Conference Proceeding Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

EdDSA: An Effectiveness and Efficiency Analysis of Ed448 and Ed25519 Algorithms used for Secured Student Academic Records

[1]S. Syed Nawas Husain and [2]Dr. R.Balasubramanian,
[1]Research Scholar, [2]Professor,
[1,2]Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Abishekpatti, Tirunelveli, India

Abstract: Computer networks and Internet application are growing fast, so data security is the challenging issue of today that touches many areas. To prevent unauthorized access to the user data, any transmitting process should be securely encrypted. Currently many Cryptography algorithms are available to secure the data but some algorithms consume more time, less security and less throughput. Student Academic Records are more important for use in Universities and Colleges, so Cryptography Algorithms are used to protect the data from third parties. A digital signature algorithm refers to a standard for digital signatures, which is based on the algebraic properties of discrete logarithm problem and modular exponentiations based on public-key cryptosystems. Digital signatures are work on the principle of two mutually authenticating cryptographic keys. There are many significant challenges are still existing in the cryptography algorithms. In this paper, we are analyzing various cryptography techniques on Student Academic Records for security. Here, EdDSA, Ed448 and Ed25519 are discussed and evaluation metrics like Encryption Time, Decryption Time, Throughput and Energy Consumption are used in Python to identify the performance of the above techniques.

Keyword: *Cryptography, Data Encryption, EdDSA, Ed448 and Ed25519*

I. INTRODUCTION

Secure transaction of confidential digital messages has become a common interest in both research and applications. Ed25519 algorithm designed with suitable to cipher such type of data. Encryption is a growth in the network and various areas are used to protect data. With the rapid development of the Internet, Education system have established confidential data in network, thus enriching students performance high efficiency, expanding Student Academic Performance space and improved in education environment.

1.1 Elliptic Curve

An Elliptic Curve [6] is the set of points that satisfy a specific mathematical equation. The equation for an elliptic curve is:

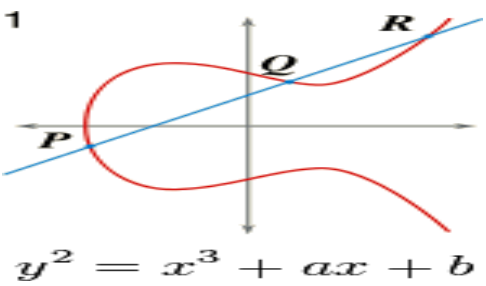

Figure 1: Elliptic Curve

For sum constants ‘a’ and ‘b’ and Point co-ordinates (x, y)

$$y^2 = x^3 + ax + b \quad (1)$$

Another Condition it should satisfy:

$$4a^3 + 27\,b^2 \neq 0 \quad (2)$$

1.2 Elliptic Curve – Over Finite Field:

The elliptic curve over finite field [1] because of the curve is used in cryptography.

1.2.1 Finite Field:

Set of integers mod(p), we assume p=11 value it return like mod(11). Set of finite elements that come under the field. We have consider these element: {0,1,2,3,4,5,6,7,8,9,10} and (x,y) will form in finite field.So the equation of the elliptic curve over a finite field is:Here, p is the finite field ‘a’ and ‘b’ are no greater than ‘p’.

II. LITERATURE REVIEW

2.1 Elliptical Curve Cryptography (ECC)

The ECC [8] based asymmetric encryption algorithm. The aim of the principle work is 1) reduce the encryption times because converts into big integers. 2) Big integers are converted with ECC a chaotic system, these process are used to improve the key transmission process and ECC as highly secured by data transmitting from one place to other place in a secure way. Decryption and conditional authentication based on ECC-based access control scheme, here introduced the pre-decryption algorithm based ECC to enhanced the security for certificate information [2]. ECQV design the authenticate certificate implicit for both privacy protection and mutual authentication.

2.2 Digital Signature Algorithm (DSA)

Digital signatures [5] use a public-key cryptosystem and use a public/private key pairs. A message is signed by a private key and the signature is verified by the corresponding public key. The message is signed by the sender’s private key (PK). Firstly, the input message is hashed and then the signature is calculated by the signing algorithm.Further, signature of the message is verified by the corresponding public key (PU). Typically the signed message is hashed and some calculation is performed by the signature algorithm using the message hash and the public key.The signed message mathematically guarantees that the message was signed with PK by a corresponding PU.

2.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

Present of medical records of COVID-19 to be capable of security by using algorithm, ECDSA based blockchain technology to make change to the information on the blocks to Digital Signature based to protect the specification of research tool model [3]. Message authenticated by guarantee integrity done help of an algorithm as ECDSA which provides message authentication to improved performance of an accuracy level. Efficient threshold signature protocols for ECDSA begin of DSA algorithm by zero knowledge proof and computing many modulus, in this simulation security under non- standard as paillier. The key generation using and derives for secret key in three prime number of this algorithm. Consortium blockchain wallet scheme based on dual threshold key protection using secret key using ECDSA algorithm for data secured [10].

2.4 Edwards Curve Digital Signature Algorithm (EdDSA)

Implement over galois field [10] in the operations include EdDSA over Galois field provides more security it to perform fast public-key digital signature algorithm. In ECDSA mistake by Identify private key error in the matching signature for various documents to overcome this problem by using EdDSA algorithm. Generating hash functions among the transactions which provide high level speed [7]. Improved security by use random number to sequence in ECDSA. Efficient signing protocol Based two party by EdDSA valid signature generating using interactive protocol without original key by protecting threshold signature method avoid fraud key usage.

III. METHODOLOGY

3.1 Edwards Digital Signature Algorithm (EdDSA)

Digital Signature provide a way to authorize and integrate only the correct and genuine persons to do the record or transaction [10]. Hashing is the process of transformation by input of types into an encrypted output which is in fixed length. In current scenario hashing process done by based of cryptography algorithms. Elliptical Curve Digital Signature Algorithm (ECDSA) used as digital signature for transaction record authentication. But the ECDSA purely and heavily relies on the point multiplication by creating problem when if an error is happened while this operation to avoid these problems, as suggest the usage of Edwards Digital Signature Algorithm (EdDSA) instead of ECDSA to avoid the multiple computations and making the digital signature very easily [3]. Various advantages there with EdDSA algorithm over ECDSA algorithm in digital Signature.

Algorithm 1: EdDSA [7]

Key Generation:

- Compute (hk, lk)=Hash(k) where hk is 32 bytes MSB and lk is 32 bytes LSB.
- Assign a=hk as little-endian notation.
- Compute Q = a ∗ G over the prime field F_P.

Signature Generation:

- Compute (hk,lk)=Hash(k) where hk is 32 bytes MSB and lk is 32 bytes LSB.
- Compute r=Hash(lk,m) mod q
- Compute R=r∗G over the prime field F_p
- Compute h=Hash(R,Q,m) mod q
- Compute s=(r+h∗a) mod q

Signature Verification:

- Compute h=Hash(R,Q,m) mod q
- Compute hQ=R+h∗Q over the prime field F_p
- Compute sG=s∗G over the prime field Fp
- If hQ=sG then
- State message m is valid

3.2 Ed448

The Digital Signature Algorithm is mainly used to verify that the communication was sent by the intended recipient. [9] The Edwards-Curve Digital Signature Algorithm (EdDSA) is defined in three phases - Key Generation, Sign and Verify. Ed448 DSA has a thorough explanation of these procedures. After running the signing function, it returns a signature R||S generated based on the secret key and the message value. Finally, the verification is executed based on the public key and the message value and returns success upon the correctness of the equation [S] · G == R + [k] · A. As noted, the scalar multiplication subroutine is forming the basis of both - elliptic curve based key agreement and digital signature algorithms.

Algorithm 2: Ed448 [9]

Key Generation

Input: seed

Output: $(p, s), p^k_A$

Step 1: $sk_A \epsilon^{seed} Z/F_p$

Step 2: $(p, s) \leftarrow H(sk_A)$

Step 3: $p^kA \leftarrow$ encode$([s] \cdot G)$

Return $(p, s), p^k_A$

Sign

Input: $p^k_A, (p, s), M$

Output: sign = $R||S$

Step 4: $r \leftarrow (H(p||M))(modL)$

Step 5: $R \leftarrow encode([r] \cdot G)$

Step 6: $k \leftarrow (H(R||p^k_A||M))(modL)$

Step 7: $S \leftarrow encode((r + k * s)(modL))$

Return $R||S$

Verifying

Input: $p^k_A, M, R||S$

Output: true/ false

Step 8: $k \leftarrow H(R||p^k_A||M)(modL)$

Step 9: A ← decode(p^k_A)

Return $[S] . G == R + [k] . A$

3.3 Ed25519

The Ed25519 [4] is SHA512 instead. That is, the input is hashed using SHA-512 before signing with Ed25519. Value of context is set by the signer and verifier and has to match octet by octet for verification to be successful. The curve used is equivalent to Curve25519, under a change of coordinates, which means that the difficulty of the discrete logarithm problem is the same as for Curve25519.

Algorithm 3: Ed25519 [4]

Define: H(x) is SHA512 hash of x

- *B* point on the curve
- *l* 253 – bit prime
- *S* is the 256-bit little-endian encoding of integer S
- *R* is encoding of point R as: RY + (Rx & 1)
- *A* is encoding of point A as: AY + (Ax & 1)

Sign

Input: A as 256-bit public key

SK as 256-bit secret key

M arbitrary length message

Output: (R, S) 512-bit signature.

Step 1: $(h_0, ...,h_{511}) \leftarrow H(SK)$

Step 2: $a \leftarrow 2^{254} + \epsilon^{253}_{i=3} {}^{2}\,h_i$

Step 3: r ← H (h_{256}…….,h_{511}, M)

Step 4: $R \leftarrow r\,B$

Step 5: $S \leftarrow (r + H\,(R, A, M)a) \bmod l$

Verifying

Input: A as 256-bit public key,

M arbitrary length message,

(*R*, *S*) 512-bit signature.

Output: A boolean decision

Step 6: $x \leftarrow SB$

Step 7: $y \leftarrow R + H(R,A, M)A$

Step 8: $x = y$

IV. EXPERIMENTAL SETUP

4.1 Data Collection

Data set collected from learning management system (LMS) Kalboard 360. There are 480 student records and 16 features in the dataset. The dataset consists of 305 males and 175 females. A feature can be categorized into three major categories: (1) Demographics such as gender and nationality. (2) A description of the student's educational background, such as the level of the academic school, the grade level, and the section. (3) Behaviors such as raising hands in class, opening resources, and responding to a survey from a parent.

4.2 Result

The Table I give the comparative analysis EdDSA, Ed488 and Ed25519 encryption algorithms that are discussed with respect to Encryption Time, Decryption Time, Throughput and Energy Consumption. It is shown in Figure. 2, 3 and 4.

Table 1: Comparative Analysis of EdDSA, Ed488 and Ed25519

Algorithm	No of Records	Encryption Time (s)	Decryption Time (s)	Total Time (s)	Throughput	Energy
EdDSA	480	5.04	4.95	9.99	29.6857	33.3957
Ed488		3.95	4.02	7.97	33.2895	29.8902
Ed25519		3.72	2.95	6.67	42.8965	27.2925

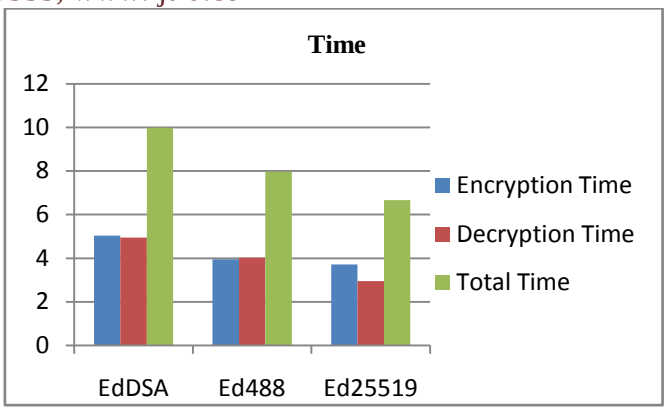

Figure 2: Comparison of Encryption, Decryption and Time Chart

The above figure 2 depicts the comparison of encryption and decryption time takenchart. The chart has x axis values as the name of the algorithms and the y axis hasthe time in seconds for encryption and decryption. From the above chart, the Ed25519 algorithm obtained the low latency for Encryption, Decryption and Total Time compare with otheralgorithms.

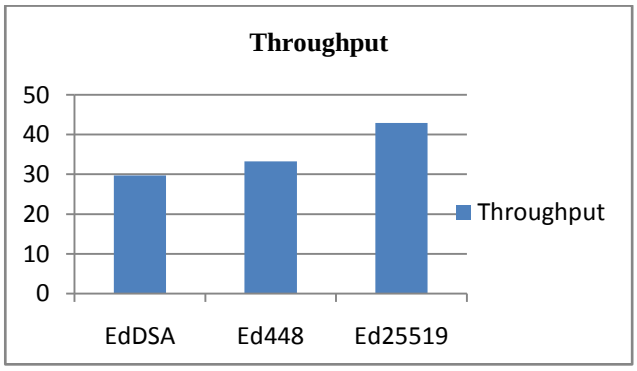

Figure 3: Throughput wise Comparison

The above figure 3 depicts the comparison of throughput chart. The chart has x axis values as the name of the algorithms and the y axis has throughput in 480 records per seconds (s) for Encryption and Decryption. From the above chart, the Ed25519 obtained the high Throughput compared with other algorithms.

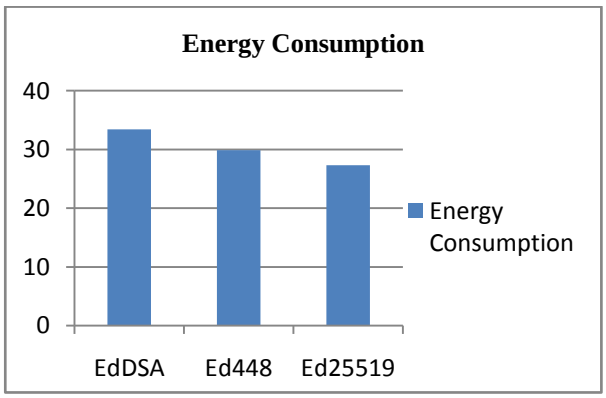

Figure 4: Energy Consumption wise Chart

The above figure 4 depicts the comparison of Energy Consumption chart. The chart has x axis values as the name of the algorithms and the y axis has energy consumption in joules. From the above chart, the Ed25519 algorithm obtained the less energy consumption compare with other algorithms.

Finally, this work concluded the Ed25519 algorithm has taken less time to encryption and decryption, taken high

throughput and less energy consumption. So Ed25519 algorithm is best for encryption and decryption compare with other algorithms.

CONCLUSION

In this work of important encryption algorithms are provided. The EdDSA, Ed448 and Ed25519 encryption algorithms are considered and analysed well to promote the performance ofencryption methods. All the algorithms are very useful for real-time encryption. Each algorithm is unique in its own way, which might be suitable for different applications.So this work concluded that Ed25519 algorithm is best for encryption and decryption better than other algorithms. Everyday new encryption technique is developinghence fast and secure conventional encryption techniques will always work outwith high rate of security.

References

[1] Armando Faz -Hernandez, Julio Lopez and Ricardo Dahab, "High-performance Implementation of Elliptic Curve Cryptography Using Vector Instructions.", ACM Transactions on Mathematical Software, Vol. 45, No. 3, pp.1-35, July 2019.

[2] Adalier, Mehmet, and AntaraTeknik. "Efficient and secure elliptic curve cryptography implementation of curve p-256." Workshop on elliptic curve cryptography standards. Vol. 66. No. 446. 2015.

[3] BinhKieu-Nguyen, Cuong Pham-Quoc, Ngoc-Thinh, Cong-Kha Pham and Trong-Thuc Hoang, "Low-Cost Area -Efficient FPGA-based Multi-Functional ECDSA/EdDSA", Cryptography, Vol. 3, Issue. 2, pp. 25, May 2022.

[4] FurkanTuran and Ingrid Verbauwhede, “Compact and Flexible FPGA Implementation of Ed25519 and X25519”, ACM Transactions on Embedded Computing Systems (TECS), Vol. 1, No. 1, pp. 1-21, February 2018.

[5] Ferraro S. OctoraGinting, VeithzalRivai Zainal and Aziz Hakim, “Digital Signature Standard Implementation Strategy by Optimizing Hash Functions Through Performance Optimization”, Journal of Accounting and Finance Management (JAFM), Vol. 3, No. 6, pp. 362-371, 2023.

[6] Javed R. Shaikh, Marina Nenova, GeorgiIliev and ZlatkaValkova-Javis, “Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications”, 2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS). IEEE, pp. 1-4, 2017.

[7] MojtabaBisheh-Niasar, Reza Azarderakhsh and MehranMozaffari-Kermani, " Cryptographic accelerators for digital signature based on Ed25519", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 29, Issue. 7, pp. 1297-1305, 2021.

[8] Mikhail Babbenko, Andrei Tchernykh, Aziz Redvanov and AnvarDjurabaev, “Comparative analysis of the scalar point multiplication algorithms in the NIST FIPS 186 elliptic curve cryptography”, In ICCS-DE, pp. 21-31. 2021.

[9] Mila Anastasova, Reza Azarderakhsh, MehranMozaffariKermani and LubjanaBeshaj, “Time-Efficient Finite Field Microarchitecture Design for Curve448 and Ed448 on Cortex-M4”, Cryptology ePrint Archive, pp. 1-22, 2023.

[10] Nelson Josias G. Saho, and Eugène C.` Ezin. "Comparative study on the performance of elliptic curve cryptography algorithms with cryptography through RSA algorithm." CARI 2020-Colloque Africainsur la Recherche en Informatique et en MathématiquesApliquées. 2020.