ISSN: 0974-5823 Vol. 7 No. 2 February, 2022

International Journal of Mechanical Engineering

Application of EC-Elgamal Digital Signature for Image Authentication in Government E-services

[1]Ambalika Ghosh, [2]Subhajit Adhikari, [3]Sunil Karforma

[1]Research Scholar, Department of Computer Science, The University of Burdwan.

[2]Assistant Professor, Dinabandhu Andrews Institute of Technology & Management

[3]Professor and Head of the Department in the Department of Computer Science

Abstract –

Digital signature schemes are useful to provide authentication and integrity of any form information such as text, image, audio and video. In this paper, traditional EC-Elgamal digital signature has been implemented using the safe elliptic curve secp256r1 to protect image information in government documents in different e-services. A novel pixel to message point mapping process has been introduced using xor operation and SHA-256 function. Simulation result proves that our method has much lower digital signature generation and verification time than existing ones.

Index Terms – Authentication, EC Elgamal, Elliptic curve, Digital signature, Message mapping, SHA-256, Signature generation, Signature verification

INTRODUCTION

Authentication and integrity as vital security parameters are must when these documents are traveling through the internet. Attacker can misuse these documents violating authentication and integrity. As for example, if the image of a person in identity card is altered in transition by the attacker, the identity card will be considered as unauthentic document. Also, at the time of storing digital documents with digital images in different government digital repositories, authentication and integrity must be enforced to protect from different security attacks. Image security is highly recommended when e-services provided by the government. like scholarship applications, job seeker registration, job skill development, online marriage certificates and driving license. Digital signature and encryption schemes are the two methods widely used to protect image data from attacker.

DIGITAL SIGNATURE

A digital signature [2] is used for authenticity validation and integrity checking of a message. It provides [3,4] confidentiality, authentication, non-repudiation, message repudiation In our paper, elliptic curve version of Elgamal digital signature is used to authenticate the message.

.

EC-ELGAMAL DIGITAL SIGNATURE ALGORITHM

A Elliptic Curve- ElGamal Digital signature algorithm depends on the parameters of elliptic curve.The parameters of secp256r1 elliptic curve is given table I

TABLE I

ELLIPTIC CURVE SECP256R1 PARAMETER

PARAMETERS	VALUES
b	41058363725152142129326129780047268409114441015993725554835256314039467401291
a	115792089210356248762697446949407573530086143415290314195533631308867097853948
p	115792089210356248762697446949407573530086143415290314195533631308867097853951
n	115792089210356248762697446949407573529996955224135760342422259061068512044369
G_x	48439561293906451759052585252797914202762949526041747995844080717082404635286
G_y	36134250956749795798585127919587881956611106672985015071877198253568414405109

Suppose sender "A "selects a random integer k_a from the interval (1, n-1) as the private key and computes the public key, $A = k_a \times G$

Signing scheme:

Step[1]. Select random integer k from the interval (1, n-1)

Step[2]. Compute $R = k \times G = (X_R, Y_R)$ where $r = X_R \bmod n$; if r = 0 go to step i.

Step[3]. Compute e = h(msg), where h is the hash function $\{0,1\}^* \longrightarrow F_n$

Step[4]. Compute s $s = k^{-1} \times (e + rkA) \bmod n$; if then go to step i. "A" sends the signature (R, S) and the message to "B".

Verification scheme of Receiver "B":

Verify that s is an integer in (1,n-1) and $R = (X_R, Y_R \in E(F_p))$

Step[1]. Compute $V_1 = s \times R$

Step[2]. Compute $V_2 = h(msg) \times G + r \times A$ where $r = X_R$.

Step[3]. If $V_1 = V_2$, then the signature is accepted by B, else declared as invalid.

LITERATURE SURVEY

In this paper[1], a review of ECC point mapping methods have been studied and security analysis has been presented. Also a new elliptic curve based encryption method has been described using message mapping. The proposed method can defend against different security attacks like known plain text, chosen plain text, known cipher text, chosen cipher text, collision attack and man-in-the-middle attacks. A secure, efficient, and complete data collection, and transmission and storage scheme for IoT in smart ocean[5] has already been developed. To guarantee the confidentiality, reliability, and integrity of transmitting data, EC-ElGamal and ECDSA are employed in this IoT framework. A new Electronic Digital Signature Scheme [6] with Message Recovery method for the creation and verification of electronic-digital signature using elliptic curves has been introduced earlier. The Shnorr signature algorithm is used, which allows to recover data directly from the signature similarly to RSA-like signature systems. A novel method with the ECDSA variant [7] has been proposed with high level security with the help of parameters. In this paper [8], a novel digital documents management scheme has been invented based on three-layer structure with the help of symmetric cryptography, combined key and hardware encryption technology to provide authentication and authorization.

PROPOSED METHOD

In our proposed method, we take grayscale images of size 256×256 with .png format. Next, 2D matrix of pixel is converted to one-dimensional list with 65536 pixels. Then pixels are grouped into 8 chunks with 8192 pixels per chunk and xored sequentially to obtain a representative pixel for a chunk. So, we get 8 representative pixels and they are fed into SHA-256 algorithm to get unique hash values. The unique hash values are inputted into EC-ELGAMAL digital signature algorithm. We take the secure elliptic curve version secp256r1 that has the order p. Total 8 curve points are used for signature generation and verification. It has been observed that if any of the pixels of a particular chunk has been modified by the attacker, the representative pixels must be different and that leads to failure of digital signature verification process. This signifies that the image is not original. The algorithm is given below.

STEP[1]. User "a" chooses the parameters of elliptic curve a,b,n,p

STEP[2]. Compute ellipticcurve(gf(p),[a,b])

STEP[3]. Specify the base point g.

STEP[4]. User a chooses a private key

STEP[5]. User "a" compute public key=private_key×g

STEP[6]. Publish public key to the server.

STEP[7]. User "a" reads grayscale image of size 256×256

STEP[8]. Store it to a 2d variable g_image[x][y].

STEP[9]. Convert the g_image to one-dimensional list called "g_imgae_list[]"

STEP[10]. Create pixel chunks and save it to list called c_points[] with n pixels form g_imgae_list[] .

STEP[11]. Apply xor operation for each pixels in c_points[] and save it to list "r_points[]"

STEP[12]. Compute hash values using sha-256(r_points) and save it to "msg_points"

STEP[13]. perform signature generation using sig_gen(msg_points).

STEP[14]. Return digital signature pair (r,s)

STEP[15]. User a send (r,s) it to receiver "b"

STEP[16]. Receiver b compute v1=s×r

STEP[17]. Receiver b compute v2=sha-256(msg) ×g+r×public_key

STEP[18]. If v1 == v2, then

STEP[19]. Print "authenticated"

STEP[20]. Else

STEP[21]. Print "not authenticated"

STEP[22]. Stop.

IMPLEMENTATION EXAMPLE

We have taken a small 5×5 2D matrix of integer values of an image. It is shown in the table II.

TABLE II

PIXEL VALUES

160	160	156	160	160
160	160	156	160	160
162	154	158	158	158
158	156	158	156	160
154	156	152	156	152

In next step, we convert the 2D array to one dimensional list and the values are [160, 160, 156, 160, 160, 160, 160, 156, 160, 160, 162, 154, 158, 158, 158, 158, 156, 158, 156, 160, 154, 156, 152, 156, 152]. These values are divided into 5 chunks of 5 pixels each. They are listed below in table III.

TABLE III

PIXEL VALUE

Chunk1	160,160,156,160,160
Chunk2	160,160,156,160,160
Chunk3	162,154,158,158,158
Chunk4	158,156,158,156,160
Chunk5	154,156,152,156,152

Each and every pixels of each chunk are xored sequentially and 5 representative points as R_points are generated. They are given in tableIV.

TABLE IV

PIXEL VALUE

Chunk1	R_point1	154
Chunk2	R_point2	156
Chunk3	R_point3	166
Chunk4	R_point4	160
Chunk5	R_point5	154

TABLE V

HASH VALUE OF R_POINTS

R_POINT	HASH VALUES
156	[72033881548352347419238317830403504105263957211084369453495522961143273138 76
156	7203388154835234741923831783040350410526395721108436945349552296114327313876
166	1017427678029541505340518297966284355865464511174848502524721586232213990096 68
160	7466493580422251530153484117191399620867665992802513871043720694460390304992 1
154	1314312425675110321482779232381078383042632476817994087169107427352306593783 0

In the above table V, five different hash values are compute using SHA-256() from the five R_points. They are considered as message which are then inputted into EC-Elgamal digital signature generation algorithm. For each R_points two signatures (s,r) are obtained and they are given in table VI.

TABLE VI

SIGNATURE VALUES OF EACH MESSGAE(R_POINTS)

Message		Signature values
156	r	32325191861646170820727200153045020440226161115493753094312025153945959180094
	s	84401156791556238390248537137913014926993427496626401301161117712603049474476
156	r	32325191861646170820727200153045020440226161115493753094312025153945959180094
	s	84401156791556238390248537137913014926993427496626401301161117712603049474476
166	r	32325191861646170820727200153045020440226161115493753094312025153945959180094
	s	76339698040227204170644602085840834816171436022985512631883358195248346392538
160	r	32325191861646170820727200153045020440226161115493753094312025153945959180094
	S	101992081854503284159954766743071179212766614241049237915863010228522261228875
154	r	32325191861646170820727200153045020440226161115493753094312025153945959180094
	s	23448858745009746014285415843566089729930329380735204880251775973061410075925

In signature verification algorithm, two signatures V1

and V2 have been computed. They are listed table VII.

TABLE VII

SIGNATURE VALUE OF R_POINTS

MESSAGE		SIGNATURE VALUES
156	V1	(77892051817199370430149098329085786801199616655375102672595019265170846873059 :112487114392350022986885470507891033536758833947895379534238530226262216245364
	V2	(77892051817199370430149098329085786801199616655375102672595019265170846873059 :112487114392350022986885470507891033536758833947895379534238530226262216245364
156	V1	(77892051817199370430149098329085786801199616655375102672595019265170846873059 :112487114392350022986885470507891033536758833947895379534238530226262216245364
	V2	(77892051817199370430149098329085786801199616655375102672595019265170846873059 :112487114392350022986885470507891033536758833947895379534238530226262216245364
166	V1	(37414309354407264648135572989995936241623941015183977470614790178921052672233 :71382002728933060220022629876609177800224549101009420625362556848874283454132
	V2	(37414309354407264648135572989995936241623941015183977470614790178921052672233 :71382002728933060220022629876609177800224549101009420625362556848874283454132
160	V1	(14896045557941308277173147269258816106950816580333440476193499035308836726505 :31555387467190197250961365031982441630186796504818981822653102260846603169702
	V2	(14896045557941308277173147269258816106950816580333440476193499035308836726505 :31555387467190197250961365031982441630186796504818981822653102260846603169702

154	V1	(12356265255807394797117027536492061371576769981152550003309500532254008485117 :68155983583660022238222066766366258352427652515404676542664678486893592687567
	V2	(12356265255807394797117027536492061371576769981152550003309500532254008485117 :68155983583660022238222066766366258352427652515404676542664678486893592687567

From the above table VII, it has been observed that for each R_ points as messages the values of V1 and V2 are same. So, it can be concluded that no modification has been done during transmission of the original image.

PERFORMANCE ANALYSIS

We have taken standard image of 256×256 with filesize 46.9Kb according to the standard for uploading images for e-services provided by government. Our algorithm has been tested in SageMath8.0 software based on python programming in Intel i3 processor with 4GB RAM and 1.70Ghz processor. The signature generation and verification time is given in table VIII.

TABLE VIII

SIGNATURE GENERATION AND VERIFICATION TIME COMPARISON

	FILE SIZE(KB)	SIG. GEN AND SIG VER.(SEC)
OUR METHOD	46.9	1.2324
REF [2]	50	0.032783
REF[9]	NA	8.75
REF[10]	NA	61.191

CONCLUSION AND FUTURE SCOPE

The traditional EC-elgamal digital signature has been slightly modified in terms of a novel message point mapping scheme and the elliptic curve used. It has been observed that the digital signature generation and verification time is very less compared to other methods of digital signatures. Also, selection of the higher order of the elliptic curve for signature generation and verification makes the proposed method robust against different security attacks. Our method can be applied in future to text, audio, video and different document formats like .pdf and .doc for e-services. In future, documents of different digital repositories can be authenticated by the proposed method of digital signature in less time.

REFERENCES

[1]. Sengupta, A., & Ray, U. K. (2016). Message mapping and reverse mapping in elliptic curve cryptosystem. Security and Communication Networks, 9(18), 5363-5375.

[2]. Adeshina, Adekunle Micheal. "Evaluation of Elliptic Curve El-Gamal and RSA Public-Key Cryptosystems for Digital Signature." (2020): 36-49.

[3]. Kazmirchuk, Svitlana, Ilyenko Anna, and Ilyenko Sergii. "Digital signature authentication scheme with message recovery based on the use of elliptic curves." International Conference on Computer Science, Engineering and Education Applications. Springer, Cham, 2019.

[4]. Kasodhan, Rashmi, and Neetesh Gupta. "A New Approach of Digital Signature Verification based on BioGamal Algorithm." 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2019.

[5]. Hu, Chunqiang, et al. "Secure and efficient data collection and storage of IoT in smart ocean." IEEE Internet of Things Journal 7.10 (2020): 9980-9994.

[6]. Kazmirchuk, Svitlana, et al. "The Improvement of digital signature algorithm based on elliptic curve cryptography." *International Conference on Computer Science, Engineering and Education Applications*. Springer, Cham, 2020.

[7]. Prabu, M., and R. Shanmugalakshmi. "A comparative analysis of signature schemes in a new approach of variant on ECDSA." 2009 International Conference on Information and Multimedia Technology. IEEE, 2009.

[8]. Zhao, Guifen, et al. "Scheme for digital documents management in networked environment." 2009 IEEE International Conference on Network Infrastructure and Digital Content. IEEE, 2009.

[9]. Singh, Laiphrakpam Dolendro, and Khumanthem Manglem Singh. "Image encryption using elliptic curve cryptography." Procedia Computer Science 54 (2015): 472-481.

[10]. Alia, Mohammad Ahmad, and Azman Bin Samsudin. "A new digital signature scheme based on Mandelbrot and Julia fractal sets." American Journal of Applied Sciences 4.11 (2007): 850-858.