0.0230 |
| | 144740111546645244279463731260859884816032 6344765032579786049412540373907997 | | | |
| 35.350MB | 137849 | 253 | 0.0246 | 0.0228 |
| | | 18 | 0.0361 | 0.0334 |
| | 5171003929967 3044861653679985063343 | 43 | 0.0346 | 0.0350 |
| | | 72 | 0.0410 | 0.0303 |
| | 198211423230930754013084525763697 | 108 | 0.0406 | 0.0411 |
| | 276602624281642239937218680557139826668747 | 138 | 0.0320 | 0.0473 |
| 59.809MB | 144740111546645244279463731260859884816032 6344765032579786049412540373907997 | 253 | 0.0246 | 0.0317 |
| 57.007NIB | 137849 | 18 | 0.0375 | 0.0384 |
| | 5171003929967 | 43 | 0.0441 | 0.0402 |
| | 3044861653679985063343 | 72 | 0.0439 | 0.0459 |
| | 198211423230930754013084525763697 | 108 | 0.0639 | 0.0775 |
| | 276602624281642239937218680557139826668747 | 138 | 0.0418 | 0.0773 |
| | 144740111546645244279463731260859884816032 | 130 | 0.0710 | 0.0340 |
| 106MB | 6344765032579786049412540373907997 | 253 | 0.0633 | 0.0655 |

TABLE V Elliptic Curve25519 Throughput

| | 18-bit Mod(p) Total Time (μs) | 43-bit Mod(p) Total Time (μs) | 72-bit Mod(p) Total Time (μs) | 108-bit Mod(p) Total Time (μs) | 138-bit Mod(p) Total Time (μs) | 253-bit Mod(p) Total Time (μs) |
|------------|----------------------------------|----------------------------------|----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|
| 915KB | 28.14 | 24.83 | 13.71 | 12.85 | 15.07 | 15.16 |
| 5.384MB | 30.24 | 29.10 | 25.92 | 30.87 | 29.12 | 28.77 |
| 11.804MB | 65.14 | 71.99 | 70.03 | 84.37 | 120.71 | 57.20 |
| 35.350MB | 229.99 | 241.77 | 234.83 | 163.76 | 171.81 | 245.98 |
| 59.809MB | 360.77 | 346.11 | 410.10 | 405.74 | 319.92 | 245.65 |
| 106MB | 375.19 | 440.82 | 438.37 | 638.91 | 417.70 | 632.83 |
| Throughput | 1207.41 | 1139.28 | 1102.67 | 984.24 | 1224.43 | 1073.31 |

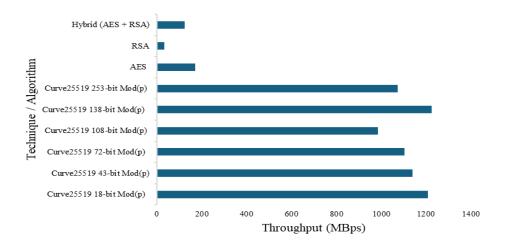


Fig. 6. Comparison of Throughput Across Different Security Algorithms

Analysis, as presented in Table V and Figure 6, reveals that adopting a 138-bit mod(p) value with Curve25519 balances robust encryption and efficient computation. The transmission of files encrypted with a 138-bit mod(p) value of the ECC Curve25519 occurs through the SDN network using the RYU controller with three topologies: single, linear, and tree. Table 6 presents the transmission times (milliseconds) for encrypted text files across network topologies.

Table VI TRANSMISSION TIMES OF ENCRYPTED TEXT FILES OVER DIFFERENT NETWORK TOPOLOGIES

| Text Files | t Files Single Linea | | Tree |
|-----------------|----------------------|----------|----------|
| | Topology | Topology | Topology |
| Text1 | 0.0036 | 0.0042 | 0.0099 |
| Text2 | 0.0052 | 0.0055 | 0.0156 |
| Text3 | 0.0053 | 0.0076 | 0.0205 |
| Text4 | 0.1013 | 0.1045 | 0.2450 |
| Text5 | 0.1115 | 0.1165 | 0.2250 |
| Text6 | 0.1301 | 0.1367 | 0.3540 |
| Total Time (µs) | 0.357 | 0.375 | 0.87 |

Fig. 7 shows that it takes the least Time for a single topology to transmit encrypted files compared to other topologies, which implies that a single topology transmits encrypted files faster than other topologies.

H). Analysis of Mitigating Attack Vectors

Integrating robust encryption and mutual authentication techniques poses a significant challenge for attackers trying to bypass security measures. Consequently, prevalent attack routes, such as Man-in-the-Middle (MiTM) attacks, packet injection, and unauthorised access attempts, are effectively mitigated, thereby enhancing the overall security posture of the SDN environment as detailed as follows:

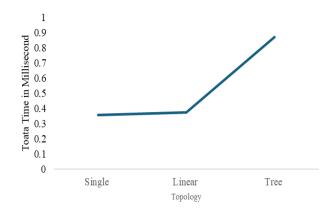


Fig. 8. Graphical Analysis of Transmission Times of Encrypted Text Files over Different Network Topologies

1). Attack by Impersonators from Host 1

Assume an attacker has gained possession of H1. This means the attacker has access to the network key and the public keys. The attacker then replaces H1 with a counterfeit device, Fake_H1. Fake_H1 uses a random number generator to compute the private key of H1 and determine curve points before initiating communication with H2. H2 computes H1_Msg1 and returns H2_Msg2. However, for the impersonator (Fake_H1) to verify authenticity, they need to know |aF|. Since |aF| is embedded in the firmware, it is impossible for the impostor to obtain this value.

2). Attack by Impersonators from Host 2

When the attacker obtains H2, they replace it with a fake device known as Fake_H2, and they are aware of all the previously mentioned parameters. Similarly, fake host gets

 $H_1 Msg_1$ from H1 and computes Prv_-H_2 . The H2 then computes $G_{en_{H2}msg}$ and returns Prv_-H_2 . Following the receipt of |aF| from H1, Fake_H2 will have to wait for the authentication acknowledgment frame from H1. In this case, the authentication procedure won't start in the absence of an authentication acknowledgment frame. The session key will expire since H1 will not be able to validate authentication and will not be able to send actual data to Fake_H2 because the authentication acknowledgment frame is not available. It demonstrates the resilience of our approach against impersonation attacks.

3). Man-in-the-Middle (MiTM) Attack

The attacker continuously watches the transmission channel for messages sent back and forth between H1 and H2. With time, MiTM can comprehend and imitate the data that is transmitted. Likewise, data spoofing allows for the analysis of H1 and H2 messages over an extended period, which allows for the prediction of keys and the discovery of authentication Frame string and acknowledge frame string. However, authentication frames are encrypted when end-toend encryption is used. MiTM finds it very challenging to decrypt and analyze the sent data because of the elliptic curve-based end-to-end encryption. Moreover, the encrypted data block's 1-bit mutation will result in points at infinity. Consequently, in the event of a single-bit mutation, H2 will not calculate points at infinity and the entire data block will produce null values.

4). Device Anonymity and Privacy

Once an attacker gains possession of a host controller, they attempt to retrieve data from a certain host. Even with complete authorization via H1 or H2, the impostor will not be able to extract the data or status of other devices since the hosts have a very particular communication pattern. Because of the way the plan is set up, H1 will only ever meet H2 once while H1 and H2 will need to mutually re-authenticate once the session terminates. Additionally, without knowledge of H1 and H2's private keys, the network administrator is unable to decrypt specific transmission data blocks. All hosts in the network have high privacy and anonymity as a result.

5). Dos / Replay Attack

The compromised host must first be connected to the network by the attacker to use DoS or replay assaults. To compute the precise amount for each devoted session, an attacker must also know a set of parameters such as the network, public and private keys. This is a challenging and computationally demanding procedure. As a result, H1 or H2 will compute curve points at infinity, preventing the ECDH process from continuing. Replay attacks work similarly, with each step's message pattern changing. The session will stop, and the message will be refused if the attacker repeatedly transmits the same message patterns since the relevant device will calculate curve points at infinity.

V CONCLUSION

This study introduced SLECP-SDN, a novel protocol designed to secure communication between SDN's data and control planes using the Elliptic Curve25519 algorithm. The protocol integrates /lightweight encryption and robust authentication to effectively address vulnerabilities in the SDN Southbound Interface (SBI). The results demonstrate the efficacy of SLECP-SDN in achieving high throughput,

energy efficiency, and enhanced resistance to security threats, such as impersonation, replay, man-in-the-middle, device anonymity and packet injection attacks. By utilizing pre-computed curve points and optimizing cryptographic operations, the protocol offers a practical solution that balances security and performance, making it highly suitable for resource-constrained environments. The implementation of Curve25519 establishes a new benchmark for securing SDN environments, ensuring data confidentiality, integrity, and availability without compromising network efficiency.

ACKNOWLEDGEMENT

We appreciate Universiti Putra Malaysia (UPM) for providing an enabling environment for conducting the research work. In addition, O. I. Aladesote would like to thank the Management of Federal Polytechnic, Ile Oluji, Ondo State, Nigeria for their support in pursuing his postgraduate studies.

REFERENCES

- [1] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *J. Netw. Comput. Appl.*, vol. 156, no. July 2019, p. 102563, 2020, doi: 10.1016/j.jnca.2020.102563.
- [2] T. Bakhshi, "State of the art and recent research advances in software defined networking," Wirel. Commun. Mob. Comput., vol. 2017, 2017, doi: 10.1155/2017/7191647.
- [3] A. Mohamed *et al.*, "Software-defined networks for resource allocation in cloud computing: A survey," *Comput. Networks*, vol. 195, no. December 2020, p. 108151, 2021, doi: 10.1016/j.comnet.2021.108151.
- [4] S. Khorsandroo, A. G. Sánchez, A. S. Tosun, J. M. Arco, and R. Doriguzzi-Corin, "Hybrid SDN evolution: A comprehensive survey of the state-of-the-art," *Comput. Networks*, vol. 192, p. 107981, 2021, doi: 10.1016/j.comnet.2021.107981.
- [5] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2637– 2670, 2019, doi: 10.1109/COMST.2019.2908266.
- [6] J. H. Cox et al., "Advancing software-defined networks: A survey," IEEE Access, vol. 5, pp. 25487–25526, 2017, doi: 10.1109/ACCESS.2017.2762291.
- [7] O. I. Aladesote and A. Abdullah, "Efficient and Secure Topology Discovery in SDN: Review," Lect. Notes Data Eng. Commun. Technol., vol. 127, pp. 397–412, 2022, doi: 10.1007/978-3-030-98741-1 33
- [8] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *J. Netw. Comput. Appl.*, vol. 156, no. February, p. 102563, 2020, doi: 10.1016/j.jnca.2020.102563
- [9] S. Ahmad and A. Hussain Mir, "SDN Interfaces: Protocols, Taxonomy and Challenges," *Int. J. Wirel. Microw. Technol.*, vol. 12, no. 2, pp. 11–32, 2022, doi: 10.5815/ijwmt.2022.02.02.
- [10] D. Comer and A. Rastegarnia, "Toward Disaggregating the SDN Control Plane," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 70–75, 2019, doi: 10.1109/MCOM.001.1900063.
- [11] S. Algarni, F. Eassa, K. Almarhabi, A. Algarni, and A. Albeshri, "BCNBI: A Blockchain-Based Security Framework for Northbound Interface in Software-Defined Networking," *Electron.*, vol. 11, no. 7, pp. 1–27, 2022, doi: 10.3390/electronics11070996.
- [12] A. H. Abdi et al., "Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions," *IEEE Access*, vol. 12, no. May, pp. 69941–69980, 2024, doi: 10.1109/ACCESS.2024.3393548.
- [13] M. S. Farooq, S. Riaz, and A. Alvi, "Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review," *Electron.*, vol. 12, no. 14, 2023, doi: 10.3390/electronics12143077.
- [14] M. Iqbal, F. Iqbal, F. Mohsin, M. Rizwan, and F. Ahmad, "Security issues in software defined networking (SDN): Risks, challenges and potential solutions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 10, pp. 298–303, 2019, doi: 10.14569/ijacsa.2019.0101042.
- [15] T. W. Chao et al., "Securing data planes in software-defined networks," IEEE NETSOFT 2016 - 2016 IEEE NetSoft Conf. Work. Software-Defined Infrastruct. Networks, Clouds, IoT Serv., pp. 465—

- 470, 2016, doi: 10.1109/NETSOFT.2016.7502486.
- [16] S. Ghaly and M. Z. Abdullah, "Design and implementation of a secured SDN system based on hybrid encrypted algorithms," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 19, no. 4, pp. 1118–1125, 2021, doi: 10.12928/TELKOMNIKA.v19i4.18721.
- [17] Y. Alemami, A. M. Al-Ghonmein, K. G. Al-Moghrabi, and M. A. Mohamed, "Cloud data security and various cryptographic algorithms," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 1867–1879, 2023, doi: 10.11591/ijece.v13i2.pp1867-1879.
- [18] V. Varadharajan and U. Tupakula, "Counteracting Attacks from Malicious End Hosts in Software Defined Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 160–174, 2020, doi: 10.1109/TNSM.2019.2931294.
- [19] H. Al-Hamdani and W. S. Bhaya, "A Proposed Cryptography Key Management in Software-Defined Networking (SDN)," 6th Iraqi Int. Conf. Eng. Technol. its Appl. IICETA 2023, pp. 22–28, 2023, doi: 10.1109/IICETA57613.2023.10351402.
- [20] N. Gray, T. Zinner, and P. Tran-Gia, "Enhancing SDN security by device fingerprinting," Proc. IM 2017 - 2017 IFIP/IEEE Int. Symp. Integr. Netw. Serv. Manag., pp. 879–880, 2017, doi: 10.23919/INM.2017.7987393.
- [21] A. Ranjbar, M. Komu, P. Salmela, and T. Aura, "An SDN-based approach to enhance the end-to-end security: SSL/TLS case study," Proc. NOMS 2016 - 2016 IEEE/IFIP Netw. Oper. Manag. Symp., no. July 2017, pp. 281–288, 2016, doi: 10.1109/NOMS.2016.7502823.
- [22] B. Yigit, G. Gur, B. Tellenbach, and F. Alagoz, "Secured Communication Channels in Software-Defined Networks," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 63–69, 2019, doi: 10.1109/MCOM.001.1900060.
- [23] Y. Peng, C. Wu, B. Zhao, W. Yu, B. Liu, and S. Qiao, "QKDFlow: QKD based secure communication towards the openflow interface in SDN," Commun. Comput. Inf. Sci., vol. 699, pp. 410–415, 2017, doi: 10.1007/978-981-10-3969-0 45
- [24] T. Adhikari, M. Kule, and A. K. Khan, "An ECDH and AES Based Encryption Approach for Prevention of MiTM in SDN Southbound Communication Interface," 2022 13th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2022, pp. 1–5, 2022, doi: 10.1109/ICCCNT54827.2022.9984509.
- [25] D. S. Sahana and S. H. Brahmananda, "Secure Authentication Framework for SDN-IoT network using Keccak-256 and Bliss-B algorithms," *International Journal of Information Technology* (Singapore), vol. 15, no. 1. pp. 335–344, 2023. doi: 10.1007/s41870-022-01074-w.
- [26] J. W. Kang, S. H. Park, and J. You, "Mynah: Enabling lightweight data plane authentication for SDN controllers," *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, vol. 2015-Octob, pp. 1–6, 2015, doi: 10.1109/ICCCN.2015.7288433.
- [27] D. J. Bernstein, "Curve25519: new Diffie-Hellman speed records," vol. 25519, 2006.
- [28] P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization," *Math. Comput.*, vol. 48, no. 177, p. 243, 1987, doi: 10.2307/2007888.