Malaya Journal of Matematik, Vol. 9, No. 1, 562-565, 2021

https://doi.org/10.26637/MJM0901/0095

A time stamped signature scheme based on elliptic curve

Manoj Kumar Chande [1]* and Swati Jain[2]

Abstract

We propose a time-stamped signature scheme based on elliptic curve. The signature consists of an authenticated time-stamp provided by a trusted authority, known as Time-Stamping System, which provides time-stamp without having any knowledge of the content of the document to be signed. Anyone can verify the validity of the signature using systems public parameters, i.e. the signature is universally verifiable. The security of the proposed scheme rely on Elliptic Curve Discrete Logarithm Problem.

Keywords

Digital Signature, Elliptic Curve Cryptosystem (ECC), Elliptic Curve Discrete Logarithm Problem (ECDLP), Interger Factorization Problem (IFP), Time Stamp.

AMS Subject Classification

94A60.

[1] *Department of Applied Mathematics, Shri Shankaracharya Institute of Professional Management & Technology, Raipur 492015, Chhattisgarh, India;*

[2] *Department of Computer Science, Govt. J. Yoganandam Chhattisgarh P. G. College, Raipur 492001, Chhattisgarh, India.*

*__Corresponding Author__: [1] manojkumarchande@gmail.com; [2] swati_12bafna@yahoo.co.in

Article History: Received **05** December **2020**; Accepted **30** December **2020**

Contents

1. Introduction

The modern cryptography has a tool known as digital signatures which provide authentication, integrity and non-repudiation, to digital documents and communications. The linkage between time and digital signature is a recent research subject. In most of real time circumstances, it is required to certify the date or time of a document, when it was created or last modified. For example, in intellectual property subjects, patents, contracts and numerous applications. In case of the crucial conditions, if any dispute arises then this date or time will help in order to establish their competing claims for concerning parties.

A time-stamp for a digital document assure that the document existed at a certain time and has not been modified since that time. Time Stamping System [1, 2], as a trusted third party provide the time-stamps for digital documents. Even though the time-stamp is included in the document, the validity of time-stamp itself is still in question. To overcome this problem, a trusted third party, is needed to authenticate the time, when the signature is generated [1]. Third party plays an important role in providing security services, specially non-repudiation services.

Time stamping systems for digital document was first introduced by Haber and Stornetta [3]. Following the concept, a lot of research [4–6], has been done in the area of time-stamped signatures. To withstand forward forgery suffered by linking schemes and to reduce verification cost, Sun et al. [1] proposed four time-stamped signature schemes in the year 2004. As per their claim, these schemes are quite secure against the forward forgery, but Z. Shao [2], find that their schemes suffered from substitution attacks, by which the signer can backward/forward forge signatures and the time-stamping service can also forge signatures. Next, Z. Shao [2], proposed four efficient time-stamped signature schemes capable of withstand both forward and backward forgery, but these schemes was very complex as there will be a large number of exponentiation and hashing operations were involved. Hence, it was very complex and computationally inefficient scheme. In the year 2012

Mohanty, Majhi and Baral's [7], novel time-stamped signature scheme based on discrete logarithm problem (DLP) and integer factorization problem (IFP).

In the year 1985, on the basis of elliptic curve the ECC was independently introduced by Victor Miller [8] and Neal Koblitz [9]. The ECC has gained advantage over other cryptosystems like RSA [10] and Elgamal [11], because of the features like: Robust security, less and faster computation, less storage space required and shorter keys.

In this paper we proposed a new time stamp signature scheme based on elliptic curve and security of our proposed time-stamp signature scheme whose security rely on ECDLP. In our scheme a signature for message is generated in collaboration by signer and TSS. No one, including the TSS can forge the signer's time-stamped signature. In addition, without help of the TSS, the signer cannot generate any valid time-stamped signature with an authenticated time-stamp.

The rest of our paper is organized as follows: Next Section presents the proposed time-stamped signature scheme based on elliptic curve. Security analysis of our scheme is discussed in Section 3. In final Section we conclude the findings of our paper.

2. Proposed Time-stamp Signature

In the proposed scheme there are three entities involve: the signer O, who signs a document; the time stamping system, who is responsible for adding time-stamps into signatures; and the verifier V, who checks the validity of the time-stamped signatures. In the proposed scheme, we shall use the following notation.

Notation	Description
O	An original signer.
V	A verifier.
p	A large odd prime number.
n	The number of points on E_p.
q	A large prime number, such that $q\|n$.
F_p	Finite prime field.
E_p	An elliptic curve defined over F_p.
P	A point on E_p having prime order q.
x_o	The private key of the signer O.
y_o	The public key of the signer O.
x_t	The private key of the TSS.
y_t	The public key of the TSS.
$h(.)$	A collision free one-way hash function.

This scheme consists of three phases; Key Generation, Signature Generation and Signature Verification.

(A) Key Generation

The TSS selects his private key $x_t \in Z_q^*$ and computes his public key, $y_t = x_t P$. Therefore private and public key pair for TSS will be (x_t, y_t). In similar manner the signer O also selects his private key $x_o \in Z_q^*$ and computes $y_o = x_o P$. Therefore private and public key pair for signer will be (x_o, y_o).

(B) Signature Generation

This algorithm takes the message m, private and public keys of signer O and TSS, then gives time-stamped signature $\sigma = (l, s)$ as output. The steps to generate time-stamp signature are as follows:

(a) The signer O computes

$$e = h(m)P$$

and sends e, to the TSS.

(b) As TSS receives e, he selects $\alpha \in Z_q^*$ and calculate

$$\beta = e + (\alpha + T)P + y_t \bmod p \tag{2.1}$$
$$r = x(\beta)$$

Here T, is the time-stamp of the signature, which may be particular date or time of signature generation. Then TSS sends r to the signer O.

(c) The original signer O, computes l and partial signature s_o as

$$l = h(m, r)$$
$$s_o = l\, x_o \bmod p$$

now signer O, sends s_o to the TSS.

(d) The TSS computes s as given below and sends it to the signer O.

$$s = (\alpha - s_o + x_t) \bmod p \tag{2.2}$$

Finally, the signature of message m is $\sigma = (l, s)$, with time-stamp T.

(C) Signature Verification

Anyone with a genuine signature $\sigma = (l, s)$, with time-stamp T, of message m can verify signature as:

(a) The verifier V computes e and γ as given below

$$e = h(m)P$$
$$\gamma = e + l\, y_o + (s + T)P \bmod p \tag{2.3}$$
$$r' = x(\gamma) \tag{2.4}$$

(b) Then compute

$$l' = h(m, r') \tag{2.5}$$

If $l = l'$, then the signature is considered to be a valid one.

Theorem 2.1. *The proposed universally verifiable signature is a valid one if and only if verifier find that* $r = x(\beta) = r' = x(\gamma)$.

Proof. To proof correctness of our scheme, we have to show that $\beta = \gamma$. As we know

$$\begin{aligned}\gamma &= e + l\, y_o + (s+T)P \bmod p \\ &= e + l\, x_o P + (\alpha - s_o + x_t + T)P \bmod p \\ &= e + l\, x_o P + (\alpha - l\, x_o + x_t + T)P \bmod p \\ &= e + (\alpha + x_t + T)P \bmod p \\ &= e + (\alpha + T)P + x_t P \bmod p \\ &= e + (\alpha + T)P + y_t \bmod p \\ &= \beta\end{aligned}$$

So $\beta = \gamma$, means $r = x(\beta) = x(\gamma) = r'$. □

Now we present process flow of our signature scheme:

Signer O		TSS
$e = h(m)P$	$\xrightarrow{e}$	$\beta = e + (\alpha + T)P + y_t \bmod p$ $r = x(\beta)$
$l = h(m,r)$	$\xleftarrow{r}$	
$s_o = l x_o \bmod p$	$\xrightarrow{s_o}$	$s = (\alpha - s_o + x_t) \bmod p$
	send $\sigma = (l,s)$; T to verifier	
	$\downarrow$	
Verifier		
$e = h(m)P$		
$\gamma = e + l y_o + (s+T)P \bmod p$		
$r' = x(\gamma)$		
$l' = h(m,r')$		
Check If $l = l'$.		

Figure 2.1 : Process flow of our proposed scheme.

3. Security Analysis of Proposed Signature

(I) An adversary tries to find secret keys x_o or x_t from public keys y_o or y_t, has to solve $y_o = x_o P \bmod p$, or $y_t = x_t P \bmod p$. This means he has to face ECDLP, which is infeasible with today's computation facilities.

(II) If an adversary attempt to alter the message m and time-stamp T. It is infeasible to find α from (2.2), because it consists of two secret parameters, s_o and x_t.

(III) A situation in which dishonest signer tries to forge a time-stamp signature $\sigma = (l,s)$. The dishonest or corrupt signer may tries to find the value of α from β. To obtain α from equation (2.2), he has to face ECDLP. The dishonest signer may also attempt to find α from the value of s. As equation (2.2), involves two unknown parameters, α and x_t, it is infeasible for him/her to get the value of α, Hence it is not possible for signer to produce a valid signature without help from the TSS.

(IV) In case the dishonest TSS try to forge time-stamp signature $\sigma = (l,s)$, he need private key x_o, of the signer O. If he attempts to find x_o from s_o, then he has to face IFP. So it is not possible for the TSS, to generate a forge time-stamp signature without help from the signer O.

(V) In our scheme, the trusted time-stamp is an important part, which is generated and certified by TSS. If the signature is verified successfully by equation (2.3, 2.4 & 2.5), then only the signature is valid.

4. Conclusion

We presents a universally verifiable time-stamped signature scheme which holds all the fundamental properties of a digital signature, especially non-repudiation. Our scheme is capable to resist attacks, which are discussed in previous section of security analysis. The algorithm is derived using elliptic curve, so the cost of signature generation and verification is low, which is very helpful for fast and secure on-line transactions. Our scheme can be used as a solution of many real time problems like; intellectual property matters, patents, contracts and numerous applications.

Acknowledgment

The authors express their gratitude towards different anonymous reviewer for their comments & suggestions towards this work.

References

[1] H. M. Sun, B. C. Chen, & H. T. Yeh, On the design of time-stamped signatures, *Journal of Computer and System Sciences*, 68(2004), 598-610.

[2] Z. Shao, Security of the design of time-stamped signatures, *Journal of Computer and System Sciences*, 72(2006), 690-705.

[3] S. Haber, & W. S. Stornetta, How to time-stamp a digital document, *In Conference on the Theory and Application of Cryptography, Springer, Berlin, Heidelberg*, (1990), 437-455.

[4] J. Benaloh & M. de Mare, Efficient broadcast time-stamping, *Technical Report 1 TR-MCS-91-1 Clarkson University Department of Mathematics and Computer Science*, (1991).

[5] A. Buldas & P. Laud, New linking schemes for digital time-stamping, *In ICISC* 98(1998), 3-14.

[6] A. Buldas, P. Laud, H. Lipmaa, & J. Villemson, Time-stamping with binary linking schemes, *In Annual International Cryptology Conference, Springer, Berlin, Heidelberg*, (1998), 486-501.

[7] Sujata Mohanty, Banshidhar Majhi, Sanjib Kumar Baral, A Novel Time-stamped Signature Scheme Based On DLP, 1st *International Conference on Recent Advances in Information Technology, RAIT-2012, IEEE.*

[8] V. S. Miller, Use of elliptic curves in cryptography, *In Conference on the theory and application of cryptographic techniques, Springer, Berlin, Heidelberg*, (1985), 417-426.

[9] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of computation*, 48(1987), 203-209.

[10] R. L. Rivest, A. Shamir, & L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 21(1978), 120-126.

[11] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE transactions on information theory*, 31(1985), 469-472.

⋆⋆⋆⋆⋆⋆⋆⋆⋆
ISSN(P):2319 – 3786
Malaya Journal of Matematik
ISSN(O):2321 – 5666
⋆⋆⋆⋆⋆⋆⋆⋆⋆