http://www.doi.org/10.62341/amuc1218

Received	**2024/12/3**	**تم استلام الورقة العلمية في**
Accepted	**2024/12/30**	**تم قبول الورقة العلمية في**
Published	**2025/01/05**	**تم نشر الورقة العلمية في**

Using Elliptic-Curve to Implements SSL Certificate Derives from CSR to Make Secure Connection between Server and Client

Abdulaziz Mahmud Suwayeb, Mahmoud Mohamed Elsaghayer

The College of Technical Sciences Misrata - Libya
aswaype@yahoo.com

Abstract

The paper discusses the implementation of Secure Sockets Layer (SSL) certificates, which are obtained from Certificate Signing Requests (CSRs), to facilitate secure connections between servers and clients. SSL serves as an essential encryption protocol that guarantees the confidentiality, integrity, and authenticity of data transmitted over networks, thus playing a vital role in safeguarding online transactions and communications.

The paper outlines SSL process, which encompasses key components such as the key generation, and data encryption. Additionally, it highlights the importance of the RSA algorithm within SSL for effective key exchange and authentication purposes. It also explains elliptic-curve cryptography (ECC), presenting it as a more efficient alternative to conventional cryptographic techniques. The advantages of ECC, particularly in terms of smaller key sizes and enhanced security, are emphasized, showcasing its superiority in modern cryptographic applications.

Furthermore, the paper provides practical implementation steps for creating a CSR using C# code, illustrating how to establish a secure connection utilizing elliptic curves. This includes a guide on generating a CSR file, which can later be utilized in the process of creating an SSL certificate, thus ensuring robust security for online communications.

Key words: Elliptic-curve, Secure Socket Layer, Certificate Signing Request, Rivest-Shamir-Adleman, Certificate Authority.

http://www.doi.org/10.62341/amuc1218

استخدام المنحنى الإهليجي لتنفيذ شهادة طبقة المقابس الآمنة المشتقة من طلب توقيع الشهادة لإجراء اتصال آمن بين الخادم والعميل

عبد العزيز محمود سويب، محمود محمد الصغير

كلية العلوم التقنية مصراتة – ليبيا

aswaype@yahoo.com

الملخص

تناقش الورقة البحثية تنفيذ شهادات طبقة مآخذ التوصيل الآمنة (SSL)، التي يتم الحصول عليها من طلبات توقيع الشهادات (CSRs)، لتسهيل الاتصالات الآمنة بين الخوادم والعملاء. تعمل طبقة المقابس الآمنة كبروتوكول تشفير أساسي يضمن سرية وسلامة وموثوقية البيانات المرسلة عبر الشبكات، وبالتالي يلعب دورًا حيويًا في حماية المعاملات والاتصالات عبر الإنترنت.

توضح الورقة البحثية عملية بروتوكول طبقة المقابس الآمنة SSL، والتي تشمل المكونات الرئيسية مثل توليد المفاتيح وتشفير البيانات. بالإضافة إلى ذلك، يسلط الضوء على أهمية خوارزمية RSA ضمن بروتوكول طبقة المقابس الآمنة (SSL) لأغراض تبادل المفاتيح والمصادقة الفعالة.

كما تشرح أيضًا التشفير المنحنى الإهليجي (ECC)، وتقدمه كبديل أكثر كفاءة لتقنيات التشفير التقليدية. يتم التأكيد على مزايا تشفير المنحنى الإهليجي (ECC)، لا سيما من حيث أحجام المفاتيح الأصغر والأمان المعزز، مما يوضح تفوقه في تطبيقات التشفير الحديثة.

علاوةً على ذلك، تقدم الورقة البحثية خطوات تنفيذ عملية لإنشاء CSR باستخدام كود C#، وتوضح كيفية إنشاء اتصال آمن باستخدام المنحنيات الإهليجية. ويتضمن ذلك دليلًا حول إنشاء ملف CSR، والذي يمكن استخدامه لاحقًا في عملية إنشاء شهادة SSL، وبالتالي ضمان أمان قوي للاتصالات عبر الإنترنت.

الكلمات المفتاحية

المنحنى الاهليجي، طبقة المقابس الآمنة، طلب توقيع الشهادة، ريفست شامير أدلمان، المرجع المصدق.

Introduction

Secure Sockets Layer (SSL) is an encryption protocol designed for secure communication over computer networks. SSL has several versions, the first of which is SSL 3.0 and the latest is TLS 1.3. The SSL is widely used by businesses and individuals because of its ability to encrypt and protect sensitive data, such as login credentials and credit card information[1]. The SSL protocol works at the transport layer of the OSI model and creates a secure connection between the client and the server. This secure connection ensures the confidentiality, integrity, and authenticity of data transmitted between client and server. [2]

SSL Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network, such as the Internet. The main difference between SSL and TLS is that TLS is designed to address the vulnerabilities of SSL and provide additional security features. [3]

SSL protocol provides a secure communication channel through a computer network. It was developed by Netscape Communications Corporation and adopted as an Internet standard.

RSA (Rivest-Shamir-Adleman) is a widely used public key encryption algorithm that provides a secure way to encrypt and decrypt messages.

SSL uses RSA in two different ways: for key exchange and server authentication as part of an asymmetric encryption system. [4]

SSL uses two main encryption algorithms to create a secure connection: symmetric encryption and asymmetric encryption. Symmetric encryption uses the same key for encryption and decryption, while asymmetric encryption uses a pair of keys - a public key for encryption and a private key for decryption.

Presented below is a quick overview of how SSL establishes a secure connection: [1] [4]

1- **Handshake**: The SSL handshake begins when the client initiates a connection with the server. During this handshake, the client and server exchange encryption parameters and verify each other's identities.
2- **Key generation**: After the handshake, the client and server generate a symmetric encryption key using the parameters exchanged during the handshake. This key is used to encrypt and decrypt data transferred between the client and server.
3- **Data Encryption**: Once the symmetric encryption key is generated, the client and server can begin exchanging encrypted data. This data is encrypted using a symmetric encryption key to ensure its confidentiality and integrity.
4- **Secure connection**: A secure connection is now established so that the client and server can exchange data safely and reliably.

SSL in a web application must obtain an SSL certificate from a trusted certification authority (CA). This publicly available certificate is used to establish a secure connection.

SSL architecture

Secure Sockets Layer (SSL) is a dangerous tool for ensuring the security of data transferred between clients and servers. SSL reaches this by encrypting the link between the server and the client, guaranteeing that all data exchanged between them remains confidential and protected from hateful attacks.

To better understand the function of SSL, it is necessary to research into its various protocols. [5]

The SSL Record Protocol is responsible for severe the data into manageable fragments, which are independently encrypted and then sent to the recipient.

The handshake protocol is used to start a secure connection between server and client and exchange encryption keys. [5].

The Cipher Change Specification Protocol is used to specify the encryption algorithms that will be used in the communication.

The alert protocol is used to report problems that may arise during the data exchange.

As shown in Figure 1. [5].

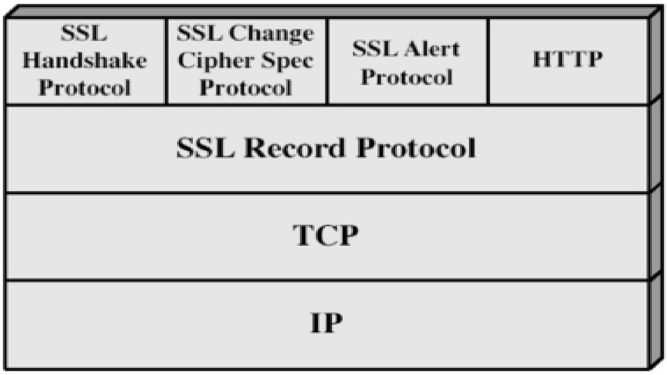


Figure (1) SSL architecture [5].

Certificate Signing Request (CSR) Overview

In order to generate SSL Certificate, it is necessary to create a Certificate Signing Request (CSR) for the domain name or hostname on server. The CSR provides a standardized way for the certificate requester to transmit their public key to the issuing Certificate Authority (CA). Additionally, it includes relevant information about the requester, as indicated below, and is paired with a secret private key on the server. [4][5]

Common Name (CN):

The Common Name (CN) is the fully qualified domain name (FQDN) of your server.

Organization Name (O):

The Organization Name (O) is the legal name of your company or organization.

Organization Unit (OU):

The Organization Unit (OU) is the unit or division of your company or organization that manages the certificate, such as the IT Department.

Locality (L):

The Locality (L) is the city where your company or organization is located.

State or Province Name (ST):

The State or Province Name (ST) is the state or province where your company or organization is located.

Country (C):

The Country (C) is the country where your company or organization is located.

Email Address:

The Email Address is an email associated with your company or organization, such as info@ctsm.edu.ly

SSL certificate

SSL connections are driven by certificates, which are files that are installed on servers. These certificates are specifically related to the URL or IP address of the server on which they are installed. This is because the attendance of the certificate on the server enables the confidence and encryption mechanisms characteristic in SSL sessions. The term ‘certificate’ makes from the fact that it confirms the identity of the server to which it is assigned. It contains vital information about the identity of the owner of the URL or IP address, information that can be detected and validated by the client device, thus confirming the identity of the server. Certificates are specifically protected against meddling and fake through various hashing algorithms that ensure they are authentic and inviolate. This ensures that no one can claim to be another identity by meddling with an issued certificate, and no one can create a fake certificate on

http://www.doi.org/10.62341/amuc1218

a trusted public root. Any certificate that deviates from its original information will be easily recognized as a forgery by any system that interacts with it, and will be considered untrustworthy [6][7].

Elliptic Curve

Elliptic-curve cryptography (ECC) represents a sophisticated method within the realm of public-key cryptography, leveraging the intricate algebraic structure of elliptic curves defined over finite fields. One of the standout advantages of ECC is its ability to deliver robust security with smaller key sizes when compared to traditional cryptosystems that rely on modular exponentiation within Galois fields, such as the widely used RSA and ElGamal systems.

The flexibility of elliptic curves extends beyond just key generation; they are useful in key agreement protocols, digital signatures, and pseudo-random number generation, among other cryptographic operations. Additionally, ECC can be used indirectly for cryptographic purposes by combining key agreement operations with symmetric encryption techniques, thus enhancing overall security. In addition, elliptic curves play a vital role in many integer factorization algorithms, such as the Lenstra elliptic curve factorization process, which is mainly important in cryptographic applications. This complex utility highlights the importance of ECC in modern cryptography, making it a vital component in securing digital communications [1].

Ed25519 and Ed25519 have appeared as highly recommended elliptic curves, recognized for their extraordinary security and performance. They are particularly preferred in the TLS 1.2 and TLS 1.3 cipher suites, which are generally used in e-commerce and online banking servers. Their strong cryptographic properties make them perfect choices for protecting sensitive transactions and guaranteeing the integrity of online communications. [8]

Let p prime number, the finite field FP, called a prime field, is comprised of the set of integers {0,1,2,……..,p-1}.

An elliptic curve E over Fp is defined by an equation of the form

$$y^2 = x^3 + ax + b$$

Where a,b∈ Fp , the set E(Fp) contain of all points (x,y), x ∈ Fp, y ∈ Fp , which satisfy the defining previous equation, and special point O called the point at infinity.as shown in figure 2.[9]

http://www.doi.org/10.62341/amuc1218

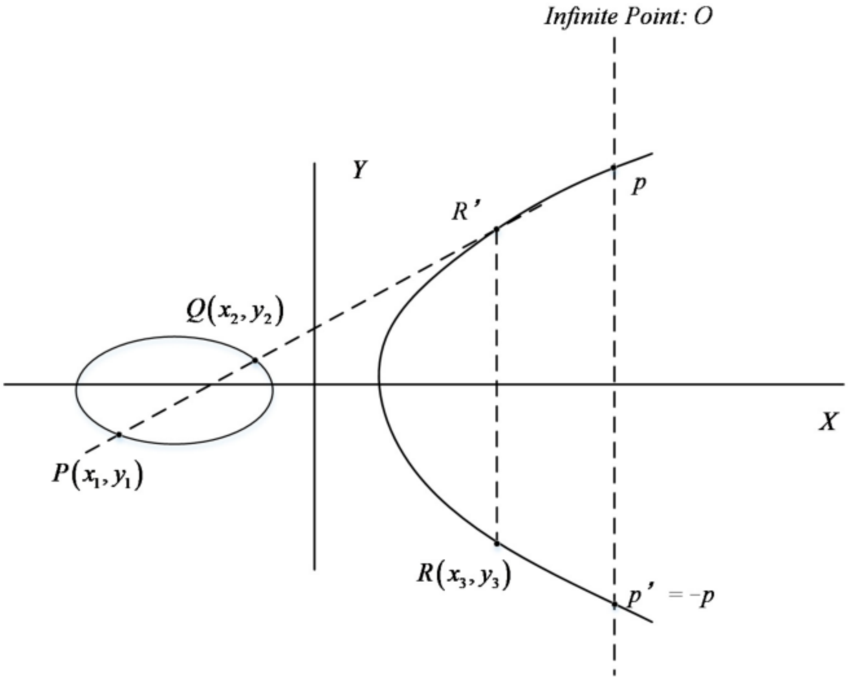


Figure (2) Double point operation on elliptic curve [9]

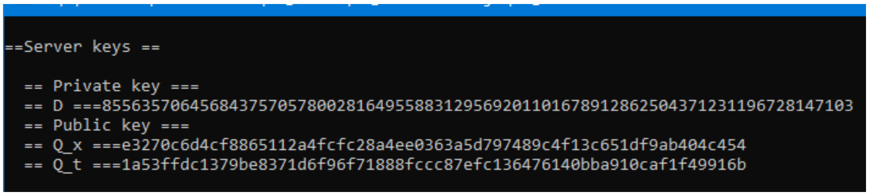
SSL Implementation

In this paper we are an implement a secure socket layer (SSL) certificate based on Certificate Signing Request (CSR)
firstly, create CSR by C# code and store the result in file with CSR extension.
Use the elliptic curve equation to establish a secure connection between two parties, server and client by the following steps:

1- Server and Client agree on the elliptic curve equation and a base point G on the curve.
2- Server generates a private key k and computes a public key P = kG as shown in figure (3).
3- Client generates a private key l and computes a public key Q = lG as shown in figure (4).
4- Server and Client exchange their public keys and compute a shared secret key S = kQ = lP.

This shared secret key S can be used to encrypt and decrypt messages between Server and Client.

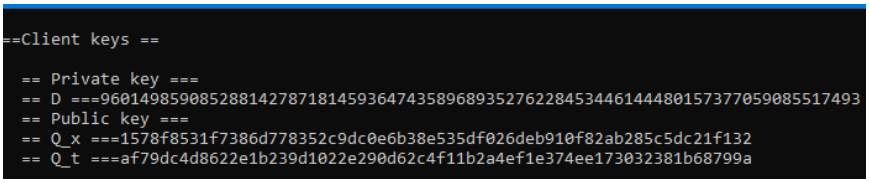
http://www.doi.org/10.62341/amuc1218



```
==Server keys ==

  == Private key ===
  == D ===85563570645684375705780028164955883129569201101678912862504371231196728147103
  == Public key ===
  == Q_x ===e3270c6d4cf8865112a4fcfc28a4ee0363a5d797489c4f13c651df9ab404c454
  == Q_t ===1a53ffdc1379be8371d6f96f71888fccc87efc136476140bba910caf1f49916b
```

Figure (3) Server public and private keys

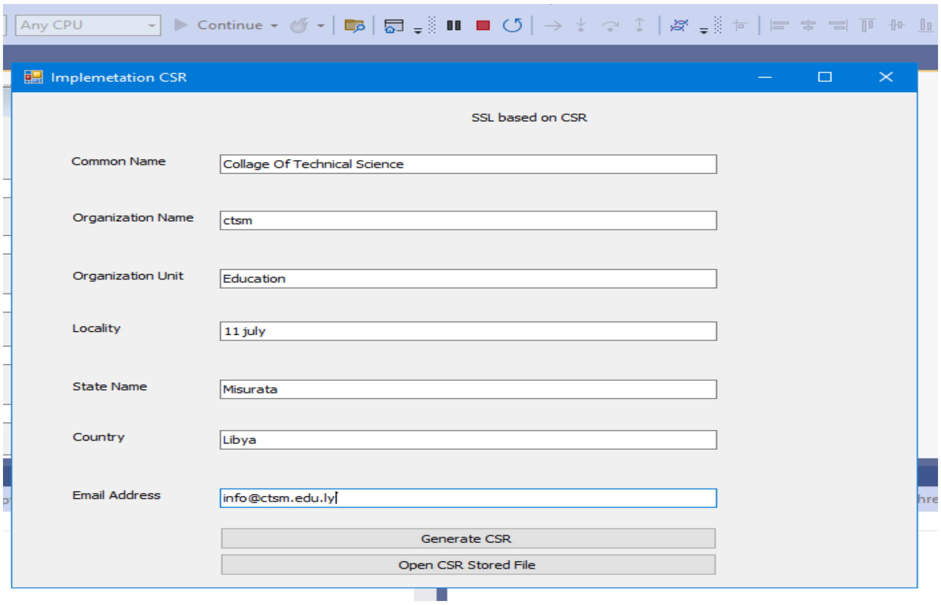


```
==Client keys ==

  == Private key ===
  == D ===96014985908528814278718145936474358968935276228453446144480157377059085517493
  == Public key ===
  == Q_x ===1578f8531f7386d778352c9dc0e6b38e535df026deb910f82ab285c5dc21f132
  == Q_t ===af79dc4d8622e1b239d1022e290d62c4f11b2a4ef1e374ee173032381b68799a
```

Figure (4) Client public and private keys

there are some parameters required before generate CSR file based on previous public keys for server and client, these parameters as shown in figure (5)



SSL based on CSR

Common Name: Collage Of Technical Science

Organization Name: ctsm

Organization Unit: Education

Locality: 11 july

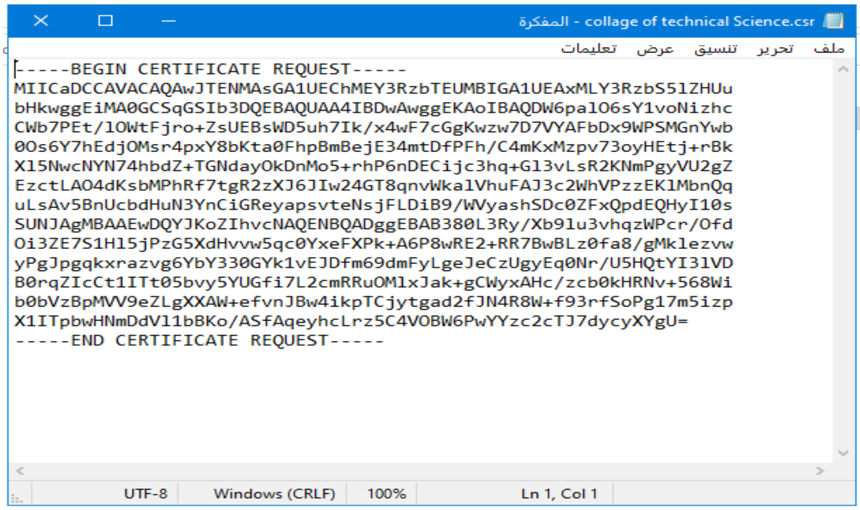
State Name: Misurata

Country: Libya

Email Address: info@ctsm.edu.ly

Figure (5) Entering CSR parameters interface

After run the code we will get the CSR file stored on Local storage When open this file with notebook it will be looks like a shown in figure (6)

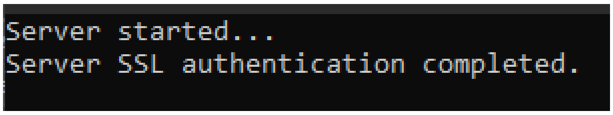

المفكرة - collage of technical Science.csr
ملف تحرير تنسيق عرض تعليمات
UTF-8
Windows (CRLF)
100%
Ln 1, Col 1

```
-----BEGIN CERTIFICATE REQUEST-----
MIICaDCCAVACAQAwJTENMAsGA1UEChMEY3RzbTEUMBIGA1UEAxMLY3RzbS51ZHUu
bHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDW6pal06sY1voNizhc
CWb7PEt/1OWtFjro+ZsUEBsWD5uh7Ik/x4wF7cGgKwzw7D7VYAFbDx9WPSMGnYwb
0Os6Y7hEdjOMsr4pxY8bKta0FhpBmBejE34mtDfPFh/C4mKxMzpv73oyHEtj+rBk
X15NwcNYN74hbdZ+TGNdayOkDnMo5+rhP6nDECijc3hq+G13vLsR2KNmPgyVU2gZ
EzctLAO4dKsbMPhRf7tgR2zXJ6JIw24GT8qnvWka1VhuFAJ3c2WhVPzzEK1MbnQq
uLsAv5BnUcbdHuN3YnCiGReyapsvteNsjFLDiB9/WVyashSDc0ZFxQpdEQHyI10s
SUNJAgMBAAEwDQYJKoZIhvcNAQENBQADggEBAB380L3Ry/Xb91u3vhqzWPcr/Ofd
Oi3ZE7S1H15jPzG5XdHvvw5qc0YxeFXPk+A6P8wRE2+RR7BwBLz0fa8/gMklezvw
yPgJpgqkxrazvg6YbY330GYk1vEJDfm69dmFyLgeJeCzUgyEq0Nr/U5HQtYI31VD
B0rqZIcCt1ITt05bvy5YUGfi7L2cmRRuOM1xJak+gCWyxAHc/zcb0kHRNv+568Wi
b0bVzBpMVV9eZLgXXAW+efvnJBw4ikpTCjytgad2fJN4R8W+f93rfSoPg17m5izp
X1ITpbwHNmDdV11bBKo/ASfAqeyhcLrz5C4VOBW6PwYYzc2cTJ7dycyXYgU=
-----END CERTIFICATE REQUEST-----
```

Figure (6) CSR file

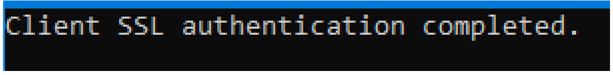
The CSR file will be used in C# code to generate a certificate file with .cer extension.

After getting the CSR file, the code will run a secure connection between server and client based on a shared key and certificate.as shown in figures (7) and (8) respectively.



```
Server started...
Server SSL authentication completed.
```

Figure (7) Server authentication



```
Client SSL authentication completed.
```

Figure (8) client authentication

Results and Findings

The paper explains implementing and basics encryption of SSL protocol, and its functionalities used up to now abstract Secure Socket Layer (SSL) creates a secure and encrypted link between the server and client, this can be explained in few words. Main results and findings from the paper are as given in the following:

Role of SSL Certificates: The paper highlights the need for SSL certificates to achieve Server-Client security. They allow SSL/TLS encryption for transferring data securely between the server and the

http://www.doi.org/10.62341/amuc1218

client. The public key is used for encoding and private keys (keep on server!), which, by definition, allows to decode.

Aside from encrypting, SSL also provides identity verification for client and server. This makes sure that client is talking to the right server and prevents man-in-the-middle attacks and other forms of impersonation.

A Brief overview on SSL The paper provides an overview how SSL works in context of here using Elliptic curve and highlights secure connections in client-server interactions. The interaction is important to ensure that the data shared and exchanged remain valuable and not malicious.

In summarize, this paper describes the SSL protocol and how it works, detailing some of its most important characteristics, being such as SSL certificates, which secure traffic between client/server having an encrypted tunnel in a safe manner using the SSL/TLS. The paper highlights that these certificates encrypt the data with public and private keys, as well as authenticating both the client and server thus protecting against any man in the middle attack. It also elaborates the Elliptic curve role in safe communication between client and server, a fundamental part to assure data is not modified or viewed without authorization

Conclusion

The main point of the given text is that Secure Socket Layer (SSL) is an encryption protocol used for secure communication over computer networks. SSL ensures the confidentiality, integrity, and authenticity of data transmitted between a client and server. SSL uses RSA for key exchange and server authentication. To implement SSL in an application, SSL certificate must be obtained from a trusted certification. Our implementation offers a secure SSL connection with special parameters that are used to generate CSR file and using elliptic curve to generate a strong a shared key between server and client This creates a specific encryptionthat utilizes unknown algorithms and parameters, thereby preventing any attacker from accessing sensitive data transmitted over the connection link. As a result of this procedure, we can confidently say that our connection between server and client is well-trusted and secure. Our implementation works seamlessly and efficiently, without compromising on security.

http://www.doi.org/10.62341/amuc1218

References

[1] V., S., Prakash., K., K., Thavamani., A., Sivakumar., Rajiv, Kumar., Margaret, Mary, T.., P., Poongothai. (2024). 1. Experimental Evaluation of an Elliptical Curve Cryptographic Model Based Data Security Over Communication Channels Using Cybersecurity Logics. ," *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, Gurugram, India, 024, DOI**:** 10.1109/ISCS61804.2024.10581344

[2] B. Arunkumar*, G. Kousalya, Secure and Light Weight Elliptic Curve Cipher Suites in SSL/TLS. Computer Systems: Science & Engineering, https://doi.org/10.32604/csse.2022.018166,2022

[3] Beurdouch, B., et al., "A Messy State of the Union: Taming the Composite State Machines of TLS," Proceedings of the 36th IEEE Symposium on Security and Privacy, San Jose´, CA, May 2015, pp. 535–552.

[4] Barnes, R., et al., "Deprecating Secure Sockets Layer Version 3.0," Standards Track RFC 7568, June 2015.

[5] Stallings, Cryptography and Network Security, 7Th Edition, pearson india, 2017,

ISBN-13 978-9332585225

[6] Adrian, D., et al., "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," Proceed- ings of the ACM Conference in Computer and Communications Security, ACM Press, New York, NY, 2015, pp. 5–17.

[7] Aciic¸mez, O., W. Schindler, and C.K. Koc¸, "Improving Brumley and Boneh Timing Attack on Unprotected SSL Implementations," Proceedings of the 12th ACM Conference on Computer and Communications Security, ACM Press, New York, NY, 2005, pp. 139–146.

[8] Wohlwend, Jeremy. Elliptic Curve Cryptography: Pre and Post Quantum. https://math.mit. edu/~apost/courses/18.204-2016/18.204_Jeremy_Wohlwend_final_paper.pdf

[9] Jiang, C.; Huang, C.; Huang, Q.; Shi, J. A Multi-Source Big Data Security System of Power Monitoring Network Based on Adaptive Combined Public Key Algorithm. Symmetry 2021, 13, 1718. https://doi.org/10.3390/sym 13091718